1. **Windows Setup**
   1. Change all passwords.
      1. net user <username> <password> NOTE: If domain user, append /domain
   2. Audit important groups.
      1. net localgroup Administrators
      2. net localgroup "Remote Desktop Users"
      3. net localgroup "Remote Management Users"
   3. Disable WinRM if not needed.
      1. Disable-PSRemoting -Force
   4. Check Windows Defender registry keys.
      1. regedit.exe HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
   5. Check that Windows Defender is (Powershell)
      1. get-MpComputerStatus
   6. Check for tasks set to run through the registry. (Control Panel)
      1. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
      2. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
      3. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
      4. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
   7. Check the system and user startup folder.

User: C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\

System: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\

* 1. Audit scheduled tasks.
     1. schtasks
  2. Check PowerShell Execution policy.
     1. Get-ExecutionPolicy
     2. Set-ExecutionPolicy -ExecutionPolicy Restricted -Scope LocalMachine
  3. Check Windows Defender status.
     1. Get-MPComputerStatus
  4. Audit SMB shares.
     1. net view \\127.0.0.1
  5. Disable the Guest account.
     1. net user guest /active no
  6. Flush DNS Records
     1. Ipconfig /flushdns

1. **Windows Monitoring**
   1. Audit listening ports
      1. netstat –na
   2. List the SMB sessions this machine has opened with other systems.
      1. net use
   3. List the open SMB sessions with this machine.
      1. net session
   4. Audit running processes. (AutoRun, task manager)
      1. task list
   5. Display active TCP Connections
      1. netstat -o 5

| **Parameter** | **Description** |
| --- | --- |
| -a | Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. |
| -b | Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions. |
| -e | Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**. |
| -n | Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names. |
| -o | Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**. |
| -p <Protocol> | Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be tcp, udp, tcpv6, or udpv6. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6. |
| -s | Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols. |
| -r | Displays the contents of the IP routing table. This is equivalent to the route print command. |