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

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**.

```
analyst@f4853110045f:~$ 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 packa
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.
```

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**.

```
analyst@f4853110045f:~$ 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 59 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] y
```

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

```
analyst@f4853110045f:~$ 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
        -v[v]                               : increase default Suricata verbosity
        --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.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
```

3. Use the APT package manager to uninstall Suricata.

```
analyst@f4853110045f:~$ 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] y
(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.