Packet Tracer – Configurando SSH

Topologia

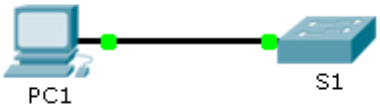

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

Parte 1: senhas seguras

Parte 2: criptografe as comunicações

Parte 3: Verificar a implementação SSH

Histórico

O SSH deve substituir o Telnet nas conexões de gerenciamento. O Telnet utiliza a comunicações em texto claro de forma não segura. O SSH fornece segurança nas conexões remotas, pois utiliza criptografia forte em todos os dados transmitidos entre dispositivos. Nesta atividade, você protegerá um switch remoto com criptografia por senha e SSH.

Parte 1: Proteger senhas

a. Usando o prompt de comando em **PC1**, execute Telnet para **S1**. A senha do EXEC do usuário e do EXEC privilegiado é **cisco**.

b. Salve a configuração atual de forma que todos os erros que você cometa possam ser revertidos ligando e desligando **S1**.

c. Exiba a configuração atual e observe que as senhas estão em texto claro. Digite o comando que criptografa senhas em texto claro.

```
S1(config)#service password-encryption
```

d. Verifique se as senhas estão criptografadas.

Parte 2: Criptografar comunicações

Etapa 1: Defina o nome de domínio IP e gere chaves de segurança.

Geralmente não é seguro usar o Telnet, pois os dados são transferidos em texto claro. Portanto, use SSH sempre que estiver disponível.

a. Configure o nome de domínio como **netacad.pka.**

```
S1(config)# ip domain-name netacad.pka
```

b. As chaves seguras são necessárias para criptografar os dados. Gere as chaves RSA usando um comprimento de chave de 1024.

```
S1(config)# crypto key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Etapa 2: Crie um usuário do SSH e reconfigure as linhas de VTY para somente acesso SSH.

a. Crie um usuário **administrator** com a senha **cisco**.

```
S1(config)# username administrator secret cisco
```

b. Configure as linhas VTY para verificar o banco de dados de nome de usuário local para ver se há credenciais de login e para permitir acesso remoto apenas para SSH. Remova a senha da linha vty existente.

```
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)# no password cisco
```

Parte 3: Verificar a implementação SSH

a. Saia da sessão Telnet e tente fazer logon em usar o Telnet. A tentativa deverá falhar.

b. Tente fazer login usando o SSH. Digite **ssh** e pressione **Enter** sem nenhum parâmetro para revelar as instruções de uso de comando. Dica: a opção `-l` é a letra “L”, não o número 1.

c. Após o login com êxito, entre no modo EXEC privilegiado e salve as configurações. Se você não conseguir acessar **S1**, desligue e ligue S1 e comece novamente na Parte 1.

