Exercício 1a - Observando pacotes com o Wireshark

Objetivo: Aprender a usar o programa Wireshark para capturar e analisar pacotes que estão trafegando na rede, na tentativa de obter informações pertinentes.

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

1. Acesse o **Cliente_Domestico** e inicie o programa Wireshark.

2. No Wireshark inicie a captura de pacotes na interface eth0.

3. Em paralelo, abra o terminal **Termit** e realize um ping IPv6 para o **Cliente_Corporativo**.

```
#ping6 -c4 4d0c:XX:0400::100
```

4. Agora, faça uma varredura das portas com serviços TCP em IPv6.

```
#nmap -6 -sS 4d0c:XX:0400::100
```

5. Realize uma nova varredura em IPv6 só que agora sendo de portas com serviços UDP. Este processo pode demorar muito, caso queira pará-lo, use CTRL+C. Para ter uma noção de quanto do processo passou, dê um *enter* durante a execução que ele retorna a porcentagem de avanço do processo.

```
#nmap -6 -sU 4d0c:XX:0400::100
```

6. Volte para o wireshark e pare a captura dos pacotes. Dessa captura, analise os pacotes capturados buscando por informações que possam comprometer a segurança da rede.

    a. Use o filtro `icmpv6` no wireshark para ver os pacotes enviados e recebidos do ping IPv6 realizado. Selecione um pacote do tipo `echo (ping) request` e veja as informações contidas nele. Observe que é possível ver o endereço IP de origem e destino deste pacote, também é possível ver os endereços MAC. Veja também as informações contidas no pacote de resposta identificado pelo tipo `echo (ping) reply`.

    b. Use o seguinte filtro no wireshark para selecionar os pacotes que contenham a informação do endereço 4d0c:XX:0400::100, do número de porta NN e tenham sido enviadas pelo protocolo TCP. Como o nmap faz um escaneamento das portas, vários pacotes foram capturados. Analise os pacotes com os números de portas retornados pelo comando NMAP TCP SYN scan IPv6 realizado anteriormente.

```
ipv6.addr == 4d0c:XX:0400::100 and tcp.port in {NN}
```

*troque NN pelo número da porta que se queira procurar. Ex: 80

c. Faça a mesma análise anterior para os pacotes IPv6 usando o seguinte filtro no wireshark.

```
ipv6.addr == 4d0c:XX:0400::100 and tcp.port in {NN}
```

d. Para os pacotes UDP, use os seguintes filtros. As portas inacessíveis retornam um pacote do tipo ICMP avisando isso.

```
ipv6.addr == 4d0c:XX:0400::100 and udp.port in {NN}
```