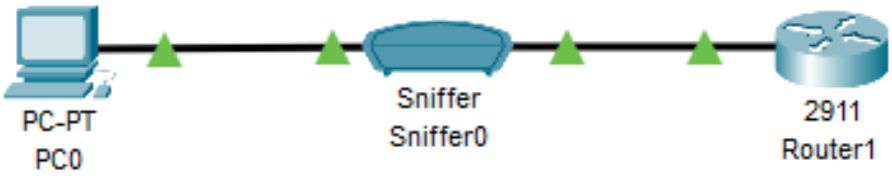
Packet Tracer – Configure Basic Security Settings



Addressing Table

Device	Interface	IP Address	Subnet Mask
Router1	Gi0/0	10.10.10.2	255.255.255.0
PC0	NIC	10.10.10.10	255.255.255.0

Objectives

Part 1: Configure basic settings

Part 2: Secure Passwords

Part 3: Encrypt Communications

Part 4: Verify SSH Implementation

Part 5: Additional Password Security

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: Configure basic settings

a. Configure device name as shown in the topology.

b. Configure IP address as listed in Addressing Table.

c. Assign **cisco** as the console and vty passwords.

d. Assign **class** as the privileged EXEC password.

Part 2: Secure Passwords

a. Using the command prompt on **PC0**, Telnet to **Router1**.

b. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **Router1**.

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

```
Router1(config)# service password-encryption
```

d. Verify that the passwords are encrypted.

Q1: Are cisco "password 7" passwords secure?

Try using the tool form the following link: https://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/358-cisco-type7-password-crack.html

Q2: Is the Telnet protocol secure?

Try using the Sniffer0 to capture telnet packets. What can be seen in the application data?

Part 3: 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 **lab10.ismai.pt**.

```
Router1(config)# ip domain-name lab10.ismai.pt
```

b. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

```
Router1 (config)# crypto key generate rsa
The name for the keys will be: Router1.lab10.ismai.pt
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]
```

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

a. Create an **admin** user with **cisco** as the secret password.

```
Router1 (config)# username admin secret cisco
```

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.

```
Router1 (config)# line vty 0 15
Router1 (config-line)# login local
Router1 (config-line)# transport input ssh
```

```
Router1 (config-line)# no password cisco
```

Part 4: 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 **-l** option is the letter “L”, not the number 1.

```
C:\> ssh -l admin 10.10.10.2
```

c. Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access **Router1**, toggle the power and begin again at Part 1.

Q3: Is the SSH protocol secure?

Try using Sniffer0 to prove it?

Part 5: Additional Password Security

a. Explore the concepts of the **security passwords min-length** and **login block-for # attempts # within #** commands.

b. What does the **exec-timeout** command do?