Day 29

Exploitation Analyst

Security Patching:

What is Security Patching in Ubuntu?

Security patching means applying security updates released by Ubuntu to fix vulnerabilities in packages like OpenSSL, Apache, kernel, etc.

- These updates are published in dedicated security repositories.
- Keeping them enabled and up to date is essential for hardening a system against known exploits (e.g., buffer overflows, privilege escalation)

Role of /etc/apt/sources.list

This file tells apt where to fetch updates/packages from — including:

Repo Type	Purpose
main	Official supported packages
universe	Community-maintained packages
security	Security patches for core packages
updates	Bug fixes and minor updates

To enable security patching, your /etc/apt/sources.list must include the security repo.
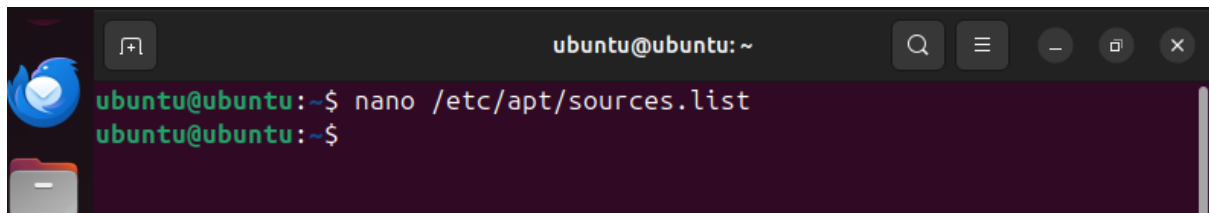
To decide what to add we need to know the codename for the ubuntu. For which we can use the command: lsb_release -c

Clearly the code name is 'noble'. Now, we can configure it further to make things happened smoothly.
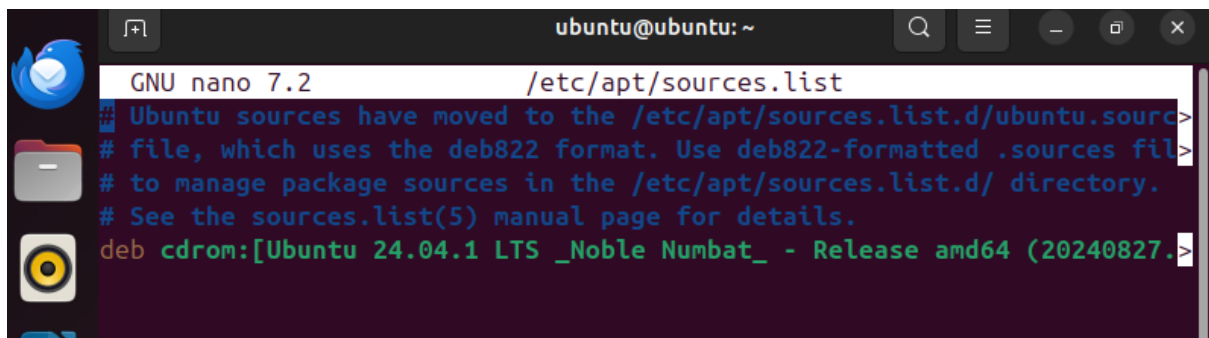
Sample /etc/apt/sources.list With Security Patching:

Open the sources.list using the "nano" command:

Following screen will appear:

Paste the text as shown below: then save the buffer and exit.
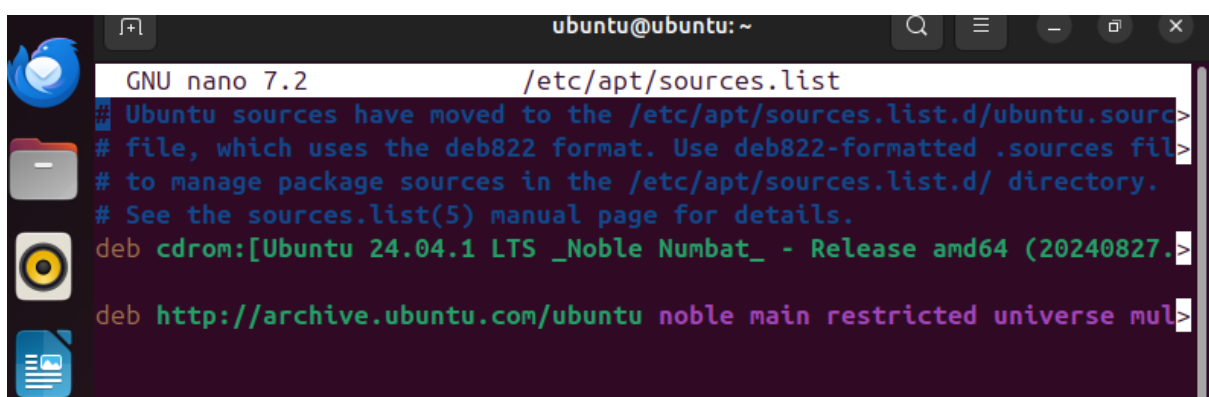
Main Ubuntu repository

deb http://archive.ubuntu.com/ubuntu noble main restricted universe multiverse

Updates (non-security)

deb http://archive.ubuntu.com/ubuntu noble-updates main restricted universe multiverse
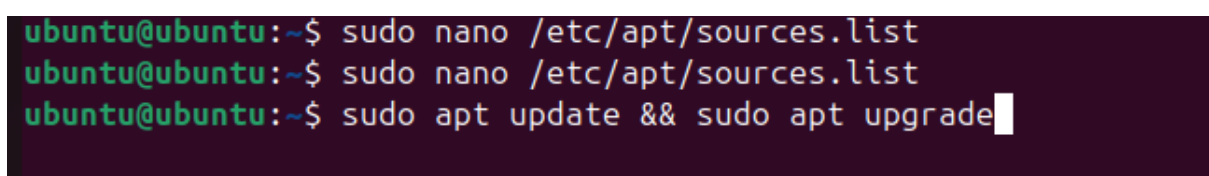
Security updates

deb http://security.ubuntu.com/ubuntu noble-security main restricted universe multiverse

Then update and apply the patches:

What we changed above?

Before editing the /etc/apt/sources.list, your system was getting general updates but not guaranteed security patches. By adding the noble-security entries, you enabled a dedicated security channel that delivers faster and targeted fixes for vulnerabilities. This ensures your system stays protected from known threats and follows proper cybersecurity hardening practices.

--The End--