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.

1. Ensure APT application installed

Command to check APT installed: apt

```
analyst@55f62d542336:~$ 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@55f62d542336:~$
```

APT is already installed by default in the Linux Bash shell in this lab because this is a Debian-based system. APT is also the recommended package manager for Debian.

2. Install and uninstall the Suricata application

Command to install Suricata: sudo apt install suricata

```
analyst@55f62d542336:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  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 suricata-oinkmaster
Suggested packages:
  libdigest-hmac-perl libgssapi-perl geoip-bin libcrypt-ssleay-perl libauthen-ntlm-perl python-doc python-tk python2-doc python2.7-doc binfmt-support snort
  | snort-pgsql | snort-mysql libtcmalloc-minimal4
The following NEW packages will be installed:
  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 suricata suricata-oinkmaster
0 upgraded, 66 newly installed, 0 to remove and 25 not upgraded.
Need to get 16.8 MB of archives.
After this operation, 62.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Command to verify that Suricata is Installed: suricata

```
analyst@55f62d542336:~$ 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 addition to suricata.yaml 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
```

Command to uninstall Suricata: sudo apt remove suricata

3. Install the tcpdump application

Command to install tcpdump: sudo apt install tcpdump

```
analyst@55f62d542336:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  apparmor
The following NEW packages will be installed:
  tcpdump
0 upgraded, 1 newly installed, 0 to remove and 25 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 (7943 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package tcpdump.
(Reading database ... 24796 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) ...
analyst@55f62d542336:~$
```

Command to uninstall tcpdump: sudo apt remove tcpdump

4. List the installed applications:

Command to check list: apt list –installed