**Scenario**

This role requires to have the Suricata and tcpdump network security applications installed on your system.

**First**, confirm that APT is installed on the Linux Bash shell. **Next**, use APT to install the Suricata application and confirm that it is installed. **Then**, uninstall the Suricata application and confirm this as well. **Finally**, install the tcpdump application and list the applications currently installed.

*The lab starts with a user account, called analyst, already logged in to the Bash shell.*

**Task 1. Ensure that APT is installed**

Typed **apt**after the command-line prompt and pressed **ENTER**.

A screenshot of a computer program

AI-generated content may be incorrect.

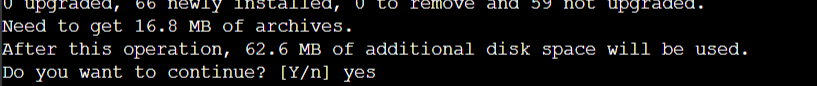
APT is already installed in this Debian-based system.

**Task 2. Install and uninstall the Suricata application**

***Note:****The apt install and apt remove commands must be prefixed with the sudo command as elevated privileges are required to install and uninstall software in Linux.*

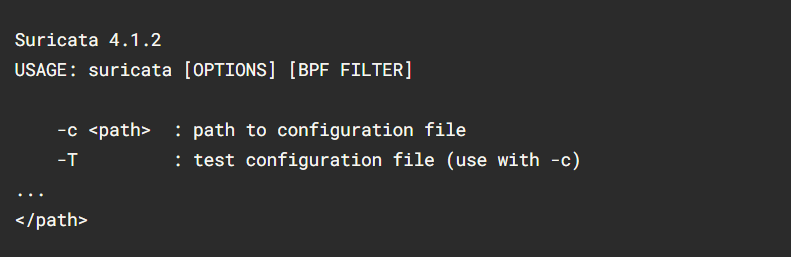
1. Typed **sudo apt install suricata** after the command-line prompt and pressed **ENTER**.

When prompted to continue, pressed the **ENTER** key to respond with the default response. (In this case, the default response is **Yes**.)

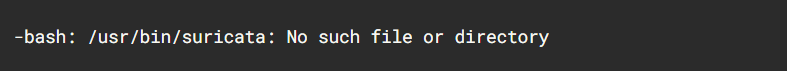


1. Typed **suricata**after the command-line prompt and pressed **ENTER** to verify that Suricata is installed.

When Suricata is installed, version and usage information is listed:



1. Typed **sudo apt remove suricata** after the command-line prompt and press **ENTER** to uninstall Suricata. Pressed **ENTER** (**Yes**) when prompted to continue.
2. Typed **suricata** after the command-line prompt and pressed **ENTER.**



The output is an error message so suricata is uninstalled.

**Task 3. Install the tcpdump application**

Typed **sudo apt install tcpdump** after the command-line prompt and pressed **ENTER.**

A black screen with white text

AI-generated content may be incorrect.

**Task 4. List the installed applications**

1. Typed **apt list --installed** after the command-line prompt and pressed ENTER.

This produces an extensive list of applications because Linux has a lot of software installed by default.

1. Searched through the list to find the tcpdump application we installed

A black background with white text

AI-generated content may be incorrect.