

Start Lab

01:00:00

Activity: Install software in a Linux distribution

Lab 1 hour No cost Introductory

★★★★★

This lab may incorporate AI tools to support your learning.

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!

Note: The lab starts with your user account, called `analyst`, already logged in to the Bash shell. This means you can start with the tasks as soon as you click the **Start Lab** button.

Disclaimer: For optimal performance and compatibility, it is recommended to use either Google Chrome or Mozilla Firefox browsers while accessing the labs.

Start your lab

You'll need to start the lab before you can access the materials. To do this, click the green "Start Lab" button at the top of the screen.

Start Lab

After you click the **Start Lab** button, you will see a shell, where you will be performing further steps in the lab. You should have a shell like this:

```
analyst@63fcceed8e3bc1:~
```

When you have completed all the tasks, refer to the End your Lab section that follows the tasks for information on how to end your lab.

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**.

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 command-line 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.

Click **Check my progress** to verify that you have completed this task correctly.

Ensure that APT is installed

Check my progress

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.

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

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

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**.)

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

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

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.

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

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

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

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.

Click **Check my progress** to verify that you have completed this task correctly.

Install and uninstall the Suricata application

Check my progress

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**.

Click **Check my progress** to verify that you have completed this task correctly.

Install the tcpdump application

Check my progress

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.

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

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

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

Click **Check my progress** to verify that you have completed this task correctly.

List the installed applications

Check my progress

Task 5. Reinstall the Suricata application

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

- Run the command to install the Suricata application.

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

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

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

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

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.

Click **Check my progress** to verify that you have completed this task correctly.

Reinstall the Suricata application

Check my progress

Conclusion

Great work!

You now have practical experience with the APT package manager. You learned to

- install applications,
- uninstall applications, and
- list installed applications.

Being able to manage installed applications in Linux is a key skill for any security analyst.

End your lab

Before you end the lab, make sure you're satisfied that you've completed all the tasks, and follow these steps:

- Click **End Lab**. A pop-up box will appear. Click **Submit** to confirm that you're done. Ending the lab will remove your access to the Bash shell. You won't be able to access the work you've completed in it again.

2. Another pop-up box will ask you to rate the lab and provide feedback comments. You can complete this if you choose to.

3. Close the browser tab containing the lab to return to your course.

4. Refresh the browser tab for the course to mark the lab as complete.

The output should include the following lines:

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

Click **Check my progress** to verify that you have completed this task correctly.

Reinstall the Suricata application

Check my progress

Task 5. Reinstall the Suricata application

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

- Run the command to install the Suricata application.

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

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

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

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

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.

Click **Check my progress** to verify that you have completed this task correctly.

Reinstall the Suricata application

Check my progress

Conclusion

Great work!

You now have practical experience with the APT package manager. You learned to

- install applications,
- uninstall applications, and
- list installed applications.

Being able to manage installed applications in Linux is a key skill for any security analyst.

Activity overview

Scenario

Start your lab

Task 1. Ensure that APT is installed

Task 2. Install and uninstall the Suricata application

Task 3. Install the tcpdump application

Task 4. List the installed applications

Task 5. Reinstall the Suricata application

Conclusion

End your lab