

Activity: Install software in a Linux distribution

Introduction

In this lab, you'll learn how to install and uninstall applications in Linux. You'll use Linux commands in the Bash shell to complete this lab. You'll also use the Advanced Package Tool (APT) package manager to install and uninstall the Suricata and tcpdump applications.

What you'll do

You have multiple tasks in this lab:

- Confirm APT is installed in Bash
- Install Suricata with APT
- Uninstall Suricata with APT
- Install tcpdump with APT
- Reinstall Suricata with APT

Lab instructions

Start the lab

Before you start, you can review the [Resources for completing Linux labs](#). Then from this page, click **Launch App**. A Qwiklabs page will open and from that page, click **Start Lab** to begin the activity! *You may attempt this lab a maximum of 5 times, and you will have 60 minutes to complete this lab during each attempt.*

End the lab

From within the lab, click **End Lab** to end your lab.

Additionally, sometimes you need to refresh your Coursera page in order for your progress to be registered. If you refresh this page after you complete your lab, the green check mark should appear.

Best practices for completing labs:

- Make sure your browser is up to date with the latest version.
- Make sure your internet connection is stable.
- After you complete the lab, leave the lab window open for at least 10 minutes in order to allow the system to record your progress.
- If you run into issues connecting to the lab, try logging into Coursera in an Incognito mode and completing the lab there.

This course uses a third-party app, Activity: Install software in a Linux distribution, to enhance your learning experience. The app will reference basic information like your name, email, and Coursera ID.

Resources for completing Linux labs

This course features hands-on lab activities where you'll have the opportunity to practice Linux commands in the terminal. You'll use a platform called Qwiklabs to complete these labs. In this reading, you'll learn how to use Qwiklabs.

This reading first provides a section on how to use Qwiklabs, which includes details on how to launch a lab, how to interact within the Qwiklabs environment, and how to end a lab. This is followed

by another section on helpful navigation tips and keyboard shortcuts; these may be useful when working in the terminal.

Note: You will not launch Qwiklabs directly from this reading and instead will do this through lab activities and exemplars that you encounter throughout the course.

How to use Qwiklabs

Launching Qwiklabs

When you select a lab, you start from a Coursera page. You will need to click **Launch App** on that page. After you click **Launch App**, a new tab will open with a Qwiklabs page that contains instructions for that particular lab.

Start Lab button

On the Qwiklabs page, you must click **Start Lab** to open a temporary terminal. The instructions for the lab will move to the right side of the screen.



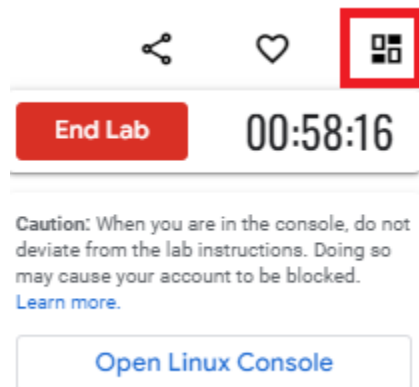
Read the instructions and complete all the tasks in the lab by entering commands in the terminal.

Note: It may take a moment for the terminal to start.

Lab control dialog box

After you click **Start Lab**, the lab control dialog box opens. It contains the **End Lab** button, the **timer**, and the **Open Linux Console** button.

You can hide or unhide the dialog box by clicking the following icon in the red box:



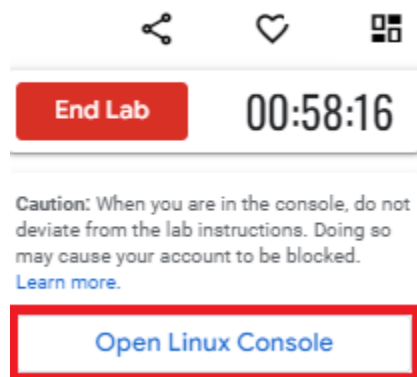
The timer

The **timer** starts when the terminal has loaded. The timer keeps track of the amount of time you have left to complete a lab. The timer counts down until it reaches 00:00:00. When it does, your temporary terminal and resources are deleted.

You will have ample time to complete the labs. But, stay focused on completing the tasks to ensure you use your time well.

Open Linux Console button

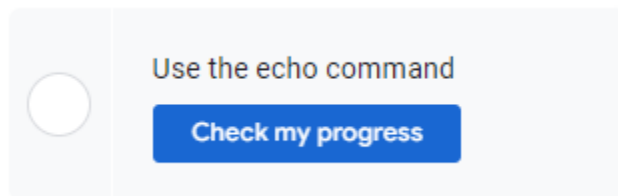
When you click the button to **Open Linux Console**, the terminal opens in a new browser window:



Use this feature if you want a full-screen view of the terminal. You can close this window at any time. Closing the window does not end your lab, and you can continue working in the terminal in the original tab.

Check progress

You can check your progress by clicking **Check my progress** at the end of each task.



If you haven't yet completed a task, you'll receive hints on what you must do to complete it. You can click **Check my progress** whenever you want to check the completion status of a task or receive a hint.

Using copy/paste commands

The first time you try to use copy or paste keyboard shortcuts (such as **CTRL + C**), you'll receive a pop-up requesting permission to use your device's clipboard: "**googlecoursera.qwiklabs.com wants to see text and images copied to the clipboard.**" Please click **Allow** if you would like to be able to use these shortcuts in the Qwiklabs platform. If you choose not to allow Qwiklabs access to your clipboard, you cannot use keyboard shortcuts but you can still complete the lab.

Code block

Certain steps may include a code block. Click the copy button to copy the code provided and then paste it into the terminal.

```
sudo apt install suricata
```



To paste code or other text content that you have copied from the instructions into the terminal, activate the terminal by clicking anywhere inside it. The terminal is active when the cursor in the terminal changes from a static empty outline to a flashing solid block.




```
analyst@14bc4618e5ba:~$ ls reports
Q1patches.txt  Q2patches.txt
analyst@14bc4618e5ba:~$ pwd
/home/analyst
analyst@14bc4618e5ba:~$ █
```

Once the terminal is active, use the keyboard shortcut **CTRL + V** (hold down the **CTRL** key and press the **V** key) to insert the copied text into the terminal at the location of the flashing cursor.

Scrolling

In certain situations, you may want to scroll within the terminal window. To do so, use the scroll wheel on your mouse or the touchpad of your computer.

End Lab button



End Lab

00:18:05

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked.
[Learn more.](#)

Open Linux Console

Finally, click **End Lab** when you've completed the tasks in the lab.

Note: Don't click **End Lab** until you're finished; you'll lose access to the work you've done throughout the lab.

Tracking progress on Coursera

If you complete a lab but your progress hasn't been tracked on Coursera, you may need to refresh the page for your progress to be registered. Once you complete the lab and refresh the page, the green check mark should appear.

Helpful navigation tips and keyboard shortcuts

The following contains a list of navigation tips and keyboard shortcuts you may find useful when completing your Linux labs. Your cursor must be in the terminal window to use these navigation tips and keyboard shortcuts.

- **CTRL + C**: Terminates a command that is currently running; from the instructions portion of Qwiklabs, you can use **CTRL + C** to copy, but within the terminal, it will only terminate a command and if one isn't running, it will display **^C** at the prompt
- **CTRL + V**: Pastes text
- **clear**: Clears the terminal screen; this can also be done by entering **CTRL + L**
- **CTRL + A**: Sets your cursor at the beginning of a command
- **CTRL + E**: Sets your cursor at the end of a command
- **Left arrow key**: Moves left within a command
- **Right arrow key**: Moves right within a command
- **Up arrow key**: Provides the last command you entered into the command line; can be entered multiple times to go through multiple commands from the command history
- **Down arrow key**: Provides the next command in the command history; must be after using the **up arrow key**
- **Tab key**: Provides available suggestions for completing your text

Key takeaways

Knowing how to navigate Qwiklabs will be useful as you complete the labs throughout this course. These labs can help you practice what you've learned in an interactive environment.

Activity: Install software in a Linux distribution

1 hourFree

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.

Start your lab

Before you begin, you can review the instructions for using the Qwiklabs platform under the **Resources** tab in Coursera.

If you haven't already done so, click **Start Lab**. This brings up the terminal so that you can begin completing the tasks!

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 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.

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.

1. 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**.)

2. 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**.)

4. 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.

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

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

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.

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.

1. 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**.)

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

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

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]  
...
```

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:

1. 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.

Optional Exemplar: Install software in a Linux distribution

A lab exemplar is an optional resource that provides a completed model of the lab activity that precedes it. You may review this exemplar, or you may proceed to the next course item without reviewing it.

Instructions for reviewing the exemplar

If you choose to review the exemplar, click **Launch App** from this page, and then from the Qwiklabs page that opens, click **Start Lab**. Review the solutions provided in the exemplar. If you choose, you can also enter these solutions in the lab environment.

If you only want to review particular sections of the lab, you can go directly to those sections and skip others. The lab activity and the exemplar are organized with the same tasks.

When you have finished reviewing the exemplar, click **End Lab** from within the lab. Additionally, sometimes you need to refresh your Coursera page in order for your progress to be registered. If you refresh this page after you complete your lab, the green check mark should appear.

Instructions for proceeding without reviewing the exemplar

If you do not need to review any sections of the lab, you can proceed to the next course item without opening the exemplar. In this case, a green check mark will *not* appear to indicate that you have completed this item, but this is okay. The exemplar is optional.

Best practices for completing labs:

- Make sure your browser is up to date with the latest version.
- Make sure your internet connection is stable.
- After you complete the lab, leave the lab window open for at least 10 minutes in order to allow the system to record your progress.
- If you run into issues connecting to the lab, try logging into Coursera in an Incognito mode and completing the lab there.

This course uses a third-party app, Optional Exemplar: Install software in a Linux distribution, to enhance your learning experience. The app will reference basic information like your name, email, and Coursera ID.