Exercício 1d - 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.

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

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. 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 em: https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf)

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

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

```
/quit

MikroTik Login: admin
Password: SenhaAdmin
```

6. Finalizada a criação dos administradores, volte para **MikrotikClientes**, crie um grupo específico e liste as permissões desse grupo.

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

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

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

8. 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
```

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

```
#scp .ssh/id_rsa.pub admin@[4d0c:XX:0c00::1]:edu.pub

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
Warning: Permanently added '4d0c:XX:c00::1' (RSA) to the list of known
hosts.
admin@4d0c:XX:c00::1's password: SenhaAdmin
```

10. 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
```

11. Teste o acesso SSH IPv6 do **Cliente_Domestico** para o **MikrotikClientes**. Acesse o terminal **Termit** no **Cliente_Domestico** e use o comando a seguir.

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

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

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

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

```
/log print
```

13. O serviço de SSH tem como padrão a porta 22. Como vimos na experiência de Ataque de dicionário, o SSH é alvo de ataques de Força Bruta. É uma boa prática mudar essa porta padrão, essa medida é eficaz contra ataques simples de varreduras por portas padrão. No **MikrotikClientes,** altere a porta padrão do SSH, isso interrompe a maioria das tentativas de login feita pelos os Ataques de Força Bruta.

```
/ip service set ssh port=6022
```

14. Teste o acesso SSH IPv6 do **Cliente_Domestico** para o **MikrotikClientes**. Acesse o terminal **Termit** no **Cliente_Domestico** e use os comandos a seguir .

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

Você conseguiu acessar o **MikrotikClientes**?

15. Agora, tente novamente acessar o **MikrotikClientes,** mas desta vez utilize o parâmetro -p e porta 6022.

```
#ssh -6 -p 6022 edu@4d0c:XX:0c00::1
```

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

Você conseguiu acessar o **MikrotikClientes**?

16. Acesse o **Terminal Emulator** do equipamento **KaliLinux** e tente realizar um Ataque de Força Bruta com o Hydra ou Medusa no **MikrotikClientes**.

```
#hydra -L usuarios.txt -P senhas.txt -e nsr 4d0c:XX::1 ssh
```

O Ataque de Força Bruta foi bem sucedido?

17. Além de mudar a porta padrão do SSH, uma boa prática é restringir o uso do usuário padrão (admin) e utilizá-lo somente para *backup* e emergências. Restrinja o acesso ao usuário admin para que ele só possa ser usado a partir do IP do **Cliente_Domestico**.

    Antes de realizar essa alteração no **MikrotikClientes,** acesse o terminal **Termit** no **Cliente_Corporativo** e teste o acesso SSH IPv6 do **Cliente_Corporativo** para o **MikrotikClientes**. Use o usuário admin.

```
#ssh -6 -p 6022 admin@4d0c:XX:0400::1
```

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

Você conseguiu acessar o **MikrotikClientes**?

18. Volte ao terminal do **MikrotikClientes** e use o seguinte comando:

```
/user set admin address=4d0c:XX:0c00::100
```

19. Retorne para o terminal **Termit** no **Cliente_Corporativo** e teste o acesso SSH IPv6 do **Cliente_Corporativo** para o **MikrotikClientes** novamente.

```
#ssh -6 -p 6022 admin@4d0c:XX:0400::1
```

Você conseguiu acessar o **MikrotikClientes**?

20. Por último, podemos restringir o acesso ao roteador via SSH a um IP ou sub-rede específica. Restrinja o acesso ao **MikrotikClientes** via SSH (independente de qual usuário esteja sendo utilizado) para permitir somente acessos vindos da sub-rede 4d0c:XX:0c00::/40.

    Porém, antes de realizar essa alteração no **MikrotikClientes,** acesse o terminal **Termit** no **Cliente_Corporativo** e teste o acesso SSH IPv6 do **Cliente_Corporativo** para o **MikrotikClientes**. Use o usuário BackupAdmin.

```
#ssh -6 -p 6022 BackupAdmin@4d0c:XX:0400::1
```

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

Você conseguiu acessar o **MikrotikClientes**?

21. Agora, volte ao terminal do **MikrotikClientes** e use o seguinte comando:

```
/ip service set ssh address=4d0c:XX:0c00::/40
```

22. Retorne para o terminal **Termit** no **Cliente_Corporativo** e teste o acesso SSH IPv6 do **Cliente_Corporativo** para o **MikrotikClientes** novamente.

```
#ssh -6 -p 6022 BackupAdmin@4d0c:XX:0400::1
```

Você conseguiu acessar o **MikrotikClientes**?