

CYBERSECURITY DAILY DAIRY

Day 11: Ubuntu Installation and Snort Setup (June 30, 2025)

Topics Covered:

- Installation of Ubuntu OS.
- Installation of Snort Intrusion Detection System (IDS).
- Initial configuration and verification.

What I Did:

I installed **Ubuntu** in a virtual machine and then **Snort**, an open-source **Intrusion Detection System (IDS)**, to monitor network traffic.

Ubuntu Installation:

- Downloaded **Ubuntu ISO**.
- Created VM in **VirtualBox**, booted from ISO.
- Followed installation steps (language, keyboard, time zone, user, updates).

Snort Installation:

- Updated package list, installed Snort.
- During setup, selected default option for local IP address.
- Snort was ready for packet capture.

Key Learnings:

- **Ubuntu** is a user-friendly Linux distro for security labs.
- **Snort** is good for real-time traffic analysis.
- Correct interface configuration is vital for Snort.
- This setup prepares for further IDS rule testing.