

Exercício 4a - 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, o protocolo de roteamento interno e o iBGP já estão configurados.

Antes de configurar as sessões eBGP e obter acesso às redes externas, aplique nos roteadores do AS 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. No terminal do **Cliente_Domestico**, execute o comando `hping3` com o endereço de origem falsificado com destino ao **Cliente_Corporativo**. Observe depois no wireshark do **Cliente_Corporativo** para ver como o pacote chegou.

```
#hping3 -a 192.168.1.3 10.XX.1.100 --interface eth0
```

4. 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**.
5. No **MikrotikClientes**, para listar o *mac address* use o seguinte comando.

```
/interface print detail
```

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

```
#ip address show
```

7. 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:4000::100 --dest-mac  
50:29:00:03:00:00 --source-mac 00:50:00:00:01:00
```

* 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**.

8. No **MikrotikClientes**, habilite o filtro RPF IPv4.

```
/ip settings  
set rp-filter=strict
```

* Uma medida redundante ao RPF é a aplicação de filtros, que pode ser feita com os seguintes comandos(contudo, não necessário):

`/ip firewall filter`

```
add chain=forward in-interface=ether2 src-address=10.XX.2.0/23  
add chain=forward in-interface=ether3 src-address=10.XX.1.0/24  
add action=drop chain=forward in-interface=ether2  
add action=drop chain=forward in-interface=ether3
```

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

```
/ipv6 firewall address-list  
add address=4D0C:XX:C000::/40 list=CLIENTE-DOMESTICO-V6  
add address=4D0C:XX:4000::/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 aplicar esses filtros, 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 **hping3** com o endereço IPv4 de origem falsificado com destino ao **Cliente_Corporativo**. E execute o **nping** com o endereço IPv6 de origem falsificado com destino também ao **Cliente_Corporativo**.

```
#hping3 -a 192.168.1.3 10.XX.1.100 --interface eth0
#nping -6 -S 3000::1 --dest-ip 4D0C:XX:C000::100 --dest-mac
50:29:00:03:00:00 --source-mac 00:50:00:00:01:00
```

* 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?

Exercício 4b - Filtros: Gerência da porta 25

Objetivo: Implementar na rede do ISP filtros de gerência da porta 25/TCP.

Cenário inicial: Os endereços das interfaces físicas, o protocolo de roteamento interno e o iBGP já estão configurados.

Outro filtro importante de ser configurado é o que impede a saída de tráfego da rede dos clientes domésticos com destino à porta 25/TCP, com o intuito de evitar o envio de spams. Nesse exercício abordaremos apenas como criar o filtro que impede o encaminhamento de pacotes com destino a porta 25 e não será tratada nenhuma configuração referente ao servidor de e-mail.

1. Este filtro também deve ser configurado o mais próximo a rede dos clientes domésticos atuando apenas sobre as interfaces que conectam este tipo de cliente.

No roteador **MikrotikClientes** utilize os seguintes comandos:

```
/ip firewall filter
  add chain=forward action=drop dst-port=25 protocol=tcp \
in-interface=ether2
/ipv6 firewall filter
  add chain=forward action=drop dst-port=25 protocol=tcp \
in-interface=ether2 place-before=0
```

2. Verifique se os filtros estão funcionando conforme o esperado. No terminal do **Cliente_Domestico**, execute o comando **hping3** para IPv4 e execute o **nping** para o IPv6. Em paralelo, capture os pacotes no wireshark que chegam no **Cliente_Corporativo**.

```
#hping3 10.XX.1.100 -p 25
#nping -6 --tcp -p 25 --dest-ip 4D0C:XX:4000::100
```

3. Faça o mesmo teste que o anterior, só que agora para a porta 22. Teve alguma diferença?

```
#hping3 10.XX.1.100 -p 22
#nping -6 --tcp -p 22 --dest-ip 4D0C:XX:4000::100
```