Activity: Install software in a Linux distribution

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.*

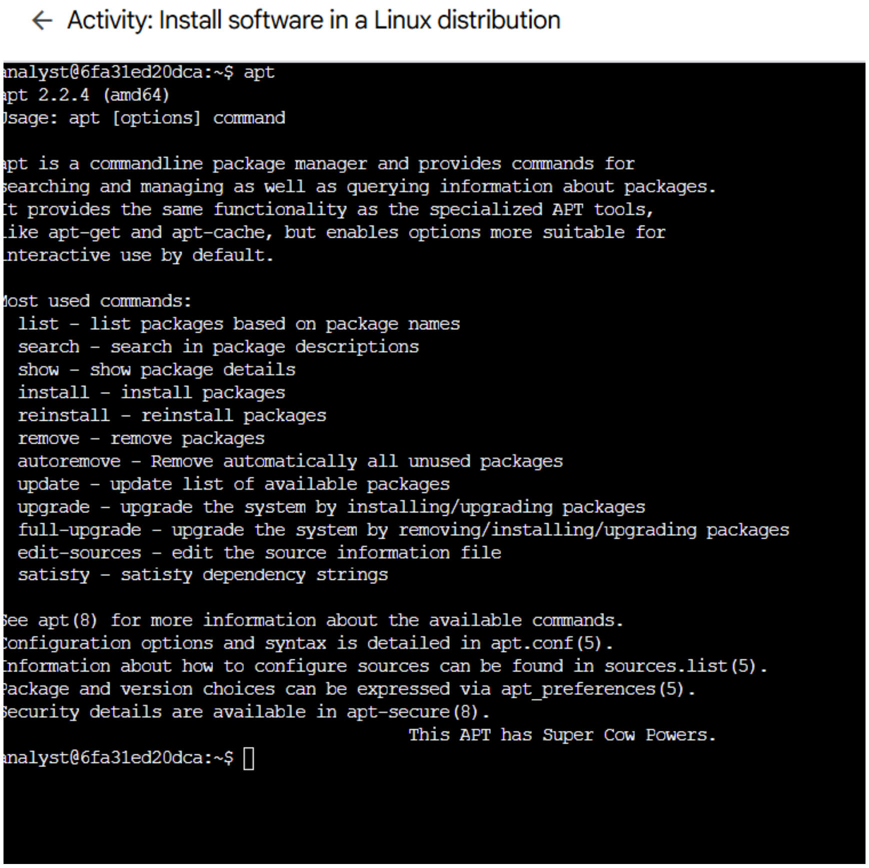
Task 1. Ensure that APT is installed

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:



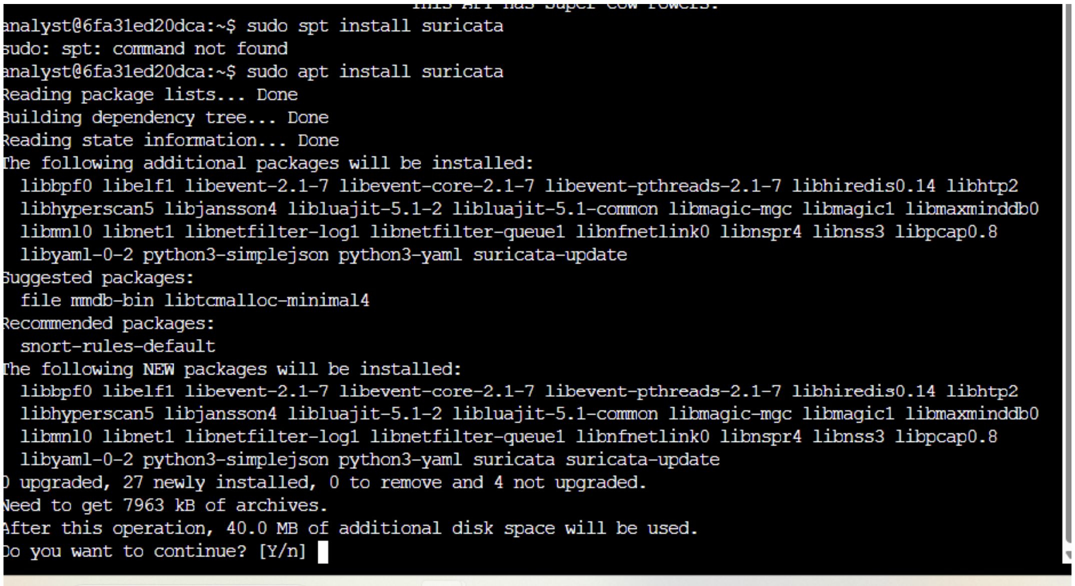
```
nalyst@6fa31ed20dca:~$ apt
pt 2.2.4 (amd64)
Jsage: apt [options] command

pt is a commandline package manager and provides commands for
earching and managing as well as querying information about packages.
t provides the same functionality as the specialized APT tools,
ike apt-get and apt-cache, but enables options more suitable for
nteractive use by default.

lost 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

ee apt(8) for more information about the available commands.
onfiguration options and syntax is detailed in apt.conf(5).
nformation about how to configure sources can be found in sources.list(5).
ackage and version choices can be expressed via apt_preferences(5).
ecurity details are available in apt-secure(8).
                                        This APT has Super Cow Powers.
nalyst@6fa31ed20dca:~$ 
```

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.

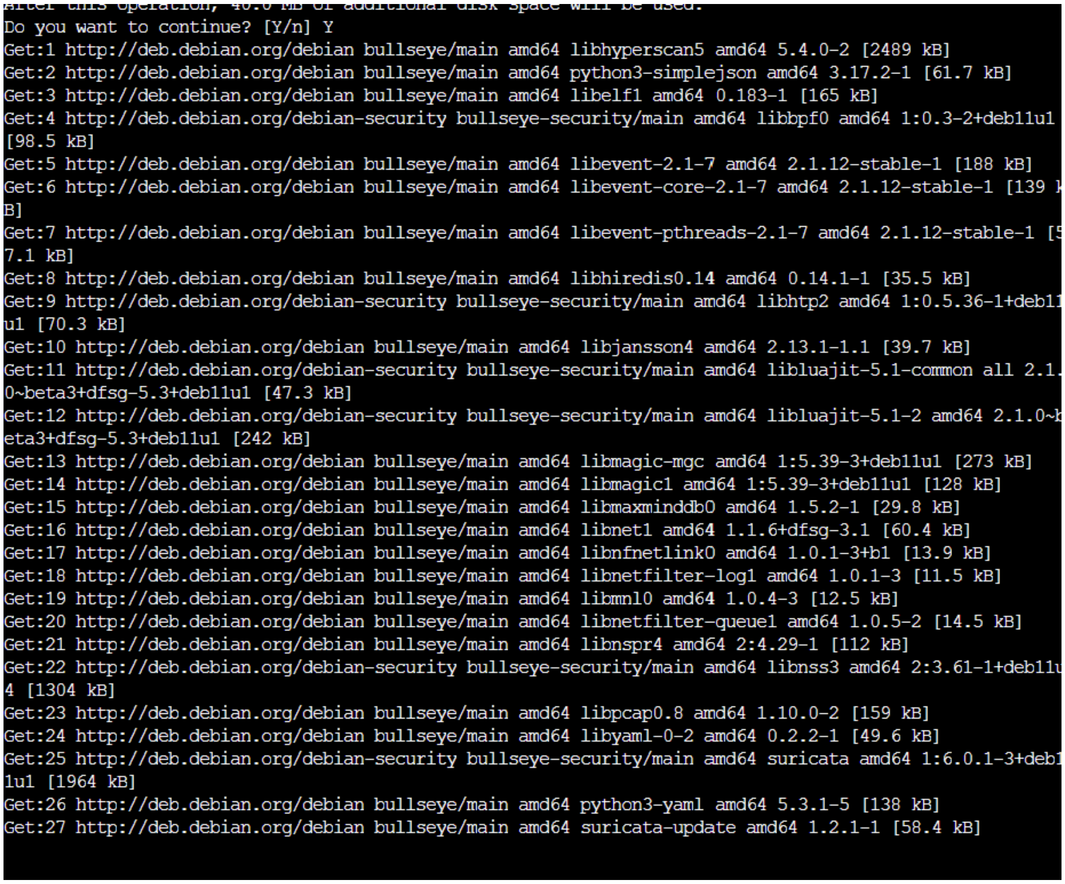
Type sudo apt install suricata after the command-line prompt and press **ENTER**.



```
                                        This APT has Super Cow Powers.
analyst@6fa31ed20dca:~$ sudo spt install suricata
sudo: spt: command not found
analyst@6fa31ed20dca:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2
  libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-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
Suggested packages:
  file mmdb-bin libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2
  libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-common libmagic-mgc libmagic1 libmaxminddb0
  libmnl0 libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8
  libyaml-0-2 python3-simplejson python3-yaml suricata suricata-update
0 upgraded, 27 newly installed, 0 to remove and 4 not upgraded.
Need to get 7963 kB of archives.
After this operation, 40.0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

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.

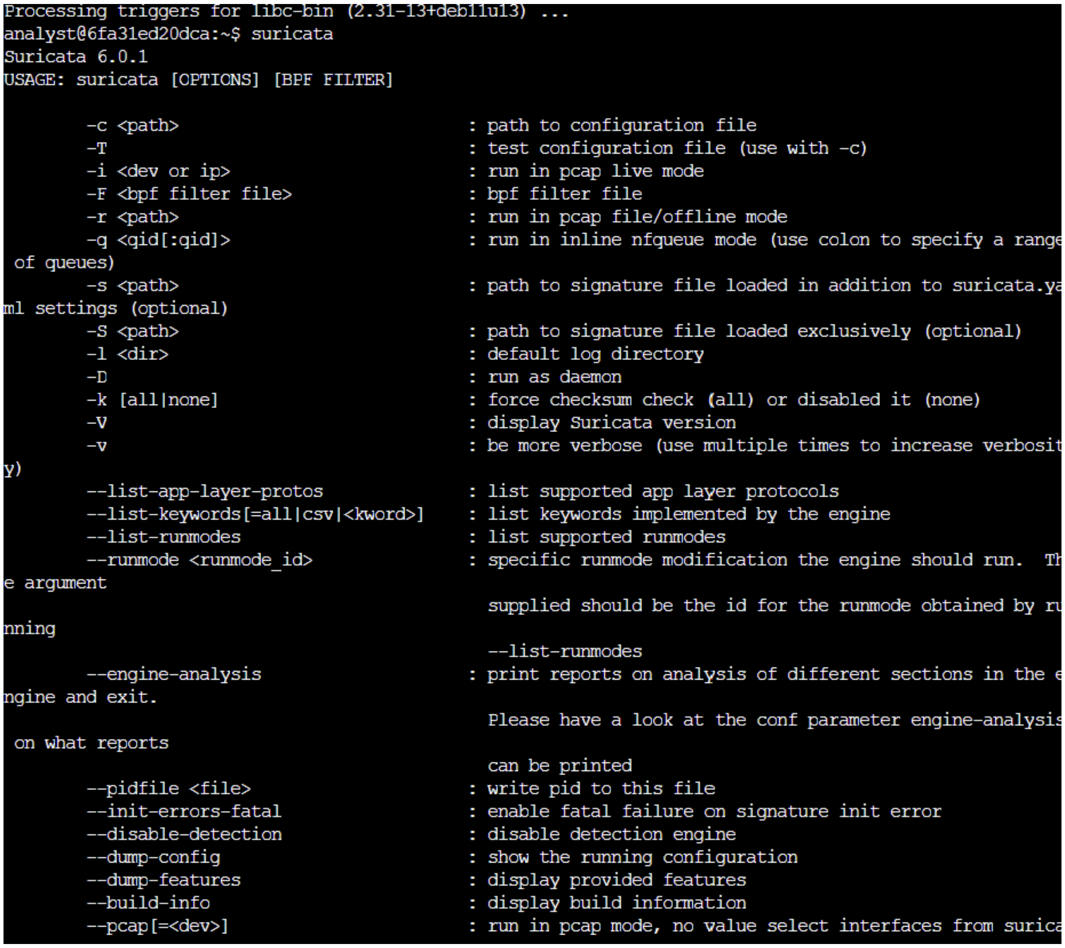
When prompted to continue, press the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)



```
After this operation, 40.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libhyperscan5 amd64 5.4.0-2 [2489 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 python3-simplejson amd64 3.17.2-1 [61.7 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libelf1 amd64 0.183-1 [165 kB]
Get:4 http://deb.debian.org/debian-security bullseye-security/main amd64 libbpf0 amd64 1:0.3-2+deb11u1
[98.5 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 libevent-2.1-7 amd64 2.1.12-stable-1 [188 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 libevent-core-2.1-7 amd64 2.1.12-stable-1 [139 k
B]
Get:7 http://deb.debian.org/debian bullseye/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1 [5
7.1 kB]
Get:8 http://deb.debian.org/debian bullseye/main amd64 libhiredis0.14 amd64 0.14.1-1 [35.5 kB]
Get:9 http://deb.debian.org/debian-security bullseye-security/main amd64 libhtp2 amd64 1:0.5.36-1+deb11
u1 [70.3 kB]
Get:10 http://deb.debian.org/debian bullseye/main amd64 libjansson4 amd64 2.13.1-1.1 [39.7 kB]
Get:11 http://deb.debian.org/debian-security bullseye-security/main amd64 libluajit-5.1-common all 2.1.
0~beta3+dfsg-5.3+deb11u1 [47.3 kB]
Get:12 http://deb.debian.org/debian-security bullseye-security/main amd64 libluajit-5.1-2 amd64 2.1.0~b
eta3+dfsg-5.3+deb11u1 [242 kB]
Get:13 http://deb.debian.org/debian bullseye/main amd64 libmagic-mgc amd64 1:5.39-3+deb11u1 [273 kB]
Get:14 http://deb.debian.org/debian bullseye/main amd64 libmagic1 amd64 1:5.39-3+deb11u1 [128 kB]
Get:15 http://deb.debian.org/debian bullseye/main amd64 libmaxminddb0 amd64 1.5.2-1 [29.8 kB]
Get:16 http://deb.debian.org/debian bullseye/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
Get:17 http://deb.debian.org/debian bullseye/main amd64 libnfnetlink0 amd64 1.0.1-3+b1 [13.9 kB]
Get:18 http://deb.debian.org/debian bullseye/main amd64 libnetfilter-log1 amd64 1.0.1-3 [11.5 kB]
Get:19 http://deb.debian.org/debian bullseye/main amd64 libmnl0 amd64 1.0.4-3 [12.5 kB]
Get:20 http://deb.debian.org/debian bullseye/main amd64 libnetfilter-queue1 amd64 1.0.5-2 [14.5 kB]
Get:21 http://deb.debian.org/debian bullseye/main amd64 libnspr4 amd64 2:4.29-1 [112 kB]
Get:22 http://deb.debian.org/debian-security bullseye-security/main amd64 libnss3 amd64 2:3.61-1+deb11u
4 [1304 kB]
Get:23 http://deb.debian.org/debian bullseye/main amd64 libpcap0.8 amd64 1.10.0-2 [159 kB]
Get:24 http://deb.debian.org/debian bullseye/main amd64 libyaml-0-2 amd64 0.2.2-1 [49.6 kB]
Get:25 http://deb.debian.org/debian-security bullseye-security/main amd64 suricata amd64 1:6.0.1-3+deb1
1u1 [1964 kB]
Get:26 http://deb.debian.org/debian bullseye/main amd64 python3-yaml amd64 5.3.1-5 [138 kB]
Get:27 http://deb.debian.org/debian bullseye/main amd64 suricata-update amd64 1.2.1-1 [58.4 kB]
```

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

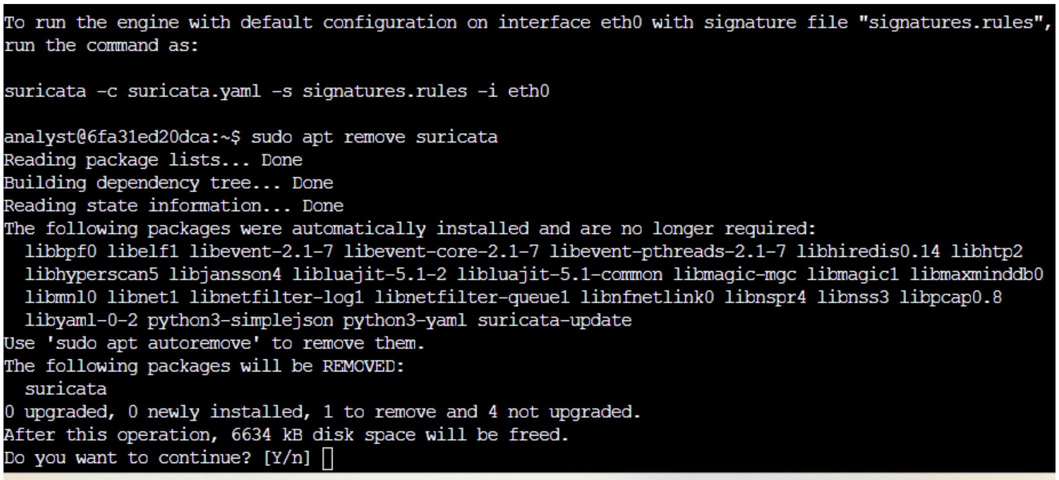
Type suricata after the command-line prompt and press **ENTER**.



```
Processing triggers for libc-bin (2.31-13+deb11u13) ...
analyst@6fa31ed20dca:~$ suricata
Suricata 6.0.1
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                            : path to configuration file
        -T                                   : test configuration file (use with -c)
        -i <dev or ip>                       : run in pcap live mode
        -F <bpf filter file>                 : bpf filter file
        -r <path>                            : run in pcap file/offline mode
        -q <qid[:qid]>                       : run in inline nfqueue mode (use colon to specify a range
 of queues)
        -s <path>                            : path to signature file loaded in addition to suricata.ya
ml settings (optional)
        -S <path>                            : path to signature file loaded exclusively (optional)
        -l <dir>                             : default log directory
        -D                                   : run as daemon
        -k [all|none]                        : force checksum check (all) or disabled it (none)
        -V                                   : display Suricata version
        -v                                   : be more verbose (use multiple times to increase verbosit
y)
        --list-app-layer-protos              : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]    : list keywords implemented by the engine
        --list-runmodes                      : list supported runmodes
        --runmode <runmode_id>               : specific runmode modification the engine should run.  Th
e argument
                                               supplied should be the id for the runmode obtained by ru
nning
                                               --list-runmodes
        --engine-analysis                    : print reports on analysis of different sections in the e
ngine and exit.
                                               Please have a look at the conf parameter engine-analysis
 on what reports
                                               can be printed
        --pidfile <file>                     : write pid to this file
        --init-errors-fatal                  : enable fatal failure on signature init error
        --disable-detection                  : disable detection engine
        --dump-config                        : show the running configuration
        --dump-features                      : display provided features
        --build-info                         : display build information
        --pcap[=<dev>]                       : run in pcap mode, no value select interfaces from surica
```

When Suricata is installed, version and usage information is listed:

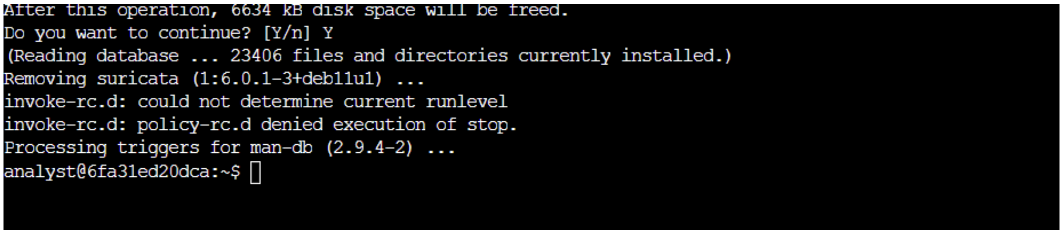
3. Use the APT package manager to uninstall Suricata.



```
To run the engine with default configuration on interface eth0 with signature file "signatures.rules",
run the command as:

suricata -c suricata.yaml -s signatures.rules -i eth0

analyst@6fa31ed20dca:~$ 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 libhtp2
  libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-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 4 not upgraded.
After this operation, 6634 kB disk space will be freed.
Do you want to continue? [Y/n] 
```

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**.)

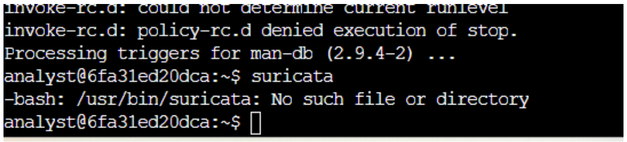


```
After this operation, 6634 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 23406 files and directories currently installed.)
Removing suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.9.4-2) ...
analyst@6fa31ed20dca:~$
```

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:



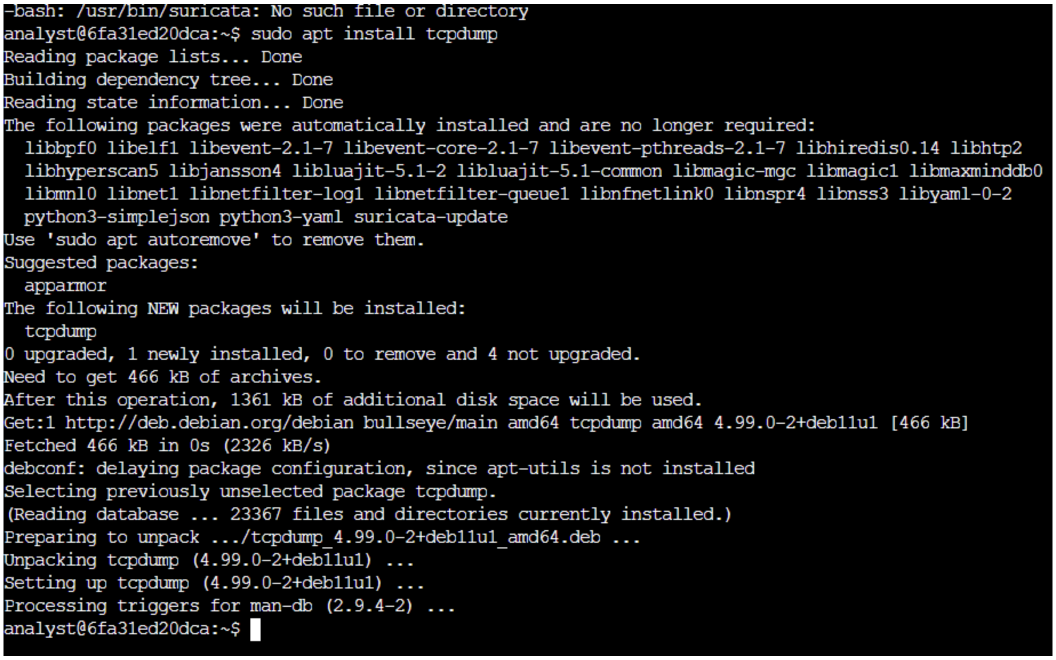
```
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.9.4-2) ...
analyst@6fa31ed20dca:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
analyst@6fa31ed20dca:~$
```

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**.



```
-bash: /usr/bin/suricata: No such file or directory
analyst@6fa31ed20dca:~$ 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 libhtp2
  libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-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 4 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 (2326 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@6fa31ed20dca:~$ 
```

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.

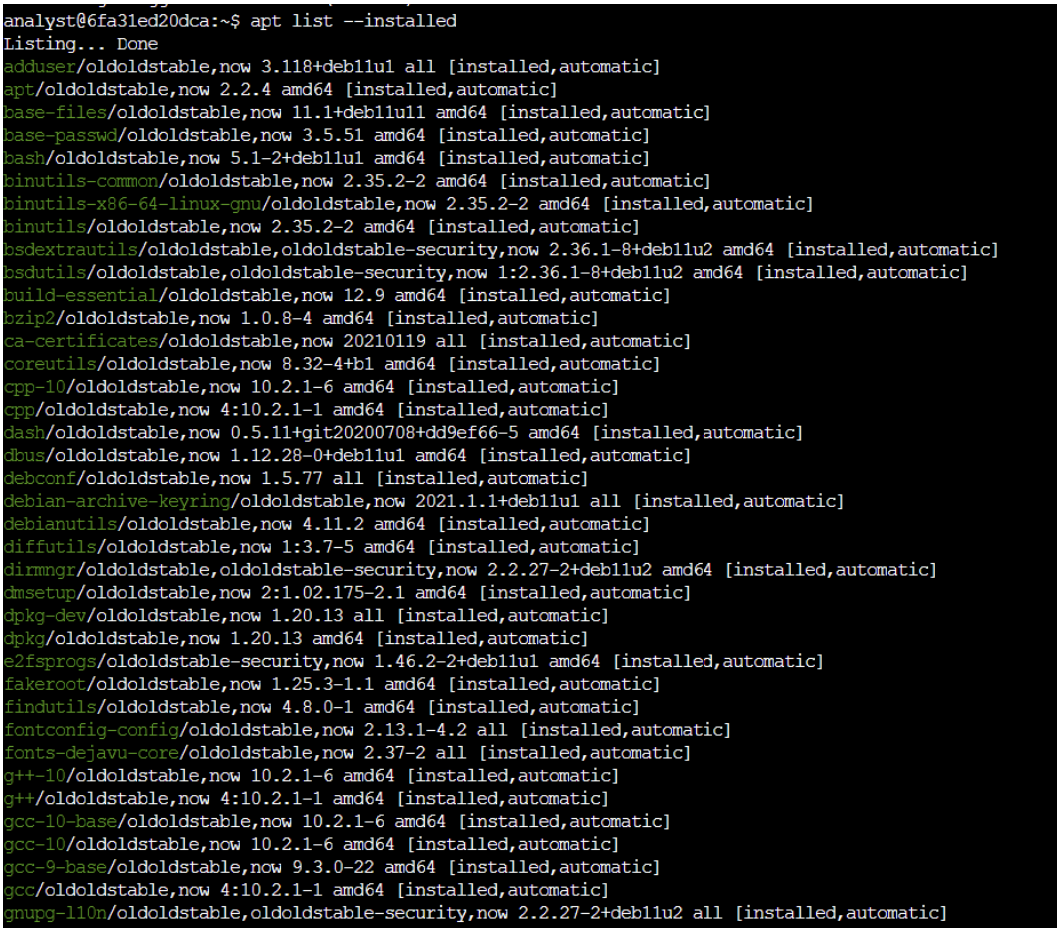
1. Use the APT package manager to list all installed applications.

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:



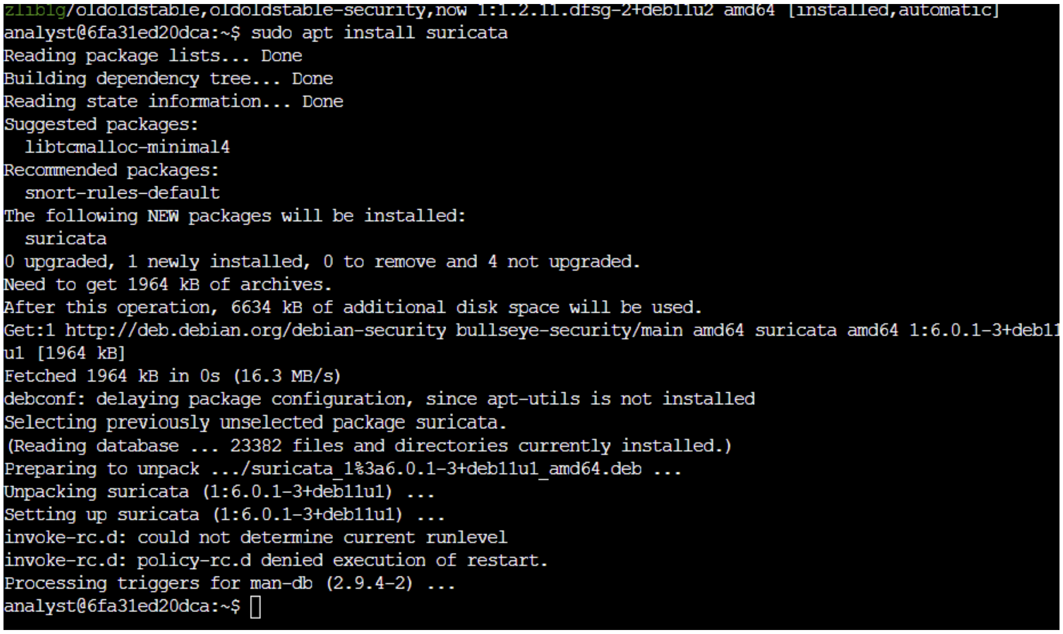
```
analyst@6fa31ed20dca:~$ apt list --installed
Listing... Done
adduser/oldoldstable,now 3.118+deb11u1 all [installed,automatic]
apt/oldoldstable,now 2.2.4 amd64 [installed,automatic]
base-files/oldoldstable,now 11.1+deb11u11 amd64 [installed,automatic]
base-passwd/oldoldstable,now 3.5.51 amd64 [installed,automatic]
bash/oldoldstable,now 5.1-2+deb11u1 amd64 [installed,automatic]
binutils-common/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
binutils-x86-64-linux-gnu/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
binutils/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
bsdextrautils/oldoldstable,oldoldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
bsdutils/oldoldstable,oldoldstable-security,now 1:2.36.1-8+deb11u2 amd64 [installed,automatic]
build-essential/oldoldstable,now 12.9 amd64 [installed,automatic]
bzip2/oldoldstable,now 1.0.8-4 amd64 [installed,automatic]
ca-certificates/oldoldstable,now 20210119 all [installed,automatic]
coreutils/oldoldstable,now 8.32-4+b1 amd64 [installed,automatic]
cpp-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
cpp/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
dash/oldoldstable,now 0.5.11+git20200708+dd9ef66-5 amd64 [installed,automatic]
dbus/oldoldstable,now 1.12.28-0+deb11u1 amd64 [installed,automatic]
debconf/oldoldstable,now 1.5.77 all [installed,automatic]
debian-archive-keyring/oldoldstable,now 2021.1.1+deb11u1 all [installed,automatic]
debianutils/oldoldstable,now 4.11.2 amd64 [installed,automatic]
diffutils/oldoldstable,now 1:3.7-5 amd64 [installed,automatic]
dirmngr/oldoldstable,oldoldstable-security,now 2.2.27-2+deb11u2 amd64 [installed,automatic]
dmsetup/oldoldstable,now 2:1.02.175-2.1 amd64 [installed,automatic]
dpkg-dev/oldoldstable,now 1.20.13 all [installed,automatic]
dpkg/oldoldstable,now 1.20.13 amd64 [installed,automatic]
e2fsprogs/oldoldstable-security,now 1.46.2-2+deb11u1 amd64 [installed,automatic]
fakeroot/oldoldstable,now 1.25.3-1.1 amd64 [installed,automatic]
findutils/oldoldstable,now 4.8.0-1 amd64 [installed,automatic]
fontconfig-config/oldoldstable,now 2.13.1-4.2 all [installed,automatic]
fonts-dejavu-core/oldoldstable,now 2.37-2 all [installed,automatic]
g++-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
g++/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
gcc-10-base/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
gcc-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
gcc-9-base/oldoldstable,now 9.3.0-22 amd64 [installed,automatic]
gcc/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
gnupg-l10n/oldoldstable,oldoldstable-security,now 2.2.27-2+deb11u2 all [installed,automatic]
```

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**.

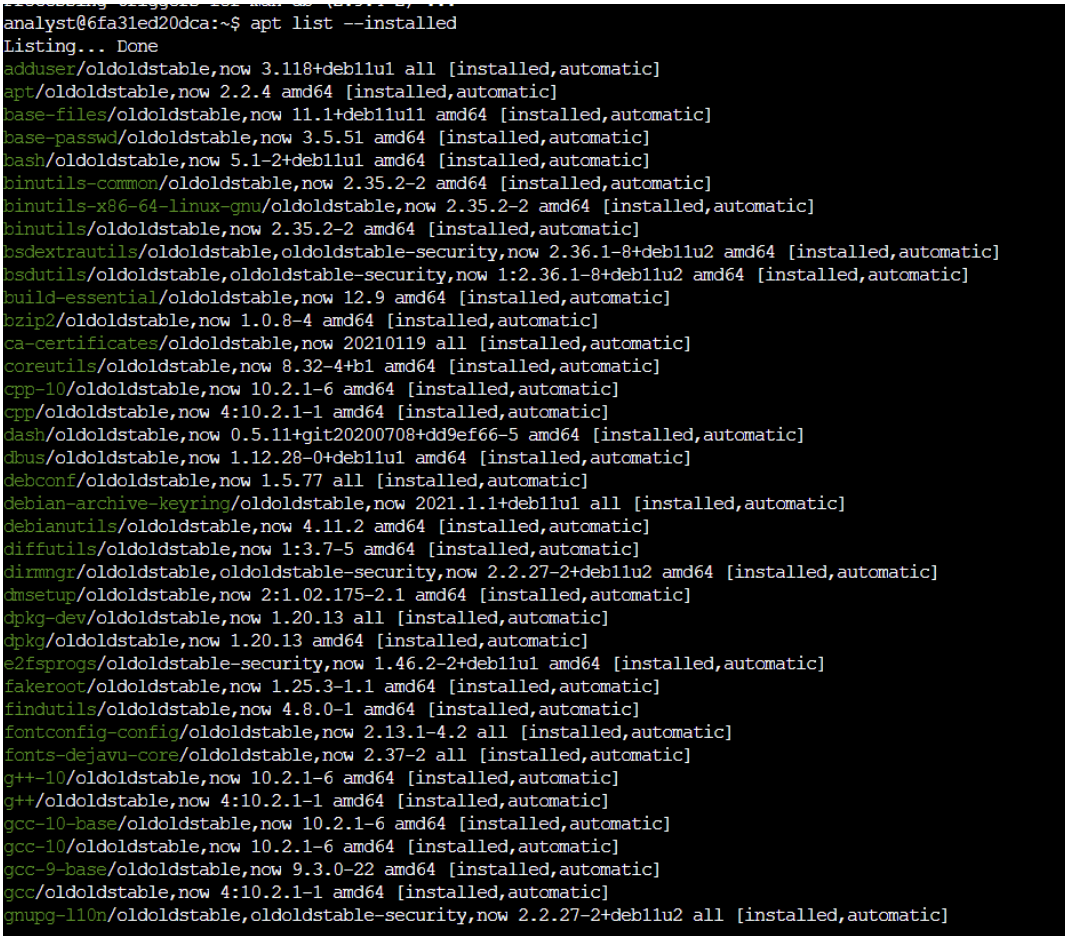


```
zlib1g/oldoldstable,oldoldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
analyst@6fa31ed20dca:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  suricata
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 1964 kB of archives.
After this operation, 6634 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian-security bullseye-security/main amd64 suricata amd64 1:6.0.1-3+deb11
u1 [1964 kB]
Fetched 1964 kB in 0s (16.3 MB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package suricata.
(Reading database ... 23382 files and directories currently installed.)
Preparing to unpack .../suricata_1%3a6.0.1-3+deb11u1_amd64.deb ...
Unpacking suricata (1:6.0.1-3+deb11u1) ...
Setting up suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of restart.
Processing triggers for man-db (2.9.4-2) ...
analyst@6fa31ed20dca:~$ 
```

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.

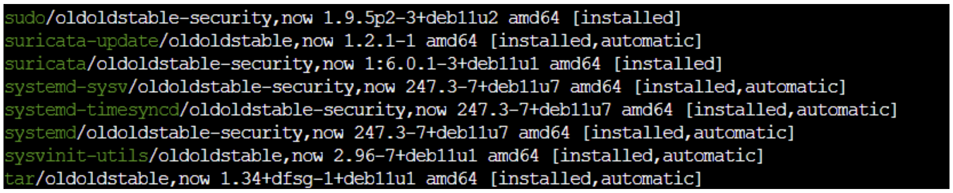
Type apt list --installed after the command-line prompt and press **ENTER**.



```
analyst@6fa31ed20dca:~$ apt list --installed
Listing... Done
adduser/oldoldstable,now 3.118+deb11u1 all [installed,automatic]
apt/oldoldstable,now 2.2.4 amd64 [installed,automatic]
base-files/oldoldstable,now 11.1+deb11u11 amd64 [installed,automatic]
base-passwd/oldoldstable,now 3.5.51 amd64 [installed,automatic]
bash/oldoldstable,now 5.1-2+deb11u1 amd64 [installed,automatic]
binutils-common/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
binutils-x86-64-linux-gnu/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
binutils/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
bsdextrautils/oldoldstable,oldoldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
bsdutils/oldoldstable,oldoldstable-security,now 1:2.36.1-8+deb11u2 amd64 [installed,automatic]
build-essential/oldoldstable,now 12.9 amd64 [installed,automatic]
bzip2/oldoldstable,now 1.0.8-4 amd64 [installed,automatic]
ca-certificates/oldoldstable,now 20210119 all [installed,automatic]
coreutils/oldoldstable,now 8.32-4+b1 amd64 [installed,automatic]
cpp-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
cpp/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
dash/oldoldstable,now 0.5.11+git20200708+dd9ef66-5 amd64 [installed,automatic]
dbus/oldoldstable,now 1.12.28-0+deb11u1 amd64 [installed,automatic]
debconf/oldoldstable,now 1.5.77 all [installed,automatic]
debian-archive-keyring/oldoldstable,now 2021.1.1+deb11u1 all [installed,automatic]
debianutils/oldoldstable,now 4.11.2 amd64 [installed,automatic]
diffutils/oldoldstable,now 1:3.7-5 amd64 [installed,automatic]
dirmngr/oldoldstable,oldoldstable-security,now 2.2.27-2+deb11u2 amd64 [installed,automatic]
dmsetup/oldoldstable,now 2:1.02.175-2.1 amd64 [installed,automatic]
dpkg-dev/oldoldstable,now 1.20.13 all [installed,automatic]
dpkg/oldoldstable,now 1.20.13 amd64 [installed,automatic]
e2fsprogs/oldoldstable-security,now 1.46.2-2+deb11u1 amd64 [installed,automatic]
fakeroot/oldoldstable,now 1.25.3-1.1 amd64 [installed,automatic]
findutils/oldoldstable,now 4.8.0-1 amd64 [installed,automatic]
fontconfig-config/oldoldstable,now 2.13.1-4.2 all [installed,automatic]
fonts-dejavu-core/oldoldstable,now 2.37-2 all [installed,automatic]
g++-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
g++/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
gcc-10-base/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
gcc-10/oldoldstable,now 10.2.1-6 amd64 [installed,automatic]
gcc-9-base/oldoldstable,now 9.3.0-22 amd64 [installed,automatic]
gcc/oldoldstable,now 4:10.2.1-1 amd64 [installed,automatic]
gnupg-l10n/oldoldstable,oldoldstable-security,now 2.2.27-2+deb11u2 all [installed,automatic]
```

3. Search through the list to confirm that the Suricata application has been installed.

The output should include the following lines:



```
sudo/oldoldstable-security,now 1.9.5p2-3+deb11u2 amd64 [installed]
suricata-update/oldoldstable,now 1.2.1-1 amd64 [installed,automatic]
suricata/oldoldstable-security,now 1:6.0.1-3+deb11u1 amd64 [installed]
systemd-sysv/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
systemd-timesyncd/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
systemd/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
sysvinit-utils/oldoldstable,now 2.96-7+deb11u1 amd64 [installed,automatic]
tar/oldoldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
```

Lab Summary: Install Software in a Linux Distribution

Course: Tools of the Trade: Linux and SQL
Lab Environment: Debian-based Linux VM (Bash shell)
Tools Used: APT, sudo, Suricata, tcpdump

Objective

The purpose of this lab was to install, uninstall, and verify network security applications using the APT package manager in a Debian-based Linux virtual machine. The tools used, Suricata and tcpdump, are commonly used by analysts to capture and inspect network traffic. This lab reinforces basic Linux administration skills, which are essential for entry-level cybersecurity roles.

Tasks Completed

Task 1: Confirm APT is installed
Ran the apt command to confirm the APT package manager is available. The expected usage output appeared, indicating APT is installed and functional.

Task 2: Install and uninstall Suricata
Used sudo apt install suricata to install the Suricata application. The lab environment did not prompt for a yes/no confirmation and proceeded automatically. Suricata was verified using the suricata command, which returned version and usage information.
Then removed Suricata using sudo apt remove suricata and confirmed it was uninstalled by rerunning suricata, which returned a command not found error.

Task 3: Install tcpdump
Installed tcpdump using sudo apt install tcpdump. The command completed successfully.

Task 4: List installed applications
Ran apt list --installed to verify installed packages. Confirmed that tcpdump was listed; Suricata was not, as it had been removed earlier.

Task 5: Reinstall Suricata
Reinstalled Suricata using sudo apt install suricata. The lab proceeded without prompting for confirmation. Verified successful installation by running apt list --installed and confirming that both Suricata and tcpdump were listed.

Summary

This lab demonstrated how to use APT and sudo to install, uninstall, and verify applications in a Linux environment. It provided hands-on experience with Suricata and tcpdump, both useful for analyzing and defending network environments. These basic Linux administration tasks are critical skills for analysts working in system-level security or incident response roles.