Operating System Security Fundamentals (Linux & Windows)

1. Objective

The objective of this task is to gain a clear and practical understanding of **Operating System (OS) security**. This includes learning how user access, permissions, services, and firewalls work together to protect an operating system from unauthorized access and attacks. The task also introduces basic **OS hardening techniques** used in real-world systems.

2. Environment & Tools Used

- **Operating System:** Ubuntu Linux (Virtual Machine)
- **Host OS:** Windows
- **Virtualization Tool:** Oracle VirtualBox
- **Security Components:** Linux User Management, File Permissions, UFW Firewall, System Services

3. User Accounts & Privilege Management

Linux uses role-based access control to manage users.

Types of Users:

- **Root User:**
- Has unrestricted access to the entire system
- Can install software, modify system files, and manage users
- **Normal User:**
- Limited privileges
- Requires authentication (sudo) to perform administrative tasks **Security Importance:**

Using a normal user for daily activities minimizes the risk of accidental damage and privilege misuse.

4. File Permissions in Linux

Linux enforces file-level security using permission bits.

Permission Types:

- **Read (r):** View file content
- **Write (w):** Modify file content
- **Execute (x):** Run the file

Permission Levels:

- Owner
- Group
- Others

Command Used:

```
ls -l
```

Example:

```
-rwxr-xr--
```

Explanation: - Owner: read, write, execute - Group: read, execute - Others: read only This ensures only

authorized users can access or modify files.

5. File Ownership & Access Control

Linux allows control over file ownership and permissions.

Commands:

```
chmod  – modify file permissions
chown  – change file owner or group
```

These commands help enforce strict access control and prevent unauthorized file access.

6. Least Privilege Principle

The **Principle of Least Privilege** states that users and applications should be granted only the minimum permissions required to perform their tasks.

Advantages:

- Limits impact of malware • Reduces system misuse
- Enhances overall security

7. Firewall Configuration (UFW)

A firewall controls incoming and outgoing network traffic.

UFW (Uncomplicated Firewall):

Commands used:

```
sudo ufw enable
sudo ufw status
```

Once enabled, UFW blocks unauthorized access and allows only permitted connections.

8. Monitoring Processes & Services

Running services can be viewed to understand what is active on the system.

Commands Used:

```
ps
top
systemctl list-units --type=service
```

Regular monitoring helps identify unnecessary or risky services.

9. Disabling Unnecessary Services

Unneeded services increase the system's attack surface.

Examples:

- Bluetooth service
- Printing service
- Remote access services

Disabling unused services improves system performance and security.

10. OS Hardening Best Practices

- Use strong and unique passwords
- Enable firewall at all times
- Disable unused services
- Keep the OS updated
- Avoid using root account regularly
- Monitor system activity

11. OS Security Checklist

- User privilege separation implemented
- File permissions reviewed using ls -l
- File ownership and permissions managed
- Firewall enabled and verified (UFW)
- Running processes monitored
- System services reviewed
- Unnecessary services disabled
- OS hardening practices documented

12. Final Outcome

This task provided hands-on understanding of **OS-level security controls** and **basic hardening techniques**. It strengthened knowledge of how operating systems protect data, users, and resources from security threats.