Task 2: OS Security Hardening Checklist (Windows)

Name: KARTHIKP Date: January 16, 2026

1. IntroducƟon to OS Hardening

OS hardening is the process of protecƟng an operaƟng system by reducing its aΣack surface. It entails seţng up system parameters to remediate vulnerabiliƟes and prevent cyber aΣacks.

2. Windows Security Checklist (Best PracƟces)

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

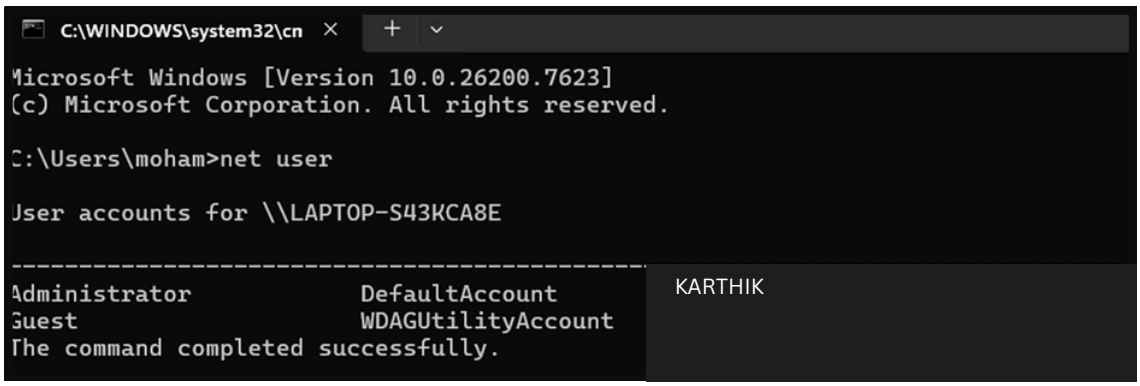

Fig 1: Verifying User Accounts via Command Prompt

• Firewall ConfiguraƟon

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

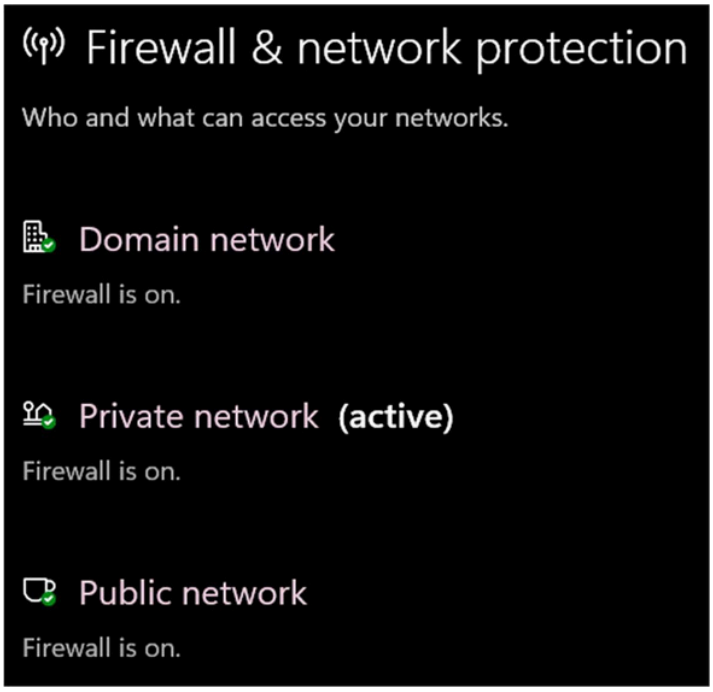

Fig 2: Windows Defender Firewall Status

•File Permissions (Access Control)

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

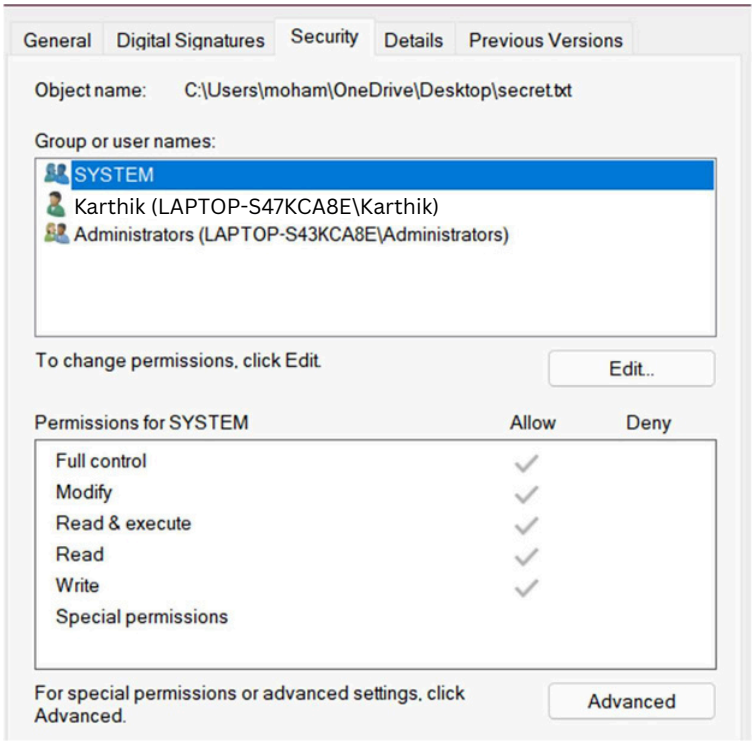

Fig 3: Checking File Permissions for secret.txt

• Service Management

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

3. Interview QuesƟons & Answers

1. What is OS hardening? It is the process of making an operaƟng system secure by removing vulnerabiliƟes, closing unused ports, and disabling unnecessary services to avoid the possibility of an aΣack.
2. What is the Principle of Least Privilege? This is granƟng 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 potenƟally be used by an aΣacker as a means of entry. If a service is running but is unnecessary, then it provides no benefit but instead poses a risk.