

Packet Tracer - Configure SSH

Name: Danica Marie A. Dumalagan

Date: February 4, 2023

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

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.

Instructions

Part 1: Secure Passwords

- Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.
- Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.
- Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords:

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

- Verify that the passwords are encrypted.

Part 2: Encrypt Communications

Step 1: 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.

- Configure the domain name to be **netacad.pka**.
- Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

Step 2: Create an SSH user and reconfigure the VTY lines for SSH-only access.

- Create an **administrator** user with **cisco** as the secret password.

Packet Tracer - Configure SSH

- 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.

Step 3: Verify SSH Implementation

- a. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.
- b. Attempt to log in using SSH. Type **ssh** and press **Enter** without any parameters to reveal the command usage instructions. **Hint:** The **-1** option is the letter "L", not the number 1.
- 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.

Part 3: Post your screenshots

On the PT Activity window, make sure that the completion grade is **100%**. Click on the **Check Results** button and select the **Assessment Items** tab. Take a screen shot of the whole window, showing the table of assessment items, and the score/item count. Own your photo by placing a watermark on your photo with your name and USC ID Number. Paste your screenshot below:

The screenshot shows the Cisco Packet Tracer Activity Results window for the task "Configure SSH.pka". The "Assessment Items" tab is selected, displaying a table of assessment items for device S1. The table lists various configuration items, their status (Correct), points awarded, and the component they belong to. A summary on the right shows a total score of 100/100 and 7/7 items completed. A watermark is overlaid on the screenshot.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
S1				
DNS				
IP Domain Name	Correct	0	Other	
Modulus Bits	Correct	20	Device Hardening ...	
Service Password Encryption	Correct	0	Other	
Username	Correct	20	Device Hardening ...	
VTY Lines				
Login	Correct	7	Device Hardening ...	
Password	Correct	6	Device Hardening ...	
Transport Input	Correct	7	Device Hardening ...	

Score: 100/100
Item Count: 7/7

Component: Device Hardening Configuration
Items/Total: 7/7
Score: 100/100

Danica Marie A. Dumalagan
18103276