System Hardening

Mia McCarthy

October 2025

1 How to Score Points

1.1 User Accounts and Permissions

- Use lusrmgr.msc in run to view
- Remove unauthorized users (authorized users listed in the ReadMe).
- Correct group membership:
  - Only authorized users in the Administrators group.
  - Remove non-administrators from the Remote Desktop Users group unless specified.
- Disable or delete the Guest account and other unused accounts.
- Enforce password and account lockout policies:
- Use secpol to access:
  - Minimum length: 10 characters.
  - Complexity requirements enabled.
  - Account lockout threshold 5-10.
  - Password history to 7.
  - Password expiration enforced (e.g., 90 days).
- Remove blank or weak passwords.
- Enable password complexity requirements.
- Do not enable password storing.
- Do not allow anonymous enumeration of SAM accounts (Enable).
- Require ctrl + alt + del to sign in.
- Disable guest and default administrator in user rights.

1.2 System Security Settings

- Ensure Windows Defender Antivirus is enabled and updated.
- Enable real-time protection and cloud-delivered protection.
- Enable and configure Windows Firewall:
  - Block inbound connections by default.
  - Allow only necessary ports and applications.
- Enable automatic Windows Updates (ensure not paused).
- Turn on User Account Control (UAC) and set to "Always notify."
- Enable Windows SmartScreen or Smart App Control.
- Verify Secure Boot and TPM are active (if applicable in ReadMe).

1.3 Software Applications

- Remove unauthorized or insecure software (games, hacking tools, torrent clients, etc.).
- Install required software updates and patches.
- Verify browsers (Edge, Chrome, etc.) are up to date.
- Remove or disable outdated runtimes (e.g., old Java, Flash).
- Ensure any server role applications (IIS, DNS, DHCP) are configured securely.

1.4 Network and Services

- Disable unnecessary services (Telnet, FTP, SNMP if not required).
- Use the control panel to access the system and security.
- Disable Remote Assistance if not needed
- Verify Remote Desktop is restricted:
- Turn it off if not specified in the read me.
  - Network Level Authentication (NLA) enabled.
  - Only authorized users allowed.
- Review firewall rules for open ports and close unnecessary ones.
  - Use wf.msc in run to open

    - In the left-hand pane, right-click Windows Defender Firewall with Advanced Security on Local Computer → Properties.
    - Under each tab, find inbound connections and set it to block
    - Right click and click on properties
    - Click on the ports, check for FTP (21) or Telnet (23) and disable it
    - Click on the services of an app, if it has svc.host.exe in it keep it
  - Disable unnecessary services not stated in the read me
  - Check the port number, 80 (HTTP), 443 (HTTPS), 445 (SMB), 139 (NetBIOS), 53 (DNS Server) should all stay open.
  - Likely no inbound ports on workstation should be open.
  - Disable it if unsure, delete it if sure.
  - Ensure file and printer sharing is disabled unless required.
  - Configure IPv6 and IPv4 settings as instructed (e.g., static IP, DNS).

1.5 Client-Side Network Configuration

- **DHCP:** Leave automatic unless the ReadMe specifies a static IP.
  - Open Settings → Network & Internet → Ethernet (or Wi-Fi) → Properties.
  - Under IP assignment, click Edit.
  - Choose Manual, then toggle IPv4 on.
  - **Enter the following from the ReadMe:**
    - IP address (e.g., 192.168.1.50)
    - Subnet mask (usually 255.255.255.0)
    - Default gateway (e.g., 192.168.1.1)
  - Click save.
  - **Verify with command prompt:** ipconfig /all
- **Static IP:** Set according to ReadMe instructions if required.
- **DNS:** Leave automatic unless the ReadMe specifies custom DNS servers.
- **IPv6:** Leave enabled unless the ReadMe instructs you to disable it.
- **Verify Connectivity:** Use `ping` and `nslookup` to confirm network connectivity.

1.6 File System and Permissions

- Remove inappropriate or illegal media from user directories.
- Secure sensitive files and folders with correct NTFS permissions.
- Ensure only intended users have access to shared folders.
- Check for hidden or suspicious files.

1.7 Audit and Logging

- Enable auditing for logon events, object access, and policy changes.
- Review Event Viewer for warnings or suspicious activity.
- Configure log retention policies (avoid overwriting important logs).

1.8 Server Role Configuration (Windows Server Specific)

- Properly configure Active Directory:
  - Correct user roles and OU placement.
  - Group Policy Objects (GPOs) enforce security baselines.
- Secure IIS web server:
  - Remove default sites and sample pages.
  - Enforce HTTPS and disable weak protocols.
- Secure DNS/DHCP roles:
  - Disable zone transfers if not required.
  - Restrict dynamic updates to secure only.
- Verify file sharing permissions for network shares (least privilege).

1.9 General Best Practices

- Read the ReadMe carefully — follow all scenario-specific requirements.
- Document every change in a "Forensics Report" text file.
- Regularly run "net user", "net localgroup", and "services.msc" to verify progress.
- Take periodic screenshots for verification.