**Net 1061 Switching, Routing, and Wireless Essentials**

**Name: Andrew Koenig**

**Lab: # 2?**

**Follow the instructions down below for the lab itself. For this lab, all answers need to be in blue font. For the questions right below, answer in complete sentences. If this is a self-grading packet tracer. Ensure you paste the screen shot of your score page at the bottom of the document. You will upload both this document and the pkt file regardless if it is self-grading or not. Let the instructor know if you have any questions.**

***Lab Analysis Report***

1. Using complete sentences summarize work you completed during the lab.

I used telnet to connect to a switch and configure ssh on it

2. Using complete sentences describe what you learned from the lab. Hint; look at the lab objectives listed at the top of the lab section.

I learned further how to remote into a switch and configure it

***Problems Encountered***

1. Using complete sentences describe any problem(s) experienced during lab.

No problems

2. Using complete sentences describe how you solved your problem(s).

No problems

3. Using complete sentences explain if you needed any assistance with the lab; then list what you learned from that assistance. No problems

Packet Tracer - Configure SSH

# 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

## Secure Passwords

* + - 1. Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.
      2. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.
      3. 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**

* + - 1. Verify that the passwords are encrypted.

## 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.

* + - 1. Configure the domain name to be **netacad.pka**.
      2. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

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

* + - 1. Create an **administrator** user with **cisco** as the secret password.
      2. 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.

### Verify SSH Implementation

* + - 1. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.
      2. 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.
      3. 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.

End of document

Graphical user interface, application

Description automatically generated