Activity: Install software in a Linux distribution

Introduction
In this lab, you'll learn how to install and uninstall applications in Linux. You'll use Linux commands in the **Bash shell** to complete this lab. You'll also use the **Advanced Package Tool** (APT) package manager to install and uninstall the Suricata and tcpdump applications.

What you'll do:
You have multiple tasks in this lab:

- Confirm APT is installed in Bash
- Install Suricata with APT
- Uninstall Suricata with APT
- Install tcpdump with APT
- Reinstall Suricata with APT

Activity overview

- In this lab activity, you'll use the **Advanced Package Tool (APT)** and sudo to install and uninstall applications in Ubuntu.
- 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.

As a security analyst, 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 Ubuntu.
- **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.

Start your lab

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**.

When installed, **apt** displays basic usage information when you run it. This includes the version information and a description of the tool:

```
jona@LAPTOP-S454QSVK:~$ apt
apt 2.4.11 (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
  satisfy - satisfy dependency strings
```

APT is the recommended package manager for Debian. If you're using another distribution, a different package manager, such as YUM, may be available instead. Ubuntu is derived from Debian and maintains compatibility with its package management system (APT) and many other aspects of the Debian ecosystem.

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**.

```
jona@LAPTOP-S454QSVK:~$ sudo apt install suricata
[sudo] password for jona:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libclone-perl libdata-dump-perl
  libencode-locale-perl libevent-2.1-7 libevent-pthreads-2.1-7
  libfile-listing-perl libfont-afm-perl 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 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
  libtimedate-perl libtry-tiny-perl liburi-perl libwww-perl
  libwww-robotrules-perl oinkmaster perl-openssl-defaults
  python3-simplejson snort-rules-default suricata-update
Suggested packages:
```

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.

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

- Type **suricata** after the command-line prompt and press **ENTER**.
- When Suricata is installed, version and usage information is listed:

```
jona@LAPTOP-S454QSVK:~$ suricata
Suricata 6.0.4
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.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                                  : be more verbose (use multiple times to increase 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
```

3. Type **`sudo apt remove suricata`** after the command-line prompt and press **ENTER**. Press **ENTER** (**Yes**) when prompted to continue.

```
jona@LAPTOP-S454QSVK:~$ 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:
  libauthen-sasl-perl libclone-perl libdata-dump-perl libencode-locale-perl libevent-2.1-7 libevent-pthreads-2.1-7 libfile-listing-perl libfont-afm-perl
  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 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 libtimedate-perl libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster
  perl-openssl-defaults python3-simplejson snort-rules-default suricata-update
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
```

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:

```
jona@LAPTOP-S454QSVK:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
```

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**.

```
jona@LAPTOP-S454QSVK:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.99.1-3ubuntu0.1).
```

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.

```
jona@LAPTOP-S454QSVK:~$ apt list --installed
Listing... Done
adduser/jammy,now 3.118ubuntu5 all [installed,automatic]
alsa-topology-conf/jammy,now 1.2.5.1-2 all [installed,automatic]
alsa-ucm-conf/jammy-updates,now 1.2.6.3-1ubuntu1.10 all [installed,automatic]
apparmor/jammy-updates,now 3.0.4-2ubuntu2.3 amd64 [installed,automatic]
```

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:

```
tcpdump/jammy-updates,now 4.99.1-3ubuntu0.1 amd64 [installed]
```