ON ALL WINDOWS SYSTEMS (10, Server 2012 & 2016)

1. Change Administrator Password; Ctrl+Alt+Del > Change Password

2. Check for Updates
   a. If Update Errors Out - Clear Update Folder by:
      i. **cmd.exe > net stop wuauserv >**
      ii. **Ren C:\Windows\SoftwareDistribution SoftwareDistribution.old >**
      iii. **net start wuauserv >** Re-Check for Updates

3. **Disable Remote Assistance & Remote Registry Service**
   a. **systempropertiesremote.exe > Uncheck** "Allow Remote Assistance connections"
   b. **cmd.exe > sc stop RemoteRegistry > sc config RemoteRegistry start= disabled**

4. **File Explorer Options**
   a. In **cmd.exe** type **control.exe folders**
   b. ***Tick*** - *Show hidden files, folders, and drives*
   c. **Uncheck** hide extensions for known file types

5. **FIREWALL CONFIGURATION**
   a. Enable Firewall on Domain, Public, and Private
      i. firewall.cpl > Turn Windows Defender Firewall on

   b. Block Unneeded Ports
      i. firewall.cpl > Advanced Settings > New Inbound Rule >
      ii. Port > All Local Ports > Block the Connection > Apply to Domain, Private, Public

   c. Allow Necessary Ports in Firewall
      i. firewall.cpl > Advanced Settings > New Inbound Rule >
      ii. Port > 80 , 443, 25, 465, 587, 110, 995, 22, 53 > Allow the Connection > Apply to Domain, Private, Public

LEAVE THESE SERVICES AND PORTS ENABLED

Service	Port	Protocol (TCP, UDP)
HTTP	80	TCP
HTTPS	443	TCP
SMTP	25, 366, (465, 587 TCP)	TCP, UDP
POP3	110, 995	TCP
SSH	22	TCP, UDP
DNS	53	TCP, UDP
NTP (Network Time Protocol)	123	UDP

6. Browse the System for unusual activities
    a. **Startup Programs in Registry (regedit.exe; Click Yes if prompted)**
        i. **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**
        ii. **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce**
        iii. **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
        iv. **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce**

    b. **Review Installed Applications**
        i. **appwiz.cpl >** Review Installed Applications and note any suspicious software
        ii. *Discuss with other team members and uninstall if agreed

    c. **HOST File** (Review for any Suspicious Malicious Redirect IP Addresses)
        i. **cmd Right Click; Run as Admin > start C:\Windows\System32\drivers\etc\hosts**
        ii. **Open with Notepad**
        iii. *Note any Suspicious IP addresses; Discuss with other Window Team Members

    d. **Review Network Usage Right Click CMD; Run as Administrator**
        i. Look for Suspicious File Shares - **cmd.exe > net view \\127.0.0.1**
        ii. Look at open SMB sessions with the machine - **net session**
        iii. List SMB sessions open with other systems - **net use**
        iv. List open shares - **net share**
        v. List listening TCP and UDP ports - cmd.exe > **netstat -an /o**

    e. **Unusual Accounts Right Click CMD; Run as Administrator**
        i. Review user accounts on the system - **cmd.exe > net user**
        ii. Review accounts in Administrators group - **cmd.exe > net localgroup administrators**
        iii. *Discuss any unusual accounts with other team members

    f. **Review Scheduled Tasks**
        i. **taskschd.msc >** Right side panel - Click **Display all Running Tasks** >
        ii. Discuss with other windows team members and end any suspicious tasks

    g. **Review %TEMP% Folder Directory**
        i. **cmd.exe > start %TEMP% >** Note any suspicious files; ****DO NOT RUN THEM****
        ii. Discuss with other Window Team Members if any odd files found

7. **Extra Recommendations**
    a. **Disable NetBIOS NBT-NS** - regedit> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\ > set DWORD value NetbiosOptions to **2**

    b. **Disable LLMNR** - gpedit.msc > Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off Multicast Name Resolution > set to **Enabled**

    c. **Disable SMB 1.0** and **Enable SMB signing**

    d. **Check Credential Cleartext Password Memory Leakage setting** - regedit > HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest > **set UseLogonCredential** value to **0** to not store credentials in memory

8. **Elevate UAC Settings to “Always Notify”**
    a. **useraccountcontrolsettings.exe > Move Bar to Highest Line “Always notify”**

9. Check open ports with Nmap on Windows 10 System
    a. Service Detection **nmap -Sv**
        i. -Sv (Service Version)

    b. Scan all ports and list open services, ports, and versions: **nmap -p 1-65535 -T4 -A -v**
        i. -p (Port) 1-65535 (All Ports)
        ii. -T4 (aggressive scan)
        iii. -A (Enable OS detection, version detection, script scanning, and traceroute)
        iv. -v (verbose mode)

    c. Scan Both TCP and UDP at the same time:
        i. nmap -p U:25,53,67-70,123 T:20-25,53,80,110,366,443,465,587,995

Group Policy - Password Policy Directory (Once finished, run gpupdate /force on all domain machines)
Computer configuration-> Policies-> Windows Settings->Security Settings -> Account Policies -> Password Policy;

Last Year RED-TEAM Recommendations:

Palo Alto SMB Access List
Change Database Password