Lab 11.3.1 Router Security and AAA Authentication

Objective

In this lab, the student will use the `login local` command to configure authentication and access levels.

Also, the student will be introduced to the Cisco IOS AAA security authentication features, including custom prompts and debug features.

Scenario

The International Travel Agency (ITA) is concerned about the security of their routers and switches. A prototype of Cisco’s login security features including AAA is to be created.

Step 1

Before beginning this lab, it is recommended that the routers be reloaded after erasing their startup configuration. This prevents problems that may be caused by residual configurations.

Build and configure the network according to the diagram. Configure the router’s FastEthernet interface and the host’s IP address, subnet mask and default gateway. Use the following commands to configure SanJose1:

```
SanJose1(config)#enable password cisco
SanJose1(config)#line vty 0 4
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
SanJose1(config-line)#line aux 0
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
```
Step 2

Security for the user EXEC mode can be configured for each of the three access methods: VTY (Telnet), AUX, and console. VTYs and AUX port access require a login password by default. If no password is set, the router will not establish a session. Instead, it will return an error message explaining that a password is required but none is set.

By default, the console port is not configured to request a login password. However, it is recommended to configure the console port with the `login` command to enforce password security. Without it, anyone with a laptop and a console cable can easily gain access to the device.

The following table displays each of the three access methods, their associated command syntax, and a configuration example for each access method. For convenience sake, the same password was used in all three examples. Although it is possible to do so, the recommended practice is to set different passwords for each access method.

<table>
<thead>
<tr>
<th>Password Type</th>
<th>Access Method</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console session</td>
<td>Console port</td>
<td><code>line con 0 password</code></td>
<td><code>line con 0 password cisco login</code></td>
</tr>
<tr>
<td>Telnet session</td>
<td>VTY interfaces. The example syntax sets all five virtual interfaces at once</td>
<td><code>line vty 0 4 password login</code></td>
<td><code>line vty 0 4 password cisco login</code></td>
</tr>
<tr>
<td>AUX session</td>
<td>AUX port If one is present, it can be accessed through a modem</td>
<td><code>line AUX 0 password login</code></td>
<td><code>line AUX 0 password cisco login</code></td>
</tr>
</tbody>
</table>

The `login` command requires that the user authenticate when connecting to the line. When the `login` command is used without optional keywords, the password must be defined by the `password` command. This is shown in the Example column of the table.

Telnet to SanJose1 from Host A. Verify that the password, `cisco`, must be changed to gain user-level access to the router.

Step 3

It is possible to require a username as well as a password for logins to the router. Furthermore, different username/password combinations can be configured for different users. These username/password combinations can be stored locally, in the database on the router, or remotely, on a specialized security server.

Configure a local username/password database for SanJose1, as follows:

```
SanJose1(config)#username remote password access
SanJose1(config)#username scott password wolfe
```

To finish the configuration, issue the `login local` command for line con 0, as the following shows:

```
SanJose1(config)#line con 0
SanJose1(config-line)#login local
```
The keyword **local** instructs the router to check username/password combinations against the local database. Now only the defined combinations of usernames and passwords can be used to access the user mode from the console on the router. Like all passwords in the Cisco IOS, these passwords are case sensitive and can include text and/or numbers. The usernames are not case sensitive.

Exit out of the session and then log in to SanJose1 from the console port. The new access prompts will look like the following:

```
User Access Verification
Username: remote
Password: 
SanJose1>exit
User Access Verification
Username: ScOtT
Password: 
% Login invalid (Used the wrong case on the password)
Username: Scott
Password: 
SanJose1> (Used the correct case on the password)
```

From Host A, Telnet to SanJose1. Confirm that the only prompt is for a password. The password `cisco` should still work.

Configure the AUX and VTYs to check username/password combinations against the local database. Enter the following commands, on SanJose1:

```
SanJose1(config)#line aux 0
SanJose1(config-line)#login local
SanJose1(config)#line vty 0 4
SanJose1(config-line)#login local
```

From Host A, Telnet to SanJose1 and authenticate using one of the locally defined username and password combinations.

**Step 4**

The Cisco IOS AAA feature offers several security measures. In this step, the authentication feature will be examined. The AAA authentication feature is used to validate users.

**Warning:** It is important to have a plan when configuring AAA because configuration commands take effect immediately. It is possible to get locked out of the router.

Enter the following lines in SanJose1:

```
SanJose1(config)#aaa new-model
SanJose1(config)#username admin password aaacisco
SanJose1(config)#aaa authentication login default local enable
```

The `aaa new-model` command enables AAA. Once this command is entered, the console, VTY, AUX, and TTY ports require a username and password for access.

The `aaa authentication login default` command defines how the username/password will be verified. Multiple options can be used with this command. The first option (local) will be tried first. In the event the attempt to check a username/password using this method returns an error, the second method (enable) will be tried, and so on. It is very important to note that an authentication failure is not an error. An error results only if the specified source, such as a remote server, cannot be read. The available options for the `aaa authentication login default` command are as follows:
SanJose1(config)#aaa authentication login default ?
   enable   Use enable password for authentication.
   group    Use Server-group (used to access TACACS or RADIUS servers
   line     Use line password for authentication.
   local    Use local username authentication.
   local-case Use case-sensitive local username authentication.

If a TACACS+ server was configured with username/password combinations, the router could be
configured with the command, `aaa authentication login default group tacacs+ local enable`. The `group` keyword indicates a server group while the `tacacs+` parameter
specifies the type of security server. As the second specified option in this example command, the
local database would only be used if the TACACS+ server could not be reached.

From Host A, Telnet to SanJose1. Confirm that there is a prompt for a username and password.
Confirm that `admin` and `aaacisco` grant access to the router.

Disconnect from SanJose1 and then attempt to log in again. This time, verify that the username is
not case sensitive but the password is.

In some cases, case sensitive usernames may be desired. AAA can be configured to make
usernames case sensitive by adding the `local-case` option as follows:

SanJose1(config)#aaa authentication login default local-case enable

After entering this command, log out and then log back in to the router. Verify that both the username
and password are now case sensitive.

**Step 5**

The default login prompt looks like the following:

```
User Access Verification
Username:
```

When using AAA, there is an option to present a more specific and/or user-friendly prompt. Issue the
following command on SanJose1:

SanJose1(config)#aaa authentication username-prompt "Enter your NT username:"

To verify the new prompt, exit out of the console session and log back in.

**Step 6**

In this step, the `debug aaa authentication` command feature will be examined. On SanJose1
activate the `debug` feature with the following command:

SanJose1#debug aaa authentication
AAA Authentication debugging is on

From Host A, Telnet to SanJose1. When prompted for a username, press Enter. The second time
there is a prompt, enter a fake username/password combination. On the third and final attempt, log
in correctly.

The following is a sample partial display of the `debug` output.

**Note:** The output may vary depending on the router platform and IOS used.
The first four lines set up the login session. Notice that the number (1421093628) tracks the session until the failed password and a new tracking number are generated.

The (297482216) attempt ends up as a failed attempt or bad password, as shown in the following:

```<Output omitted>
02:48:49: AAA/AUTHEN (297482216): password incorrect
02:48:49: AAA/AUTHEN (297482216): status = FAIL
```

The following lines are a partial display of the successful attempt:

```<Output omitted>
02:48:57: AAA/AUTHEN (782251026): continue_login (user='bob')
02:48:57: AAA/AUTHEN (782251026): status = GETPASS
02:48:57: AAA/AUTHEN/CONT (782251026): status = PASS
```

Use `undebug all` to turn off all debugging.