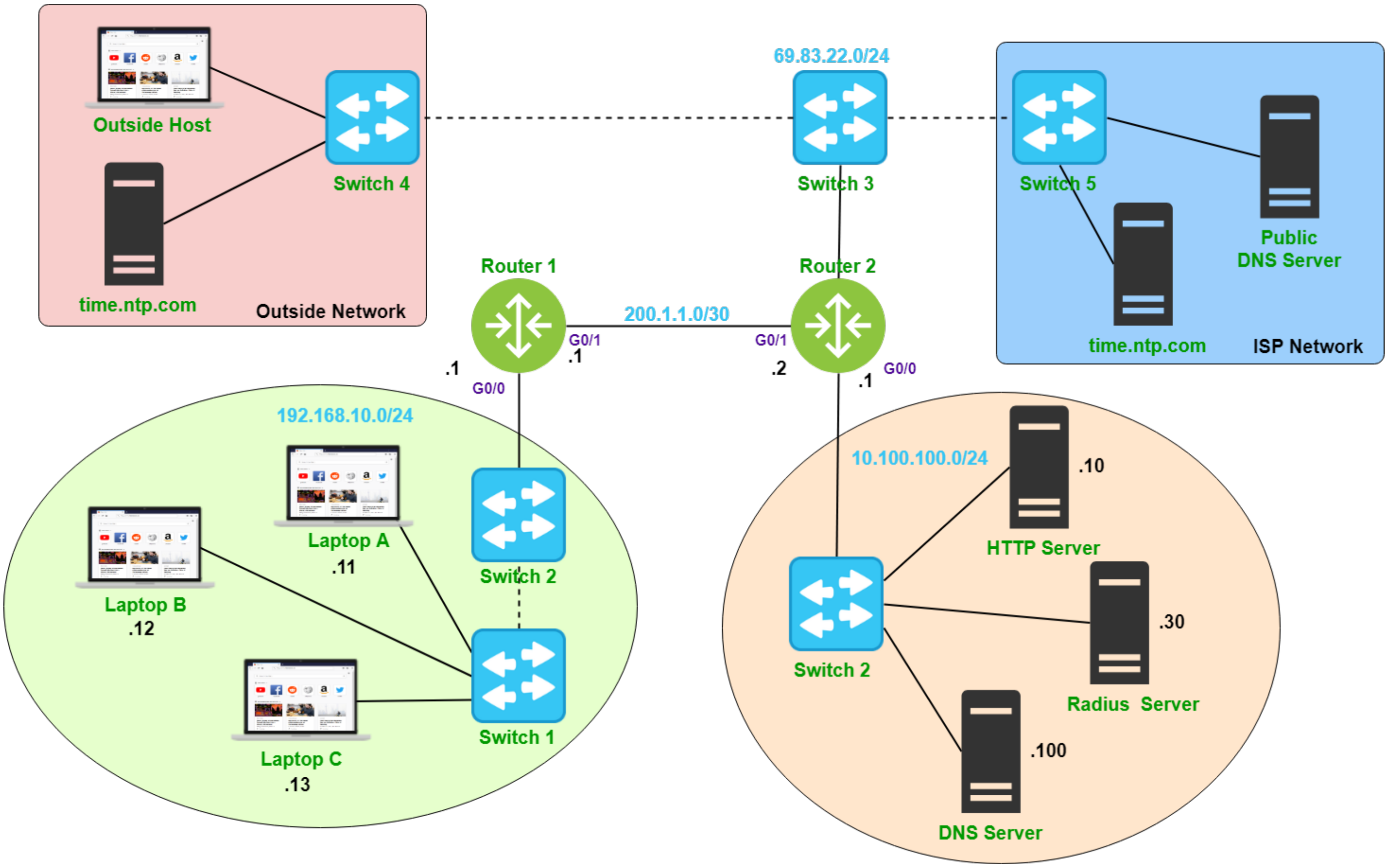
Lab 6 – Secure Administration & SNMP

Lab Topology and Learning Goals



Network device configurations often leave the network at risk of attack. If a network infrastructure device is compromised, it is possible that the traffic it processes could be monitored or altered. In this lab, we explore the configurations required to improve the methods used to access infrastructure devices by network administrators.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 6 – Secure Administration & SNMP.pkz**
- Take Lab Quiz: **Lab 6 - Requires Respondus LockDown Browser**

Improve Basic Security Settings

Passwords are the most common form of user authentication. In production environments, passwords protect network devices from unauthorized access. With this in mind, we should configure devices with strong passwords and make sure that the password hash cannot be easily cracked.

Restricting Device Access with Passwords

Configure the enable password:

```
Router1(config)# enable password cisco
```

Configure access passwords on the console and vty lines:

```
Router1(config)# line console 0
Router1(config-line)# logging synchronous
Router1(config-line)# password class
Router1(config-line)# login
Router1(config-line)# exit
```

```
Router1(config)# line vty 0 4
Router1(config-line)# logging synchronous
Router1(config-line)# password class
Router1(config-line)# login
Router1(config-line)# transport input all
Router1(config-line)# exit
```

Telnet from the laptop to Router1 and login
View the results of the password configuration:

```
Router1# show run | include password
```

Notice that all of the configured passwords are stored in plain text.

Modify the Minimum Password Length

Require passwords to be a minimum length of 8 characters:

```
Router1(config)# security passwords min-length 8
```

Improving Password Security with Encryption

Configure an encrypted enable password:

```
Router1(config)# enable secret Cisco6078
```

Encrypt passwords stored in clear text:

```
Router1(config)# service password-encryption
```

View the results of the password configuration:

```
Router1# show run | include (password|secret)
```

Notice that all of the configured passwords are now hashed; however, not all hashing algorithms are the same.

Cisco IOS can use the following hashing methods to encrypt the enable secret password:

Level	Algorithm
4	SHA-256
5	MD5
8	Password-Based Key Derivation Function 2 (PBKDF2)
9	Scrypt

Copy the hash for the **enable password** and test it against the database located at:
http://www.ifm.net.nz/cookbooks/passwordcracker.html

Copy the hash for the **enable secret** and test it against the database located at:
https://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html

Most current Cisco devices will support Scrypt encrypted passwords. Packet Tracer does not currently support this level of encryption.

Prompt Users with Legal Notices

When logging into devices it is common to find a warning message designed to deter unauthorized users from attempting to login. While it is easy to bypass the warning, any user that logs in has entered into a legal contract based on the displayed terms. If the user was not authorized to access the system, they have violated your policies, and you may be able to take legal action against them.

The three main banners used on Cisco devices:

login	This banner is displayed before the user logs into the device
motd (Message of the Day)	This banner is displayed after the user logs in
exec	This banner is displayed when the user enters privileged exec mode

Configure the login banner

```
Router1(config)# banner login $
```

Enter the following banner when prompted:

WARNING: This system is monitored, and all actions will be recorded. Unauthorized or improper use of this system may result in civil charges or criminal penalties. By continuing to use this system you indicate your consent to these terms and conditions.

$

View the results of the newly configured banner:

```
Router1# show run | begin banner
```

Improving Logon Security with Usernames

Requiring users to login with both a username and password can help protect a device from automated password cracking attacks. When an attacker must guess both the username and password, it will take exponentially longer to get access to the system.

Create a User account with an Encrypted Password

```
Router1(config)# username localadmin privilege 15 secret Cisco123
```

The privilege 15 option configures the user to a privilege level equivalent to enable secret (the maximum default level).

Configure the Remote Access Lines to Use the Local Database

```
Router1(config)# line console 0
Router1(config-line)# login local
Router1(config)# line vty 0 4
Router1(config-line)# login local
```

From the **Laptop A**, open a telnet session to **Router1** (**192.168.10.1**). What has changed about the login process?

Expire Inactive Sessions

If an attacker can access a device when the administrator walks away from his desk without locking their workstation, the attacker does not need to crack any password and may have the privileges to create an account to access the device at a later time.

Configure the Virtual Terminal Line to Expire Inactive Sessions

```
Router1(config)# line vty 0 4
Router1(config-line)# exec-timeout 5 0
```

Inactive sessions will logout after 5 minutes and 0 seconds. **It is important to allow a session enough time to make configuration changes to the executive timeout.**

Encrypted Remote Management Sessions

Secure Shell (SSH) is a remote management protocol similar to telnet; however, SSH encrypts all traffic related to the terminal session. SSH is the only protocol that should be used to access a remote terminal on production devices. SSH requires some additional configuration as compared to telnet.

Configure SSH for Remote Terminal Sessions

Configure a domain name:

```
Router1(config)# ip domain-name fanshawe.ca
```

Modify the vty lines to allow login only by SSH:

```
Router1(config)# line vty 0 4
Router1(config-line)# transport input ssh
Router1(config-line)# exit
```

Erase any existing key pairs on the router:

```
Router1(config)# crypto key zeroize rsa
```

If no keys exist, you will receive this message: **% No Signature RSA Keys found in configuration.**

Generate a new RSA key pair:

```
Router1(config)# crypto key generate rsa modulus 2048
```

NOTE: Depending on the device and IOS version, the command **crypto key generate rsa modulus 2048** may fail. The supplementary command is **crypto key generate rsa**, and you will be prompted for the modulus size. The recommended minimum modulus size is currently **2048**.

Enable SSH version 2:

```
Router1(config)# ip ssh version 2
```

Harden Login security

It is inevitable that an attacker will try to gain access to your system at some point. One of the goals of device hardening is to delay the access attempt so that monitoring software and administrators have enough time to react to the access attempt.

View Default Login Settings

```
Router1# show login
```

Configure Router1 to Output Logging Messages Related to Logon to the Console

```
Router1(config)# login on-failure log
Router1(config)# login on-success log
```

Configure a Login Block

Configure the router to block login attempts for 60 seconds after 2 failed attempts within 30 seconds:

```
Router1(config)# login block-for 60 attempts 2 within 30
```

Trigger the login block by making three failed login attempts within 30 seconds.

Harden SSH Settings Related to Login

```
Router1(config)#  ip ssh time-out 60
Router1(config)#  ip ssh authentication-retries 2
```

Configure Centralized Management of Users

Remote Authentication in Dial-In User Service (RADIUS) is the open standard authentication protocols implemented on most networks. RADIUS allows centralized user management for all configured network devices. This often includes integration with a directory service such as Microsoft's Active Directory. Users logging into a network device do so with their regular domain credentials.

Configure the RADIUS Server for Remote Authentication

On the **Radius Server**, open the **Services** tab and switch to the **AAA** item.
Create a new Network Configuration with the following settings:

Radius Port	1812		
Client Name	Router1	**Client Name**	Router2
Client IP	200.1.1.1	**Client IP**	192.168.20.1
Secret	Cisco123	**Secret**	Cisco123
ServerType	Radius	**ServerType**	Radius

Create a user **admin** with the password **Cisco6078** that will authenticate via RADIUS

Configure RADIUS Authentication on Router1

```
Router1(config)# radius-server host 192.168.20.30 auth-port 1812
Router1(config)# radius-server key Cisco123
```

Current IOS devices support the newer **radius server** command. Both the **radius-server host** and **radius-server key** commands have been depreciated; however, Packet Tracer does not support the new syntax.

Configure logon requests to authenticate using the RADIUS server

```
Router1(config)# aaa new-model
Router1(config)# aaa authentication login default group radius local enable
```

It is important to have a local administrator created on the router in the event that the RADIUS server is unavailable. In this case the **localadmin** user created previously can serve as the backup user. The **login** and **enable** parameters at the end of the command specifies that the local user database will be used for authentication if the RADIUS server is unavailable, and the enable secret or password should the local database fail.

Set authentication on the vty lines and console to use the configured RADIUS authentication method

```
Router1(config)# line vty 0 4
Router1(config-line)# login authentication default
```

```
Router1(config)# line console 0
Router1(config-line)# login authentication default
```

Configure RADIUS Authentication on Router2

Configure **Router2** with the appropriate settings to authenticate via the RADIUS server. Don't forget to create a backup user.

Test Radius Authentication

On **Laptop B**, ssh to **Router1** (**192.168.10.1**)
Login with the username **admin** and the password **Cisco6078**

Close the session and login to **Router2** (**200.1.1.2**)

Close the session to **Router2**
Try to login to **Router1** with the backup user **localadmin**; is the login successful?

Without changing the RADIUS configuration, what actions would be required to allow you to login with the locally created user?

Configure Simple Network Management Protocol (SNMP)

SNMP enables administrators to remotely monitor and configure network devices. Packet Tracer does not support much of the SNMP protocol such as SNMP traps, but we can do some GET and SET commands.

Enable SNMP on Router1

View the available options, then configure SNMP in read/write mode

```
Router1(config)# snmp-server community SNMP ?
Router1(config)# snmp-server community SNMP rw
```

Connect to Router1 from Laptop C

On **Laptop C**, open the **MIB Browser** and click the **Advanced** button to configure settings
Configure the MIB Browser with the following settings:

Address	192.168.10.1
Port	161
Read Community	SNMP
Write Community	SNMP
SNMP Version	v3

Expand the SNMP MIB tree, browse the available OIDs.
Can you tell how long the system has been up?
Can you identify the interface names and their status?

Locate the OID that relates to the hostname, change the value of the hostname to **Router10** using the set command.