Ultimate Windows Checklist:

User Auditing Section:

- □ **Press the start button, type "Computer Management", open it. Do the following steps:**

- □ **Create group if needed:**
  - □ 1. Open Local Users and Groups category.
  - □ 2. Right click on Groups, and add a group.

- □ **Adding users to a group if needed:**
  - □ 1. Go to the list of groups.
  - □ 2. Select the group you want to add the user to, right click and press add to group.

- □ **Creating user accounts if needed:**
  - □ 1. Right click on the users folder.
  - □ 2. Press New User.

-TIP- See all users by pressing WIN + R and typing "netplwiz"

- □ **Remove terminated employees/unauthorized user accounts if needed:**
  - □ 1. Select Start > Settings > Accounts > Family & other users.
  - □ 2. Select the person's name or email address, then select Remove.

- □ **Add/Remove Admins if needed:**
  - □ 1. Select Start > Settings > Accounts .
  - □ 2. Under Family & other users, select the account owner name (you should see "Local account" below the name), then select Change account type.

- □ 3. Under Account type, select Administrator, and then select OK.

□ Change users passwords:

- □ 1. Open the Control Panel, and click on the User Accounts icon.
- □ 2. Click on the Manage another account link.
- □ 3. If prompted by User Account Control, click on Yes.
- □ 4. Click on a local account that you want to change or remove the password of.
- □ 5. Click on Change the password.
- □ 6. Type in a new password and password hint, and click on Change password.

□ Enable/Disable user accounts if needed:

- □ In the search bar or in the menu to execute (execute is called with the Win + r keys) type lusrmgr.msc and press Enter.
- □ Go to “Users” ⇨ right-click on the user whom you want to disable (enable) and select “Properties.”
- □ In the “General” tab, check the “Disable account” field and click “OK.” If you need to enable an account — uncheck the box “Disable account” and click “OK”.

□ Disable admin account:

- □ Go to the Start menu (or press Windows key + X) and select Computer Management.
- □ Then expand to Local Users and Groups, then Users.
- □ Select the Administrator and then right-click and select Properties.
- □ Uncheck Account is disabled to enable it, or check it to disable it.

□ Lockout/Un-Lockout User Account if needed:

- □ 1. Press the Win+R keys to open Run, type lusrmgr.msc into Run, and click/tap on OK to open Local Users and Groups.
- □ 2. Click/tap on Users in the left pane of Local Users and Groups.
- □ 3. Right click or press and hold on the name (ex: "Brink2") of the local account you want to unlock, and click/tap on Properties.
- □ 4. In the General tab, uncheck the Account is locked out box, and click/tap on OK.

□ Allow/Disallow users to change passwords if needed:

- □ 1. Press the Win+R keys to open Run, type lusrmgr.msc into Run, and click/tap on OK to open Local Users and Groups.
- □ 2. Click/tap on Users in the left pane of Local Users and Groups.
- □ 3. Right click or press and hold on the name (ex: "Brink2") of the user account you want, and click/tap on Properties.
- □ 4. Check or uncheck (default) the User cannot change password box for what you want to do, and click/tap on OK. (see screenshot below)

□ Disabling password never expires on all users:

- □ 1. Press the Win+R keys to open Run, type lusrmgr.msc into Run, and click/tap on OK to open Local Users and Groups.
- □ 2. Click/tap on Users in the left pane of Local Users and Groups.
- □ 3. Right click on every user account seen and go to properties.
- □ 4. Make sure password never expires is unchecked for ALL USERS.

Security Policy Section:

- □ **Block user from creating global objects if needed:**
  - □ 1. Open secpol.msc
  - □ 2. Open local policies, click on User Rights Assignment
  - □ 3. Double click on “Create global objects” and remove users if needed

Services Section:

□ Services:

Service Auditing:

96. DNS Server service has been stopped and disabled
97. FTP service has been stopped and disabled
98. Microsoft FTP service has stopped and disabled
99. Microsoft ISNS service has stopped and disabled
100. MultiPoint Service has been stopped and disabled
101. LPD service has been stopped and disabled
102. Net. TCP Port Sharing service has been stopped and disabled
103. RIP Listener service has been stopped and disabled
104. RPC Locator service has been stopped and disabled
105. Remote Access Connection Manager service has been stopped and disabled
106. Remote Registry service has been stopped and disabled
107. Simple Mail Transfer Protocol (SMTP) service has been stopped and disabled
108. SNMP service has been stopped and disabled
109. SNMP Trap service has been stopped and disabled
110. SSDP Discovery service has been stopped and disabled
111. Simple TCP/IP service has been stopped and disabled
112. Telephony service has been stopped and disabled
113. Telnet service has been stopped and disabled
114. UPnP Device Host service has been stopped and disabled
115. WebClient service has been stopped and disabled
116. World Wide Web Publishing Service has been stopped and disabled
117. Xbox Live Auth Manager has been stopped and disabled
118. Xbox Live Game Save service has been stopped and disabled
119. Windows Update service is enabled
120. Event Log service is enabled
121. Adobe Acrobat Update service is enabled
122. Windows Firewall service is enabled

Enable defensive countermeasures:

- □ **Enable windows defender antivirus:**
  - □ 1. Press start button, search “Windows Security” press enter
  - □ 2. Click “Virus and Threat Protection”, then “manage settings” under “Virus & threat protection settings”
  - □ 3. Enable Real-time protection, Cloud-delivered protection, and Automatic sample submission, (maybe tamper protection at the end if there is nothing left on this checklist)

- □ **Enable Bitlocker:**
  - □ 1. Press start button, search edit group policy, click computer configuration, click administrative templates, click windows components, click bitlocker drive encryption, and finally click operation system drives.
  - □ 2. Enable “Require additional authentication at startup”
  - □ 3. After that, in the same pop up window, choose “Do not allow TPM” under Configure TPM startup.
  - □ 4. Enable “Disallow standard users from changing the PIN or password”
  - □ 5. Close those tabs, press the start button, search “Bitlocker” and click manage bitlocker
  - □ 6. Click “Turn on BitLocker”
  - □ 7. Enter a complex password **YOU WILL REMEMBER** (You’ll be locked out if you don’t)
  - □ 8. Print recovery key to Microsoft pdf, call it “bitlocker_key”
  - □ 9. Choose encrypt entire drive
  - □ 10. Choose new encryption mode
  - □ 11. Click continue, run system check

- □ 12. Finally, restart the computer

Uncategorized OS Settings Section:

- □ **Turn off Remote Desktop Sharing:**
  - □ 1. Search “Remote Desktop Settings” in the start menu
  - □ 2. Make sure “Enable Remote Desktop” is switched off
  - □ 3. Click “Select users that can remotely access this PC” make sure there is nothing/nobody there

- □ **Disable remote assistance connections:**
  - □ Launch Windows Start Search. You can also launch Control Panel > System and Security > System.
  - □ Now click Advanced System Settings.
  - □ Click the Remote tab under System Properties.
  - □ To disable, uncheck Allow Remote Assistance connections to this computer. Click OK

- □ **Disable sharing:**
  - □ 1. Press WINDOWS + R and type services.msc
  - □ 2. Scroll down to Server and double click on it
  - □ 3. Change the “Startup type:” from Automatic to disabled.
  - □ 4. Press stop under “Service status”
  - □ 5. Press OK and close it

- □ **Disable C:/Hidden drive sharing:**
  - □ 1. First, see all drives being shared including hidden ones.
  - □ 2. To do this, open command prompt (start button, type “cmd”)
  - □ 3. Type “net share”
  - □ 4. That will print out a list of all currently shared drives.
  - □ 5. Next, type net share {SHARE} /delete to delete a share (works for hidden shares too)

- □ **Enable DEP (Data Execution Protection) for all programs and services:**
  - □ 1. Search “Control Panel” in the start button search box.
  - □ 2. Next, click System and Security > System > Advanced System Settings.
  - □ 3. On the Advanced tab, next to the Performance heading, click Settings.
  - □ 4. Click the Data Execution Prevention tab.
  - □ 5. Click “Turn on DEP for all programs and services except those | select:”
  - □ 6. Click Apply, OK, and exit the window.

- □ **Password protect screen saver: (Do for all users)**
  - □ 1. Open Settings.
  - □ 2. Go to Personalization - Lock screen.
  - □ 3. On the right side, scroll down until you see the link Screen saver settings. Click it to open screen saver options.
  - □ 4. The screen saver options dialog window will appear on the screen. There, pick a screen saver in the list if you haven't done this before (you can use any screen saver).
  - □ 5. Turn on the option On resume, display logon screen.
  - □ 6. Change wait to 10 minutes

- □ **Disable AutoPlay:**
  - □ 1. Press the start button, search “AutoPlay Settings” press enter
  - □ 2. Make sure AutoPlay is off, and change “Removable drive” and “Memory card” dropdowns to “Take no action”
  - □ 3. Do for all users

- ☐ **Exploit Protection Settings:**
  - ☐ 1. Search “Windows Security” in the start search box
  - ☐ 2. Click “App & Browser control” then “Exploit Protection Settings”
  - ☐ 3. Make sure everything is turned on except for “Force randomization for images (Mandatory ASLR)”
  - ☐ 4. Go into the program tab and look for any sus programs with overrides

Windows Updates:

- ☐ **Update Windows:**
  - ☐ 1. Search “Windows Update” in the start menu search box
  - ☐ 2. Click install updates and optional updates
  - ☐ 3. Restart computer

- ☐ **Update other microsoft products when updating windows:**
  - ☐ 1. Search “Windows Update” in the start menu search box
  - ☐ 2. Click “Advanced Options” toggle on the first option, “Receive updates for other Microsoft products when you update Windows”

- ☐ **Enable automatic updates:**
  - ☐ 1. Tap or click on the Start button, followed by Settings. You’ll need to be on the Windows 10 Desktop to do this.
  - ☐ 2. From Settings, tap or click on Update & security.
  - ☐ 3. Choose Windows Update from the menu on the left, assuming it’s not already selected.

- □ 4. Tap or click on the Advanced options link on the right, which will open a window headlined Choose how updates are installed.
- □ 5. Select Automatic (recommended) from the drop-down, check “Give me updates for other Microsoft products when I update Windows.” And do not check the Defer upgrades option.

Application Security Settings:

- □ **Enable smart screen settings:**
  - □ 1. Search “App and browser control” in the start search box
  - □ 2. Click “Reputation-based protection settings”
  - □ 3. Make sure everything is turned on

- □ **Internet options:**
  - □ 1. Search “Internet Properties” in the start button search box
  - □ 2. Click delete browsing history on exit
  - □ 3. Click on the security tab
  - □ 4. Set the slider all the way up
  - □ 5. Set the slider all the way up for the “Trusted sites” tab too
  - □ 6. Click the privacy tab
  - □ 7. Make sure all 3 boxes are checked
  - □ 8. Click advanced
  - □ 9. Make sure both cookies are on block and “Always allow session cookies” is unchecked.

- □ **Windows Features Settings:**
  - □ 1. Search “Turn windows features on and off”
  - □ 2. Ensure that Internet Information Services, SMB.1.*, and NFS are off/disabled.
  - □ 3. Ensure that no extra stuff was added there.

- □ **Default apps:**
  - □ 1. Search “Default apps” in the start search box
  - □ 2. Click “Choose default apps by file type”
  - □ 3. Make sure no file formats are being opened by a weird/unusual programs

Firefox Settings:

- □ **Firefox Settings:**
  - □ 1. Open Firefox
  - □ 2. Click the 3 lines in the top right, then help → about firefox
  - □ 3. Make sure you have the most current version
  - □ 4. Click options, look at all options and ****USE COMMON SENSE**** when going through these options.
  - □ 5. Click “Privacy and Security”
    - □ a) Enhanced tracking protection - strict
    - □ b) Send do not track signal - always
    - □ c) Cookies and sites data → manage data, see if anything needs to be removed
    - □ d) Delete cookies - check
    - □ e) Logins and password: don’t save logins, don’t autofill
    - □ f) History: Never remember
  - □ 6. Permissions:
    - □ a) Make sure no websites can use your camera, microphone, or location
    - □ b) Enable pop up blocker ****IMPORTANT****
    - □ c) Block dangerous content: Check all 3
    - □ d) Query OCSP responder: Check
    - □ e) Enable https only mode in all windows: check
  - □ 7. Other checks in Security tab:
    - □ a) Check both Block reported attack sites & Block reported web forgeries then press OK
    - □ b) Check all of the following in the Security tab: Warn me when sites try to install add-ons, Block reported attack sites, Block reported web forgeries
  - □ 8. Addons and themes tab:
    - □ a) Extensions
      - □ a) Delete any sus extensions
      - □ b) Check for updates for extensions (Gear icon near the top of the screen)
    - □ b) Themes:

        - □ a) Delete any weird/crazy themes
    - □ c) Plug-ins:
        - □ a) Delete any sus plug-ins
    - □ 9. Lastly, enable automatic firefox updates.

Prohibited Files/Malware Section:

- □ **Find and delete prohibited files:**
    - □ 1. Install [voidtools]
    - □ 2. Search for music/video file formats, commonly used ones include: .mp3, .mp4, .ogg, .avi, .wav, and any other media types.
    - □ 3. If you find any, delete them from the system and recycle bin.
    - □ 4. Search compressed files (.zip) and delete any sus ones
    - □ 5. Search executables (.exe) and delete any sus ones. (Sort by date modified, usually sus ones are recent)

- □ **Malware analysis:**
    - □ 1. Install Avast One
    - □ 2. Run a Deep/Full Scan and resolve any threats

- □ **OS Forensics:**
    - □ 1. Install OS Forensics with the free trial
    - □ 2. Go to the "User Activity" tab, live acquisition of current machine, and scan it
    - □ 3. Look for programs that have been recently run, especially any sus lookings ones under "user assist"
    - □ 4. Go to "Shellbags" look for any sus folders looked through
    - □ 5. Go to "Installed Programs" look for malicious files, if you find one chances are other files installed at that time/date are also malicious.
    - □ 6. Go to browser history and search terms, look for malicious stuff.
    - □ 7. Go to USB, look to see if any malicious things were added
    - □ 8. Go to passwords and change all weak passwords to secure

- □ **Delete Prohibited Programs:**

- □ 1. Search “Add or Remove Programs” in the start menu search box, remove any programs that shouldn’t be there or “hacking tools” (Java can stay)

□ **Delete any malicious scheduled tasks:**

- □ 1. Search “Task Scheduler” in the start menu search box
- □ 2. Click into “Task Scheduler Library”
- □ 3. Look for any malicious tasks, usually if it's from system 32 it can be trusted. Previous malicious tasks had names of “Bad_Task”

□ **Look for the following or similar backdoors (If time allows):**

- □ 217. Removed netcat backdoor
- □ 218. Removed tini backdoor
- □ 219. Remove ntbindshell backdoor
- □ 220. Removed TX backdoor
- □ 221. Removed NetBus Pro
- □ 222. Removed Sticky Keys backdoor
- □ 223. Removed Custom backdoor
- □ 224. Removed Actual Keylogger
- □ 225. Removed Keylogger
- □ 226. Removed Spyrix Keylogger
- □ 227. Removed Reveal Keylogger
- □ 228. Removed WindowsRAT
- □ 229. Removed WinUserProfileManager
- □ 230. Removed mimikatz script file
- □ 231. Removed NTDS dump script file
- □ 232. Reverse TCP DLL Removed from DNS Server

Firefox Configuration:

□ **Import firefox settings:**

- □ First, download both files from this folder:
- □ Next, go to the firefox preferences located at:

```
C:\Program Files\Mozilla Firefox\defaults\pref
```

- □ Paste the file “local-settings.js” into this folder
- □ Then go to the firefox installation directory:

```
C:\Program Files\Mozilla Firefox\
```

- □ Paste the other file, “mozilla.cfg”
- □ Restart firefox, then ensure it says “Some settings managed by your domain”
- □ For the settings that you’re still able to set, set them

- □ **Install Microsoft Baseline Security Analyzer 2 if out of things to score for points**

Finish Forensics Questions