Exercício 1g - Spoofing

Objetivo: Analisar o funcionamento de um ataque de spoofing e aplicar medidas para evitar a propagação desse ataque na rede.

Cenário inicial: Os endereços das interfaces físicas já estão configurados.

Aplicar nos roteadores filtros de proteção que impedirão que seus clientes enviem pacotes para a Internet com endereços IP falsos (spoofing). Importante destacar que quanto mais próximo do cliente, mais restritiva devem ser as regras aplicadas. Dentro desse conceito, no roteador que atua como “concentrador”, **MikrotikClientes**, o filtro `rp_filter` deve ser habilitado. Deve-se evitar utilizar o filtro de anti spoofing na borda do provedor.

1. Acesse o **Cliente_Corporativo** e capture os pacotes da interface eth0 usando o wireshark.

2. Acesse o **Cliente_Domestico** e capture os pacotes da interface eth0 usando o wireshark.

3. Para falsificar um pacote IPv6, podemos utilizar o comando nping. No entanto, para isso é necessário saber o endereço MAC da interface eth0 do Linux e da interface ether2 do **MikrotikClientes**.

4. No **MikrotikClientes**, para listar o m*ac address* use o seguinte comando.

```
/interface print detail
```

5. No terminal **Termit**, liste o *mac address* do **Cliente_Domestico** com o comando.

```
#ip address show
```

6. Ainda no terminal do **Cliente_Domestico**, execute o **nping** com o endereço IP de origem falsificado com destino ao **Cliente_Corporativo**, sendo que o parâmetro dest-mac é o endereço MAC da interface ether2 do **MikrotikClientes** e o source-mac é o endereço MAC da interface eth0 do **Cliente_Domestico**.

```
#nping -6 -S 3000::1 --dest-ip 4D0C:XX:0400::100 --dest-mac \
50:29:00:03:00:00 --source-mac 00:50:00:00:01:00 --interface eth0
```

* Lembre de substituir os endereços --dest-mac e --source-mac para os encontrados nos passos anteriores.

Observe que o spoofing foi bem sucedido e as respostas das solicitações estão chegando e sendo capturadas no wireshark do **Cliente_Corporativo**.

Tendo em vista essa situação, o recomendado é o uso de filtros anti-spoofing. O ideal é que esse filtro seja feito o mais perto da origem possível. Assim, o ideal é aplicarmos os filtros no roteador mais próximo dos clientes, no caso o **MikrotikClientes**. No Mikrotik, para endereços IPv4 poderíamos habilitar o filtro RFP com o comando /ip settings set rp-filter=strict

7. Como não há filtro RPF para IPv6 no Mikrotik, aplique filtros manuais.

```
/ipv6 firewall address-list
  add address=4d0c:XX:0c00::/40 list=CLIENTE-DOMESTICO-V6
  add address=4d0c:XX:0400::/40 list=CLIENTE-CORPORATIVO-V6
/ipv6 firewall filter
  add chain=forward in-interface=ether2 \
src-address-list=CLIENTE-DOMESTICO-V6
  add chain=forward in-interface=ether3 \
src-address-list=CLIENTE-CORPORATIVO-V6
  add action=drop chain=forward in-interface=ether2
  add action=drop chain=forward in-interface=ether3
```

Após aplicá-los, tente realizar novamente o spoofing.

10. Acesse novamente o **Cliente_Corporativo** e capture os pacotes da interface eth0 usando o wireshark.

11. Acesse novamente o **Cliente_Domestico** e capture os pacotes da interface eth0 usando o wireshark.

12. No terminal do **Cliente_Domestico**, execute o comando **nping** com o endereço IPv6 de origem falsificado com destino ao **Cliente_Corporativo**.

```
#nping -6 -S 3000::1 --dest-ip 4d0c:XX:0c00::100 --dest-mac \
00:50:08:00:05:00 --source-mac 00:50:02:00:03:00 --interface eth0
```

* Lembre de substituir os endereços --dest-mac e --source-mac para os encontrados nos passos anteriores.

Veja o resultado das capturas no wireshark do **Cliente_Domestico** e do **Cliente_Corporativo**. Percebeu alguma diferença em relação ao teste anterior?