Exercício 1 - Segurança em equipamentos: 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 102.1XX.2.100
      netmask 255.255.254.0
      gateway 102.1XX.2.1

iface eth0 inet6 static
      address 4D0C:ABXX:C000::100
      netmask 40
      gateway 4D0C:ABXX:C000::1
```

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

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.
   a. Abra o terminal Termit.
   b. Edite o arquivo "interfaces" (/etc/network/interfaces) adicionando as seguintes linhas.

```
auto eth0

iface eth0 inet static
      address 102.1XX.1.100
      netmask 255.255.255.0
      gateway 102.1XX.1.1

iface eth0 inet6 static
      address 4D0C:ABXX:4000::100
      netmask 40
      gateway 4D0C:ABXX:4000::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.

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

3. Agora vamos mudar o nome do roteador. 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.

```
/ip address add address=102.1XX.0.1/30 interface=ether1
/ipv6 address add address=4D0C:ABXX:0:1::1/126 interface=ether1
```

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.

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

3. Agora vamos mudar o nome do roteador. 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.

```
/ip address
  add address=102.1XX.0.2/30 interface=ether1
  add address=102.1XX.2.1/23 interface=ether2
  add address=102.1XX.1.1/24 interface=ether3

/ipv6 address
  add address=4D0C:ABXX:0:1::2/126 interface=ether1
  add address=4D0C:ABXX:C000::1/40 interface=ether2
  add address=4D0C:ABXX:4000::1/40 interface=ether3
```

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 102.1XX.1.100
```

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

```
#ping6 -c4 4D0C:ABXX:4000::100
```

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

```
#nmap -sS 102.1XX.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 102.1XX.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:ABXX:4000::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:ABXX:4000::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 102.1XX.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 == 102.1XX.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.

```
ip6.addr == 4D0C:ABXX:4000::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 == 102.1XX.1.100 and udp.port in {NN}
ip6.addr == 4D0C:ABXX:4000::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.

2. 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. (Veja quais são características necessárias para a criação de uma boa senha segura: https://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas.pdf)

```
/user set 0 password=Uma5enha5eguraEuma5enhaExtensa
```

3. Crie um grupo específico e liste as permissões desse grupo.

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

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

```
/user add name=eduardo password=Naodevemo5usaramesma5enha group=tecnico
\ comment=consultor
```

5. 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
"Enter file in which to save the key (/root/.ssh/id_rsa):" -> Deixar
nesse default mesmo. Basta dar enter.
password=SenhadousuarioCliente_Domestico
```

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

```
#scp .ssh/id_rsa.pub admin@102.1XX.2.1:eduardo.pub
```

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

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

8. 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 eduardo@102.1XX.2.1
```

*Lembre da senha: SenhadousuarioCliente_Domestico

9. 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 eduardo@4D0C:ABXX:C000::1
```

*Lembre da senha: SenhadousuarioCliente_Domestico

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 102.1XX.2.1
user: admin
password: Uma5enha5eguraEuma5enhaExtensa
```

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 102.1XX.2.1
#nmap -sU 102.1XX.2.1
#nmap -6 -sS 4D0C:ABXX:C000::1
#nmap -6 -sU 4D0C:ABXX:C000::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
```

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 set 0 disabled=yes
```

7. Listar todos os pacote habilitados no roteador.

```
/system package print
```

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

```
/system package disable wireless,dude,ups,hotspot,mpls,ppp,dhcp,\
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
```

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

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

Exercício 1d - Spoofing

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

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

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 192.168.1.3 102.1XX.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 m*ac 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:ABXX: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=102.1XX.2.0/23
  add chain=forward in-interface=ether3 src-address=102.1XX.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:ABXX:C000::/40 \
list=CLIENTE-DOMESTICO-V6
/ipv6 firewall address-list add address=4D0C:ABXX:4000::/40 \
list=CLIENTE-CORPORATIVO-V6
/ipv6 firewall filter add chain=forward in-interface=ether2 \
src-address-list=CLIENTE-DOMESTICO-V6
/ipv6 firewall filter add chain=forward in-interface=ether3 \
src-address-list=CLIENTE-CORPORATIVO-V6
/ipv6 firewall filter add action=drop chain=forward in-interface=ether2
/ipv6 firewall filter 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 192.168.1.3 102.1XX.1.100 --interface eth0
#nping -6 -S 3000::1 --dest-ip 4D0C:ABXX: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?