16.4.6 Packet Tracer - Configure Secure Passwords and SSH (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	172.16.1.1	255.255.255.0	N/A
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Scenario

The network administrator has asked you to prepare **RTA** and **SW1** for deployment. Before they can be connected to the network, security measures must be enabled.

Intructions

Step 1: Configure Basic Security on the Router

a. Configure IP addressing on **PCA** according to the Addressing Table.

b. Console into RTA from the Terminal on PCA.

c. Configure the hostname as **RTA**.

d. Configure IP addressing on **RTA** and enable the interface.

e. Encrypt all plaintext passwords.

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

f. Set the minimum password length to 10.

```
RTA(config)# security password min-length 10
```

g. Set a strong secret password of your choosing. **Note**: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

h. Disable DNS lookup.

```
RTA(config)# no ip domain-lookup
```

i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

```
RTA(config)# ip domain-name CCNA.com
```

j. Create a user of your choosing with a strong encrypted password.

```
RTA(config)# username any_user secret any_password
```

k. Generate 1024-bit RSA keys.

Note: In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue.

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

```
The name for the keys will be: RTA.CCNA.com
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
```

l. Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

m. Configure all VTY lines for SSH access and use the local user profiles for authentication.

```
RTA(config)# line vty 0 4
RTA(config-line)# transport input ssh
RTA(config-line)# login local
```

n. Set the EXEC mode timeout to 6 minutes on the VTY lines.

```
RTA(config-line)# exec-timeout 6
```

o. Save the configuration to NVRAM.

p. Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA**.

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

Step 2: Configure Basic Security on the Switch

Configure switch **SW1** with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

a. Click on **SW1** and select the **CLI** tab.

b. Configure the hostname as **SW1**.

c. Configure IP addressing on SW1 **VLAN1** and enable the interface.

d. Configure the default gateway address.

e. Disable all unused switch ports.

Note: On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the '**shutdown**' command. This would require accessing each port individually. There is a shortcut method for making modifications to several ports at once by using the **interface range** command. On **SW1** all ports except FastEthernet0/1 and GigabitEthernet0/1 can be shutdown with the following command:

```
SW1(config)# interface range F0/2-24, G0/2
SW1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

The command used the port range of 2-24 for the FastEthernet ports and then a single port range of GigabitEthernet0/2.

f. Encrypt all plaintext passwords.

g. Set a strong secret password of your choosing.

h. Disable DNS lookup.

i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

j. Create a user of your choosing with a strong encrypted password.

k. Generate 1024-bit RSA keys.

l. Configure all VTY lines for SSH access and use the local user profiles for authentication.

m. Set the EXEC mode timeout to 6 minutes on all VTY lines.

n. Save the configuration to NVRAM.