**Net 3068 CCNA Security Name: Andrew Koenig Lab: # 4.4.8**

**Follow the instructions down below for the lab itself. Anything you type on this document needs to be in blue font. Ensure you put your name and lab number at the top of the document (in blue). 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 this document. Ensure you upload the packet tracer file along with this document. Let the instructor know if you have any questions.**

***Lab Analysis Report***

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

I configured addressing and basic security on a few devices

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 solidified my knowledge of basic device security

***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 Secure Passwords and SSH

# Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| --- | --- | --- | --- | --- |
| RTA | G0/0/0 | 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 |

Blank Line, No additional information

# 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

## Configure Basic Security on the Router

* + - 1. Configure IP addressing on **PCA** according to the Addressing Table.
      2. Console into **RTA** from the Terminal on PCA.
      3. Configure the hostname as **RTA**.
      4. Configure IP addressing on **RTA** and enable the interface.
      5. Encrypt all plaintext passwords.

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

* + - 1. Set the minimum password length to 10.

RTA(config)# **security passwords min-length 10**

* + - 1. 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.

* + - 1. Disable DNS lookup.

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

* + - 1. Set the domain name to **netsec.com** (case-sensitive for scoring in PT).

RTA(config)# **ip domain-name netsec.com**

* + - 1. Create a user of your choosing with a strong encrypted password.

RTA(config)# **username *any\_user* secret *any\_password***

* + - 1. 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.netsec.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**

* + - 1. 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**

* + - 1. 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**

* + - 1. Set the EXEC mode timeout to 6 minutes on the VTY lines.

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

* + - 1. Save the configuration to NVRAM.
      2. 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:\>

## 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.

* + - 1. Console into **SW1** from the Terminal on PCA.
      2. Configure the hostname as **SW1**.
      3. Configure IP addressing on SW1 **VLAN1** and enable the interface.
      4. Configure the default gateway address.
      5. 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.

* + - 1. Encrypt all plaintext passwords.
      2. Set a strong secret password of your choosing.
      3. Disable DNS lookup.
      4. Set the domain name to **netsec.com** (case-sensitive for scoring in PT).
      5. Create a user of your choosing with a strong encrypted password.
      6. Generate 1024-bit RSA keys.
      7. Configure all VTY lines for SSH access and use the local user profiles for authentication.
      8. Set the EXEC mode timeout to 6 minutes on all VTY lines.
      9. Save the configuration to NVRAM.

### A screenshot of a computer Description automatically generated

End of document