Packet Tracer - Configuring SSH

Topography

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>10.10.10.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC1</td>
<td>NIC</td>
<td>10.10.10.10</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Objectives

Part 1: Secure Passwords
Part 2: Encrypt Communications
Part 3: Verify SSH Implementation

Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

Part 1: Secure Passwords

a. Using the command prompt on PC1, Telnet to S1. The user EXEC and privileged EXEC password is cisco.

Packet Tracer PC Command Line 1.0
PC>telnet 10.10.10.2
Trying 10.10.10.2 ...Open
User Access Verification

Password: (Not displayed)
S1>en
Password: (Not displayed)

S1#

b. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for S1.
**Packet Tracer - Configuring SSH**

```
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

c. Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords.

```
line vty 0 4
password cisco
login
line vty 5 15
password cisco
```

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service password-encrypt
```

d. Verify that the passwords are encrypted.

```
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
```

**Encrypt Communications**

**Set the IP domain name and generate secure keys.**

It is generally not safe to use Telnet, because data is transferred in plain text. Therefore, use SSH whenever it is available.

a. Configure the domain name to be `netacad.pka`.

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

b. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.
Packet Tracer - Configuring SSH

S1(config)#crypt 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]

Create an SSH user and reconfigure the VTY lines for SSH-only access.

a. Create an administrator user with cisco as the secret password.
   
   S1(config)#username administrator secret cisco
   
   *Mar 1 0:47:28.687: %SSH-5-ENABLED: SSH 1.99 has been enabled
   
   S1(config)#

b. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.
   
   S1(config)#line vty 0 15
   S1(config-line)#login local
   S1(config-line)#transport input ssh
   S1(config-line)#no password cisco

Verify SSH Implementation

a. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.
   
   PC>telnet 10.10.10.2
   Trying 10.10.10.2 ...Open
   
   [Connection to 10.10.10.2 closed by foreign host]

b. Attempt to log in using SSH. Type ssh and press Enter without any parameters to reveal the command usage instructions. Hint: The –l option is the letter “L”, not the number 1.
   
   PC>ssh -l administrator 10.10.10.2
   Open
   Password: (Not displayed)
   
   S1>en
   Password: (Not displayed)

c. Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access S1, toggle the power and begin again at Part 1.
   
   PC>ssh -l administrator 10.10.10.2
   Open
   Password:
S1>en
Password:
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#