NAME: GOKUL NATH S
EMAIL ID: 12345.gokulnath.s@gmail.com

Packet Tracer - Secure Network Devices

Addressing Table

Device	Interface	Address	Mask	Gateway
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.2.1	255.255.255.0	N/A
SW-1	SVI	192.168.1.254	255.255.255.0	192.168.1.1
PC	NIC	192.168.1.2	255.255.255.0	192.168.1.1
Laptop	NIC	192.168.1.10	255.255.255.0	192.168.1.1
Remote PC	NIC	192.168.2.10	255.255.255.0	192.168.2.1

Requirements

Note: To keep this activity brief and easy to manage, some security configuration settings have not been made. In other cases, security best practices have not been followed.

In this activity you will configure a router and a switch based on a list of requirements.

Instructions

Step 1: Document the Network

Complete the addressing table with the missing information.

Step 2: Router configuration requirements:

- Prevent IOS from attempting to resolve mistyped commands to domain names.
- Hostnames that match the values in the addressing table.

```
Router (config) #hostname RTR-A
```

- Require that newly created passwords be at least 10 characters in length.

```
RTR-A (config)#security passwords min-length 10
```

- A strong ten-character password for the console line. Use **@Cons1234!**

```
RTR-A(config)#line console 0
RTR-A(config-line)#password @Cons1234!
RTR-A(config-line)#login
```

- Ensure that console and VTY sessions close after 7 minutes exactly.

```
//RTR-A(config)#line console 0
RTR-A(config-line)#exec-timeout 7 0
RTR-A(config-line)#line vty 0 4
RTR-A(config-line)#exec-timeout 7 0
```

- A strong, encrypted ten-character password for the privileged EXEC mode. For this activity, it is permissible to use the same password as the console line.

  ```
  RTR-A(config)#enable secret @Cons1234!
  ```

- A MOTD banner that warns about unauthorized access to the devices.

  ```
  RTR-A(config)#banner motd  #Unauthorized access prohibited.#
  ```

- Password encryption for all passwords.

  ```
  RTR-A(config)#service password-encryption
  ```

- A user name of **NETadmin** with encrypted password **LogAdmin!9**.

  ```
  RTR-A(config)#username NETadmin secret LogAdmin!9
  ```

- Enable SSH.
  - Use **security.com** as the domain name.
  - Use a modulus of **1024**.

  ```
  RTR-A(config)#no ip domain-lookup
  RTR-A(config)#ip domain-name security.com
  RTR-A(config-line)#crypto key generate rsa
  The name for the keys will be: RTR-A.security.com
  Choose the size of the key modulus in the range of 360 to 4096 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
  ```

- The VTY lines should use SSH for incoming connections.

  ```
  RTR-A(config-line)#line vty 0 4
  RTR-A(config-line)#transport input ssh
  ```

- The VTY lines should use the username and password that were configured to authenticate logins.

```
RTR-A(config-line)#line vty 0 4
RTR-A(config-line)#login local
```

- Impede brute force login attempts by using a command that blocks login attempts for 45 seconds if someone fails three attempts within 100 seconds.

```
RTR-A(config)#login block-for 45 attempts 3 within 100
```

Step 3: Switch configuration requirements:

```
Switch(config)#hostname SW-1
```

- All unused switch ports are administratively down.

```
SW-1(config)#interface range fastEthernet0/1, fastEthernet0/3-9, fastEthernet0/11-24, GigabitEthernet0/2
SW-1(config-if-range)#shutdown
```

- The SW-1 default management interface should accept connections over the network. Use the information shown in the addressing table. The switch should be reachable from remote networks.

```
SW-1(config-if-range)#interface Vlan1
SW-1(config-if)#ip address 192.168.1.254 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#ip default-gateway 192.168.1.1
```

- Use **@Cons1234!** as the password for the privileged EXEC mode.

```
SW-1(config)#enable secret @Cons1234!
```

- Configure SSH as was done for the router.

```
SW-1(config)#ip domain-name security.com
SW-1(config-line)#crypto key generate rsa
The name for the keys will be: SW-1.security.com
Choose the size of the key modulus in the range of 360 to 4096 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]
```

- Create a user name of **NETadmin** with encrypted secret password **LogAdmin!9**

```
SW-1(config)#username NETadmin secret LogAdmin!9
```

- The VTY lines should only accept connections over SSH.

```
SW-1(config)#line vty 0 4
SW-1(config-line)#transport input ssh
```

- The VTY lines should only allow the network administrator account to access the switch management interface.

```
SW-1(config)#line vty 0 4
SW-1(config-line)#login local
```

- Hosts on both LANs should be able to ping the switch management interface.

RTR-A

```
enable

conf t

service password-encryption

security passwords min-length 10

hostname RTR-A

login block-for 45 attempts 3 within 100

enable secret @Cons1234!

username NETadmin secret LogAdmin!9

no ip domain-lookup

ip domain-name security.com

banner motd #Unauthorized access prohibited.#

line con 0

exec-timeout 7 0

password @Cons1234!

login

line vty 0 4

exec-timeout 7 0

login local

transport input ssh

line vty 5 15

no login

crypto key generate rsa

1024

End
```

SW-1

```
enable

conf t

hostname SW-1

ip domain-name security.com

enable secret @Cons1234!

username NETadmin secret LogAdmin!9

interface range fastEthernet0/1, fastEthernet0/3-9, fastEthernet0/11-24,
      GigabitEthernet0/2

shutdown

interface Vlan1
```

```
ip address 192.168.1.254 255.255.255.0
no shutdown
ip default-gateway 192.168.1.1
line vty 0 4
login local
transport input ssh
crypto key generate rsa
1024
end
```