■ Project Title: Linux Package Management and Network Analysis Tool Installation

This lab provided hands-on experience using the APT (Advanced Package Tool) package manager in a Debian-based Linux environment to install, manage, and verify cybersecurity applications. It reinforced essential system administration and security operations skills that are critical for analysts working in network defense, incident response, and threat detection roles. Through a series of guided tasks, I installed, uninstalled, and verified applications such as Suricata and Tcpdump, two industry-standard tools for network monitoring and intrusion detection. This activity strengthened my understanding of Linux package management, dependency handling, and command-line efficiency — foundational competencies for configuring and maintaining secure systems.

Task 1: Verify APT Installation
- Used the apt command to confirm that the Advanced Package Tool (APT) was installed and operational.
- Observed the output to validate that the package manager was functioning correctly. - Gained insight into APT's capabilities, including installation, updates, upgrades, and package queries.

Task 2: Install and Uninstall Suricata
- Installed Suricata, a network intrusion detection system (NIDS), using sudo apt install suricata. - Verified installation by running the suricata command.
- Practiced uninstallation using sudo apt remove suricata and confirmed removal.

Task 3: Install Tcpdump
- Installed Tcpdump, a command-line network capture utility, using APT.
- Verified installation using apt list --installed.

Task 4: List Installed Applications
- Used apt list --installed to view installed packages.
- Verified that Tcpdump appeared and Suricata was removed.

Task 5: Reinstall Suricata
- Reinstalled Suricata to reinforce command repetition and ensure functionality. - Verified Suricata and Tcpdump installations.

Technical Tools and Commands Used
- APT (Advanced Package Tool)
- Suricata
- Tcpdump
- Sudo (Superuser Do)
- Bash Terminal

Key Takeaways

- Gained hands-on experience with Linux software installation and management. - Learned how to install, remove, and verify security tools using APT.
- Developed comfort with the Bash terminal and interpreting output logs.
- Strengthened understanding of network analysis tools used in SOC workflows.

Conclusion

This lab demonstrated the ability to manage and maintain key cybersecurity tools in a Linux environment — a core skill for analysts responsible for network defense and intrusion detection. Installing and verifying tools such as Suricata and Tcpdump provides practical grounding in network monitoring, log analysis, and packet-level threat detection across enterprise systems.