Packet Tracer - Configuring SSH

Topology
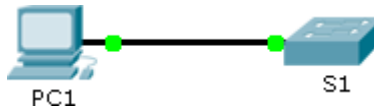
Addressing Table

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.

Part 1: Secure Passwords

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

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

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

d. 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.

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

b. 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.

a.   Create an **administrator** user with **cisco** as the password.

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.

Part 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.

IT pishro