Analisando o Consumo de um Scan

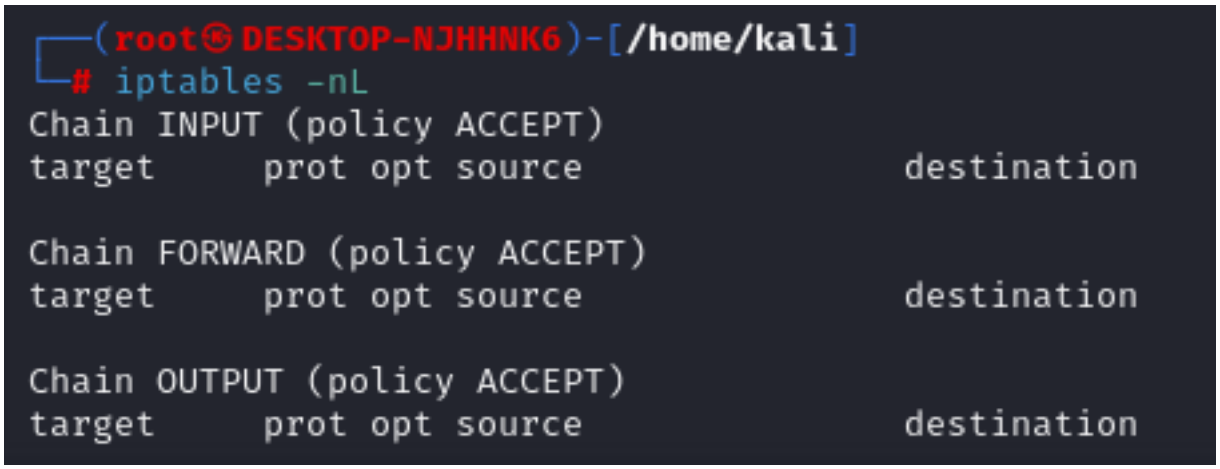
+ Aqui usaremos o iptables para fazer a leitura dos tamanhos dos pacotes enviados e recebidos durante a realização de um scan.

+ Faremos testes apenas locais (entre eu e eu) para fazer essa leitura

+ Iniciaremos os serviços do apache2 e do ssh para abrir portas

+ O teste iptables -nL mostra quais são as configurações iniciais

```
iptables -nL
```



+ Meu IP é 192.168.1.138. Faremos então a abertura de comunicação para esse IP, tanto entrada quanto saída.

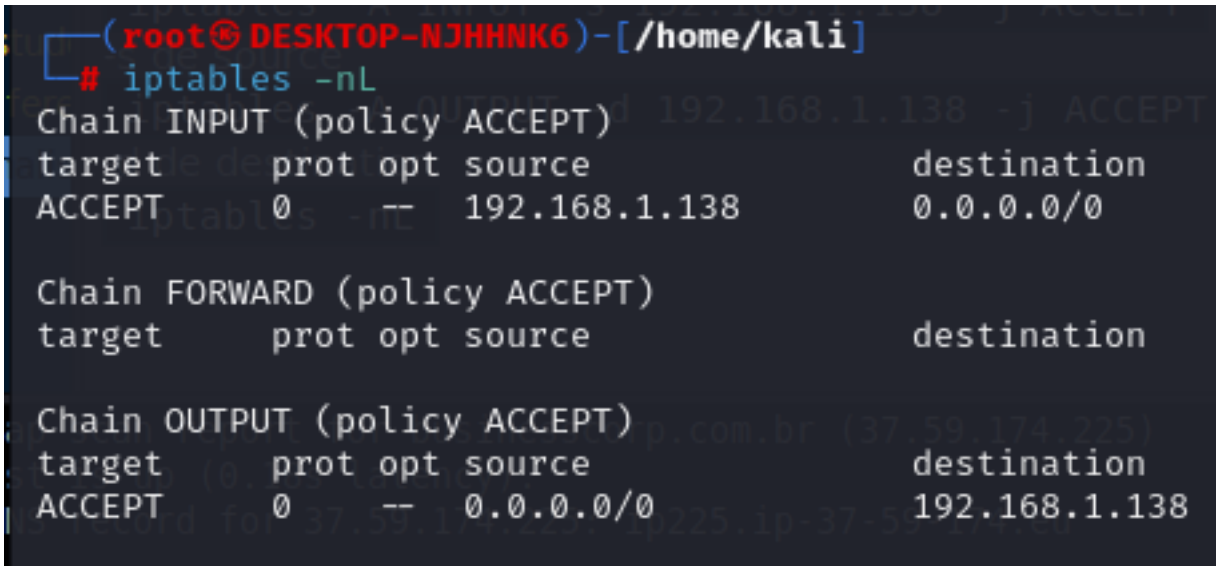
```
iptables -A INPUT -s 192.168.1.138 -j ACCEPT
```

-s de source

```
iptables -A OUTPUT -d 192.168.1.138 -j ACCEPT
```

-d de destination

```
iptables -nL
```



+ Agora faremos o scanneamento com o nmap e analisaremos o tamanho e quantidade dos pacotes por meio do comando iptables -nvL

+ Primeiramente, faremos um scan com TCP Connect

```
nmap -sT -p 80 -Pn 192.168.1.138
```

-Pn para que não seja verificado se o host está ativo ou não (já sabemos que ele está)

```
iptables -nvL
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# iptables -nvL
Chain INPUT (policy ACCEPT 60501 packets, 77M bytes)
 pkts bytes target     prot opt in     out     source               destination

    4   224 ACCEPT     0    --  *      *       192.168.1.138        0.0.0.0/0


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 15946 packets, 2929K bytes)
 pkts bytes target     prot opt in     out     source               destination

    4   224 ACCEPT     0    --  *      *       0.0.0.0/0            192.168.1.1
38
```

→ Veja que temos 4 pacotes entrando e 4 saindo com o TCP Connect

+ Para continunar nossa análise, devemos zerar esses valores, para que não fiquem sendo somados com os resultados novos. Isso se dá por meio do comando

```
iptables -Z
```

+ Agora faremos um scanneamento com o SYN Scan

```
nmap -sS -p 80 -Pn 192.168.1.138
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# iptables -nvL
Chain INPUT (policy ACCEPT 983 packets, 1355K bytes)
 pkts bytes target     prot opt in     out     source               destination

    3   128 ACCEPT     0    --  *      *       192.168.1.138        0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 123 packets, 8680 bytes)
 pkts bytes target     prot opt in     out     source               destination

    3   128 ACCEPT     0    --  *      *       0.0.0.0/0            192.168.1.1
38
```

→ Veja que agora foram mandados apenas 3 pacotes, que foram também recebidos

+ Podemos realizar um scan em todas as portas executando apenas o comando

```
nmap -sS -p- -Pn 192.168.1.138
```

```
iptables -nvL
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# iptables -nvL
Chain INPUT (policy ACCEPT 4772 packets, 6170K bytes)
 pkts bytes target     prot opt in     out     source               destination

 131K 5505K ACCEPT     0    --  *      *       192.168.1.138        0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 984 packets, 167K bytes)
 pkts bytes target     prot opt in     out     source               destination

 131K 5505K ACCEPT     0    --  *      *       0.0.0.0/0            192.168.1.1
38
```

+ Fazer a verificação só em portas mais usuais pode ser uma boa ideia pelo motivo de fazer "menos barulho" durante o mapeamento.