Windows 10 & Server 2016 Checklist

- ❏ **Take notes on the README file**
- ❏ **Answer the Forensics Questions (Look at how-to's section at end of document)**
- ❏ **Change security policies**
  - ❏ Open Local Security Policy: Click the Start button, type "Secpol" on the search bar, click enter, & select "Yes" if prompted. Local Security Policy will open.
  - ❏ Edit Password Policies:
    - ❏ Select "Account Policies" on the left & select "Password Policy".
    - ❏ Select "Enforce Password History" & choose 5 passwords.
    - ❏ Select "Maximum Password age" & choose 30 days.
    - ❏ Select "Minimum password age" & choose 5 days.
    - ❏ Select "Minimum Password Length" & choose 10 characters.
    - ❏ Select "Password must meet complexity requirements" & enable it.
    - ❏ Select "Store passwords using reversible encryption" & disable it.
  - ❏ Edit Account Lockout Policies:
    - ❏ Select "Account Lockout Policy" on the left.
    - ❏ Select "Account lockout threshold" & choose 5 invalid logon attempts.
    - ❏ Select "Account lockout duration" & choose 30 minutes (It could already be set).
    - ❏ Select "Reset account lockout counter after" & choose 30 minutes (It could already be set).
  - ❏ Edit Audit Policies
    - ❏ Select "Local Policies" on the left & select "Audit Policy".
    - ❏ For each policy, check both "Success" & "Failure" in "Audit these attempts:".
    - ❏ Next, in "Local Policies" on the left, select "Security Options".
    - ❏ Scroll all the way down to where it says "User Account Control: Switch to the secure desktop when prompting for elevation". Select this & choose "Enabled".
  - ❏ Edit User Rights Assignment:
    - ❏ Select "Local Policies" on the left & select "User Rights Assignment".
    - ❏ Select "Access Credential Manager as a trusted caller", & remove any users.
    - ❏ Select "Access this computer from the network", & make sure there is only "Administrators, Backup Operators, Users".
    - ❏ Select "Act as part of the operating system", & remove any users.
    - ❏ Select "Adjust memory quotas for a process", & remove make sure there is only "Administrators, LOCAL SERVICE, NETWORK SERVICE".
    - ❏ Select "Backup files & directories", & make sure there is only "Administrators".
    - ❏ Select "Change the system time", & make sure there is only "Administrators, LOCAL SERVICE"..
    - ❏ Select "Change the time zone", & make sure there is only "Administrators, LOCAL SERVICE, Users".
    - ❏ Select "Create a pagefile", & make sure there is only "Administrators".
    - ❏ Select "Create a token object", & remove any users.

- ❏ Select “Create global objects”, & make sure there is only “Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE”.
- ❏ Select “Create permanent shared objects”, & remove any user accounts.
- ❏ Select “Debug programs”, & make sure there is only “Administrators”.
- ❏ Select “Deny access to this computer from the network”, & make sure there is only “Guest”.
- ❏ Select “Deny log on a batch job”, & make sure there is only “Guest”.
- ❏ Select “Deny log on as a service”, & make sure there is only “Guest”.
- ❏ Select “Deny log on locally”, & make sure there is only “Guest”.
- ❏ Select “Enable computer & user accounts to be trusted for delegation”, & remove any users.
- ❏ Select “Force shutdown from a remote system”, & make sure there is only “Administrators”.
- ❏ Select “Generate security audits”, & make sure there is only “LOCAL SERVICE, NETWORK SERVICE”.
- ❏ Select “Impersonate a client after authentication”, & make sure there is only “Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE”.
- ❏ Select “Increase scheduling priority” & “Load & unload device drivers”, & make sure there is only “Administrators”.
- ❏ Select “Lock pages in memory”, & remove any users.
- ❏ Select “Log on as a batch job”, & make sure there is only “Administrators”.
- ❏ Select “Log on as a service”, & remove any users.
- ❏ Select “Manage auditing & security log”, & make sure there is only “Administrators”.
- ❏ Select “Modify an object label”, & remove any users.
- ❏ Select “Modify firmware environment values”, “Perform volume maintenance tasks”, & “Profile single processes”, & make sure there is only “Administrators”.
- ❏ Select “Profile system performance”, & make sure there is only “Administrators, NT SERVICE/WdiServiceHost”.
- ❏ Select “Replace a process level token”, & make sure there is only “LOCAL SERVICE, NETWORK SERVICE”.
- ❏ Select “Restore files & directories”, & make sure there is only “Administrators”.
- ❏ Select “Shut down the system”, & make sure there is only “Administrators, Users”.
- ❏ Select “Take ownership of files or other objects”, & make sure there is only “Administrators”.

❏ <u>Edit Security Options:</u>

- ❏ Select “Local Policies” on the left & then select “Security Options”.
- ❏ Select “Accounts: Guest account status” & disable it.
- ❏ Select “Devices: Prevent users from installing printer drivers”, “Devices: Restrict CD-ROM access to locally logged-on user only”, & “Interactive logon: Do not display last user name” & enable all three.
- ❏ Select “Network access: Allow anonymous SID/Name translation” & disable it.

- Select “Network access: Do not allow anonymous enumeration of SAM accounts” & “Network access: Do not allow anonymous enumeration of SAM accounts & shares” & enable both.
- Select “Network security: Do not store LAN Manager hash value on next password change” & enable it.
- Select “Network security: LAN Manager authentication level” & select “Send NTLMv2 response only. Refuse LM” from the dropdown.

- **Edit Users & Administrators**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Select “User Accounts” in the Control Panel & select “Manage another account”.
  - If you find any unauthorized accounts, delete them by selecting the account, clicking “Delete the account”, & selecting “Keep files”.
  - If you need to add an account, click “Add”, type the name of the account, the password for the account, & the account type (Standard for a User & Administrator for an Administrator). Then, click “Create a password” & create a strong password.
  - If you need to change the account type, select the account, click “Change account type” & choose whether they are an Administrator or User. Then, click “Create a password” & enter a strong password.
  - If you find any account with no password (It will not say “Password protected” if so), then select the account, click “Create a password”, & enter a strong password.
- **Disable Guest Account**
  - Through Microsoft Management Console:
    - Open Microsoft Management Console: Click the Start button, type “Mmc”, click enter, & select “Yes” if prompted. Microsoft Management Console should open.
    - Select “File” on the top-right & select “Add/Remove Snap-in”
    - In the available snap-ins column, select “Local Users & Groups” & select the “Add” button in the center. Select “Finish” in the pop-up & then select “OK”
    - From the main window, select the “Local Users & Groups” snap-in, select the “Users” folder, & select “Guest”. Guest User Properties should open.
    - Check the box that says “Account is disabled”, select “Apply”, & then select “Ok”.
  - Through Batch Files:
    - Open Notepad(++): Click the Start button, type “Notepad”, click enter, & select “Yes” if prompted. Notepad(++) should open.
    - In the notepad file, type in “@echo off”, & then press enter twice.
    - Then, type “title Disable Guest Account”, & press enter twice.
    - After that, type “net user guest /active:no”.
    - Finally, type “pause”. The file should look like this:

```
@echo off

title Disable Guest Account

net user guest /active:no

pause
```

- **Enable Windows Firewall**
  - Through Control Panel:
    - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
    - Make sure the “View By” option on the top-right is selected as “Category”.
    - Select “System & Security” & then select “Windows Defender Firewall”.
    - On the left-pane, select “Turn Windows Defender Firewall on or off”
    - Select “Turn on Windows Defender Firewall” on both Public & Private networks.
    - Add Windows Firewall Exceptions:
      - On the Windows Firewall Page left-pane, select “Allow an app or feature through Windows Defender Firewall”
      - Select apps to accept through Windows Firewall (Used for applications that need to be enabled as per the read-me).
  - Through Batch Files:
    - Open Notepad(++): Click the Start button, type “Notepad”, click enter, & select “Yes” if prompted. Notepad(++) should open.
    - In the notepad file, type in “@echo off”, & then press enter twice.
    - Then, type “title Enable Firewall”, & press enter twice.
    - After that, type “netsh advfirewall set allprofiles state on”.
    - Finally, type “pause”. The file should look like this:

```
@echo off

title Enable Firewall

netsh advfirewall set allprofiles state on

pause
```

  - Advanced Firewall Settings:
    - Open Local Security Policy: Click the Start button, type “Secpol” on the search bar, click enter, & select “Yes” if prompted. Local Security Policy will open.
    - CLick “Windows Defender Firewall with Advanced Security - Local Group Policy Object”, & then click “Windows Defender Firewall Properties”.
    - Domain Profile:
      - In the “Domain Profile” tab, make sure “Firewall state” is on, “Inbound connections” is blocked, & “Outbound connections” is allowed.
      - Customize General & Logging Settings:
        - Click on the “Customize” button in the “Settings” section.
        - Make sure “Display a notification” is set to “No”, “Apply local firewall rules” is set to “Yes”, & “Apply local connection security rules” is set to “Yes”. Click “Ok”.
        - Click on the “Customize” button in the “Logging” section.
        - Make sure “Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log”, “Size limit (KB)” is set to 16384 KB, “Log dropped packets” is set to “Yes”, & “Log successful connections” is set to “Yes”. Click “Ok”.
    - Private Profile:
      - In the “Private Profile” tab, make sure “Firewall state” is on, “Inbound connections” is blocked, & “Outbound connections” is allowed.

- Customize General & Logging Settings:
  - Click on the “Customize” button in the “Settings” section.
  - Make sure “Display a notification” is set to “No”, “Apply local firewall rules” is set to “Yes”, & “Apply local connection security rules” is set to “Yes”. Click “Ok”.
  - Click on the “Customize” button in the “Logging” section.
  - Make sure “Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log”, “Size limit (KB)” is set to 16384 KB, “Log dropped packets” is set to “Yes”, & “Log successful connections” is set to “Yes”. Click “Ok”.
- Public Profile:
  - In the “Public Profile” tab, make sure “Firewall state” is on, “Inbound connections” is blocked, & “Outbound connections” is allowed.
  - Customize General & Logging Settings:
    - Click on the “Customize” button in the “Settings” section.
    - Make sure “Display a notification” is set to “No”, “Apply local firewall rules” is set to “No”, & “Apply local connection security rules” is set to “No”. Click “Ok”.
    - Click on the “Customize” button in the “Logging” section.
    - Make sure “Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log”, “Size limit (KB)” is set to 16384 KB, “Log dropped packets” is set to “Yes”, & “Log successful connections” is set to “Yes”. Click “Ok”.

- **Check Event Viewer**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “System & Security” & then select “Administrative Tools”.
  - In the new window, select “Event Viewer”, & another new window should open.
  - On the left-pane, select “Windows Logs”, & check each log for any bad stuff.
- **Turn Windows Features on or off**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “Programs” & then select “Programs & Features”.
  - On the left-pane, select “Turn Windows features on or off”, & a new window will open.
  - There, select any Windows features to turn on, & unselect any to turn off.
- **Disable Remote Connections**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “System & Security” & then select “System”.
  - On the left-pane, select “Remote settings”, & a new window will open.
  - There, select “Don’t allow remote connections to this computer”.

- **Enable Internet Security & Privacy Settings**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “Network & Internet” & then select “Internet Options”.
  - In the Security tab, slide the slider up so that the description says “High”
  - In the Privacy tab, check “Never allow websites to request your physical location” & “Turn on Pop-Up Blocker”.
  - Then select “Advanced” on the top-right & select “Block” for both First-party & Third-party Cookies.
- **Enable User Account Control (UAC)**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “System & Security” & then select “Security & Maintenance”.
  - On the left-pane, select “Change User Account Control settings”.
  - In the new window, move the slider to the top near where it says “Always notify”.
- **Require CTRL + ALT + DEL**
  - Through Local Security Policy:
    - Open Local Security Policy, select “Local Policies” & select “Security Options”.
    - Select “Interactive logon” & select “Do not require CTRL + ALT + DEL”
    - Change the setting to disabled & select “OK”
  - Through Network Places Wizard:
    - Open Network Places Wizard: Click the Start button, type “netplwiz” on the search bar, click enter, & select “Yes” if prompted. Network Places Wizard will open.
    - In the “Advanced” tab, “Secure sign-in” section, check the “Require users to press Ctrl+Alt+Delete” box.
    - Select “Apply”, & then select “Ok”.
- **Remove C-Drive file sharing**
  - Through Computer Management:
    - Open Computer Management: Click the Start button, type “Computer Management”, click enter, & select “Yes” if prompted. Computer Management should open.
    - Select “Shared Folders”, select “Shares”, & right-click the “C” share (Not “C$”)
    - Select “Stop Sharing” & select “Yes”
  - Through Command Prompt:
    - Open Command Prompt: Click the start button, type in “Command Prompt” on the search bar, & click enter. Command Prompt should open.
    - Type in “net share” in command prompt. A list of all shares should appear.
    - If one of the shares is “C” or “Users”, type in “net share [share] /delete”.

- **Turn on Back-Ups**
  - Open Control Panel: Click the Start button, type “Control Panel” on the search bar, click enter, & select “Yes” if prompted. Control Panel will open.
  - Make sure the “View By” option on the top-right is selected as “Category”.
  - Select “System & Security” & then select “Backup & Restore”.
  - On the left-pane, select both “Create a system image” & “Create a system repair disc”.
  - Then change the settings to set up regular, automatic full backups.
- **Clear DNS (Domain Name Servers)**
  - Open Command Prompt: Click the start button, type in “Command Prompt” on the search bar, & click enter. Command Prompt should open.
  - Type in “ipconfig /flushdns” in command prompt. It should read “Windows IP Configuration” & “Successfully flushed the DNS Resolver Cache.”
- **Check for & deny listening ports**
  - Open Command Prompt: Click the start button, type in “Command Prompt” on the search bar, & click enter. Command Prompt should open.
  - In Command Prompt, type in “netstat -aon | findstr :<#>”, where <#> is the port number you want to deny. Note the Port ID, the left-most number, of the port.
  - If the port says “LISTENING”, type in “taskkill /PID <Port Id> /F”, with <Port ID> being the Port ID.
  - Some common ports to deny: SSH - Port 22, Telnet - Port 23, FTP - Ports 20 & 21, RPC - Port 135, Direct Connect - Ports 411 & 412, RDP - Port 3389, POP3 - Port 110.
- **Set Automatic Updates**
  - Windows 10:
    - Open Windows Update Settings: Click the start button, type in “Windows Update Settings” in the search bar, & click enter. Windows Update Settings should open.
    - Select “Advanced Options” & chose automatic. You might either need to choose from a dropdown or enable it by selecting “Automatically Download Updates”.
  - Windows Server 2016:
    - Open Command Prompt: Click the start button, type in “Command Prompt” on the search bar, & click enter. Command Prompt should open.
    - Type in “sconfig” in command prompt. There should be a numbered list under the words “Server Configuration”.
    - Type in 5 & press enter. The type in “a” & press enter. Automatic updates should be enabled.
  - Through Batch Files (SOME SMALL ERRORS MAY BREAK MACHINE!):
    - Open Notepad(++): Click the Start button, type “Notepad”, click enter, & select “Yes” if prompted. Notepad(++) should open.
    - In the notepad file, type in “@echo off”, & then press enter twice.
    - Then, type “title Enable Windows Updates”, & press enter twice.
    - Next, type “reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update” /v AUOptions /t REG_DWORD /d 4 /f”.
    - Finally, type “pause”. The file should look like this:

```
@echo off

title Enable Updates

REM This registry key enables updates
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 4 /f

pause
```

- **Create Complete Batch File (Instead of Disable Guest Account, Firewall, Auto Updates)**
  - Open Notepad(++): Click the Start button, type "Notepad", click enter, & select "Yes" if prompted. Notepad(++) should open.
  - In the notepad file, type in "@echo off", & then press enter twice.
  - Then, type "title Complete Batch", & press enter twice.
  - After that, type "net user guest /active:no", & press enter twice.
  - Then, type "netsh advfirewall set allprofiles state on", & press enter twice.
  - Next, type "reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 4 /f".
  - Finally, type "pause". The file should look like this:

```
@echo off

Title CyberPatriot Script

REM Disable Guest Account
net user guest /active:no

REM Turn on Firewall
netsh advfirewall set allprofiles state on

REM Turn on Automatic Updates
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 4 /f

pause
```

- **Change Group Policies**
  - Open Group Policy Editor: Click the Start button, type "Gpedit" on the search bar, click enter, & select "Yes" if prompted. Group Policy Editor should open.
  - Edit Computer Configuration:
    - Select "Computer Configuration" on the left & then "Administrative Templates".
    - In the "Windows Components" folder, select "Windows Installer", & select "Prohibit User Installs".
  - Edit User Configuration:
    - Select "User Configuration" on the left & select "Administrative Templates".
    - In the "Control Panel" folder, select "Prohibit access to Control Panel & PC settings" & enable it.
    - In the "System" folder, select "Removable Storage Access", select "All Removable Storage classes: Deny all access", & enable it. Then select "Prevent access to the command prompt", & enable it.
    - In the "Windows Components" folder, select "Windows update", select "No auto-restart with logged on users for scheduled automatic updates installations", & enable it.

Windows 10 & Server 2016 How-To's

- **How to remove a program**
  - Go to Control Panel & select "Programs & Features"
  - Right-click the program, select "Uninstall", & select "Yes" if prompted. A screen showing "Uninstallation Complete" should appear.
  - Open File Explorer: Click the Start button, type in "File Explorer" on the search bar, & click enter. File explorer should open.
  - Select "This PC" on the left & search up the name of the program.
  - Delete it & any folders relating to it.
- **How to search for a file or file extension**
  - Open File Explorer, select "This PC", & click on the search bar on the top-right.
  - To search for a file, type in the name of the file & its extension (like .txt or .docx) & then click enter. The document & any related documents or folders will appear.
  - To search for a specific file extension, type in * & then the name of the file extension (like *.mp3). All the files with the file extension should appear (Useful for finding non-work related items like music).
- **How to identify a md5 hash of a document**
  - Open Powershell: Click the Start button, type "Powershell" on the search bar, click enter, & select "Yes" if prompted. Powershell should open.
  - Type in Powershell "Get-FileHash -Algorithm md5 (file directory here, like C:\Users\me\Documents\filename.txt for example)". A file hash should be generated.
  - Look under where is says "Hash" & you should see a file hash generated.
- **How to find the owner of a document**
  - Right-Click the document & select "Properties".
  - Select the "Security" tab and select "Advanced" at the bottom. The owner should appear at the top of the screen.
- **How to identify users in groups**
  - Open Microsoft Management Console: Click the Start button, type "mmc", click enter, & select "Yes" if prompted. Microsoft Management Console should open.
  - Select "File" on the top-right & select "Add/Remove Snap-in"
  - In the available snap-ins column, select "Local Users & Groups" & select the "Add" button in the center. Select "Finish" in the pop-up & then select "OK"
  - From the main window, select the "Local Users & Groups" snap-in, select the "Groups" folder, & select the desired group.
- **How to find the SID of a user**
  - Open Command Prompt: Click the start button, type in "Command Prompt" on the search bar, & click enter. Command Prompt should open.
  - In Command Prompt, type in "wmic useraccount where name="USER" get sid" where USER is the name of the user you want the SID for.