

Black HatGuide

por Alan Sanches

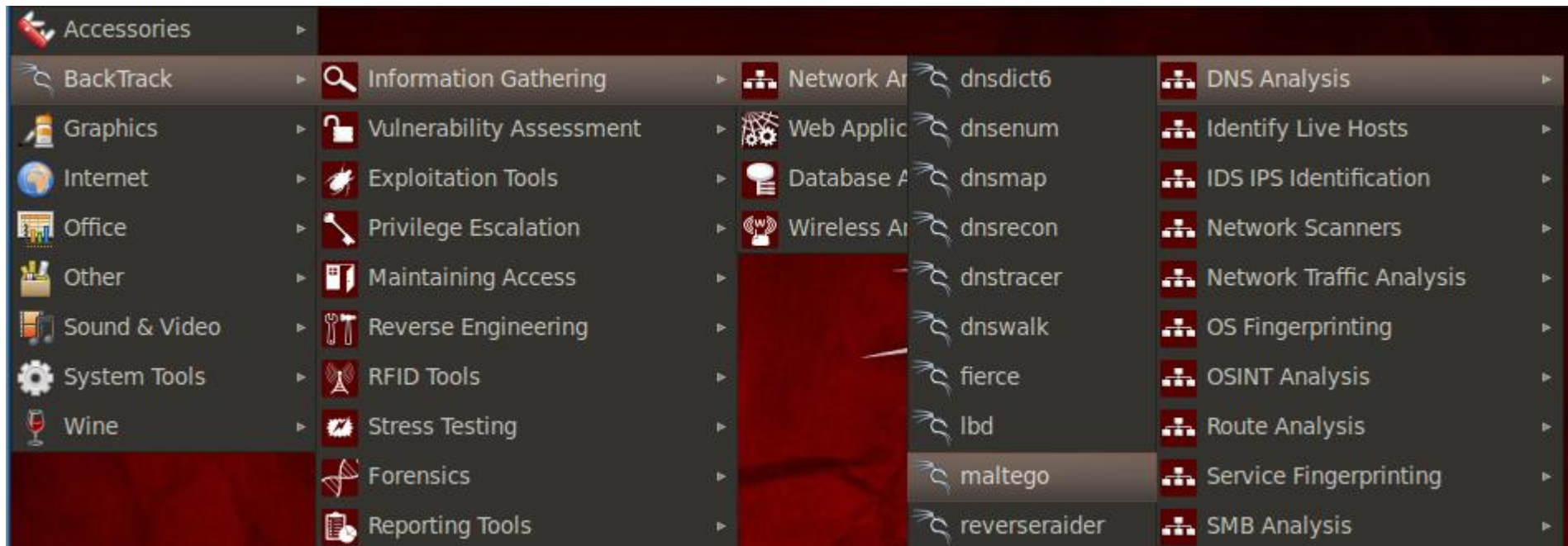
Sejam bem vindos

Coletando informações - Maltego



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

No Backtrack

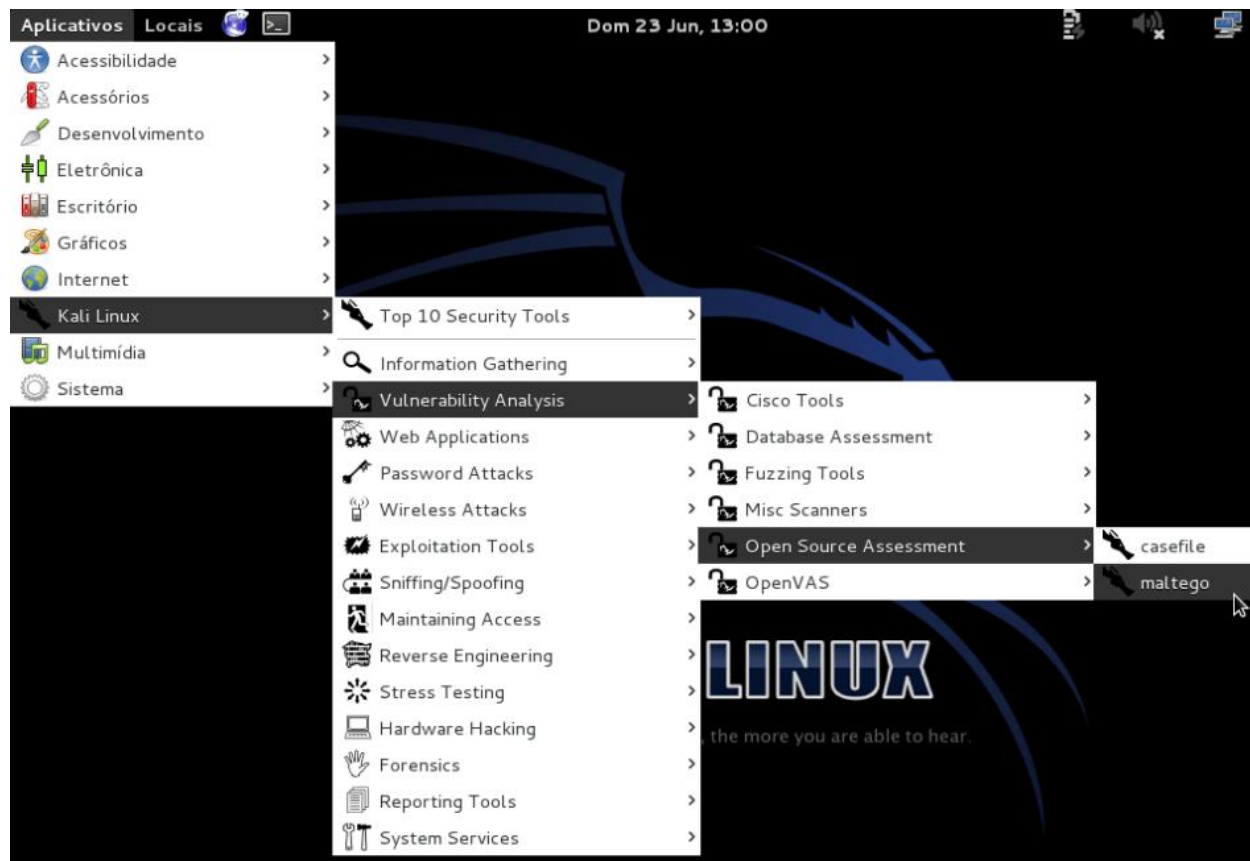


Coletando informações - Maltego



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

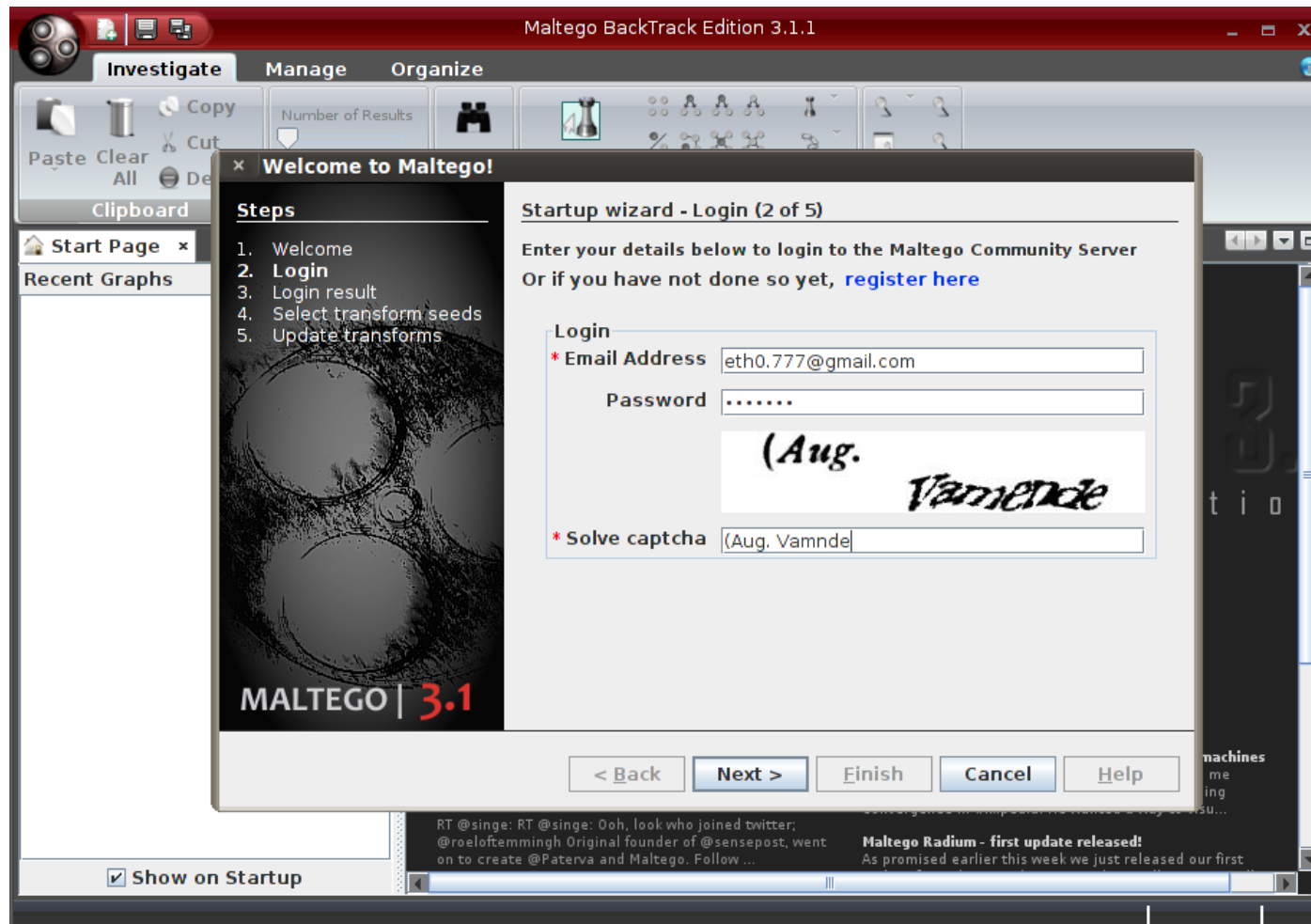
No Kali



Coletando informações - Maltego



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat



Coletando informações



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

× Welcome to Maltego!

Steps

1. Welcome
2. Login
3. Login result
4. **Select transform seeds**
5. Update transforms

Startup wizard - Select transform seeds (4 of 5)

Discover transforms from:

- ☒ Maltego public servers
- ☐ Local TAS (Transform Application Server)

Hostname/IP:

Note: The transform seed settings can be changed later through Manage->Discover Transforms.

MALTEGO | 3.1

< Back Next > Finish Cancel Help

Coletando informações



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

The screenshot displays the Maltego BackTrack Edition 3.1.1 interface. The main window shows a graph titled "New Graph (1)" with a central node "laboratoriohacker.com.br" and several outgoing links to other domains and email addresses. The left sidebar contains a list of entity types, and the right sidebar shows a "Detail View" for the selected entity, displaying its properties and relationships.

Entity List (Left Sidebar):

- Dev...
- Device
- Infr...
- AS
- DNS Na
- Domain
- IPv4 Ac
- MX Rec
- NS Rec
- Netblo
- URL
- Websit
- Loc...
- Locati
- Pen...

Graph (Main View):

The graph shows the following entities and their relationships:

- laboratoriohacker.com.br (Central node)
- eth0@777.gmail.com
- ns1.laboratoriohacker.com.br
- ns2.laboratoriohacker.com.br
- www.laboratoriohacker.com.br
- webmail.laboratoriohacker.com.br

Output - Transform Output (Bottom Panel):

```
Transform To Emails (@domain [using Search Engine]) returned with 0 entities.  
Interesting files cannot be obtained with this Search Engine Type, but I'll try anyhow!  
No results from SearchEngine  
Transform To Files (Interesting) [using Search Engine] returned with 0 entities.  
Transform To Domain [Find other TLDs] returned with 0 entities.  
Running transform To IP Address [DNS] on 1 entities.  
Transform To IP Address [DNS] returned with 1 entities
```

Detail View (Right Panel):

MX Record
maltego.MXRecord
laboratoriohacker

Property View (Right Panel):

Properties	
Type	MX Record
Priority	0
MX Record	laborat...
Graph info	
Weight	100
Incoming links	1
Outgoing links	0

Scanner com Acunetix



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat



- *Nessus é um programa de verificação de falhas/vulnerabilidades de segurança. Ele é composto por um cliente e servidor, sendo que o scan propriamente dito é feito pelo servidor. O nessusd (servidor Nessus) faz um port scan ao computador alvo, depois disso vários scripts (escritos em NASL, Nessus Attack Scripting Language) ligam-se a cada porta aberta para verificar problemas de segurança.*
- *Até há pouco tempo o Nessus só funcionava no Linux, mas recentemente foi lançado o Nessus para Windows. É uma excelente ferramenta designada para testar e descobrir falhas de segurança (portas, vulnerabilidades, exploits) de uma ou mais máquinas.*

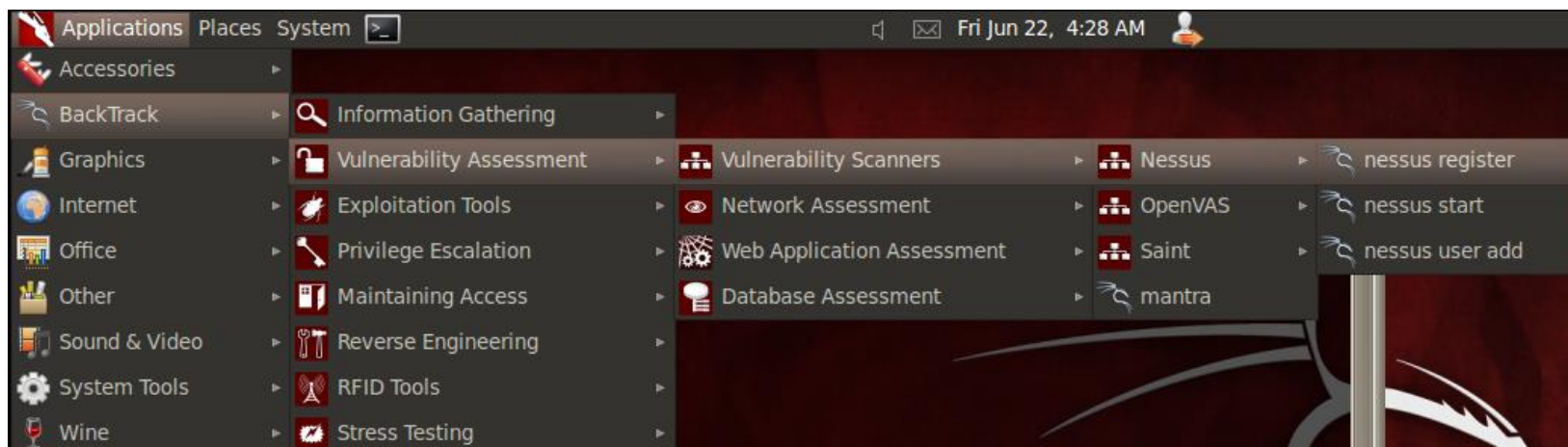


Backtrack - Scanner com Nessus



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

- *É necessário registrar o Nessus antes do uso:*



- *Você receberá um e-mail com um código de ativação parecido com esse:*

Thank you for registering with us!

Your activation code for the Nessus HomeFeed is 9C69-DF39-CC8D-8E7C-91CF

Remember that the HomeFeed subscription is for home use only. If you use Nessus at work, you need to obtain a ProfessionalFeed.

Windows Users :

To activate your account, open the program 'Nessus Server Manager'
located under C:\Program Files\Tenable\Nessus\ and enter your activation code in the program.

Linux and Solaris Users :

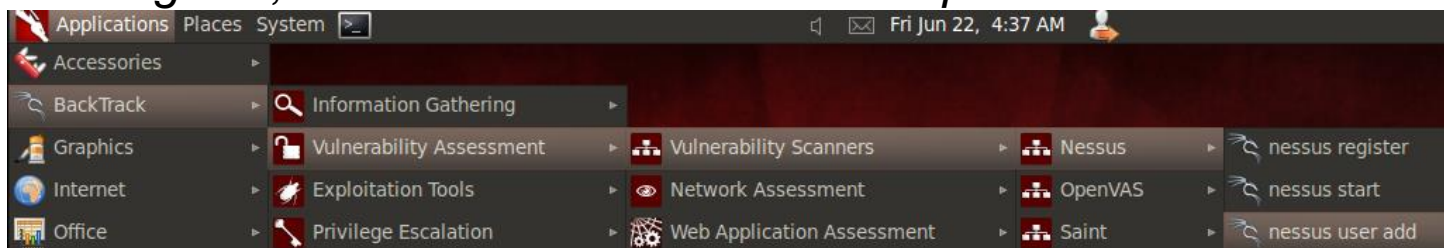
To activate your account, simply execute the following command :

Backtrack - Scanner com Nessus

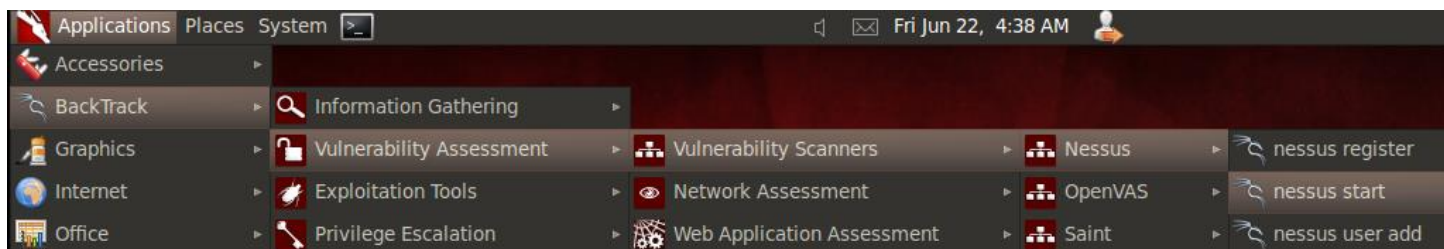


Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

- Após receber o e-mail, efetue o comando:
`/opt/nessus/bin/nessus-fetch –register` código do email
- Em seguida, é necessário criar um usuário para o Nessus:



- Depois, inicie o serviço:



- Agora você poderá acessá-lo através do endereço:
`http://ipdobacktrack:8834`

- ❑ Efetue o download na página abaixo e selecione seu sistema operacional
- ❑ <http://www.tenable.com/products/nessus/select-your-operating-system>
- ❑ Use o comando abaixo para instala-lo

dpkg -i kali....deb

- ❑ Efetue o registro do seu Nessus no link abaixo
- ❑ <http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>
- ❑ Acesse a pasta `cd /opt/nessus/bin`

- ❑ Entre com o comando abaixo para registrar seu Nessus

./nessus-fetch --register "QREDDR-3\$FDF-DFSE3-DFSD3"

- ❑ Inicie o serviço do Kali com o comando abaixo:

service nessusd start

- ❑ Agora você poderá acessa-lo através do endereço:
`http://ipdobacktrack:8834`

Kali - Scanner com Nessus





Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

A screenshot of a web browser displaying the Nessus login page. The browser's address bar shows the URL "https://127.0.0.1:8834/html5.html#/". The page has a dark gray background. In the center, there is a white box containing the Nessus logo and the text "vulnerability scanner". Below this, there are two input fields: "Username" with a user icon and "Password" with a lock icon. A large blue button labeled "Sign In To Continue" is positioned below the password field. At the bottom of the white box, there is a link that says "Looking for the older Flash interface?". The footer of the page features the Tenable logo and the text "TENABLE Network Security*".

https://127.0.0.1:8834/html5.html#/


Nessus[®] vulnerability scanner

Username 

Password 

Sign In To Continue

[Looking for the older Flash interface?](#)

 **TENABLE** Network Security*

Man in the Middle: DNS Poisoning



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

Set (Social Engineer Toolkit)

Ferramenta para Engenharia Social

Com esta ferramenta é capaz de criar páginas fakes para ataques de engenharia social, tais como: Gmail, facebook, etc.

Você também pode selecionar uma página para que ele Clone

Local: /pentest/exploits/set

Use: ./set

No Kali, use o comando

set-toolkit

Man in the Middle: DNS Poisoning



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

Ettercap

Ettercap é um dos melhores Sniffers de rede para ataques Man in the Middle. Possui suporte com SSH1, SSL, Injeção de Caracteres, etc.

Uso:

```
ettercap -Tqi eth0 -M ARP // // -P dns_spoof
```

-T = Apresenta em texto na tela o conteúdo sniffado

-M = Man in the Middle Attack (arp, ICMP, DHCP, etc)

-o = Only-mitm, desativa o Sniff e executa apenas o MITM

-q = Quiet

-i = iface, placa de rede ao qual quer capturar o conteúdo

-P = Plugin, ativa o plugin necessário para o ataque

// // = Seleciona todas as redes e todos os gateways, trocando broadcast entre todos.

Você pode substituir o // por /192.168.1.1/ /192.168.1.2-10/

O primeiro // é seu gateway, o segundo é sua rede e as máquinas a serem sniffadas

Man in the Middle: DNS Poisoning



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

Roubar dados do site do Gmail, Bradesco ou Facebook

Verificar se o IP_Foward está ativo

Editar o arquivo ettercap.conf

```
#gedit /etc/ettercap.conf
```

Zerar as linhas, ec_uid e ec_gid e descomentar as linhas do IPTABLES

Corrigir o DNS do Ettercap

```
#gedit /usr/local/share/ettercap/etter.dns
```

Adicionar os dominios necessários

Executar o SET

Selecionar o item 1 (Social Engineering Attack)

Selecionar o item 2 (Website Attack Vectors)

Selecionar o item 3 (Cred. Harvester Attack Method)

Selecionar o item 1 (Websites templates)

Selecionar o item 2 (Gmail)

Executar o ettercap com captura de DNS Spoof

```
# ettercap -Tqi eth0 -M ARP // // -P dns_spoof
```

Ir até o alvo e executar o site do Gmail

```
printf ("\Chega por hoje\n");
```



Aula 3 – Treinamento: Técnicas de Invasão - BlackHat

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker

