CYBER SECURITY INTERNSHIP – TASK 2 REPORT

Operating System Security Fundamentals (Linux)

Student Name: Lithin Kumar

Platform Used: Kali GNU/Linux Rolling
Tools: UFW Firewall, Linux Terminal

1. Introduction
Operating System (OS) security is the foundation of cybersecurity. If an OS is weak, attackers can exploit it to gain unauthorized access, steal data, or control the system. In this task, I learned how to secure a Linux system using basic OS hardening techniques such as user control, file permissions, firewall configuration, and service management.

2. Steps Performed
- Installed and enabled UFW firewall in Kali Linux.
- Understood user roles: root vs normal user.
- Learned Linux file permissions using chmod and chown.
- Checked running processes and services.
- Disabled unnecessary services to reduce attack surface.
- Created an OS security checklist.

3. Firewall Configuration (UFW)
Kali Linux does not come with UFW by default. I installed it using apt and enabled it to protect the system from unauthorized network traffic. The firewall blocks unknown connections and only allows trusted services like SSH when required.

Commands Used:
sudo apt update
sudo apt install ufw -y
sudo ufw enable
sudo ufw status

4. File Permissions in Linux
Linux uses read (r), write (w), and execute (x) permissions for files and directories. Permissions are assigned to the owner, group, and others. Using chmod, I changed file permissions, and using chown, I changed file ownership to improve security.

Example:
chmod 700 file.txt
chown user1 file.txt

5. Root vs Normal User
The root user has full system access, while a normal user has limited permissions. For security, daily tasks should be performed using a normal user account and sudo should only be used when necessary. This follows the Least Privilege Principle.

6. Process & Service Management
I used commands like ps aux and systemctl to check running processes and services. Unnecessary

services were disabled to reduce the attack surface and improve system security.

7. OS Security Checklist

- Strong password enabled
- Normal user account used
- Firewall installed and active
- Unused services disabled
- File permissions configured
- System kept updated

8. Conclusion

This task helped me understand the importance of OS-level security. By implementing firewall rules, managing users, controlling permissions, and disabling unnecessary services, I improved the security of my Linux system. These practices are essential for protecting systems from cyber attacks.