CYBER SECURITY INTERNSHIP

Task 14: Linux Server Hardening & Secure Configuration

Tools Used:

- Ubuntu / Kali Linux
- UFW (Firewall)
- OpenSSH
- Lynis (Security Auditing Tool)
- System Logs (/var/log/)

Linux Hardening Checklist:

- Reviewed default users, services, and open ports using netstat/ss.
- Removed unused user accounts and restricted sudo access (principle of least privilege).
- Disabled root SSH login and enabled key-based authentication.
- Updated all system packages and enabled automatic security updates.
- Configured UFW firewall to allow only required ports (e.g., SSH).
- Disabled unnecessary services using systemctl.
- Hardened file permissions for sensitive files (e.g., /etc/passwd, /etc/shadow).
- Reviewed authentication logs for suspicious activity.

Security Configuration Summary:

The Linux server was hardened by minimizing attack surface, enforcing secure authentication, restricting unnecessary services, and implementing firewall rules. Root login was disabled, SSH was secured using key-based authentication, and automatic updates were enabled to ensure continuous patching. Logs were monitored to detect abnormal activity. These measures significantly reduce exposure to brute-force attacks, privilege escalation, and unauthorized access.

Interview Questions & Answers:

- What is server hardening? → The process of securing a server by reducing vulnerabilities and minimizing attack surface.
- Why disable root login? → To prevent direct brute-force attacks and enforce controlled privilege escalation.
- What is least privilege? → Users are given only the minimum access required to perform their tasks.

- Purpose of firewall? → To filter network traffic and allow only authorized connections.
- Risks of unused services? → They increase attack surface and may contain exploitable vulnerabilities.