First 1-Hour

1. Look at all the users and change their passwords.
   - Change Administrator's password
     - 12 characters
     - lusrmgr.msc
   - Through Computer Management
2. Check all the users' privileges and correct them if needed
   - Through Computer Management
3. Disable Guest Login
   - Lusrmgr.msc
   - Disable in the property (Check it then apply)
4. Set up a Password Policy

   NIST compliant
   - History - 6 password
   - Age - 90 days
   - Length - 8 characters
   - Min pass Audit - 8 char (not mentioned in NIST)
   - Pass complexity - Enabled
   - Relax min pass - Disabled
   - Store pass using encryption - Disabled
5. Set up an Account Lockout Policy
   - Lockout attempts - 10 or less
   - Lockout duration - 15 mins
   - Reset account - 10 mins
6. Set up audit policy
   - Acc logon events - Success and Failure
   - Acc Management - Success and Failure
   - Logon Events - Success and Failure
   - Object Access - Success and Failure
   - Policy Change - Success and Failure
   - Privilege Use - Success
   - System events - Success
   - Directory and process tracking is off because it may flood the logs but can help track malware/processes.
7. Disable RDP (If they don't say to keep it enabled)
   - Open up Server Manager, Then left side “Local Server”
   - Look for remote management and disable it.
8. Disable SMBv1
   - Set-SmbServerConfiguration -EnableSMB1Protocol $false
9. Check FireWall rules

    - Inbound connection Block (Default)
    - Outbound connection Allow (Default)
10. Run NTP to have accurate loggings
    - w32tm /query /status
11. Set UAC to highest/always notify

12. Disable CTRL+ALT+DEL login
    - gpedit.msc
    - Comp config > Windows settings > Security Settings > Local Policies> Security option
    - Look for interactive logon CTRL+ALT+DEL then disable it
13. Disable Unused DNS (ONLY IF NOT USED)

14. Install Chrome and uninstall Internet Explorer

15. Disable NetBIOS (file sharing vulnerability for old legacy)
    - Go to the internet connection
    - Properties, then advance, wins tab, disable NetBIOS
16. Look at registry if LSA is turned on
    - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
    - Look for RunAsPPL
    - If not there run the script
    - reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RunAsPPL /t REG_DWORD /d 2 /f;reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RunAsPPLBoot /t REG_DWORD /d 2 /f;
    - Set to “1” to enable it

17. Look at the control panel and uninstall any suspicious or unnecessary applications

18. Disable IPv6 unless DHCP hands them out

18. Update Windows

19. Create a backup (After hardening)
    - Server Manager
    - Add roles and features, till you select the feature page
    - Look for Windows Server Backup then install
    - Run “wbadmin.msc”
    - Top right-click “Backup Once”
    - Select full Server

20. Look at the running processes
    - Run the running script from the repo
    - Kill any unnecessary process that's running through the task manager

Steps for Installing Docker

1. Run Script

```
Invoke-WebRequest -UseBasicParsing "https://raw.githubusercontent.com/microsoft/Windows-Containers/Main/helpful_tools/Install-DockerCE/install-docker-ce.ps1" -o install-docker-ce.ps1
.\install-docker-ce.ps1
```

```
docker pull mcr.microsoft.com/windows/servercore:ltsc2019
```

```
Set-MpPreference -DisableRealtimeMonitoring $false
```

2. Verify that the docker is running

- docker –version
- docker info

3. Useful Commands

- docker images
- docker run
- docker stop
- docker pull (image name)
- docker rmi (ID) or (name)
- docker build -t image name

4. Limiting resources

- docker run --cpus="1.0" <image_name>
- docker run --memory="1g" --memory-swap="1.5g" <image_name>
-
- docker run --memory="1g" --memory-swap="1.5g" --cpus="0.5" <image_name>

5. Limiting privileges

- docker run --privileged=false <image_name>
- docker run --read-only <image_name>

6. Combination of limiting

- docker run --memory="1g" --cpus="0.5" --privileged=false mcr.microsoft.com/windows/servercore/iis

```
dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart
```

```
dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
```