Firewall e IPTables

Ary Felipe Farah e Silva

1. Criar e configurar o ambiente com as VMs do Kali Linux e do Linux com o VMWare, conforme oritenção do 2º slide da aula.
2. Executar os exercícios do texto "Firewalls e IPTables", registrando em um relatório os resultados obtidos.
3. Executar os comandos do slide 27 da aula (SNORT & IPTables - fwsnort), registrando em um relatório os resultados obtidos.
4. Finalizar o relatório com seus comentários sobre os resultados obtidos, o que aprendeu, as dúvidas, críticas e sugestões sobre a atividade.
5. Fazer a entrega do relatório em formato PDF ou TXT.

Praticando

IP Linux → 192.168.236.128

IP Kali → 192.168.236.130

Bloqueando o acesso SSH

Linux → `sudo iptables -A INPUT -s 192.168.236.128 -p tcp --dport 22 -j DROP`

```
user@virtual-machine:~$ sudo iptables -A INPUT -s 192.168.236.128 -p tcp --dport
 22 -j DROP
user@virtual-machine:~$
```

Kali → `ssh 192.168.236.130`

```
┌──(kali㉿kali)-[~]
└─$ ssh 192.168.236.130
ssh: connect to host 192.168.236.130 port 22: Connection refused
```

Permitir apenas o tráfego HTTP e HTTPS

Linux:

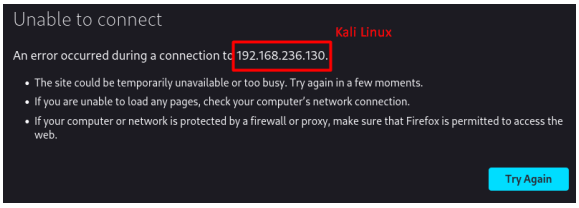
```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

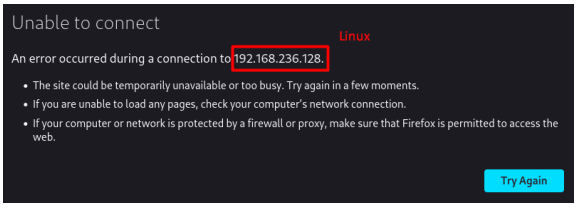
```
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
sudo iptables -A INPUT -s 192.168.236.128 -j DROP
```

```
user@virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
user@virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
user@virtual-machine:~$ sudo iptables -A INPUT -s 192.168.0.102 -j DROP
user@virtual-machine:~$ sudo iptables -A INPUT -s 192.168.236.128 -j DROP
```

Kali → acessar IP no navegador



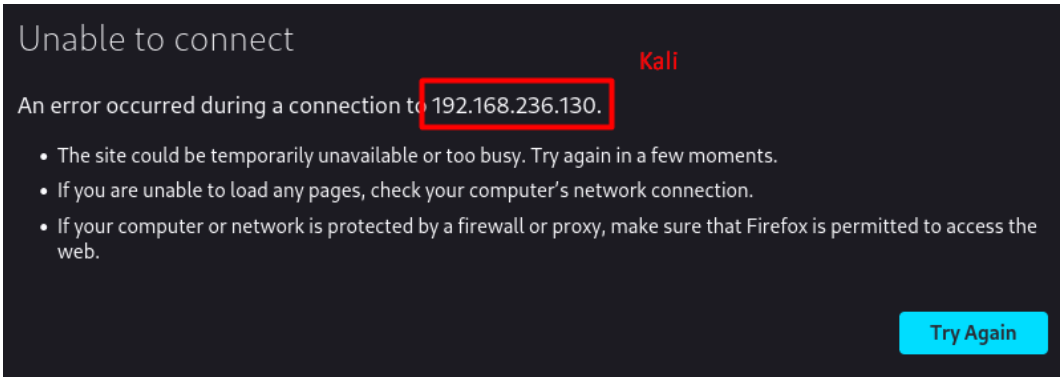


Redirecionar o tráfego da porta 80 para a porta 8080

Linux → `sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080`

```
user@virtual-machine:~$ sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j
REDIRECT --to-ports 8080
```

Kali → acessar IP no navegador



Configurar um servidor DHCP

Linux:

```
sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT
```

```
sudo iptables -A INPUT -p udp --dport 68 -j ACCEPT
```

```
sudo iptables -A OUTPUT -p udp --sport 67 -j ACCEPT
```

```
sudo iptables -A OUTPUT -p udp --sport 68 -j ACCEPT
```

```
user@virtual-machine:~$ sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT
user@virtual-machine:~$ sudo iptables -A INPUT -p udp --dport 68 -j ACCEPT
user@virtual-machine:~$ sudo iptables -A OUTPUT -p udp --sport 67 -j ACCEPT
user@virtual-machine:~$ sudo iptables -A OUTPUT -p udp --sport 68 -j ACCEPT
```

Kali → *Configure a interface de rede para obter um endereço IP automaticamente via DHCP. Verifique se a VM Kali Linux recebeu um endereço IP da VM Linux.* **(?)**

Bloquear o tráfego ICMP (ping)

Linux → `sudo iptables -A INPUT -s 192.168.236.128 -p icmp -j DROP`

```
user@virtual-machine:~$ sudo iptables -A INPUT -s 192.168.236.128 -p icmp -j DRO
P
```

Kali → `ping 192.168.236.130`

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.236.130
PING 192.168.236.130 (192.168.236.130) 56(84) bytes of data.
64 bytes from 192.168.236.130: icmp_seq=1 ttl=64 time=5.87 ms
64 bytes from 192.168.236.130: icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from 192.168.236.130: icmp_seq=3 ttl=64 time=0.083 ms
64 bytes from 192.168.236.130: icmp_seq=4 ttl=64 time=0.081 ms
64 bytes from 192.168.236.130: icmp_seq=5 ttl=64 time=0.105 ms
64 bytes from 192.168.236.130: icmp_seq=6 ttl=64 time=0.123 ms
64 bytes from 192.168.236.130: icmp_seq=7 ttl=64 time=0.082 ms
```

Salvando e Comando slide 27

`sudo iptables-save`

`fwsnort`

```
Ficheiro de configuração '/etc/snort/gen-msg.map'
 ==> Ficheiro no sistema criado por si ou por um script.
 ==> Ficheiro também no pacote disponibilizado pelo maintainer do pacote.
   O que deseja fazer? As suas opções são:
    Y ou I  : instalar a versão do pacote do maintainer
    N ou O  : manter a versão actualmente instalada
      D     : mostrar diferenças entre as versões
      Z     : iniciar uma shell para examinar a situação
 A ação padrão é manter sua versão atual.
*** gen-msg.map (Y/I/N/O/D/Z) [padrão=N] ? ^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^
[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^
[[A^[[A^[[A^[[A^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
[[B^[[B
Progress: [ 63%] [#####################################......................]
```

Travou aqui por um tempão

Resultados

Conclusão

Acredito que, mesmo seguinto todo o passo a passo da atividade, não consegui desempenhar ela de forma 100% correta, mas tentei e acredito que entendi o propósito dela lendo e colocando em prática o arquivo ***Firewall IPTables*** postado