Exercício 1 - Hardening

Objetivo: Realizar testes de vulnerabilidades nos equipamentos do AS para identificar as falhas de segurança e assim aplicar as devidas soluções para sanar esses problemas.

* É preciso substituir XX nas configurações a seguir pelo número do seu grupo. Sempre utilizando dois dígitos.

Parte 1 - Antes de iniciar os testes, realize as configurações prévias descritas a seguir.

1. Acesse o **Cliente_Domestico**. As credenciais dessa máquina são:
   Login: root
   Senha: toor

2. Configure os endereços IPv4 e IPv6 na interface eth0 dessa máquina.
   a. Abra o terminal **Termit**.
   b. Edite o arquivo "interfaces" (/etc/network/interfaces) usando algum editor no terminal como, por exemplo, Vim **ou** Nano.

```
#vim /etc/network/interfaces
```

Veja como usar o Vim em:
https://www.vivaolinux.com.br/dica/Usando-o-editor-de-texto-VIM-para-editar-o-sources.list

ou

```
#nano /etc/network/interfaces
```

Veja como usar o Nano em:
https://www.vivaolinux.com.br/artigo/Introducao-ao-Linux-O-editor-de-texto-Nano

   c. Adicione as seguintes linhas no final do arquivo.

```
auto eth0

iface eth0 inet static
      address 10.XX.2.100
      netmask 255.255.254.0
      gateway 10.XX.2.1

iface eth0 inet6 static
      address 4d0c:XX:0c00::100
      netmask 40
      gateway 4d0c:XX:0c00::1
```

3. Após salvar as mudanças do arquivo, reinicie a máquina para que as mudanças sejam aplicadas. No terminal **Termit**

```
#reboot now
```

4. Acesse novamente a máquina e verifique as configurações usando os seguintes comandos no terminal **Termit**.

```
#cat /etc/network/interfaces
#ip address show
```

Parte 2 - Faça o mesmo processo na máquina **Cliente_Corporativo**.

1. Acesse o **Cliente_Corporativo**. As credenciais dessa máquina também são:
   Login: root
   Senha: toor

2. Configure os endereços IPv4 e IPv6 na interface eth0 dessa máquina **Cliente_Corporativo**.
   a. Abra o terminal **Termit**.
   b. Edite o arquivo "interfaces" (/etc/network/interfaces) adicionando as seguintes linhas.

```
auto eth0

iface eth0 inet static
      address 10.XX.1.100
      netmask 255.255.255.0
      gateway 10.XX.1.1

iface eth0 inet6 static
      address 4d0c:XX:0400::100
      netmask 40
      gateway 4d0c:XX:0400::1
```

3. Salve as mudanças do arquivo, reinicie a máquina para que as mudanças sejam aplicadas.

4. Acesse novamente a máquina e verifique se as configurações foram aplicadas.

Parte 3 - Agora faça as seguintes configurações nos roteadores.

1. Acesse o roteador **MikrotikBorda**. As credenciais de acesso dessa máquina são:
   Login: admin
   Não tem senha, basta dar *enter*.

2. Infelizmente nessa versão do Mikrotik o IPv6 não vem habilitado por padrão. Habilite o protocolo IPv6 e, logo em seguida, reinicie o roteador **MikrotikBorda**.

```
/system package enable ipv6
/system reboot
```

3. Agora vamos mudar o nome do roteador **MikrotikBorda**. Essa é uma boa prática, pois facilita na identificação do equipamento durante *troubleshootings* e ajuda a evitar configurações em equipamentos equivocados que podem ter o mesmo nome de fábrica. Acesse novamente como admin e aplique o comando a seguir.

```
/system identity set name=mkt_bordaXX
```

4. Configure os endereços IPv4 e IPv6 nas interfaces do roteador **MikrotikBorda**.

```
/ip address
  add address=10.XX.0.1/30 interface=ether1 comment=MKT-CLIENTES
/ipv6 address
  add address=4d0c:XX:0:1::1/126 interface=ether1 comment=MKT-CLIENTES
```

Parte 4 - Realize o mesmo procedimento para o outro roteador.

1. Acesse o roteador **MikrotikClientes**. As credenciais de acesso dessa máquina são:
   Login: admin
   Não tem senha, basta dar *enter*.

2. Habilite o protocolo IPv6 e, logo em seguida, reinicie o roteador **MikrotikClientes**.

```
/system package enable ipv6
/system reboot
```

3. Agora vamos mudar o nome do roteador **MikrotikClientes**. Acesse novamente como admin e aplique o comando a seguir.

```
/system identity set name=mkt_clientesXX
```

4. Configure os endereços IPv4 e IPv6 nas interfaces do roteador **MikrotikClientes**.

```
/ip address
  add address=10.XX.0.2/30 interface=ether1 comment=MKT-BORDA
  add address=10.XX.2.1/23 interface=ether2 comment=CLI-DOMESTICO
  add address=10.XX.1.1/24 interface=ether3 comment=CLI-CORPORATIVO

/ipv6 address
  add address=4d0c:XX:0:1::2/126 interface=ether1 comment=MKT-BORDA
  add address=4d0c:XX:0c00::1/40 interface=ether2 comment=CLI-DOMESTICO
  add address=4d0c:XX:0400::1/40 interface=ether3 comment=CLI-CORPORATIVO
```

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 IPv4 para o **Cliente_Corporativo**.

```
#ping -c4 10.XX.1.100
```

4. Em seguida, realize um ping IPv6 para o **Cliente_Corporativo**.

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

5. Agora faça uma varredura das portas com serviços TCP em IPv4.

```
#nmap -sS 10.XX.1.100
```

6. Realize uma nova varredura em IPv4 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, deu um *enter* durante a execução que ele retorna a porcentagem de avanço do processo.

```
#nmap -sU 10.XX.1.100
```

7. Vamos realizar o mesmo processo para o IPv6. Realize uma varredura das portas com serviços TCP em IPv6. Assim como em IPv4, este procedimento levará alguns minutos.

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

8. Por fim, faça uma varredura em IPv6 em 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, deu um enter durante a execução que ele retorna a porcentagem de avanço do processo.

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

9. 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 `icmp` no wireshark para ver os pacotes enviados e recebidos do ping IPv4 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 do pacote de resposta identificado pelo tipo `echo (ping) reply`.

    b. Agora faça a mesma análise para os pacotes IPv6. Use o filtro `icmpv6` para ver os pacotes enviados e recebidos do ping IPv6 realizado.

    c. Use o seguinte filtro no wireshark para selecionar os pacotes que contenham a informação do endereço 10.XX.1.100, 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 IPv4 realizado anteriormente.

```
ip.addr == 10.XX.1.100 and tcp.port in {NN}
```

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

    d. 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}
```

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

```
ip.addr == 10.XX.1.100 and udp.port in {NN}
ipv6.addr == 4d0c:XX:0400::100 and udp.port in {NN}
```

Exercício 1b - Configurando senha no Mikrotik

Objetivo: Alterar o acesso padrão aos roteadores mikrotik configurando uma senha segura no equipamento.

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

1. Acesse o **MikrotikClientes** usando a credencial admin (senha vazia).

```
MikroTik Login: admin
Password:
```

2. Crie um segundo administrador para sua conta

```
/user add name=BackupAdmin password=SenhaDoBackupAdmin group=full
```

3. Faça logout de sua sessão e tente entrar com o novo usuário

```
/quit

MikroTik Login: BackupAdmin
Password: SenhaDoBackupAdmin
```

4. Faça o mesmo para o roteador **MikrotikBorda**

```
/user add name=BackupAdmin password=SenhaDoBackupAdmin group=full

/quit

MikroTik Login: BackupAdmin
Password: SenhaDoBackupAdmin
```

5. Troque a senha do usuário admin padrão. Lembrando que por padrão essa senha não existe, o que permite que qualquer pessoa, que saiba disso, possa invadir este roteador. Configure uma senha segura em **MikrotikClientes**. (Veja quais são características necessárias para a criação de uma boa senha segura: https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf)

```
/user set 0 password=SenhaAdmin
```

6. Faça logout de sua sessão em **MikrotikClientes** e tente entrar com o administrador original

```
/quit

MikroTik Login: admin
Password: SenhaAdmin
```

7. Faça o mesmo para o roteador **MikrotikBorda**

```
/user set 0 password=OutraSenha
```

8. Faça logout de sua sessão em **MikrotikBorda** e tente entrar com o administrador original

```
/quit

MikroTik Login: admin
Password: OutraSenha
```

9. Finalizado a criação dos administradores volte para **MikrotikClientes** e crie um grupo específico e liste as permissões desse grupo

```
/user group add name=tecnico policy=ssh,ftp,reboot,read,write,policy
```

10. Adicione um novo usuário em **MikrotikClientes** no grupo criado anteriormente. Ao usar suas credenciais, este novo usuário só terá acesso as funções liberadas para o seu grupo.

```
/user add name=edu password=SenhaEdu group=tecnico
```

11. Agora vamos tomar as devidas medidas para permitir o acesso remoto e seguro aos equipamentos. Acesse o **Cliente_Domestico**, abra o terminal **Termit** e gere um par de chave RSA que serão usadas para o SSH.

```
#ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): [Enter]
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase): SenhaClienteDomestico
Enter same passphrase again: SenhaClienteDomestico
```

12. Após a criação das chaves, ainda no terminal **Termit**, transfira a chave pública gerada para o **MikrotikClientes**.

```
#scp .ssh/id_rsa.pub admin@10.XX.2.1:edu.pub

The authenticity of host '10.XX.2.1 (10.XX.2.1)' can't be established.
RSA key fingerprint is
SHA256:****************************************.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.XX.2.1' (RSA) to the list of known
hosts.
admin@10.XX.2.1's password: SenhaAdmin
```

13. No **MikrotikClientes** importe a chave pública recebida e marque para o ssh usar uma criptografia forte.

```
/user ssh-keys import public-key-file=edu.pub user=edu
/ip ssh set strong-crypto=yes
```

14. Teste o acesso SSH IPv4 do **Cliente_Domestico** para o **MikrotikClientes**. Acesse o terminal **Termit** no **Cliente_Domestico** e use o comando a seguir.

```
#ssh edu@10.XX.2.1

Enter passphrase for key '/root/.ssh/id_rsa': SenhaClienteDomestico
```

15. Agora teste o acesso SSH IPv6 do **Cliente_Domestico** para **MikrotikClientes**. Acesse o terminal **Termit** no **Cliente_Domestico** e use o comando a seguir.

```
#ssh -6 edu@4d0c:XX:0c00::1

The authenticity of host '4d0c:XX:c00::1 (4d0c:XX:c00::1)' can't be
established.
RSA key fingerprint is
SHA256:****************************************.
Are you sure you want to continue connecting (yes/no)? yes
Enter passphrase for key '/root/.ssh/id_rsa': SenhaClienteDomestico
```

10. No **MikrotikClientes** verifique o log e veja que a conexão foi realizada por ssh (O log vem habilitado por padrão).

```
/log print
```

Exercício 1c - 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 10.XX.2.1
user: admin
password: SenhaAdmin
```

3. No wireshark, análise 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 IPv4 e IPv6.

```
#nmap -sS 10.XX.2.1
#nmap -sU 10.XX.2.1
#nmap -6 -sS 4d0c:XX:0c00::1
#nmap -6 -sU 4d0c:XX:0c00::1
```

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                22
 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 este 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 desabilitada 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. Listar todos os pacote 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. Desabilitar os pacotes não utilizados e depois 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 indice 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
```

11. Agora faça o mesmo para o **MikrotikBorda** (do passo 5. ao 10.)