

Linux Lab Report - Google Cybersecurity Certification

Step 1: Introduction & Lab Goals

This lab focuses on using APT (Advanced Package Tool) to manage software on a Linux distribution. You will confirm the presence of APT, install and uninstall Suricata, install tcpdump, list all installed applications, and then reinstall Suricata.

The screenshot displays a web browser window with the URL https://www.cloudskillsboost.google/focuses/43068254?parent=lti_session. The page title is "Activity: Install software in a Linux distribution".

On the left, a terminal window shows the following output:

```
analyst@0de03d63de78:~$ apt
apt 2.2.4 (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.

Most used commands:
  list - list packages based on package names
  search - search in package descriptions
  show - show package details
  install - install packages
  reinstall - reinstall packages
  remove - remove packages
  autoremove - Remove automatically all unused packages
  update - update list of available packages
  upgrade - upgrade the system by installing/upgrading packages
  full-upgrade - upgrade the system by removing/installing/upgrading packages
  edit-sources - edit the source information file
  satisfy - satisfy dependency strings

See apt(8) for more information about the available commands.
Configuration options and syntax is detailed in apt.conf(5).
Information about how to configure sources can be found in sources.list(5).
Package and version choices can be expressed via apt_preferences(5).
Security details are available in apt-secure(8).
analyst@0de03d63de78:~$
```

On the right, the "Task 2. Install and uninstall the Suricata application" section is visible. It includes the following text:

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

Step 2: Confirm APT is Installed

Used the command ``apt`` to verify that the APT package manager is installed.

Linux Lab Report - Google Cybersecurity Certification

Activity: Install software in a Linux distribution

```
analyst@0de03d63de78:~$ sudo apt remove suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7
  libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5
  libjansson4 liblua5.1-2 liblua5.1-common libmagic-mgc
  libmagic1 libmaxminddb0 libmnl0 libnet1 libnetfilter-log1
  libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8
  libyaml-0-2 python3-simplejson python3-yaml suricata-update
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  suricata
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 6634 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 23406 files and directories currently installed.)
Removing suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.9.4-2) ...
analyst@0de03d63de78:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
analyst@0de03d63de78:~$
```

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

You have completed this task and successfully installed and uninstalled the Suricata application. Go to Settings to activate Windows.

Step 3: Install Suricata

Executed `sudo apt install suricata` to install Suricata, a network intrusion detection tool.

Activity: Install software in a Linux distribution

```
analyst@0de03d63de78:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7
  libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5
  libjansson4 liblua5.1-2 liblua5.1-common libmagic-mgc
  libmagic1 libmaxminddb0 libmnl0 libnet1 libnetfilter-log1
  libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libyaml-0-2
  python3-simplejson python3-yaml suricata-update
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  apparmor
The following NEW packages will be installed:
  tcpdump
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 466 kB of archives.
After this operation, 1361 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 tcpdump amd64 4.99.0-2+deb11u1 [466 kB]
Fetched 466 kB in 0s (4449 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package tcpdump.
(Reading database ... 23367 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.99.0-2+deb11u1_amd64.deb ...
Unpacking tcpdump (4.99.0-2+deb11u1) ...
Setting up tcpdump (4.99.0-2+deb11u1) ...
Processing triggers for man-db (2.9.4-2) ...
analyst@0de03d63de78:~$
```

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

You have completed this task and installed the tcpdump application.

Task 4. List the installed applications

Step 4: Uninstall Suricata

Executed `sudo apt remove suricata` and verified uninstallation with an error message when running

Linux Lab Report - Google Cybersecurity Certification

`suricata`.

Activity: Install software in a Linux distribution

```
python3.9/oldstable-security,now 3.9.2-1+deb11u3 amd64 [installed,automatic]
python3/oldstable,now 3.9.2-3 amd64 [installed]
readline-common/oldstable,now 8.1-1 all [installed,automatic]
runit-helper/oldstable,now 2.10.3 all [installed,automatic]
sed/oldstable,now 4.7-1 amd64 [installed,automatic]
sensible-utils/oldstable,now 0.0.14 all [installed,automatic]
sudo/oldstable-security,now 1.9.5p2-3+deb11u2 amd64 [installed]
suricata-update/oldstable,now 1.2.1-1 amd64 [installed,auto-removable]
systemd-sysv/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd-timesyncd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
sysvinit-utils/oldstable,now 2.96-7+deb11u1 amd64 [installed,automatic]
tar/oldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldstable,now 1.8.0-1+b1 amd64 [installed]
tzdata/oldstable-security,now 2025b-0+deb11u1 all [installed,automatic]
ucf/oldstable-security,now 3.0043+deb11u2 all [installed,automatic]
util-linux/oldstable,oldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
wget/oldstable-security,now 1.21-1+deb11u2 amd64 [installed]
xauth/oldstable,now 1:1.1-1 amd64 [installed,automatic]
xz-utils/oldstable,oldstable-security,now 5.2.5-2.1+deb11u1 amd64 [installed,automatic]
zlib1g-dev/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
zlib1g/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
analyst@0de03d63de78:~$
```

...
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

You have completed this task and displayed a list of installed applications.

Task 5. Reinstall the Suricata application

Step 5: Install tcpdump

Used `sudo apt install tcpdump` to install tcpdump, a packet capturing tool.

Activity: Install software in a Linux distribution

```
python3.9/oldstable-security,now 3.9.2-1+deb11u3 amd64 [installed,automatic]
python3/oldstable,now 3.9.2-3 amd64 [installed]
readline-common/oldstable,now 8.1-1 all [installed,automatic]
runit-helper/oldstable,now 2.10.3 all [installed,automatic]
sed/oldstable,now 4.7-1 amd64 [installed,automatic]
sensible-utils/oldstable,now 0.0.14 all [installed,automatic]
sudo/oldstable-security,now 1.9.5p2-3+deb11u2 amd64 [installed]
suricata-update/oldstable,now 1.2.1-1 amd64 [installed,automatic]
suricata/oldstable-security,now 1:6.0.1-3+deb11u1 amd64 [installed]
systemd-sysv/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd-timesyncd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
sysvinit-utils/oldstable,now 2.96-7+deb11u1 amd64 [installed,automatic]
tar/oldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldstable,now 1.8.0-1+b1 amd64 [installed]
tzdata/oldstable-security,now 2025b-0+deb11u1 all [installed,automatic]
ucf/oldstable-security,now 3.0043+deb11u2 all [installed,automatic]
util-linux/oldstable,oldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
wget/oldstable-security,now 1.21-1+deb11u2 amd64 [installed]
xauth/oldstable,now 1:1.1-1 amd64 [installed,automatic]
xz-utils/oldstable,oldstable-security,now 5.2.5-2.1+deb11u1 amd64 [installed,automatic]
zlib1g-dev/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
zlib1g/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
analyst@0de03d63de78:~$
```

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

You have completed this task and reinstalled Suricata.

Conclusion

Step 6: List Installed Applications

Linux Lab Report - Google Cybersecurity Certification

Listed all currently installed applications using the `dpkg --get-selections` command.

The screenshot shows a web browser window displaying a Google Cloud Skills Boost lab titled "Activity: Install software in a Linux distribution". The terminal window on the left shows the output of the command `dpkg --get-selections`, listing various installed packages and their architectures. The right panel provides a summary of the lab, stating "Great work!" and "You now have practical experience with the APT package manager. You learned to" followed by a list of tasks: "install applications, uninstall applications, and list installed applications." Below this, it says "Being able to manage installed applications in Linux is a key skill for any security analyst." The section "End your lab" instructs the user to click "End Lab" and "Submit" to complete the lab. The terminal output lists the following packages:

```
python3.9/oldstable-security,now 3.9.2-1+deb11u3 amd64 [installed,automatic]
python3/oldstable,now 3.9.2-3 amd64 [installed]
readline-common/oldstable,now 8.1-1 all [installed,automatic]
runit-helper/oldstable,now 2.10.3 all [installed,automatic]
sed/oldstable,now 4.7-1 amd64 [installed,automatic]
sensible-utils/oldstable,now 0.0.14 all [installed,automatic]
sudo/oldstable-security,now 1.9.5p2-3+deb11u2 amd64 [installed]
suricata-update/oldstable,now 1.2.1-1 amd64 [installed,automatic]
suricata/oldstable-security,now 1:6.0.1-3+deb11u1 amd64 [installed]
systemd-sysv/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd-timesyncd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
systemd/oldstable-security,now 247.3-7+deb11u6 amd64 [installed,automatic]
sysvinit-utils/oldstable,now 2.96-7+deb11u1 amd64 [installed,automatic]
tar/oldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldstable,now 1.8.0-1+b1 amd64 [installed]
tzdata/oldstable-security,now 2025b-0+deb11u1 all [installed,automatic]
ucf/oldstable-security,now 3.0043+deb11u2 all [installed,automatic]
util-linux/oldstable,oldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
wget/oldstable-security,now 1.21-1+deb11u2 amd64 [installed]
xauth/oldstable,now 1:1.1-1 amd64 [installed,automatic]
xz-utils/oldstable,oldstable-security,now 5.2.5-2.1~deb11u1 amd64 [installed,automatic]
zlib1g-dev/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
zlib1g/oldstable,oldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
analyst@0de03d63de78:~$
```

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.

Step 7: Reinstall Suricata

Reinstalled Suricata using `sudo apt install suricata` and confirmed installation was successful.