

SQLMAP - Informações adicionais

Transcrição

Essa aula foi reservada para sanar dúvidas e problemas que ainda podem ocorrer no **SQL Map**, principalmente, em relação a conexão.

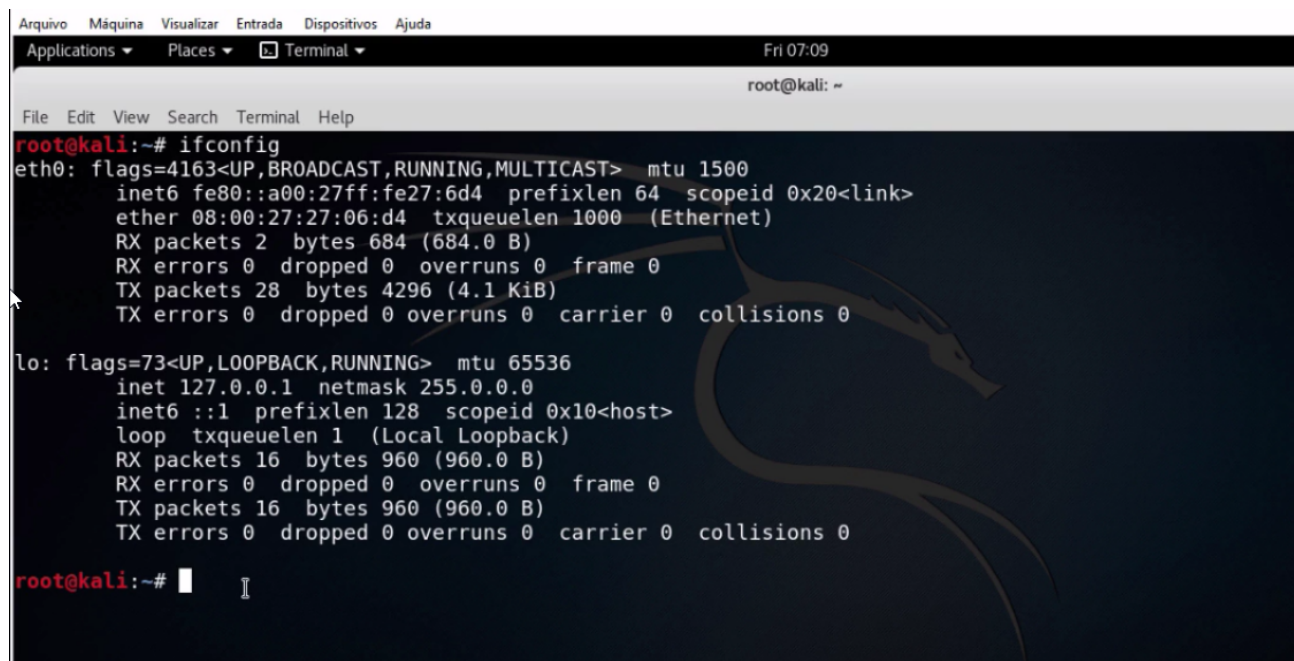
Tanto o Kali Linux quanto o servidor são uma extensão do computador que utilizamos para ministrar o curso e ambas são definidas como conectadas a uma "Placa em modo Bridge". Entretanto, a renovação dos endereços IPs que o roteador fornece, pode acontecer a cada 5 ou 10 minutos. Assim, durante os testes realizados, nós podemos perder a conexão, pois o endereço IP já é renovado.

Caso isso apresente-se como problema, uma solução é colocar tanto o Kali Linux como o servidor conectados em uma rede interna. Primeiro, abrimos o **Virtual Box** e clicamos em "Configurações > Rede" e alteramos o conectado a para Rede Interna fazemos esse procedimento no Kali Linux e também no servidor. Feita essa modificação podemos inicializar as duas máquinas.

Assim que o Kali Linux terminar de iniciar nós vamos acessá-lo. Vamos abrir seu terminal e o primeiro passo é listar as placas de rede! Basta digitar:

```
> ifconfig
```

Teremos o seguinte:



```
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
Applications  Places  Terminal
Fri 07:09
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet6 fe80::a00:27ff:fe27:6d4  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:27:06:d4  txqueuelen 1000  (Ethernet)
    RX packets 2  bytes 684 (684.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 28  bytes 4296 (4.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1  (Local Loopback)
    RX packets 16  bytes 960 (960.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 16  bytes 960 (960.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~#
```

Perceba que não temos um endereço IP! Portanto, é preciso inserir um na máquina. Digitamos `ifconfig` acompanhado de `eth0` e `down` que serve para desabilitar essa rede. Tendo escrito isso podemos adicionar um endereço, no caso, `192.168.10.10`. Teremos, `ifconfig eth0 192.168.10.10` e adicionamos também uma máscara de rede, a `netmask 255.253.255.0`. Por fim, adicionamos um `up`:

```
> ifconfig eth0 down
> ifconfig eth0 192.168.10.10 netmask 255.255.255.0 up
```

Agora, digitando `ifconfig` teremos o endereço introduzido estaticamente!

Uma vez com o Kali Linux arrumado, podemos nos concentrar no servidor. Primeiro, preenchemos login (root) e senha (owasp) e depois usamos o `ifconfig` para listar as placas de rede. Da mesma forma que o *Kali Linux*, o servidor tão pouco está com algum endereço IP. Portanto, será preciso reproduzir os passos:

- 1) `ifconfig eth0 down` : para desabilitar
- 2) `ifconfig eth0 192.168.20 netmask 255.255.255.0 up` : para adicionar a rede e habilitá-la
- 3) `ifconfig` : para confirmar se o IP foi introduzido.

E teremos o endereço definido para o servidor também!

```

      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:58 errors:0 dropped:0 overruns:0 frame:0
      TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:17073 (17.0 KB)  TX bytes:17073 (17.0 KB)

root@owaspbwa:~# ifconfig eth0 down
root@owaspbwa:~# ifconfig eth0 192.168.10.20 netmask 255.255.255.0 up
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:22:bd
          inet addr:192.168.10.20  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe88:22bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5220 (5.2 KB)  TX bytes:3332 (3.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17873 (17.8 KB)  TX bytes:17873 (17.8 KB)

root@owaspbwa:~#

```

Vamos retornar ao Kali Linux e verificar a conectividade da máquina, portanto, digitamos `ping 192.168.10.20` e com isso podemos verificar que as máquinas estão se conectando!

Com os endereços configurados podemos abrir a aba do **Firefox** e inserir o endereço IP que nós criamos. Na URL escrevemos `192.168.10.20` e acessamos "OWASP Multillidae II". Ao abrir a página entramos em "OWASP 2013 > A1 - Injection(SQL) > SQLi - Extract Data > User Info (SQL)". No *Name* preenchemos `admin` e a senha deixamos vazia, damos um "Enter" e copiamos a URL como ela está. Como o IP é estático, então, não é preciso depender do roteador ou da renovação.

Vamos abrir o terminal do Kali Linux para visualizar o **Sql Map**. Escrevemos :

```
> sqlmap -u "http://192.168.10.20/multillidae/index.php?page=user-info.php&username=admin&passw
```

Dessa maneira, é esperado que os problemas de conexão não aconteçam mais!

Lembrando que essa é uma solução caso você esteja com os problemas de conexão, mas ela não é permanente. Ao longo dos exercícios será necessário retornar a placa definida pelo modo *Bridge*.