Activity: Install software in a Linux distribution

Scenario

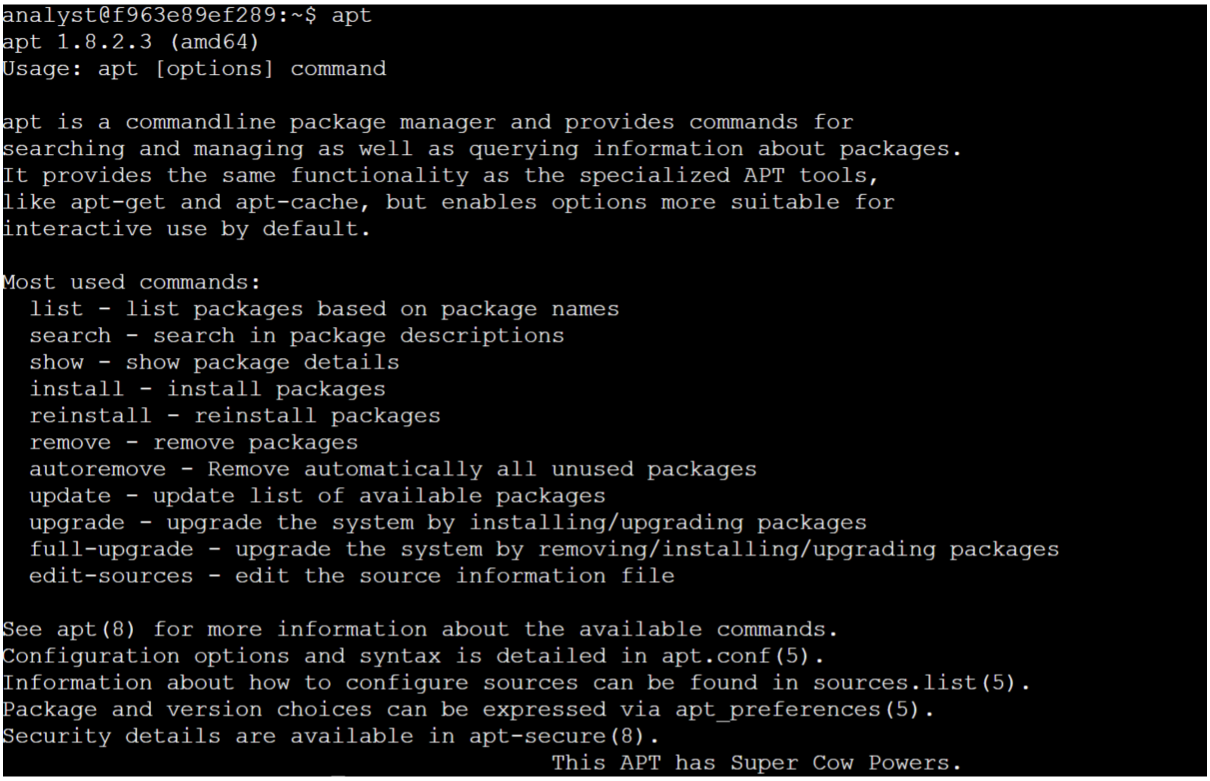
Your role as a security analyst requires that you have the Suricata and tcpdump network security applications installed on your system.

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.

Task 1. Ensure that APT is installed

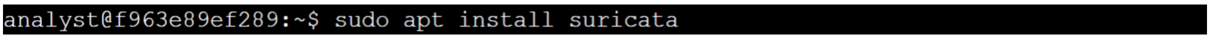
- Confirm that the APT package manager is installed in your Linux environment. To do this, type **apt** after the command-line prompt and press **ENTER**.



```
analyst@f963e89ef289:~$ apt
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.

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

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).
                                        This APT has Super Cow Powers.
```

Task 2. Install and uninstall the Suricata application

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



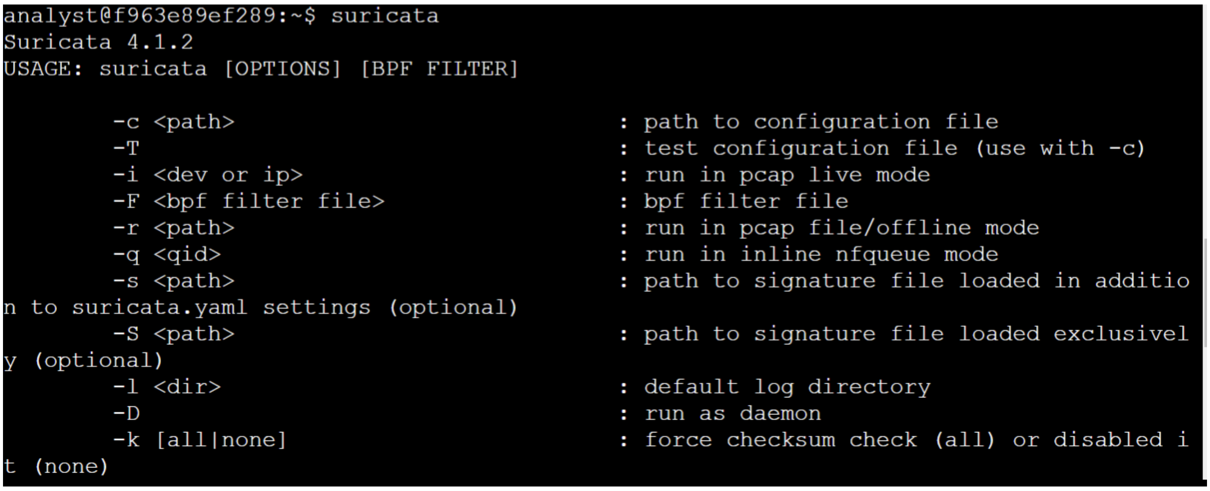
```
analyst@f963e89ef289:~$ sudo apt install suricata
```

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

```
Do you want to continue? [Y/n]
```

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

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

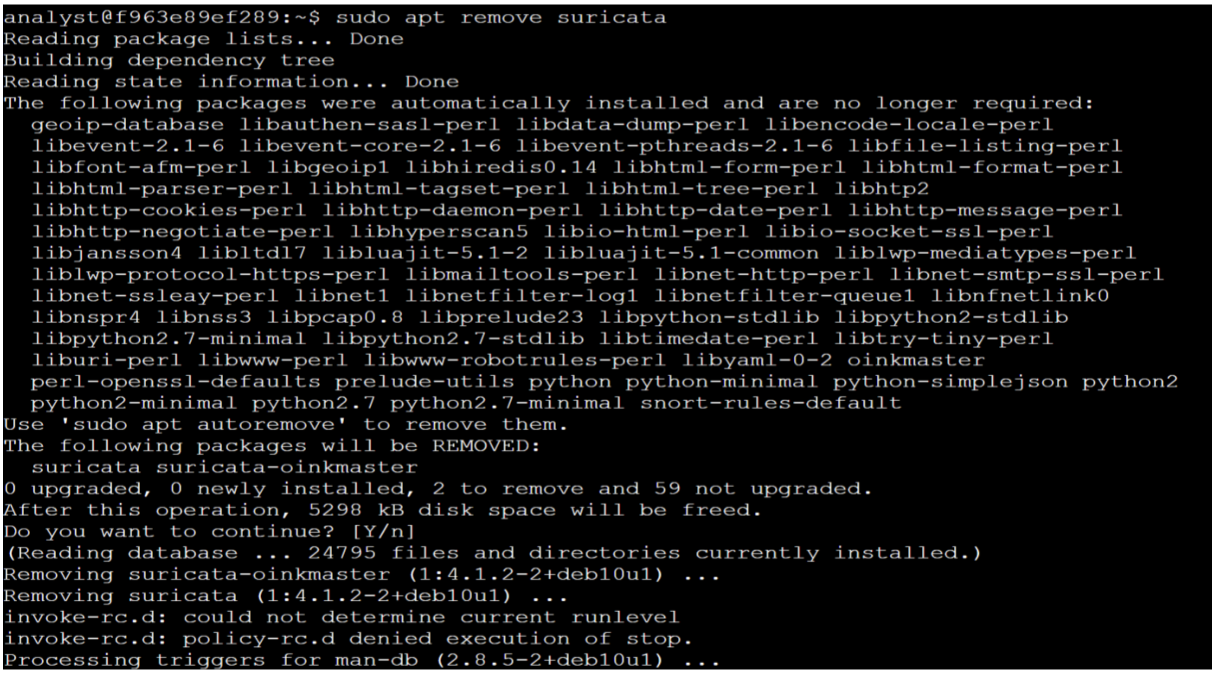


```
analyst@f963e89ef289:~$ suricata
Suricata 4.1.2
USAGE: suricata [OPTIONS] [BPF FILTER]

        -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>                             : run in inline nfqueue mode
        -s <path>                            : path to signature file loaded in additio
n to suricata.yaml settings (optional)
        -S <path>                            : path to signature file loaded exclusivel
y (optional)
        -l <dir>                             : default log directory
        -D                                   : run as daemon
        -k [all|none]                        : force checksum check (all) or disabled i
t (none)
```

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.

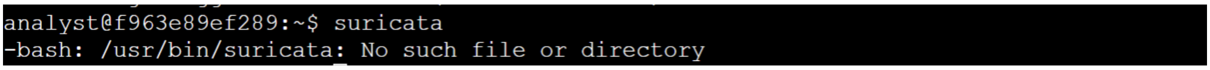
When prompted to continue, press the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)



```
analyst@f963e89ef289:~$ sudo apt remove suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database libauthen-sasl-perl libdata-dump-perl libencode-locale-perl
  libevent-2.1-6 libevent-core-2.1-6 libevent-pthreads-2.1-6 libfile-listing-perl
  libfont-afm-perl libgeoip1 libhiredis0.14 libhtml-form-perl libhtml-format-perl
  libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhtp2
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libhyperscan5 libio-html-perl libio-socket-ssl-perl
  libjansson4 libltdl7 libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
  libnet-ssleay-perl libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0
  libnspr4 libnss3 libpcap0.8 libprelude23 libpython-stdlib libpython2-stdlib
  libpython2.7-minimal libpython2.7-stdlib libtimedate-perl libtry-tiny-perl
  liburi-perl libwww-perl libwww-robotrules-perl libyaml-0-2 oinkmaster
  perl-openssl-defaults prelude-utils python python-minimal python-simplejson python2
  python2-minimal python2.7 python2.7-minimal snort-rules-default
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  suricata suricata-oinkmaster
0 upgraded, 0 newly installed, 2 to remove and 59 not upgraded.
After this operation, 5298 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 24795 files and directories currently installed.)
Removing suricata-oinkmaster (1:4.1.2-2+deb10u1) ...
Removing suricata (1:4.1.2-2+deb10u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.8.5-2+deb10u1) ...
```

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

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

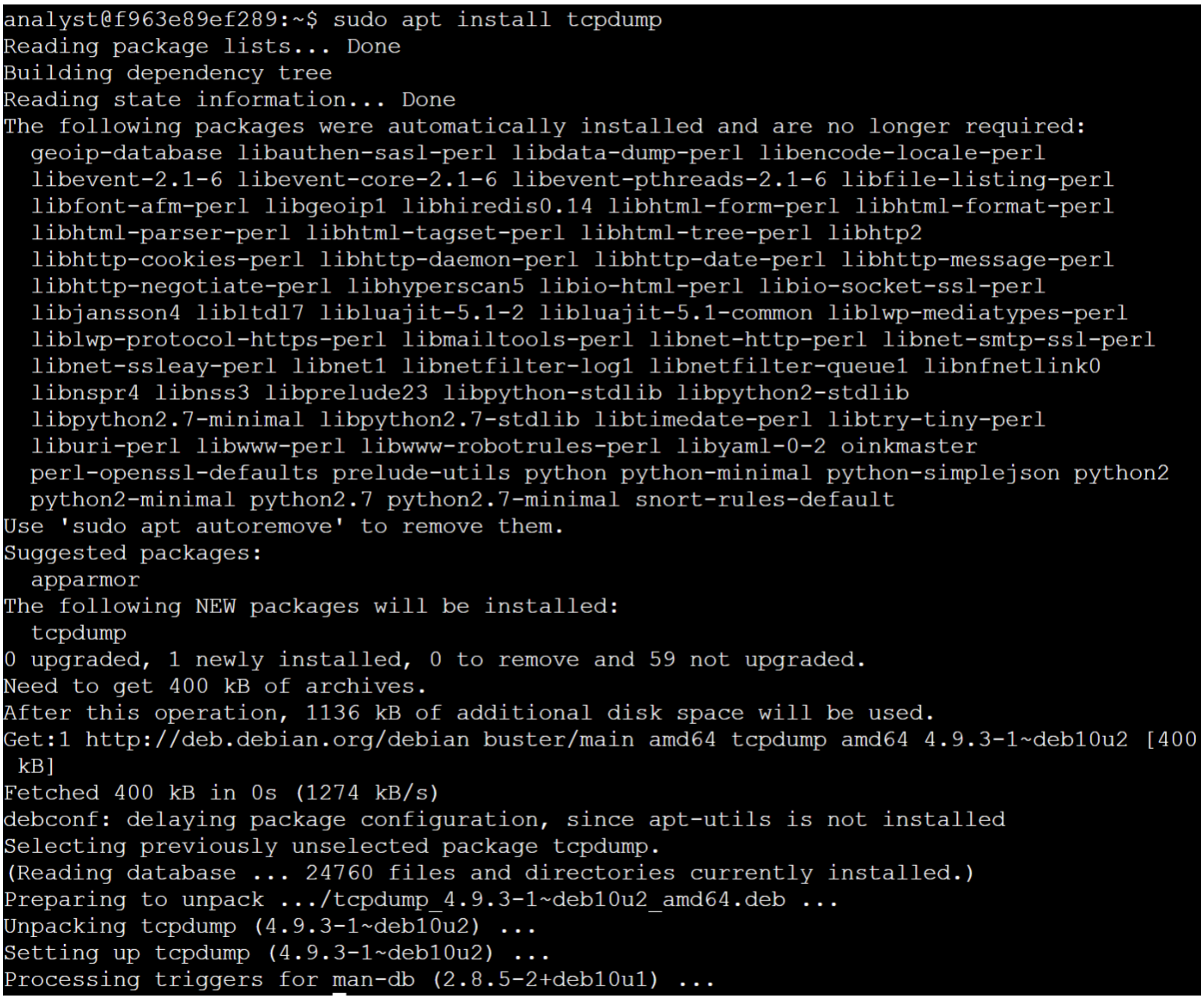


```
analyst@f963e89ef289:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
```

Task 3. Install the tcpdump application

- Use the APT package manager to install tcpdump.

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



```
analyst@f963e89ef289:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database libauthen-sasl-perl libdata-dump-perl libencode-locale-perl
  libevent-2.1-6 libevent-core-2.1-6 libevent-pthreads-2.1-6 libfile-listing-perl
  libfont-afm-perl libgeoip1 libhiredis0.14 libhtml-form-perl libhtml-format-perl
  libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhtp2
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libhyperscan5 libio-html-perl libio-socket-ssl-perl
  libjansson4 libltdl7 libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
  libnet-ssleay-perl libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0
  libnspr4 libnss3 libprelude23 libpython-stdlib libpython2-stdlib
  libpython2.7-minimal libpython2.7-stdlib libtimedate-perl libtry-tiny-perl
  liburi-perl libwww-perl libwww-robotrules-perl libyaml-0-2 oinkmaster
  perl-openssl-defaults prelude-utils python python-minimal python-simplejson python2
  python2-minimal python2.7 python2.7-minimal snort-rules-default
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 59 not upgraded.
Need to get 400 kB of archives.
After this operation, 1136 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 tcpdump amd64 4.9.3-1~deb10u2 [400
 kB]
Fetched 400 kB in 0s (1274 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package tcpdump.
(Reading database ... 24760 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.9.3-1~deb10u2_amd64.deb ...
Unpacking tcpdump (4.9.3-1~deb10u2) ...
Setting up tcpdump (4.9.3-1~deb10u2) ...
Processing triggers for man-db (2.8.5-2+deb10u1) ...
```

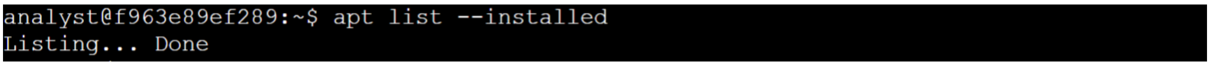
Task 4. List the installed applications

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

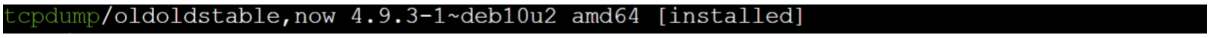
Type **apt list --installed** after the command-line prompt and press **ENTER**.

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@f963e89ef289:~$ apt list --installed
Listing... Done
```



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

Task 5. Reinstall the Suricata application

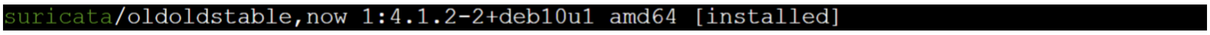
1. Run the command to install the Suricata application.

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

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.



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