Task 1. Ensure that APT is installed

First, you’ll check that the APT application is installed so that you can use it to manage applications. The simplest way to do this is to run the apt command in the Bash shell and check the response.

The Bash shell is the command-line interpreter currently open on the left side of the screen. You’ll use the Bash shell by typing commands after the prompt. The prompt is represented by a dollar sign ($) followed by the input cursor.

- Confirm that the APT package manager is installed in your Linux environment. To do this, type `apt` after the command-line prompt and press **ENTER**.

The command to complete this step:

apt

When installed, `apt` displays basic usage information when you run it. This includes the version information and a description of the tool:

```
apt 1.8.2.3 (amd64)
Usage: apt [options] command
apt is a commandline package manager and provides commands for
searching and managing as well as querying information about packages.
It provides the same functionality as the specialized APT tools,
like apt-get and apt-cache, but enables options more suitable for
interactive use by default.
...
```

APT is already installed by default in the Linux Bash shell in this lab because this is a Debian-based system. APT is also the recommended package manager for Debian. If you’re using another distribution, a different package manager, such as YUM, may be available instead.

Task 2. Install and uninstall the Suricata application

In this task, you must install Suricata, a network analysis tool used for intrusion detection, and verify that it is installed correctly. Then, you’ll uninstall the application.

1. Use the APT package manager to install the Suricata application.

Type `sudo apt install suricata` after the command-line prompt and press **ENTER**.

The command to complete this step:

sudo apt install suricata

Note: *The `apt install` and `apt remove` commands must be prefixed with the sudo command as elevated privileges are required to install and uninstall software in Linux. The Suricata application can take a few minutes to install.*

When you install an application with APT, the output displays details of all the software to be installed. This may include additional applications that depend on the new software. These additional applications are called the dependencies of the software to be installed.

When prompted to continue, press the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)

2. Verify that Suricata is installed by running the newly installed application.

Type `suricata` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
suricata
```

When Suricata is installed, version and usage information is listed:

```
Suricata 4.1.2

USAGE: suricata [OPTIONS] [BPF FILTER]

    -c   : path to configuration file

    -T         : test configuration file (use with -c)

...
```

3. Use the APT package manager to uninstall Suricata.

Type `sudo apt remove suricata` after the command-line prompt and press **ENTER**. Press **ENTER** (**Yes**) when prompted to continue.

The command to complete this step:

```
sudo apt remove suricata
```

When prompted to continue, press the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)

4. Verify that Suricata has been uninstalled by running the application command again.

Type `suricata` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
suricata
```

If you have uninstalled Suricata, the output is an error message:

```
-bash: /usr/bin/suricata: No such file or directory
```

This message indicates that Suricata can't be found anymore.

Task 3. Install the tcpdump application

In this task, you must install the tcpdump application. This is a command-line tool that can be used to capture network traffic in a Linux Bash shell.

- Use the APT package manager to install tcpdump.

Type `sudo apt install tcpdump` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
sudo apt install tcpdump
```

Task 4. List the installed applications

Next, you need to confirm that you've installed the required applications. It's important to be able to validate that the correct applications are installed. Often you may want to check that the correct versions are installed as well.

1. Use the APT package manager to list all installed applications.

Type `apt list --installed` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
apt list --installed
```

This produces a long list of applications because Linux has a lot of software installed by default.

2. Search through the list to find the tcpdump application you installed.

The Suricata application is not listed because you installed and then uninstalled that application:

```
...

tcpdump/oldstable,now 4.9.3-1~deb10u2 amd64 [installed]

...
```

Note: The specific version of `tcpdump` that you see displayed may be different from what is shown above.

Task 5. Reinstall the Suricata application

In this task, you must reinstall the Suricata application and verify that it has been installed correctly.

1. Run the command to install the Suricata application.

Type `sudo apt install suricata` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
sudo apt install suricata
```

When prompted to continue, press the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)

2. Use the APT package manager to list the installed applications.

Type `apt list --installed` after the command-line prompt and press **ENTER**.

The command to complete this step:

```
apt list --installed
```

3. Search through the list to confirm that the Suricata application has been installed.

The output should include the following lines:

```
...

suricata/oldstable,now 1:4.1.2-2+deb10u1 amd64 [installed]

...

tcpdump/oldstable,now 4.9.3-1~deb10u2 amd64 [installed]

...
```