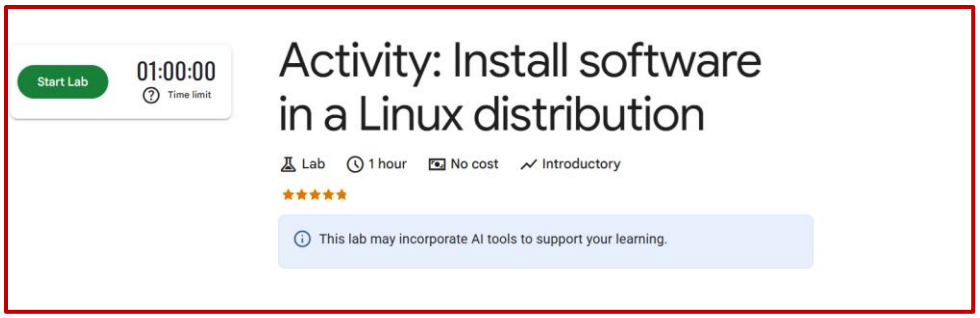


You have multiple tasks in this lab:

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

Task Completed:

Confirm APT is installed in Bash☑
install suricata with APT☑
Uninstall suricata with APT☑
install tcpdump with APT☑
Reinstall suricata with APT☑
List Installed application ☑

🌸 APT (Advanced Package Tool)
🌸 sudo (for admin privileges)
🌸 Applications: Suricata and tcpdump

This lab uses a Debian-based Linux system inside a virtual machine (VM):
👄 Prevents system damage
👄 Allows system reset if needed

As a security analyst, we must know how to:
🌷 Install security tools
🌷 Manage applications
🌷 Confirm tools are correctly installed

TASK 1: CHECK IF APT IS INSTALLED

```
analyst@b9963f02b3b6:~$ apt
apt 2.2.4 (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

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@b9963f02b3b6:~$
```

If APT is installed, it will show:

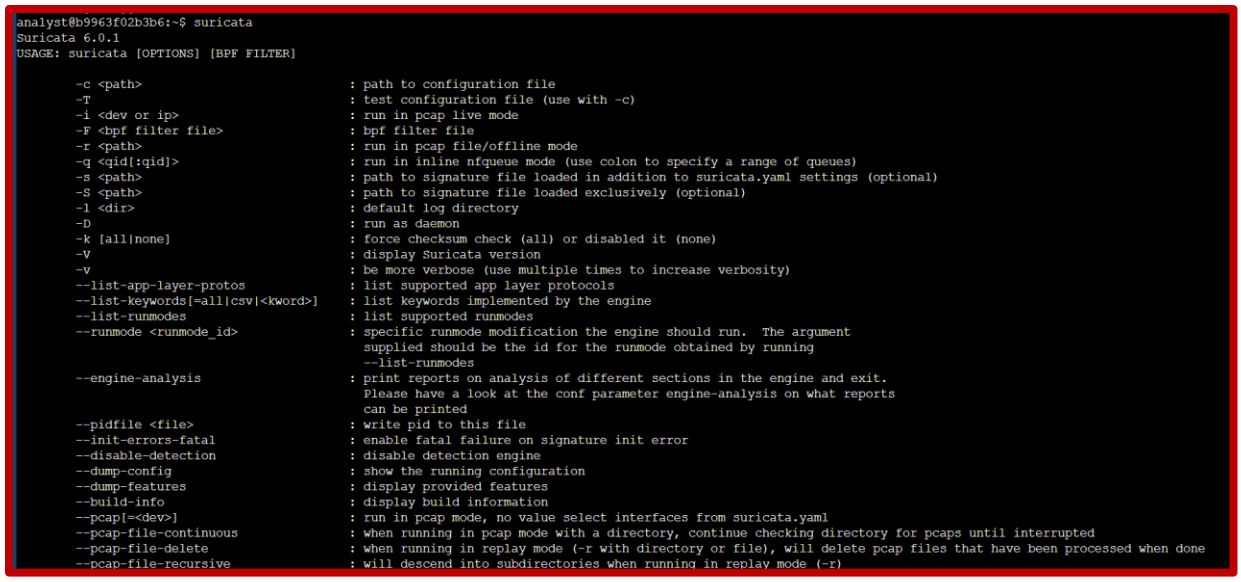
- Version info
- Usage instructions

APT is already installed in Debian systems.

Task 2: Install and Remove Suricata

```
analyst@b9963f02b3b6:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-common
  libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8 libyaml-0-2 python3-simplejson
  python3-yaml suricata-update
Suggested packages:
  file mmdb-bin libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-common
  libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8 libyaml-0-2 python3-simplejson
  python3-yaml suricata suricata-update
0 upgraded, 27 newly installed, 0 to remove and 26 not upgraded.
Need to get 7963 kB of archives.
After this operation, 40.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libhyperscan5 amd64 5.4.0-2 [2489 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 python3-simplejson amd64 3.17.2-1 [61.7 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libelf1 amd64 0.183-1 [165 kB]
Get:4 http://deb.debian.org/debian-security bullseye-security/main amd64 libbpf0 amd64 1:0.3-2+deb11u1 [98.5 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 libevent-2.1-7 amd64 2.1.12-stable-1 [188 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 libevent-core-2.1-7 amd64 2.1.12-stable-1 [139 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1 [57.1 kB]
Get:8 http://deb.debian.org/debian bullseye/main amd64 libhiredis0.14 amd64 0.14.1-1 [35.5 kB]
Get:9 http://deb.debian.org/debian-security bullseye-security/main amd64 libhtp2 amd64 1:0.5.36-1+deb11u1 [70.3 kB]
Get:10 http://deb.debian.org/debian bullseye/main amd64 libjansson4 amd64 2.13.1-1.1 [39.7 kB]
Get:11 http://deb.debian.org/debian-security bullseye-security/main amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-5.3+deb11u1 [47.3 kB]
Get:12 http://deb.debian.org/debian-security bullseye-security/main amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-5.3+deb11u1 [242 kB]
Get:13 http://deb.debian.org/debian bullseye/main amd64 libmagic-mgc amd64 1:5.39-3+deb11u1 [273 kB]
Get:14 http://deb.debian.org/debian bullseye/main amd64 libmagic1 amd64 1:5.39-3+deb11u1 [128 kB]
Get:15 http://deb.debian.org/debian bullseye/main amd64 libmaxminddb0 amd64 1.5.2-1 [29.8 kB]
Get:16 http://deb.debian.org/debian bullseye/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
```

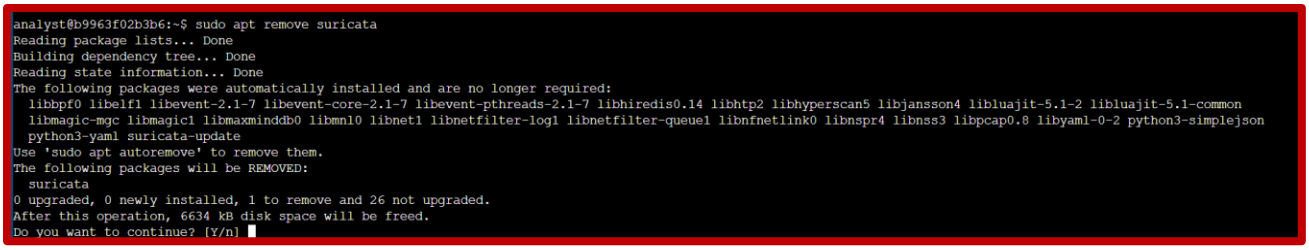
Install Suricata



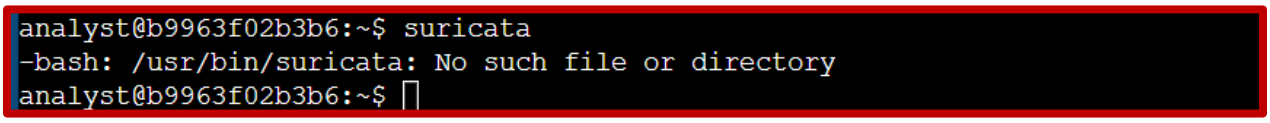
Confirm installation

If installed correctly, it shows:

- Version number
- Usage instructions



Remove Suricata



Confirm Removal Suricata

Task 3: Install tcpdump

```
analyst@b9963f02b3b6:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2 libluajit-5.1-common
  libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libyaml-0-2 python3-simplejson python3-yaml
  suricata-update
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 26 not upgraded.
Need to get 466 kB of archives.
After this operation, 1361 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 tcpdump amd64 4.99.0-2+deb11u1 [466 kB]
Fetched 466 kB in 0s (3693 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package tcpdump.
(Reading database ... 23367 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.99.0-2+deb11u1_amd64.deb ...
Unpacking tcpdump (4.99.0-2+deb11u1) ...
Setting up tcpdump (4.99.0-2+deb11u1) ...
Processing triggers for man-db (2.9.4-2) ...
analyst@b9963f02b3b6:~$
```

This installs a tool used to capture network traffic.

Task 4: List Installed Applications:tcpdump

The command should be: ***apt list --installed*** *but I didn't have the ScreenShot. I just has the result.*

```
tar/oldoldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldoldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldoldstable,now 1.8.0-1+b1 amd64 [installed]
tzdata/now 2025b-0+deb11u1 all [installed,upgradable to: 2025b-0+deb11u2]
ucf/oldoldstable-security,now 3.0043+deb11u2 all [installed,automatic]
util-linux/oldoldstable,oldoldstable-security,now 2.36.1-8+deb11u2 amd64 [installed,automatic]
wget/oldoldstable-security,now 1.21-1+deb11u2 amd64 [installed]
xauth/oldoldstable,now 1:1.1-1 amd64 [installed,automatic]
xz-utils/oldoldstable,oldoldstable-security,now 5.2.5-2.1~deb11u1 amd64 [installed,automatic]
zlib1g-dev/oldoldstable,oldoldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
zlib1g/oldoldstable,oldoldstable-security,now 1:1.2.11.dfsg-2+deb11u2 amd64 [installed,automatic]
analyst@b9963f02b3b6:~$
```

Task 5: Reinstall Suricata

```
analyst@b9963f02b3b6:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  suricata
0 upgraded, 1 newly installed, 0 to remove and 26 not upgraded.
Need to get 1964 kB of archives.
After this operation, 6634 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian-security bullseye-security/main amd64 suricata amd64 1:6.0.1-3+deb11u1 [1964 kB]
Fetched 1964 kB in 0s (16.4 MB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package suricata.
(Reading database ... 23382 files and directories currently installed.)
Preparing to unpack .../suricata_1%3a6.0.1-3+deb11u1_amd64.deb ...
Unpacking suricata (1:6.0.1-3+deb11u1) ...
Setting up suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of restart.
Processing triggers for man-db (2.9.4-2) ...
analyst@b9963f02b3b6:~$
```

Task 6: Check List Installed Applications

```
analyst@b9963f02b3b6:~$ apt list --installed
Listing... Done
adduser/oldoldstable,now 3.118+deb11u1 all [installed,automatic]
apt/oldoldstable,now 2.2.4 amd64 [installed,automatic]
base-files/oldoldstable,now 11.1+deb11u11 amd64 [installed,automatic]
base-passwd/oldoldstable,now 3.5.51 amd64 [installed,automatic]
bash/oldoldstable,now 5.1-2+deb11u1 amd64 [installed,automatic]
binutils-common/oldoldstable,now 2.35.2-2 amd64 [installed,automatic]
```

```
suricata-update/oldoldstable,now 1.2.1-1 amd64 [installed,automatic]
suricata/oldoldstable-security,now 1:6.0.1-3+deb11u1 amd64 [installed]
systemd-sysv/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
systemd-timesyncd/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
systemd/oldoldstable-security,now 247.3-7+deb11u7 amd64 [installed,automatic]
sysvinit-utils/oldoldstable,now 2.96-7+deb11u1 amd64 [installed,automatic]
tar/oldoldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldoldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldoldstable,now 1.8.0-1+b1 amd64 [installed]
```

Suricata and tcpdump