Activity overview

In this lab activity, you'll use the Advanced Package Tool (APT) and `sudo` to install and uninstall applications in a Linux Bash shell.

While installing Linux applications can be a complex task, the APT package manager manages most of this complexity for you and allows you to quickly and reliably manage the applications in a Linux environment.

You'll use Suricata and tcpdump as an example. These are network security applications that can be used to capture and analyze network traffic.

The virtual machine you access in this lab has a Debian-based distribution of Linux running, and that works with the APT package manager. Using a virtual machine prevents damage to a system in the event its tools are used improperly. It also gives you the ability to revert to a previous state.

As a security analyst, it's likely you'll need to know how to install and manage applications on a Linux operating system. In this lab activity, you'll learn how to do exactly that!

Scenario

Your role as a security analyst requires that you have the Suricata and tcpdump network security applications installed on your system.

In this scenario, you have to install, uninstall, and reinstall these applications on your Linux Bash shell. You also need to confirm that you've installed them correctly.

Here's how you'll do this: **First**, you'll confirm that APT is installed on your Linux Bash shell. **Next**, you'll use APT to install the Suricata application and confirm that it is installed. **Then**, you'll uninstall the Suricata application and confirm this as well. **Next**, you'll install the tcpdump application and list the applications currently installed. **Finally**, you'll reinstall the Suricata application and confirm that both applications are installed.

OK, it's time to learn how to install some applications!

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 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 installed correctly. Then, you'll uninstall the application.

```
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.*

1. 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:

```
1   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:

```
1   suricata
```

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

```
1   -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.

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

The command to complete this step:

```
1  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:

```
1  apt list --installed
```

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 installed correctly.

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]
...
```