Faculté des Sciences et de la Technologie
Master en Réseaux et Télécommunication
TP administration des services réseaux

Lab4 : SSH service using Cisco Packet Tracer

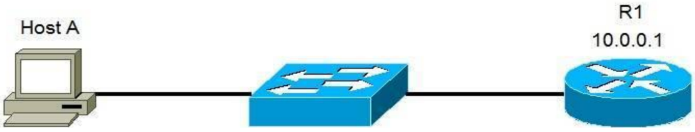
1 Background

SSH is a network protocol used to remotely access and manage a device. The key difference between Telnet and SSH is that SSH uses encryption, which means that all data transmitted over a network is secure from eavesdropping.

SSH relies on public key cryptography for its encryption and uses TCP port 22.

*In the following example, t*he network administrator wants to use his computer (*Host A*) to access and manage the router with the IP address of

10.0.0.1:



The administrator will start an SSH client program on Host A and run the following CMD commad:

```
C:\> ssh -l [username] 10.0.0.1
```

Where ***user*** is a pre-configured local user in the router. Alternatively, He could use a GUI SSH client (***Putty*** for example) to access and manage the router. On a Linux machine, the command will be : **`ssh username@10.0.0.1`**

To enable SSH on a a Cisco device, the following steps are required:

1) Set up a hostname and and a domain name,

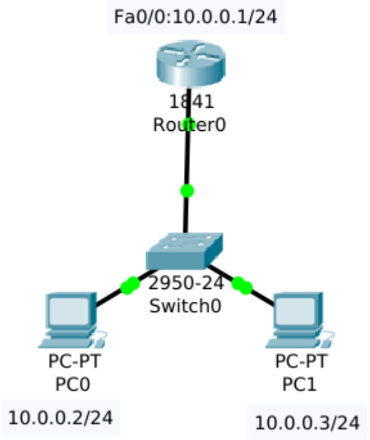
2) Configure local username and password,

3) Generate RSA public and private keys,

4) Enable SSH access to the device.

2 SSH Lab

Let’s construct this simple topology:



Steps:

- **Set up a hostname and and a domain name:**

```
Router(config)# hostname R1

R1(config)# ip domain-name cisco
```

- **Configure local username and password:**

```
R1(config)# username master password djelfa123
```

- **Generate RSA public and private keys:**

```
R1(config)# crypto key generate rsa
```

- **`Enable SSH access to the router:**

```
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
```

Notes:- The telnet access to the device is automatically disabled in this case. If we use instead the "***transport input ssh all***" command, the telnet access to the device will be also enabled.

- We could use the more recent version of the protocol, SSH version 2. This is done by using the "***ip ssh version 2***" global configuration command.

- The commands **"ip ssh authentication-retries x"** and "**ip ssh time-out x x** " Specify respectively the number of authentication retries, (default=3) nad SSH login time-out interval, (default=120s).

- To display the fingerprint of an RSA key in IOS, we use ***"show crypto key mypubkey rsa"*** command.

Now, go to PC0, then to PC1 and run the command:

```
C:\>ssh -l master 10.0.0.1
```

To display who is currently connected to the router via ssh (or telnet) and how long they have been connected for, run:

```
R1#show users
```

Finally, modify the authentication-retries number to 1, and the time-out to 10s, and try to see the effect of this modification.

<u>Homework</u>:

1- Repeat the same topology of this Lab, and enable Telnet and SSH on the router. Using PDU information in the simulation mode of packet Tracer, try to figure out (Add figures from PT to your report for justification):

- The ports used by telnet and SSH,

- The source and the destination IP addresses in both cases,

- The SSH and the telnet data in the authentication phase (when entering password for ssh or telnet), and when issuing commands like "***conf t***".

2- Add a sniffer device to the topology and try to figure out the same information like above.