Cybersecurity Daily Dairy

Day 11: Ubuntu Installation and Snort Setup

Date: June 30, 2025

Topics Covered:

- Installation of the Ubuntu operating system
- Installation of Snort Intrusion Detection System (IDS)
- Initial configuration and verification steps

What I Did:

Today, I installed the **Ubuntu operating system** on a virtual machine and followed up with the installation of **Snort**, a widely used open-source **Intrusion Detection System (IDS)**. The main objective was to understand how to configure Snort during installation and confirm that it is monitoring network traffic correctly.

Ubuntu Installation:

- Downloaded the **Ubuntu ISO** file from the official website.
- Used **VirtualBox** to create a virtual machine and booted from the ISO.
- Went through the installation steps:
    - Selected preferred language and keyboard layout
    - Chose time zone and created user credentials
    - Installed updates and completed the setup

Snort Installation:

- After Ubuntu was ready, I updated the package list and installed Snort using the system's package manager.
- During installation, a configuration prompt appeared:
    - It displayed the **local IP address** of the system
    - I selected the **default option** to proceed
- Once complete, Snort was installed and ready for basic packet capture and analysis.

Key Learnings:

- **Ubuntu** is a user-friendly and stable Linux distro commonly used in security labs and virtual environments.

- **Snort** is an effective tool for real-time traffic analysis and packet logging.
- Understanding **interface binding and configuration** during setup is critical for Snort to function correctly.
- This foundational setup prepares the environment for further IDS rule customization and testing.

By Ritesh Kumar Gupta CRN : 2315195 URN : 2302650