Install software in a Linux distribution

Skills Acquired:

- Install applications
- Uninstall applications
- List installed applications.

Scenario:

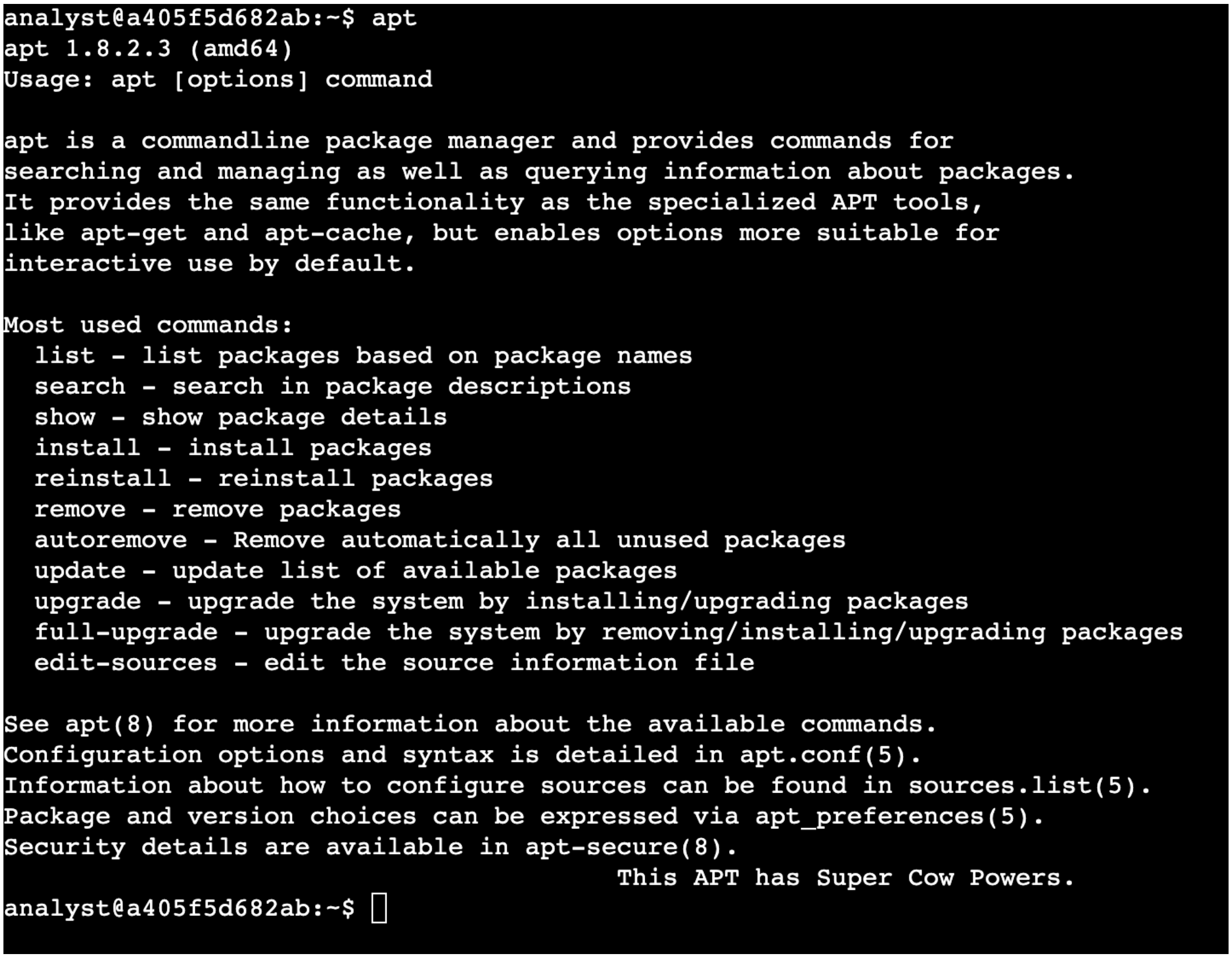
Your role as a security analyst requires that you have the Suricata and tcpdump network security applications installed on your system.

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.

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.

- 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**.

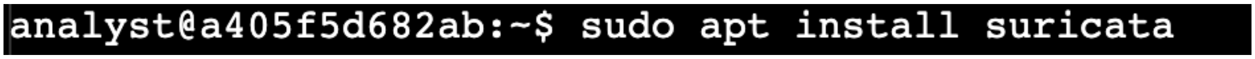


```
analyst@a405f5d682ab:~$ apt
apt 1.8.2.3 (amd64)
Usage: apt [options] command

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.
analyst@a405f5d682ab:~$ 
```

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 is installed correctly. Then, you’ll uninstall the application.

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



```
analyst@a405f5d682ab:~$ sudo apt install suricata
```

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

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

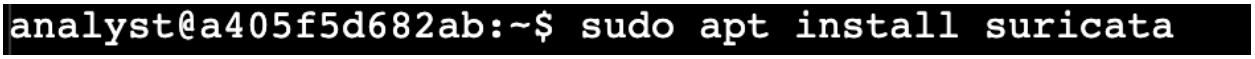
```
-bash: /usr/bin/suricata: No such file or directory
```

This message indicates that Suricata can't be found anymore.

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.



```
analyst@a405f5d682ab:~$ sudo apt install suricata
```

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.

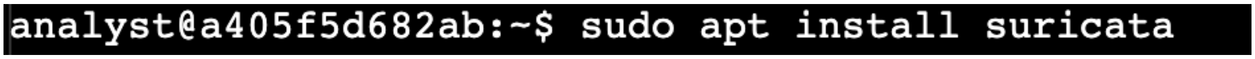
1. Use the APT package manager to list all installed applications.
2. Search through the list to find the tcpdump application you installed.

```
...

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

...
```

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.



```
analyst@a405f5d682ab:~$ sudo apt install suricata
```

2. Use the APT package manager to list the installed applications.
3. Search through the list to confirm that the Suricata application has been installed.

```
...

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

...

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

...
```