Exercício 1e - Ataque de *Sniffing* de pacotes em protocolos sem segurança

Objetivo: Realizar uma análise de um ataque de *sniffing* (que intercepta pacotes trafegados na rede para analisar o seu conteúdo) para depois aplicar configurações devidas para sanar esses problemas de segurança.

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

1. Acesse o **Cliente_Domestico** e inicie uma captura no wireshark na interface eth0.

2. No terminal **Termit,** realize uma conexão via telnet ao **MikrotikClientes**.

```
#telnet 4d0c:XX:0c00::1
user: admin
password: SenhaAdmin
```

Para fazer logoff do terminal do **MikrotikClientes** e voltar para o terminal **Termit** do **Cliente_Domestico** use o comando: **quit**

3. No wireshark, analise os pacotes e busque a senha usada durante a conexão telnet.
   a. Para isso, use o seguinte filtro `telnet` no wireshark.
   b. Selecione um dos pacotes telnet.
   c. Com o botão direito do mouse, selecione a opção "`follow tcp stream`".
   d. Veja as informações da comunicação telnet e busque a senha usada.

4. No terminal, realize os seguintes comandos NMAP para descobrir as portas e serviços abertos em TCP e UDP em IPv6.

```
#nmap -6 -sS 4d0c:XX:0c00::1
#nmap -6 -sU 4d0c:XX:0c00::1
```

A varredura de portas dos serviços UDP pode demorar muito, caso queira pará-la, use CTRL + C.

5. Após identificar todas essas portas e serviços abertos, vamos tomar algumas medidas de segurança para proteger o **MikrotikClientes**. Acesse esse roteador e liste todos os serviços habilitados nele usando o comando a seguir.

```
/ip service print

Flags: X - disabled, I - invalid
 #   NAME             PORT ADDRESS
 0   telnet             23
 1   ftp                21
 2   www                80
 3   ssh                6022
 4 XI www-ssl           443
 5   api              8728
 6   winbox           8291
 7   api-ssl          8729
```

6. Desabilite todos os serviços que não serão usados nesse roteador.

    a. Desabilite o telnet, porque esse protocolo não é seguro para acesso remoto ao roteador, como vimos anteriormente. Para acesso remoto use SSH.

```
/ip service disable telnet
```

    b. Desabilite o FTP, pois não usaremos transferência de arquivos.

```
/ip service disable ftp
```

    c. Desabilite o HTTP.

```
/ip service disable www
```

    d. Desabilite o HTTPS, que nessa versão está desabilitado por padrão.

```
/ip service disable www-ssl
```

    e. Desabilite a opção de pegar informações do roteador por API.

```
/ip service disable api
/ip service disable api-ssl
```

f. Desabilite o testador de banda.

```
/tool bandwidth-server set enabled=no
```

g. Desabilite que o mikrotik atue como um servidor DNS cache. Nessa versão, ele está desabilitado por padrão.

```
/ip dns set allow-remote-requests=no
```

h. Desabilite o acesso via sockets no mikrotik. Nessa versão, ele está desabilitado por padrão.

```
/ip socks set enabled=no
```

i. Desabilite o acesso via LAN sem IP definido.

```
/tool mac-server set allowed-interface-list=none
/tool mac-server mac-winbox set allowed-interface-list=none
```

j. Desabilite a descoberta na LAN.

```
/tool mac-server ping set enabled=no
```

k. Desabilite o *Router Management Overlay Network* para diminuir a interface de ataque. Nessa versão, ele está desabilitado por padrão.

```
/tool romon set enabled=no
```

l. Desabilite os protocolos MNDP, CDP e LLDP que ficam procurando roteadores na rede.

```
/ip neighbor discovery-settings set discover-interface-list=none
```

m. Desabilite o proxy. Nessa versão, ele está desabilitado por padrão.

```
/ip proxy set enabled=no
```

n. Desabilite o UPnP. Nessa versão, ele está desabilitado por padrão.

```
/ip upnp set enabled=no
```

o. Desabilite o cliente DHCP da interface ether1.

```
/ip dhcp-client print
/ip dhcp-client remove 0
```

7. Liste todos os pacotes habilitados no roteador.

```
/system package print

Flags: X - disabled
 #   NAME                                VERSION                                SCHEDULED
 0   dude                                6.45.8
 1   routeros-x86                        6.45.8
 2   system                              6.45.8
 3   ipv6                                6.45.8
 4   ups                                 6.45.8
 5   wireless                            6.45.8
 6   hotspot                             6.45.8
 7   mpls                                6.45.8
 8   routing                             6.45.8
 9   ppp                                 6.45.8
10   dhcp                                6.45.8
11   security                            6.45.8
12   advanced-tools                      6.45.8
```

8. Desabilite os pacotes não utilizados e reinicie o roteador para aplicar as mudanças.

```
/system package disable wireless,dude,ups,hotspot,mpls,dhcp,ppp,\
advanced-tools
/system reboot
```

*Verifique se você realmente não utiliza esses pacotes antes de desabilitar

9. Liste as interfaces para ver o índice de cada uma.

```
/interface print

Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU
 0  R  ether1                              ether            1500
 1  R  ether2                              ether            1500
 2  R  ether3                              ether            1500
 3  R  ether4                              ether            1500
```

10. Desabilite as interfaces que não estão em uso (ether4 que está listada com índice 3).

```
/interface set 3 disabled=yes
```