Packet Tracer – Configure o SSH (Versão do Instrutor)

**Nota do Instrutor**: Cor vermelha da fonte ou realces em cinza indicam o texto que aparece apenas na cópia do instrutor.

# 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: Proteger senhas

Parte 2: Criptografar 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 para conexões remotas, fornecendo criptografia forte de todos os dados transmitidos entre os dispositivos. Nesta atividade, você protegerá um switch remoto com criptografia de senha e SSH.

# Instruções

## Proteger senhas

* + - 1. Usando o prompt de comando em **PC1**, execute Telnet para **S1**. A senha do EXEC do usuário e do EXEC privilegiado é **cisco**.
      2. Salve a configuração atual de forma que todos os erros que você cometa possam ser revertidos ligando e desligando **S1**.
      3. Exiba a configuração atual e observe que as senhas estão em texto claro. Digite o comando que criptografa senhas em texto simples:

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

* + - 1. Verifique se as senhas estão criptografadas.

## Criptografar comunicações

### 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.

* + - 1. Configure o nome de domínio como **netacad.pka.**

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

* + - 1. 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]

### Crie um usuário do SSH e reconfigure as linhas de VTY para somente acesso SSH.

* + - 1. Crie um usuário **administrator** com a senha **cisco**.

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

* + - 1. 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 vty 0 15**

S1(config-line)# **login local**

S1(config-line)#**transport input ssh**

S1(config-line)# **no password cisco**

### Verificar a implementação SSH

* + - 1. Saia da sessão Telnet e tente fazer logon em usar o Telnet. A tentativa deverá falhar.
      2. 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: > **ssh -l administrador 10.10.10.2**

* + - 1. 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.

Fim do documento