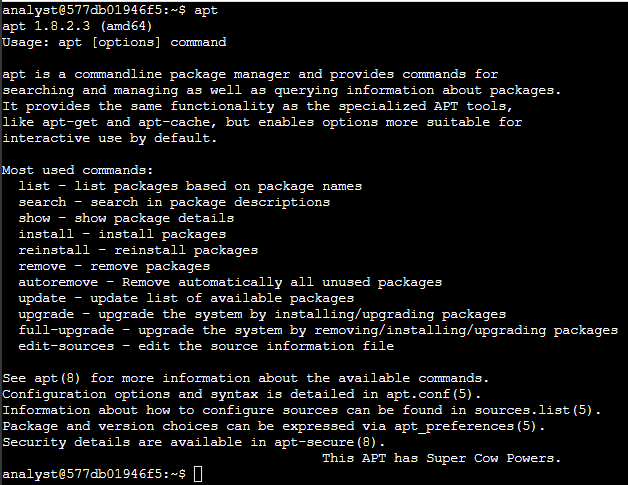
# Install software in a Linux distribution

## Project description

My role as a security analyst requires that we have the Suricata and tcpdump network security applications installed on my system. In this scenario, I will demonstrate how to install, uninstall, and reinstall these applications on my Linux Bash shell. I will also confirm that I have installed them correctly.

## Task 1. Ensure that APT is installed

First, I’ll check that the APT application is installed so that I 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.

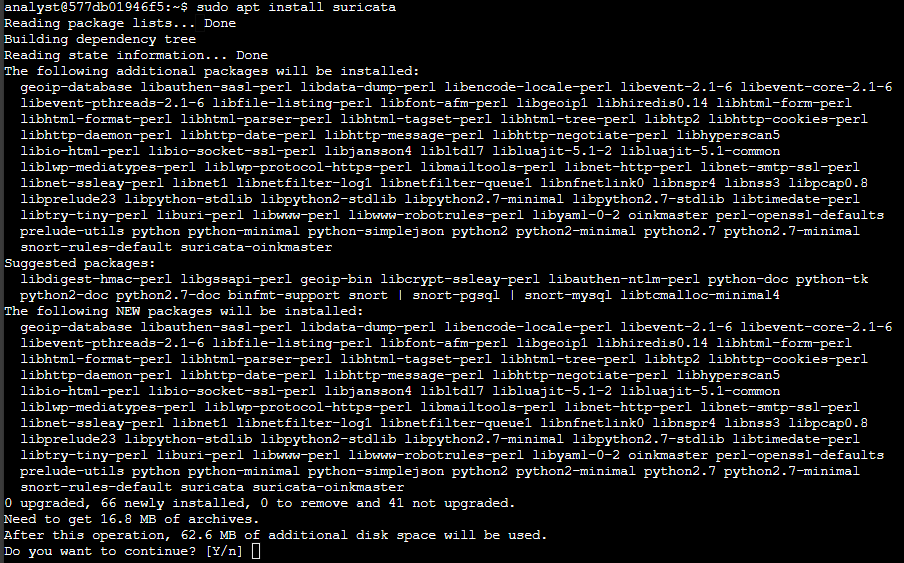
The Bash shell is the command-line interpreter currently open on the left side of the screen. I’ll use the Bash shell by typing commands after the prompt. The prompt is represented by a dollar sign ($) followed by the input cursor.

## Install and uninstall the Suricata applicationRetrieve login attempts on specific dates

In this task, I will install Suricata, a network analysis tool used for intrusion detection, and verify that it installed correctly. Then, I’ll uninstall the application.

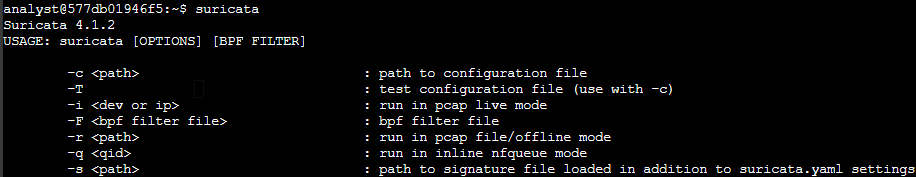
In order to install applications, I need to user the super user command sudo

I use the following commands : sudo apt install suricata



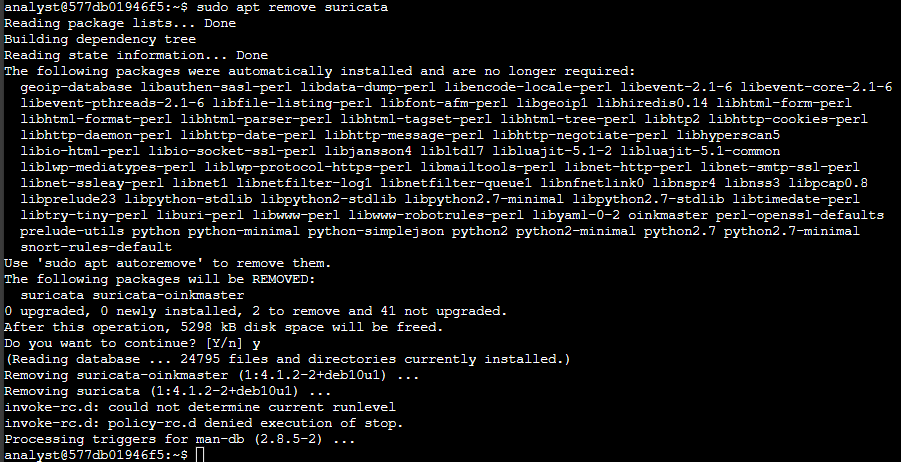
In order to verify a successful install of Suricata

I use the following commands : suricata



I will use the APT package manager to uninstall Suricata. In order to perform a uninstallation, I require superuser privileges sudo.

I use the following commands : sudo apt remove suricata



To verify that Suricata has been uninstalled, I will attempt to run the application command again.

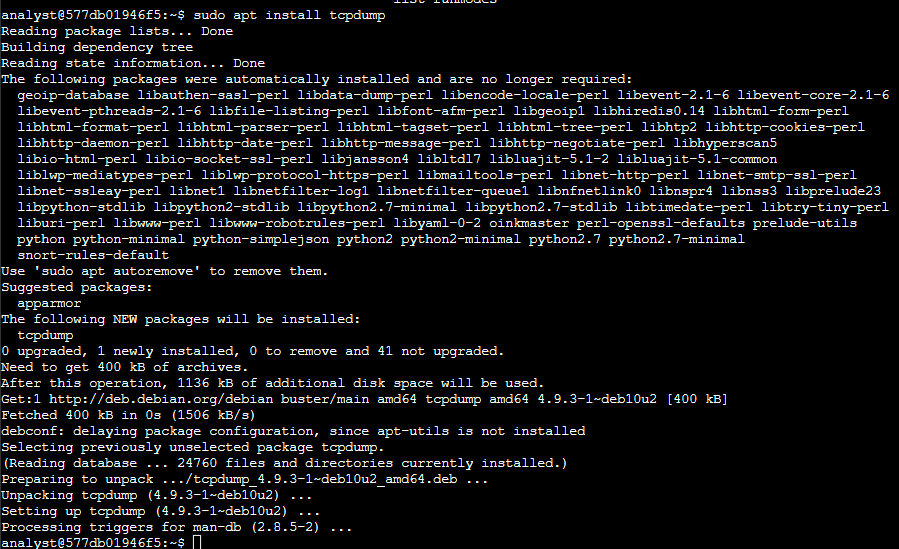
I use the following commands : suricata



## Install the tcpdump application

In this task, I will install the tcpdump application. This is a command-line tool that can be used to capture network traffic in a Linux Bash shell.

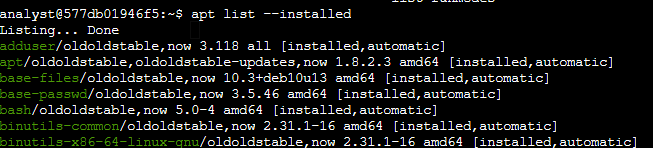
I use the following commands : sudo apt install tcpdump



## List the installed applications

Next, I will confirm that I’ve installed the required applications. It's important to be able to validate that the correct applications are installed.

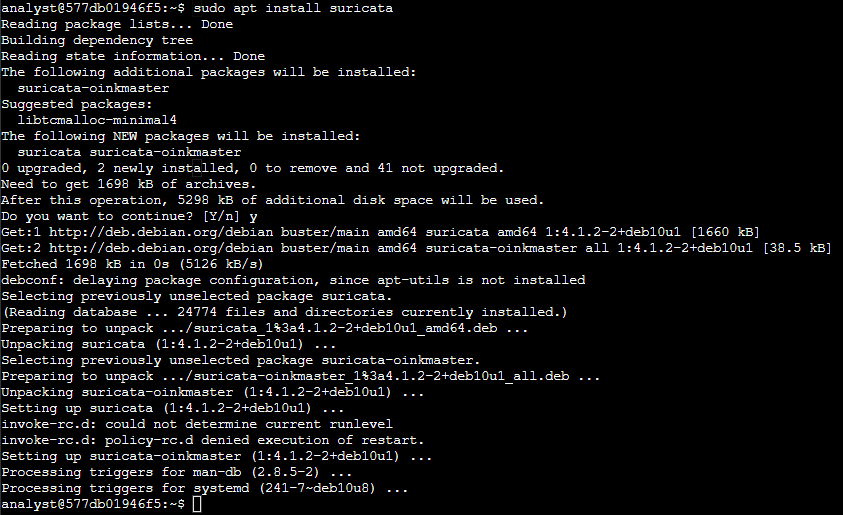
I use the following commands : sudo apt install tcpdump



## Reinstall the Suricata application

In this task, I will reinstall the Suricata application and verify that it has installed correctly.

I use the following commands : sudo apt install suricata



I will use the APT package manager to list the installed applications, look for suricata

I use the following commands : apt list --installed



## Summary

I have demonstrated how to

1. Install applications,
2. Uninstall applications, and
3. List installed applications.

Being able to manage installed applications in Linux is a key skill for any security analyst.