Install software in a Linux distribution

Scenario

My role as a security analyst requires that I have the Suricata and tcpdump network security applications installed on a system.

In this scenario, I must install, uninstall, and reinstall these applications on the Linux Bash shell. I also need to confirm that I've installed them correctly.

Here's how I'll do this: **First**, I'll confirm that APT is installed on the Linux Bash shell. **Next**, I'll use APT to install the Suricata application and ensure that it is installed. **Then**, I'll uninstall the Suricata application and confirm this as well. **Next**, I'll install the tcpdump application and list the applications currently installed. **Finally**, I'll reinstall the Suricata application and ensure that both applications are installed.

1. Ensure that APT is installed

First, I checked that the APT application was 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 command to complete this step:

```
Apt
```

2. Install and uninstall the Suricata application

In this task, I installed Suricata, a network analysis tool used for intrusion detection, and verify that it is installed correctly. Then, I uninstalled the application.

1. I used the APT package manager to install the Suricata application.

```
sudo apt install suricata
```

The Suricata application can take a few minutes to install.

2. I verified that Suricata is installed by running the newly installed application.

The command to complete this step:

```
suricata
```

3. I used the APT package manager to uninstall Suricata.

The command to complete this step:

```
sudo apt remove suricata
```

4. I verified that Suricata has been uninstalled by running the application command again.

The command to complete this step:

```
Suricata
```

3. Install the tcpdump application

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

The command to complete this step:

```
sudo apt install tcpdump
```

4. List the installed applications

Next, I need to confirm that I've installed the required applications. It's important to be able to validate that the correct applications are installed. Often I may want to check that the correct versions are installed as well.

1. I used the APT package manager to list all installed applications.

The command to complete this step:

```
apt list --installed
```

2. I searched through the list to find the tcpdump application I installed.

5. Reinstall the Suricata application

In this task, I reinstalled the Suricata application and verified that it was installed correctly.

1. I ran the command to install the Suricata application.

The command to complete this step:

```
sudo apt install suricata
```

2. I used the APT package manager to list the installed applications.

The command to complete this step:

```
apt list --installed
```

6. Conclusion

In this scenario, we successfully installed, uninstalled, and reinstalled Suricata and tcpdump on the Linux Bash shell. We confirmed that the applications were installed correctly by checking the version numbers and listing the applications currently installed. We also noted that we first need to confirm that APT is installed before we can install Suricata or tcpdump. Finally, we mentioned that we can also uninstall and reinstall Suricata and tcpdump using the `sudo apt remove` and `sudo apt install` commands.