Assignment 11

Configuring Security and Access-Lists on Cisco Devices and Simulating Infrastructure Attacks

Siddhartha Pandey (s316620)

November 11, 2016

Contents

Part I
Introduction

The purpose of this assignment is to learn how to secure Cisco devices and how to configure an access list on the routers, which is basically a firewall. To complete the assignment you need to have Cisco Packet Tracer installed on your system.

Part II
Methods and Materials

1 Creating the topology

1.1 Deploying the routers and the switch

We use the 1841 model when deploying the router and the model 2960-24TT for the switch. We deploy both the routers and the switch in Packet Tracer.

1.2 Configuring Passwords

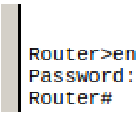
After deploying the router and the switch, we start configuration for the router. We use the **enable** command to enter the privileged EXEC mode, then the **configure terminal** command to enter the configuration mode. We add security to the router by configuring a password. We use the command **enable secret <*your password*>** to enable the password, where *your password* is replaced with the actual password. There is two ways to configure the password to access the router's priveleged EXEC mode. We can either use the **enable secret** or the **enable password** command. The *enable secret* takes precedence over the *enable password* command.

a *enable password*

The *enable secret* command sets a password for the various privilege levels. We use the command **enable password <*password*>** to set the password. This command does not encrypt the password saved in the *running-config* file.

b *enable secret*

The *enable secret* command establishes a password for the privilege levels. The difference to the *enable password* is that this command encrypts the password stored in the *running-config* file providing better security.



```
Router>en
Password:
Router#
```

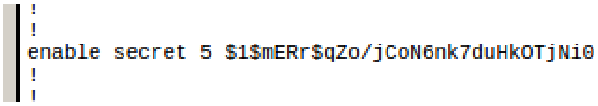
Figure 1: Entering the privelege EXEC mode with password enable with **enable secret** command.

1.3 Observing the changes with password enabled

After we issue the **enable secret** command we have to enter the password when going from the user EXEC mode to the priveleged EXEC mode, we can this in Figure 1.

1.4 Storing password in *running-config*

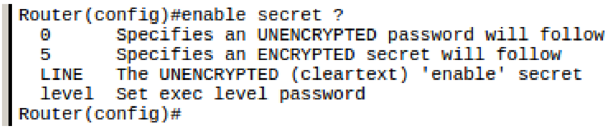
We can see the *running-config* using the **show running-config** command in the CLI of the router. We can observe as seen in Figure 2 that the password is encrypted.



```
!
!
enable secret 5 $1$mERr$qZo/jCoN6nk7duHkOTjNi0
!
!
```

Figure 2: The *running-config* in router, storing the password after **enable secret** command.

The 5 that follows after *enable secret* implies that the following is a hash for the password, encrypted using MD5 algorithm. We can see this in Figure 3, there is an encrypted hash of the password following the 5.

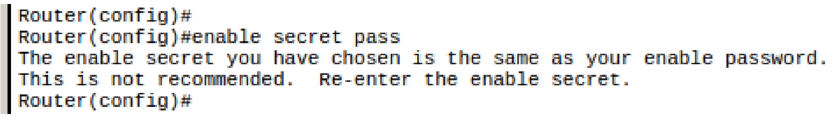


```
Router(config)#enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies an ENCRYPTED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password
Router(config)#
```

Figure 3: Checking *enable secret* options

a Extra

We can use both the **enable secret** and the **enable password** command at the same time. The router uses the encrypted password when both are present. When using the same password for both the encrypted and the unencrypted password, the CLI warns us to use different but still allows it as seen in Figure 4.



```
Router(config)#
Router(config)#enable secret pass
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
Router(config)#
```

Figure 4: Using the same password for both **enable secret** and **enable password**

1.5 Enable password for console access

Then we will also configure a password for the console access. We use the commands **line con 0** in the configuration mode. This lets us configure the primary terminal line.

a Set password

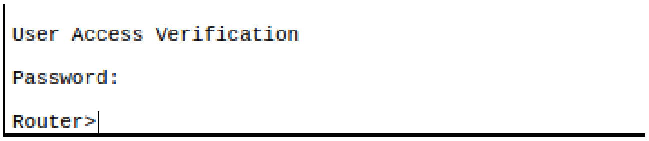
Then we use the **password** command to set the password.

b Enable login for console access

We use the **login** command to enable password checking.

c Loggin prompt

After setting the password for console access we get prompted to enter the password when we open the CLI, we need to enter the password even to enter the user EXEC mode as can be seen in Figure 5.



```
User Access Verification

Password:

Router>
```

Figure 5: Login prompt for access to the console.

1.6 Console Access Password in *running-conf*

The password set for console access is not encrypted when we check the *running-configuration* using **show running-conf**, the password is stored in plain text.

1.7 configuring password for telnet

a Telnet configuration mode

We enter the telnet configuration mode using the **line vty 0 4** command in the global configuration mode.

We then set the password with the **password** command and enable login using the **login** command.

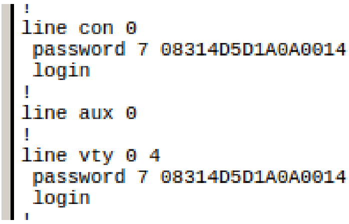
Checking the *running-configuration* we can see that the passwords for the *console access* and the *terminal access* are stored in plain text.

1.8 Encrypt all passwords

As many of the passwords are stored in plain text we need to increase the security of the plain-text password. We use the **service password-encryption** command in the global configuration mode to encrypt all the unencrypted passwords.

a *running-conf* after encrypting password

We can see in Figure 6 that all the password have been encrypted. We can see that there is a number, 7, after password. This specifies that this was encryption Type 7.



```
!
line con 0
 password 7 08314D5D1A0A0014
 login
!
line aux 0
!
line vty 0 4
 password 7 08314D5D1A0A0014
 login
!
```

Figure 6: The encrypted password after running **service password-encryption**

1.9 Type 5 and Type 7 encryptions

As seen in Figure 6 all the passwords that were encrypted using the **service password-encryption** command was encrypted with encryption Type 7. Previously when running the **enable secret** command the passwords were encrypted using Type 5, as seen in Figure 2.

The Type 5 encryption is done using an MD5 algorithm to generate the password hash. Whereas the Type 7 encryption is done using a weak algorithm, it is just XORs the password.

1.10 Securing the Switch

We follow the same procedures to secure the switch by adding password and encrypting them. We use the same password as in the previous assignment.

- **enable secret** Add password for accessig the privileged EXEC mode.

- **line con 0** Configure console access

  password Set password for console access

  login Enable password login for console access

- **line vty 0 4** Configure telnet access

  password Set password for telnet access

  login Enable password login for telnet access

- **service password-encryption** Encrypt all pasword in the *runnnig-config*

2 Configuring Access lists