OS Security Checklist & Practical OS Hardening Implementation

Task 2 – Operating System Security Fundamentals (Linux & Windows)

---

1. Overview

This document outlines the **Operating System (OS) Security Checklist**, **practical OS hardening steps**, and **essential commands** used to secure Linux and Windows systems. The objective is to reduce the system attack surface, enforce least privilege, and improve OS-level security posture.

This task is part of a **Cyber Security Internship** and supports foundational skills required for **SOC, Blue Team, and GRC roles**.

---

2. OS Security Checklist

2.1 User Accounts & Access Control

- Review all existing user accounts
- Identify privileged users (root / administrator)
- Remove or disable unused user accounts
- Restrict administrative access to trusted users only
- Enforce strong password policies

Security Purpose:
Prevents unauthorized access and limits privilege misuse.

2.2 File Permissions & Ownership (Linux)

- Verify file permissions using ls -l
- Apply least privilege permissions using chmod
- Ensure correct file ownership using chown
- Avoid insecure permissions such as full read-write-execute for all users

Security Purpose:
Protects sensitive files from unauthorized access or modification.

2.3 Administrator vs Standard User

- Avoid routine use of root/administrator accounts
- Perform administrative tasks only when required
- Use privilege escalation tools (sudo) securely

Security Purpose:
Limits system-wide impact in case of account compromise.

2.4 Firewall Configuration

- Enable host-based firewall
- Allow only required network ports and services
- Block unnecessary inbound and outbound traffic

Security Purpose:
Prevents unauthorized network access and reduces exposure to attacks.

2.5 Process & Service Management

- Identify running processes and background services
- Stop unnecessary or unused services
- Prevent unnecessary services from starting at boot

Security Purpose:
Reduces attack vectors and resource misuse.

2.6 OS Hardening Best Practices

- Keep operating system updated
- Apply security patches regularly
- Disable unused features and services
- Use strong authentication mechanisms
- Monitor system activity and logs

Security Purpose:
Improves overall system resilience against threats.

3. Practical OS Hardening Implementation

3.1 Linux (Ubuntu VM)

User Management

- Reviewed user accounts using system configuration files
- Verified sudo privileges
- Removed unnecessary user access

File Permission Hardening

- Checked permissions of critical files
- Modified permissions to restrict access
- Ensured correct ownership for system and user files

Firewall Hardening

- Enabled UFW firewall
- Allowed only essential services (e.g., SSH)
- Verified firewall rules and status

Service Hardening

- Listed active system services
- Disabled unnecessary services
- Reduced system startup services

3.2 Windows

User Privilege Management

- Reviewed administrator and standard user accounts
- Disabled unused accounts
- Avoided daily usage of administrator account

Firewall Hardening

- Ensured Windows Defender Firewall was enabled
- Reviewed inbound and outbound firewall rules

Process & Startup Control

- Analyzed running processes using Task Manager

4. Necessary Command Table (Linux)

Category	Command	Purpose
View Users	cat /etc/passwd	Lists all user accounts
Check Permissions	ls -l	Displays file permissions
Change Permissions	chmod 640 file	Restricts file access
Change Ownership	chown user:group file	Sets file owner and group
Switch to Root	sudo -i	Temporary administrative access
List Processes	ps aux	Shows running processes
Real-Time Monitoring	top	Live process monitoring
List Services	systemctl list-units --type=service	Displays active services
Stop Service	systemctl stop service_name	Stops a running service
Disable Service	systemctl disable service_name	Prevents service at boot
Firewall Enable	ufw enable	Enables UFW firewall
Firewall Status	ufw status	Shows firewall rules
Allow Port	ufw allow ssh	Allows SSH traffic
Block Port	ufw deny 8080	Blocks specific port

5. Key Security Concepts Applied

- OS Hardening
- Least Privilege Principle
- Attack Surface Reduction
- User Access Control
- Host-Based Firewall Security
- Service & Process Control

6. Screenshots Mapping – OS Security & Hardening Evidence

This section documents the screenshots captured as evidence of practical OS hardening activities.
Each screenshot is mapped to a specific security control, ensuring transparency, reproducibility, and assessment readiness.

User Accounts & Privilege Management

Screenshot 1: Linux User Accounts

Command Used: **cat /etc/passwd**

What the Screenshot Shows:

- List of all user accounts on the Linux system
- Identification of system users vs normal users

Security Control Validated:
User enumeration and access control review

Screenshot 2: Sudo Privileges

Command Used: **sudo -l**

What the Screenshot Shows:

- Users with sudo (administrative) privileges

Security Control Validated:
Administrator vs standard user privilege separation

File Permissions & Ownership (Linux)

Screenshot 3: File Permission Analysis

Command Used: **ls -l**

What the Screenshot Shows:

- Read, write, and execute permissions
- Owner and group assignment

Security Control Validated:
File access control and least privilege enforcement

Screenshot 4: Permission Hardening

Command Used: **chmod 640 filename**

What the Screenshot Shows:

- Permission modification before and after execution

Security Control Validated:
Prevention of unauthorized file access

Screenshot 5: Ownership Management

Command Used: **chown user:group filename**

What the Screenshot Shows:

- Correct ownership assignment

Security Control Validated:
Accountability and access restriction

Firewall Configuration Evidence

Screenshot 6: UFW Firewall Status (Linux)

Commands Used: **sudo ufw enable**

sudo ufw status

What the Screenshot Shows:

- Firewall enabled state
- Allowed and denied rules

Security Control Validated:
Host-based firewall enforcement

Screenshot 7: Windows Defender Firewall

Tool Used: **Windows Security → Firewall & Network Protection**

What the Screenshot Shows:

- Firewall enabled for all network profiles

Security Control Validated:
Network access control on Windows OS

Process & Service Monitoring

Screenshot 8: Running Processes (Linux)

Commands Used: **ps aux**

top

What the Screenshot Shows:

- Active processes and resource usage

Security Control Validated:
Process monitoring and anomaly detection readiness

Screenshot 9: Active Services (Linux)

Command Used: **systemctl list-units --type=service**

What the Screenshot Shows:

- Running system services

Security Control Validated:
Service inventory and attack surface assessment

Service Hardening

Screenshot 10: Disabling Unnecessary Services

Commands Used: **sudo systemctl stop service_name**

sudo systemctl disable service_name

What the Screenshot Shows:

- Service stopped and disabled successfully

Security Control Validated:
Attack surface reduction through service hardening

Windows Process & Startup Control

Screenshot 11: Task Manager – Processes

Tool Used: **Windows Task Manager → Processes Tab**

What the Screenshot Shows:

- Active running processes

Security Control Validated:
Endpoint monitoring and process visibility

Screenshot 12: Startup Services (Windows)

Tool Used:**Task Manager → Startup Tab**

What the Screenshot Shows:

- Enabled and disabled startup programs

Security Control Validated:
Persistence prevention and boot-time hardening

Screenshot Folder Structure

Screenshots/

01_users_linux.png

02_sudo_privileges.png

03_file_permissions.png

04_chmod_hardening.png

05_chown_ownership.png

06_ufw_status.png

07_windows_firewall.png

08_process_monitoring_linux.png

09_services_list.png

10_service_disable.png

11_windows_processes.png

12_startup_services.png

All screenshots are captured from a controlled lab environment using Kali Linux (VM) and Windows OS for educational and internship purposes only.

7. Final Outcome

Through this task, a strong foundation in **operating system security and hardening** was established.
The practical implementation improved understanding of **Linux and Windows security controls**, essential for **SOC, Blue Team, and entry-level cybersecurity roles**.

---

8. Author

Parijat Das
B.Tech Computer Science | Aspiring Cyber Security Professional