Exercício 1a - 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 **HuaweiBorda**.

2. Para entrar no modo de configuração do Huawei, digite o seguinte comando no **HuaweiBorda**.

```
system-view
```

3. Agora vamos mudar o nome do roteador **HuaweiBorda**. 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. Aplique o comando a seguir.

```
sysname HuaweiBordaXX
```

4. Mude a forma como o **HuaweiBorda** mostra o ASN.

```
as-notation plain

Warning: If the configuration takes effect, the regular expression of the filter for
4-byte AS path should be changed to the asplain format, otherwise match will fail.
Continue? [Y/N]: Y
```

5. Configure os endereços IPv4 e IPv6 nas interfaces do roteador **HuaweiBorda**.

```
interface Ethernet1/0/1
 ipv6 enable
 ip address 10.XX.0.1 255.255.255.252
 ipv6 address 4D0C:XX:0:1::1/126
 quit
```

6. Aplique as configurações no roteador **HuaweiBorda**.

```
commit
```

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

1. Acesse o roteador **HuaweiClientes**. No primeiro acesso ele vai pedir para mudar a senha, coloque a senha **ceptro** (para facilitar o troubleshooting). As credenciais de acesso iniciais dessa máquina são:

```
Username: super
Password: super

Warning: The password is already expired.
The password needs to be changed. Change now? [Y/N]: Y
Please enter old password: super
Please enter new password: ceptro
Please confirm new password: ceptro
```

2. Para entrar no modo de configuração do Huawei, digite o seguinte comando no **HuaweiClientes**.

```
system-view
```

3. Infelizmente nessa versão do Huawei o IPv6 não vem habilitado por padrão. Habilite o protocolo IPv6 no **HuaweiClientes**.

```
ipv6
```

4. Agora vamos mudar o nome do roteador **HuaweiClientes**. Aplique o comando a seguir.

```
sysname HuaweiClientesXX
```

5. Mude a forma como o **HuaweiClientes** mostra o ASN.

```
as-notation plain

Warning: If the configuration takes effect, the regular expression of the filter for
4-byte AS path should be changed to the asplain format, otherwise match will fail.
Continue? [Y/N] Y
```

6. Configure os endereços IPv4 e IPv6 nas interfaces do roteador **HuaweiClientes**.

```
interface GigabitEthernet0/0/1
 ipv6 enable
 ip address 10.XX.0.2 255.255.255.252
 ipv6 address 4D0C:XX:0:1::2/126
 quit

interface GigabitEthernet0/0/2
 ipv6 enable
 ip address 10.XX.2.1 255.255.254.0
 ipv6 address 4D0C:XX:C00::1/40
 quit

interface GigabitEthernet0/0/3
 ipv6 enable
 ip address 10.XX.1.1 255.255.255.0
 ipv6 address 4D0C:XX:400::1/40
 quit
```

Exercício 1b - 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 1c - Aplicando as práticas de hardening

Objetivo: Aplicar configurações devidas para sanar 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 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
```

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

```
display tcp status

TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
-------- 51 /1    0.0.0.0:443           0.0.0.0:0             23553  Listening
```

4. Desabilite todos os serviços que não serão usados nesse roteador (alguns desses serviços já estarão desabilitados).

    a. Desabilite o servidor FTP, pois não usaremos transferência de arquivos.

```
undo ftp server
```

    b. Desabilite o acesso via HTTP e HTTPS.

```
undo http secure-server enable

Warning: The operation will stop HTTPS service. Continue? [Y/N]: Y
```

    c. Desabilite o protocolo DHCP.

```
undo dhcp enable

Warning: All DHCP functions will be disabled. Continue? [Y/N] Y
```

5. Desabilite as interfaces que não estão em uso.

```
interface GigabitEthernet0/0/0
 shutdown
 quit

interface GigabitEthernet0/0/4
 shutdown
 quit

interface GigabitEthernet0/0/5
 shutdown
 quit

interface GigabitEthernet0/0/6
 shutdown
 quit
```

6. Agora faça o mesmo para o **HuaweiBorda.**

```
display tcp status

------------------------------------------------------------------------------
Cid/SocketID         Local Addr:Port       Foreign Addr:Port     VPNID      State
------------------------------------------------------------------------------
------------         0.0.0.0:23            0.0.0.0:0             -----      LISTEN
------------------------------------------------------------------------------
```

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

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

```
undo telnet server enable

Warning: The operation will stop the Telnet server. Do you want to continue? [Y/N]: Y
```

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

```
undo ftp server enable
```

    c. Desabilite o acesso via HTTP e HTTPS.

```
undo http
```

d. Desabilite o protocolo LLDP que fica procurando roteadores na rede.

```
undo lldp enable

Warning: This command will delete the configurations of LLDP on all the ports. Continue?
[Y/N]: Y
```

e. Desabilite o protocolo DCN.

```
undo dcn

Warning: This operation will disable DCN function. Continue? [Y/N]: Y
```

8. Desabilite as interfaces que não estão em uso.

```
interface Ethernet1/0/0
 shutdown
 quit

interface Ethernet1/0/5
 shutdown
 quit

interface Ethernet1/0/6
 shutdown
 quit

interface Ethernet1/0/7
 shutdown
 quit

interface Ethernet1/0/8
 shutdown
 quit

interface Ethernet1/0/9
 shutdown
 quit
```

9. Aplique as configurações no roteador **HuaweiBorda**.

```
commit
```