

Task 2: OS Security Hardening Checklist (Windows)

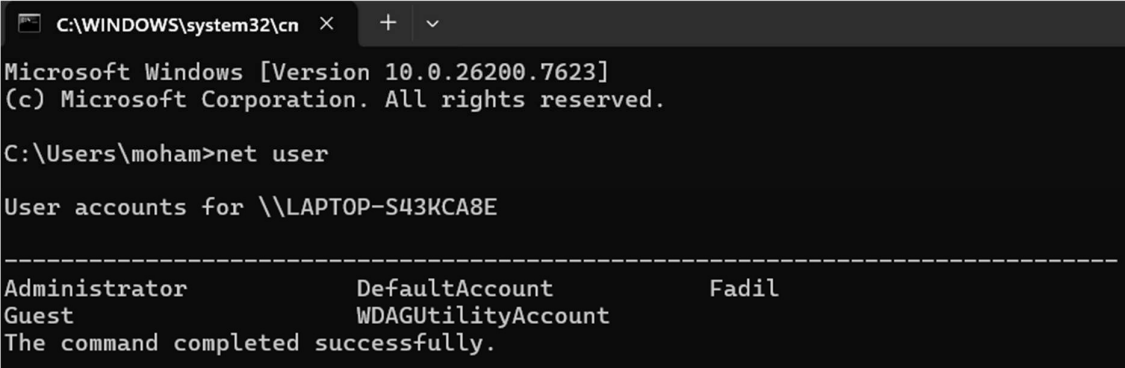
Name: Mohammed Fadil PK **Date:** January 16, 2026

1. Introduction to OS Hardening

OS hardening is the process of protecting an operating system by reducing its attack surface. It entails setting up system parameters to remediate vulnerabilities and prevent cyber attacks.

2. Windows Security Checklist (Best Practices)

- **User Account Management**
 - **Concept:** Administrator accounts and Standard user accounts should be differentiated.
 - **Action:** Verified the list of users to make sure that there are no unauthorized accounts.
 - **Command Used:** net user
 - **Best Practice:** Normal work should be done on a Standard account and not on an Administrator account to prevent malware from installing itself.



```
C:\WINDOWS\system32\cmd
Microsoft Windows [Version 10.0.26200.7623]
(c) Microsoft Corporation. All rights reserved.

C:\Users\moham>net user

User accounts for \\LAPTOP-S43KCA8E

-----
Administrator          DefaultAccount          Fadil
Guest                   WDAGUtilityAccount
The command completed successfully.
```

Fig 1: Verifying User Accounts via Command Prompt

- **Firewall Configuration**

- Concept: Monitor and control incoming and outgoing network traffic.
- Action: Confirmed that Windows Defender Firewall is enabled for Private and Public networks.
- Best Practice: The firewall should always be enabled to prevent unauthorized access to the ports.

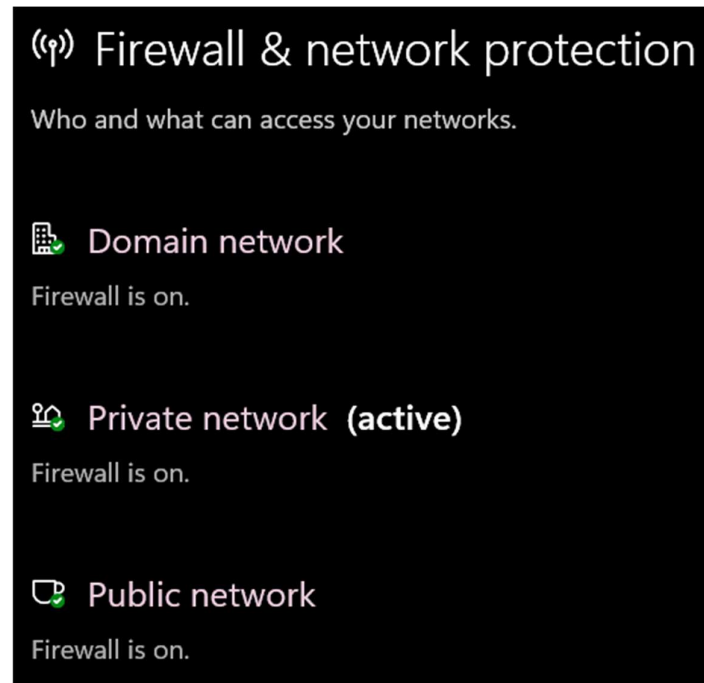


Fig 2: Windows Defender Firewall Status

- **File Permissions (Access Control)**

- Concept: Control who can Read, Write, or Execute a file.
- Action: Verified the Access Control List (ACL) of a sensitive file.
- Comparison: In Linux, we use chmod (for example, chmod 700). In Windows, use the Security tab to deny access to Guest users.

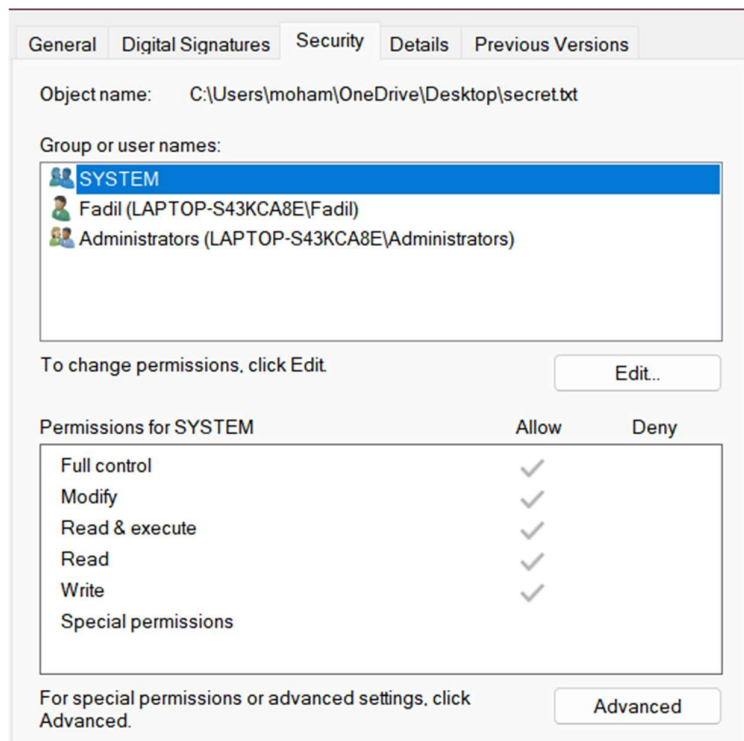


Fig 3: Checking File Permissions for secret.txt

• Service Management

- Concept: Turn off unnecessary background programs.
- Action: Unused services like Remote Registry or Print Spooler (if there is no printer installed) should be turned off to remove security vulnerabilities.

3. Interview Questions & Answers

1. **What is OS hardening?** It is the process of making an operating system secure by removing vulnerabilities, closing unused ports, and disabling unnecessary services to avoid the possibility of an attack.
2. **What is the Principle of Least Privilege?** This is granting a user or a program the least amount of access necessary to perform their task (for instance, a user can read a file but not delete it).
3. **Why is it necessary to disable unnecessary services?** Each service that is running can potentially be used by an attacker as a means of entry. If a service is running but is unnecessary, then it provides no benefit but instead poses a risk.