**Exemplar: Install software in a Linux distribution**

**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. 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.

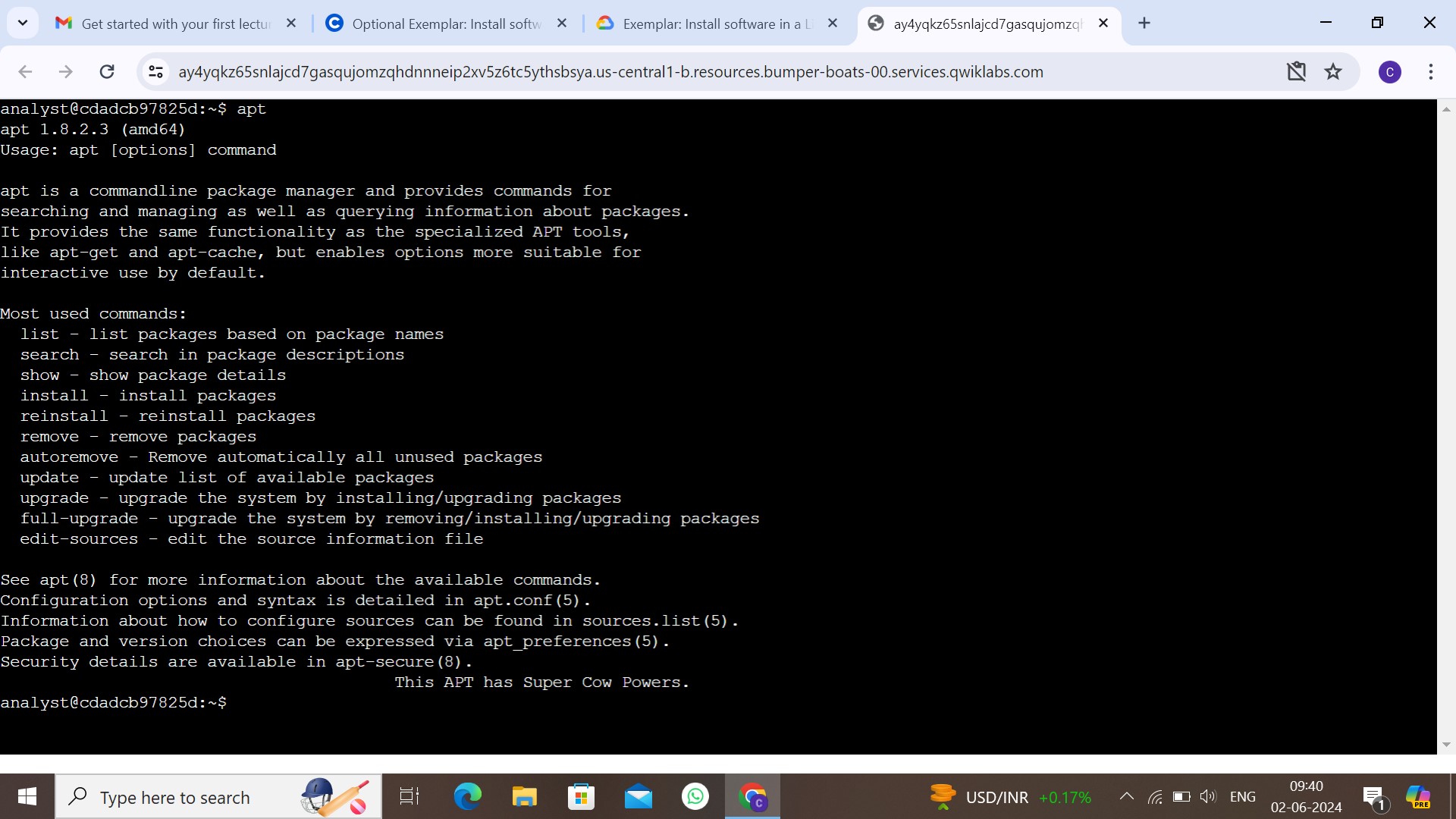
**Scenario :** Your role as a security analyst requires that you have the Suricata and tcpdump network security applications installed on your system. In this scenario, you have to install, uninstall, and reinstall these applications on your Linux Bash shell. You also need to confirm that you’ve installed them correctly.

**Start the lab:** click on “start lab” to start the lab. Then click on “open terminal”, it will redirect you to the virtual machine terminal, which is debian-based distribution of Linux.

**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. Run the following command in bash shell:

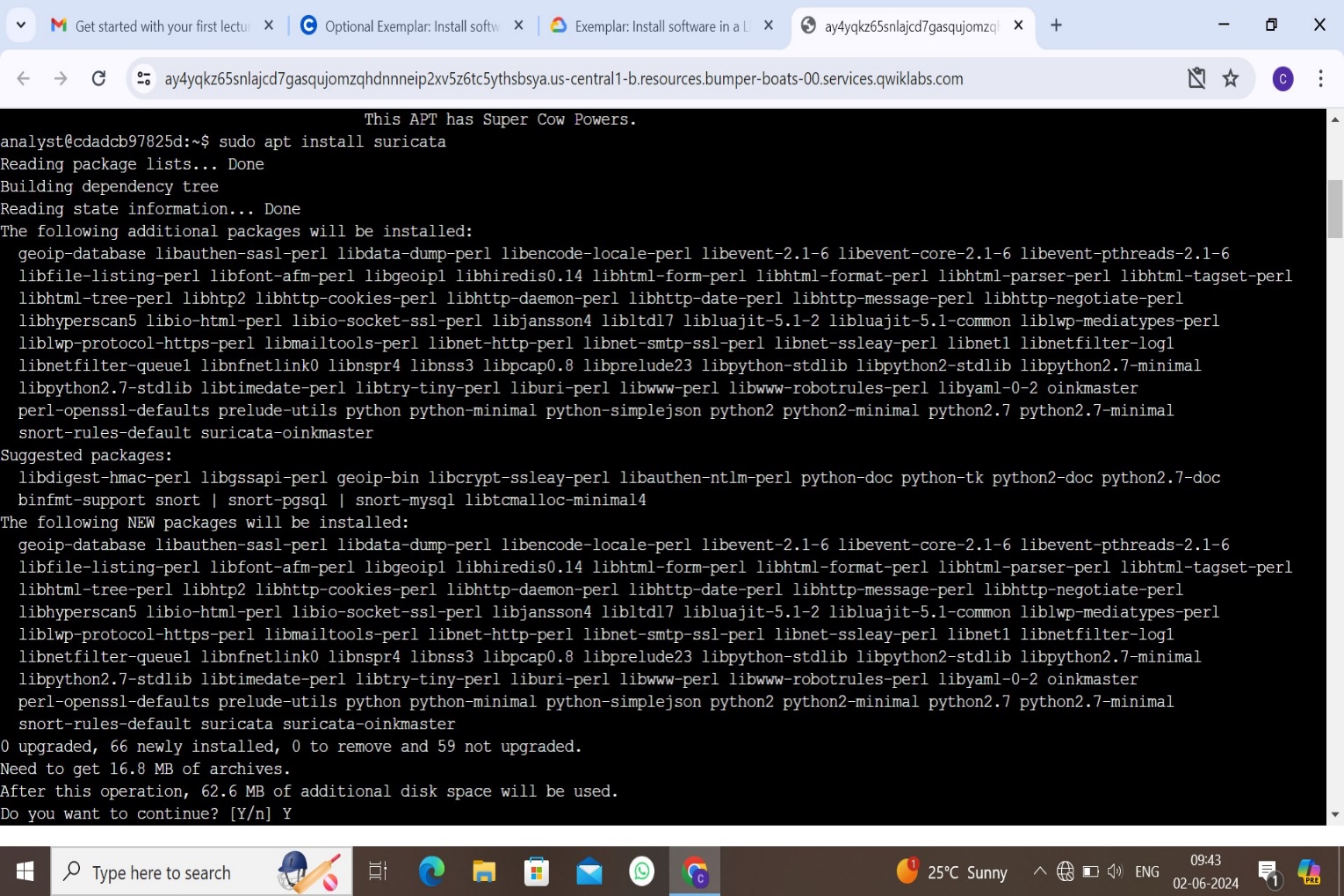
$apt

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

## **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.

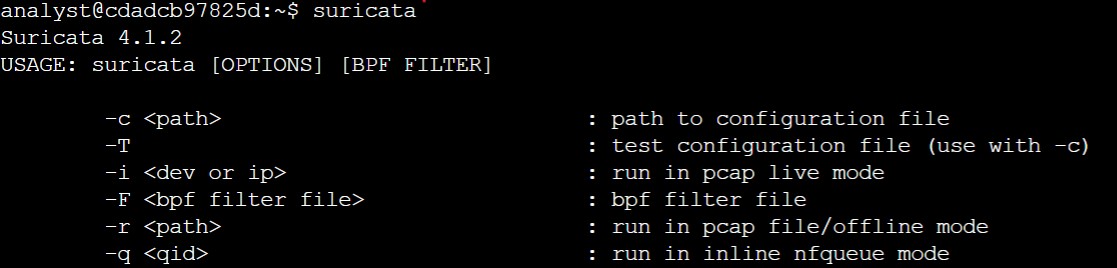
1. Use the APT package manager to install the Suricata application.

$sudo apt install suricata

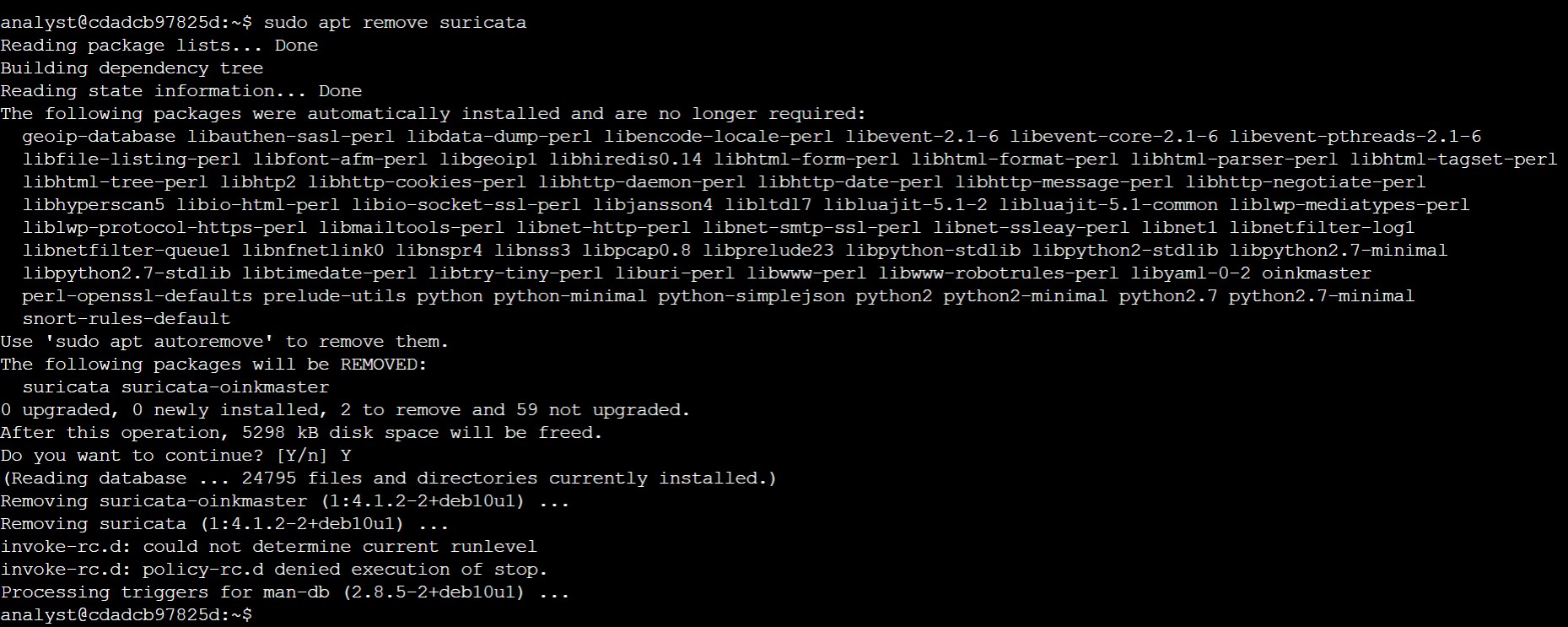
1. Verify that Suricata is installed by running the newly installed application.

$suricata

If it is installed, it will display the version of suricata as shown below:

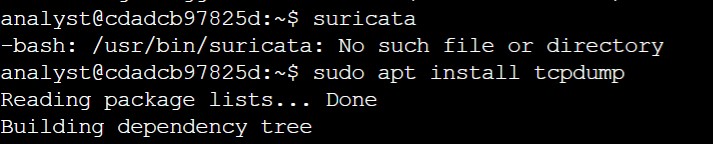


1. Use the APT package manager to uninstall Suricata.

$sudo apt remove suricata

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

$suricata

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

**Task 3. Install the tcpdump application:**

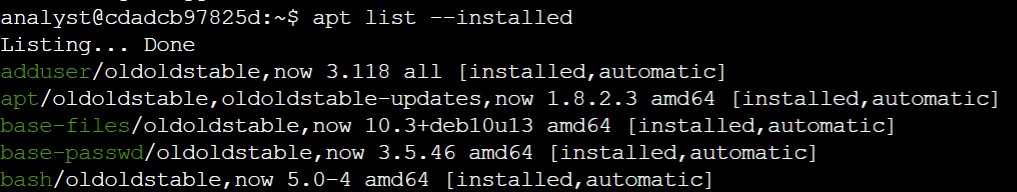
In this task, you must install the tcpdump application. This is a command-line tool that can be used to capture network traffic in a Linux Bash shell. Run the following command to install tcpdump:

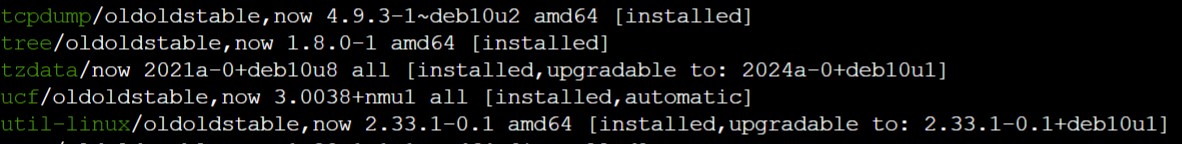
$sudo apt install tcpdump

**Task 4. List the installed applications :**

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. Run the following command to list the installed applications:

$apt list –installed



Look for the tcpdump application among those :

**Task 5. Reinstall the Suricata application :**

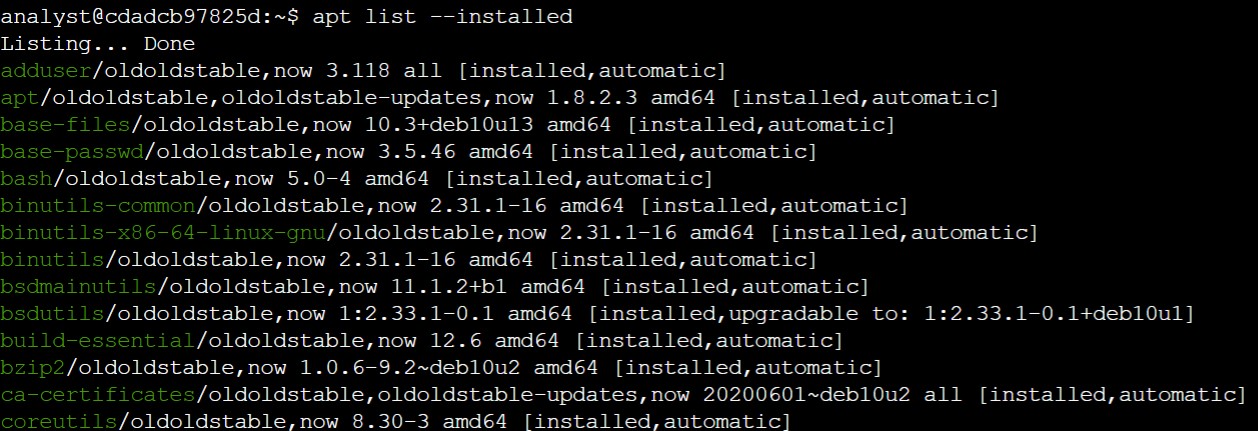
you must reinstall the Suricata application and verify that it has installed correctly.

1. Run the command to install the Suricata application.

$sudo apt install suricata

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

$apt list –installed



We can see the two application in this list.

...

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

...

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

...

**CONCLUSION:**

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

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