16.5.1 Packet Tracer - Secure Network Devices (Instructor Version)

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

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.
- Require that newly created passwords be at least 10 characters in length.
- A strong ten-character password for the console line. Use **@Cons1234!**
- Ensure that console and VTY sessions close after 7 minutes exactly.
- 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.
- A MOTD banner that warns about unauthorized access to the devices.
- Password encryption for all passwords.
- A user name of **NETadmin** with encrypted password **LogAdmin!9**.
- Enable SSH.
  - Use **security.com** as the domain name.
  - Use a modulus of **1024**.

- The VTY lines should use SSH for incoming connections.
- The VTY lines should use the username and password that were configured to authenticate logins.
- Impede brute force login attempts by using a command that blocks login attempts for 45 seconds if someone fails three attempts within 100 seconds.

Step 3: Switch configuration requirements:

- All unused switch ports are administratively down.
- 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.
- Use **@Cons1234!** as the password for the privileged EXEC mode.
- Configure SSH as was done for the router.
- Create a user name of **NETadmin** with encrypted secret password **LogAdmin!9**
- The VTY lines should only accept connections over SSH.
- The VTY lines should only allow the network administrator account to access the switch management interface.
- Hosts on both LANs should be able to ping the switch management interface.

Answer Scripts

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 ^C
Unauthorized access prohibited. ^C
line con 0
 exec-timeout 7 0
 password @Cons1234!
 login
line aux 0
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
```