Task - 2: Operating System Security Fundamentals (Linux & Windows)

Internship Task – Elevate Labs

This task focuses on understanding operating system level security, user management, permissions, and basic hardening techniques in Linux and Windows environments.

1. Understanding Operating System Security

Operating System security involves protecting the OS from threats, unauthorized access, malware, and misuse. A secure OS ensures proper user control, file protection, and network safety.

2. User Accounts and Privileges

Operating systems support different types of users: - Administrator or root user with full control. - Standard users with limited privileges.

Administrator accounts should be used only when necessary to reduce security risks.

3. Linux File Permissions

In Linux, file access is controlled using permissions: - Read (r) - Write (w) - Execute (x)

Commands used: - ls -l : to view permissions - chmod : to modify permissions - chown : to change file ownership

Proper permissions help prevent unauthorized access to sensitive files.

4. Firewall Configuration

Firewalls protect systems from unwanted network connections. - In Linux: UFW (Uncomplicated Firewall) is used. - In Windows: Windows Defender Firewall is used.

Enabling firewall blocks malicious traffic and reduces attack surface.

5. Running Processes and Services

Operating systems run many background services. Identifying unnecessary services and disabling them improves security. Fewer running services mean fewer entry points for attackers.

6. OS Hardening

OS Hardening is the process of securing an operating system by: - Disabling unused services - Applying updates - Using strong passwords - Enabling firewalls - Restricting administrator access

7. Best Practices Followed

- Created standard user accounts for daily work - Avoided using administrator privileges - Enabled firewall protection - Checked file permissions regularly - Disabled unnecessary startup services -

Kept the system updated

8. Learning Outcome

Through this task, I learned how operating system security works in real environments. I understood user privileges, Linux permissions, firewall usage, and OS hardening techniques. This knowledge is essential for protecting systems from cyber attacks.