SERVER 2022 SCRIPTING CHECKLIST (CYBERPATRIOT-STYLE)
(Designed so you can turn each line into PowerShell / GPO changes)

Note: This is written so you can:
- Read through top to bottom on the image manually, or
- Translate each sub-step into script functions (for example, one function per section).

Avoid hard-coding specific usernames from past images; always replace with the actual names in the README for your round.

==========
0. PRE-SCRIPT / PRE-FLIGHT
==========

0.1 Create a safe baseline
- Take a snapshot or checkpoint if it is a VM.
- Copy the original README and Forensics Questions to a safe location.
- Do not script actions that would delete or modify data needed to answer forensics.

0.2 Open admin PowerShell and basic logging
- Start PowerShell as Administrator.
- Make sure the log folder exists:
  - New-Item -ItemType Directory -Path "C:\HardeningLogs" -Force
- Turn on a transcript so you have a full log:
  - Start-Transcript -Path "C:\HardeningLogs\Server2022-Transcript-$(Get-Date -Format yyyyMMdd-HHmmss).txt" -Force

0.3 General script design choices
- Make the script idempotent:
  - Running it multiple times should not break anything.
- For each section:
  - Enumerate current state.
  - Decide desired state.
  - Apply changes only if needed.
  - Re-check and log "OK" or "FIXED".

==========
1. LOCAL USERS, ADMINS, AND GROUPS
==========

Goal: Remove bad users, fix admin rights, enforce proper groups to match scoring items.

1.1 Enumerate all local users
- Command:

  - Get-LocalUser | Select Name,Enabled,LastLogon
- Export to a CSV for review:
  - Get-LocalUser | Export-Csv "C:\HardeningLogs\LocalUsers-Before.csv" -NoTypeInformation

1.2 Build allow lists (from README and team notes)
- Create arrays in your script such as:
  - $AllowedAdmins = @("Administrator", "Domain Admins", "CoachAdmin")
  - $AllowedLocalUsers = @("legituser1", "legituser2")
- Include service accounts that must stay.

1.3 Remove clearly unauthorized local users
- Example from CP style images: users like "ttanner" or "tgianopolous" might be unauthorized.
- In script:
  - $BadLocalUsers = @("ttanner","tgianopolous","otherBadNames")
  - ForEach ($u in $BadLocalUsers) {
      if (Get-LocalUser -Name $u -ErrorAction SilentlyContinue) {
          Remove-LocalUser -Name $u
      }
    }

1.4 Fix local Administrators group
- Get the current members:
  - Get-LocalGroupMember "Administrators"
- Build a list of allowed admin principals, for example:
  - $AllowedAdminPrincipals = @("BUILTIN\Administrators","DOMAIN\Domain Admins","CoachAdmin")
- For each member:
  - If member is not in $AllowedAdminPrincipals, remove it with Remove-LocalGroupMember "Administrators" -Member <name>.
- Make sure you do not remove core built-ins that are required by the system.

1.5 Enforce non-admin standard users
- For each user that must exist but should not be admin:
  - Ensure they are not in "Administrators".
  - Ensure they are in the "Users" group or other limited group.

1.6 Ensure Guest is disabled
- In script:
  - $guest = Get-LocalUser -Name "Guest" -ErrorAction SilentlyContinue
  - If $guest exists, set Enabled to $false:
    - Disable-LocalUser -Name "Guest"

1.7 Create required group "Exec SMB Users" if needed
- For CP 18 style Server 2022 images, there is a group called "Exec SMB Users".

- If needed in your scenario:
  - If (-not (Get-LocalGroup -Name "Exec SMB Users" -ErrorAction SilentlyContinue)) {
      New-LocalGroup "Exec SMB Users"
    }
  - Add required executive accounts:
    - Add-LocalGroupMember -Group "Exec SMB Users" -Member "execuser1","execuser2"

1.8 Ensure no local account uses a blank or non-expiring password
- For local users:
  - If password does not expire or blank passwords are suspected, enforce a change:
    - net user username * /logonpasswordchg:yes
- For domain users, use AD cmdlets instead.

==========
2. PASSWORD AND ACCOUNT LOCKOUT POLICY
==========

Goal: Configure strong password and lockout policy according to CIS and CyberPatriot style.

2.1 Password history, age, length, and complexity
- Desired values (CIS Server 2022 Level 1 style):
  - Enforce password history: at least 24 passwords remembered.
  - Maximum password age: 60 to 365 days, but not 0.
  - Minimum password age: at least 1 day.
  - Minimum password length: at least 14 characters.
  - Password must meet complexity requirements: Enabled.
  - Store passwords using reversible encryption: Disabled.

2.2 Account lockout policy
- Desired values:
  - Account lockout threshold: 5 invalid logon attempts (do not leave at 0).
  - Account lockout duration: at least 15 minutes.
  - Reset account lockout counter after: at least 15 minutes.
- On some images there is an item for "secure lockout threshold" and "lockout duration".

2.3 Script approach for account policies
- Export current security policy:
  - secedit /export /cfg C:\HardeningLogs\secpol-before.inf
- Edit the .inf file or create a hardened version with:
  - PasswordHistorySize = 24
  - MaximumPasswordAge = 60
  - MinimumPasswordAge = 1
  - MinimumPasswordLength = 14
  - PasswordComplexity = 1

  - LockoutBadCount = 5
  - ResetLockoutCount = 15
  - LockoutDuration = 15
- Apply hardened policy:
  - secedit /configure /db C:\Windows\Security\Database\secedit.sdb /cfg C:\Hardening\server2022-secpol.inf /overwrite /quiet
- Export again to confirm:
  - secedit /export /cfg C:\HardeningLogs\secpol-after.inf

2.4 Limit local use of blank passwords to console logon only
- Security Option: "Accounts: Limit local account use of blank passwords to console logon only" should be Enabled.
- Registry:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
  - Value: LimitBlankPasswordUse (DWORD) = 1
- Script:
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "LimitBlankPasswordUse" /t REG_DWORD /d 1 /f

==========
3. USER RIGHTS ASSIGNMENT (LOGON RIGHTS)
==========

Goal: Restrict who can log on and access the server over the network.

3.1 "Access this computer from the network"
- Should be restricted to:
  - Administrators
  - Authenticated Users
  - Domain-specific groups if needed (Domain Controllers group if it is a DC).
- It must not include "Everyone".
- Implement through Security Policy INF or secedit.
  - In INF: SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11
  - Apply via secedit as in Section 2.3.

3.2 "Deny access to this computer from the network"
- Should include:
  - Guests
  - Local account (and other unneeded groups).
- Set in INF:
  - SeDenyNetworkLogonRight = *S-1-5-32-546,*S-1-5-113
  (These SIDs are examples; map correctly in your INF.)

3.3 Other important user rights to consider

- Debug programs: Administrators only.
- Back up files and directories: Administrators only.
- Restore files and directories: Administrators only.
- Enable computer and user accounts to be trusted for delegation:
  - On DC: usually Domain Admins.
  - On member servers: No one.
- Allow log on through Remote Desktop Services:
  - Administrators and Remote Desktop Users only.
- Deny log on through Remote Desktop Services:
  - Guests and any unauthorized groups.

3.4 Script approach
- General method:
  - secedit /export /cfg secpol-current.inf
  - Modify the Se* entries under [Privilege Rights].
  - secedit /configure /db secedit.sdb /cfg secpol-hardened.inf /areas USER_RIGHTS /quiet
- Re-export to confirm.

==========
4. SECURITY OPTIONS (LOCAL SECURITY POLICY)
==========

Goal: Align with hardening guidelines and scoring items.

4.1 Anonymous restrictions and LM/NTLM settings
- Do not allow anonymous enumeration of SAM accounts and shares.
- Do not let "Everyone" permissions apply to anonymous users.
- Security Options should include:
  - Network access: Do not allow anonymous enumeration of SAM accounts: Enabled.
  - Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled.
  - Network access: Let Everyone permissions apply to anonymous users: Disabled.
- LMCompatibilityLevel:
  - Set "Network security: LAN Manager authentication level" to "Send NTLMv2 responses only. Refuse LM & NTLM."
- Registry examples:
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "RestrictAnonymousSAM" /t REG_DWORD /d 1 /f
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "RestrictAnonymous" /t REG_DWORD /d 1 /f
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "EveryoneIncludesAnonymous" /t REG_DWORD /d 0 /f
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "LmCompatibilityLevel" /t REG_DWORD /d 5 /f

4.2 SMB related options (client and server)
- Microsoft network server: Digitally sign communications (always): Enabled.
- Microsoft network client: Digitally sign communications (if server or domain member): Enabled.
- Microsoft network client: Send unencrypted password to third-party SMB servers: Disabled.

4.3 Interactive logon and banners
- Interactive logon: Do not require CTRL+ALT+DEL should be Disabled (so users must press CTRL+ALT+DEL).
- Optionally set:
  - Interactive logon: Message title for users attempting to log on.
  - Interactive logon: Message text for users attempting to log on.
- Registry for DisableCAD:
  - reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCAD" /t REG_DWORD /d 0 /f

4.4 UAC (User Account Control)
- Make sure UAC is fully enabled:
  - EnableLUA = 1
  - PromptOnSecureDesktop = 1
  - ConsentPromptBehaviorAdmin = 2 or stricter.
- Registry:
  - $uacKey = "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
  - reg add $uacKey /v "EnableLUA" /t REG_DWORD /d 1 /f
  - reg add $uacKey /v "PromptOnSecureDesktop" /t REG_DWORD /d 1 /f
  - reg add $uacKey /v "ConsentPromptBehaviorAdmin" /t REG_DWORD /d 2 /f

==========
5. SMB CONFIGURATION, SHARES, AND PERMISSIONS
==========

Goal: Disable SMBv1, remove or restrict bad shares, properly set Exec SMB share.

5.1 Disable SMBv1 server and client
- Disable feature:
  - Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol" -NoRestart
- Or disable via registry/service:
  - For the mrxsmb10 driver:
    - reg add "HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10" /v "Start" /t REG_DWORD /d 4 /f
- Confirm using:
  - Get-SmbServerConfiguration | Select EnableSMB1Protocol

5.2 Enumerate and clean up shares

- List shares:
  - Get-SmbShare
- System default shares to keep:
  - C$
  - ADMIN$
  - IPC$
  - Any domain-required shares like SYSVOL, NETLOGON on a DC.
- For every non-system share not in README:
  - Consider removing with:
    - Remove-SmbShare -Name "ShareName" -Force

5.3 Hidden share "Private$"
- In some CP images, there is a hidden share Private$ that must have file sharing disabled.
- If "Private$" exists and scenario wants it disabled:
  - Remove-SmbShare -Name "Private$" -Force

5.4 Create and configure Executive SMB Share
- Create folder for the share:
  - New-Item -ItemType Directory -Path "C:\Shares\Executive" -Force
- Remove "Everyone" from folder NTFS ACL.
- Grant:
  - Administrators: Full control.
  - Exec SMB Users: Modify, Read & Execute, List folder contents, Read.
- Create the share:
  - New-SmbShare -Name "Exec" -Path "C:\Shares\Executive" -FullAccess "Administrators" -ChangeAccess "Exec SMB Users"
- Confirm:
  - Get-SmbShare -Name "Exec"
  - Get-Acl "C:\Shares\Executive"

5.5 Ensure all non-system shares restrict access to required groups
- For each non-system share:
  - Check share permissions:
    - Get-SmbShare -Name <name> | Get-SmbShareAccess
  - Remove unwanted groups (Everyone, Authenticated Users) if the scenario expects restricted access.
  - Only keep groups and users that actually need access.

==========
6. WINDOWS UPDATE AND APPLICATION UPDATES
==========

Goal: Ensure that Windows and key applications are updated and configured to check for updates.

6.1 Windows Update configuration
- Make sure Windows Update service is running and Startup Type is Manual or Automatic, not Disabled.
- Configure automatic updates via Group Policy or registry so that Windows automatically checks for and installs updates.
- Trigger a scan (when allowed by time and network):
  - usoclient StartScan

6.2 Application updates (for example, Notepad++ and Wireshark)
- Many CP images score for "Notepad++ updated" and "Wireshark updated".
- In script design:
  - Detect installed version from registry or by running the application with a version argument.
  - If outdated:
    - Perform silent upgrade using MSI or EXE if allowed.
  - If not required, but installed:
    - Decide whether update or uninstall fits the scenario better.

==========
7. MALICIOUS FILES, BACKDOORS, AND UNWANTED SOFTWARE
==========

Goal: Remove TightVNC, netcat backdoor, plain text passwords, and any prohibited tools or games.

7.1 Remove TightVNC Server and netcat if they are not required
- Enumerate installed programs from registry:
  - Check HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall and Wow6432Node.
- When you confirm:
  - Uninstall "TightVNC" or "netcat" using their uninstall strings.
- Also search for binaries under Program Files and Program Files (x86) and remove left-over directories if safe.

7.2 Remove plain-text password files
- Search for suspicious password files:
  - Use Get-ChildItem across user folders with names like:
    - passwords.txt
    - creds.txt
  - If found:
    - Move to a secure evidence directory or delete, depending on README and scoring.

7.3 Remove prohibited MP3s, media, or games
- Search for:
  - *.mp3, *.wav, *.mp4, *.avi in users' Music, Desktop, Downloads, and Documents.

- For each file that is clearly prohibited:
  - Remove-Item with Force.
- Also search for games or unauthorized software:
  - Look for .exe in user directories with known game names.

7.4 Remove any other hacking tools and malware
- Check:
  - C:\Users\Public\Downloads
  - C:\Users\<user>\Downloads
  - C:\Tools or similar directories if present.
- Remove archives, tools, or scripts that are obviously hacking tools unless the README explicitly requires them.

==========
8. AUDIT POLICY AND LOGGING
==========

Goal: Configure auditing for file shares and important events.

8.1 Configure audit policy via auditpol
- Enable auditing for:
  - File share access:
    - auditpol /set /subcategory:"File Share" /success:enable /failure:enable
  - Logon/Logoff categories:
    - auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
  - Account management:
    - auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
  - System integrity:
    - auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable
  - Policy change:
    - auditpol /set /category:"Policy Change" /success:enable /failure:enable

8.2 Enforce advanced audit subcategories over legacy settings
- Set:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
  - SCENoApplyLegacyAuditPolicy (DWORD) = 1

8.3 Event log size and retention
- Increase Security log size and configure retention appropriately:
  - wevtutil sl Security /ms:20971520
- Repeat for Application and System logs with reasonable sizes.

==========
9. WINDOWS DEFENDER AND ANTIVIRUS CONFIGURATION

==========

Goal: Ensure Windows Defender is active and configured to detect PUA and other threats.

9.1 Confirm Windows Defender Antivirus is running
- Check in Windows Security center or via PowerShell:
  - Get-MpComputerStatus
- Ensure real-time protection is enabled.

9.2 Configure Defender preferences with Set-MpPreference
- Examples:
  - Set-MpPreference -PUAProtection Enabled
  - Set-MpPreference -ScanRemovableDrives $true
  - Set-MpPreference -MAPSReporting Advanced
  - Set-MpPreference -SubmitSamplesConsent SendSafeSamples

9.3 Run a quick scan if time allows
- Start:
  - Start-MpScan -ScanType QuickScan

==========
10. REMOTE DESKTOP AND OTHER REMOTE ACCESS
==========

Goal: Harden RDP configuration and block unnecessary remote access.

10.1 RDP security settings
- Require Network Level Authentication for RDP:
  - SystemPropertiesRemote.exe or Group Policy:
    - Require user authentication for remote connections using NLA.
- Set RDP encryption level to High or SSL-based, if exposed in policy.
- Always prompt for password upon connection.

10.2 Restrict redirection of devices in RDP
- Use Group Policy (gpedit.msc):
  - Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Device and Resource Redirection.
- Disable:
  - COM port redirection.
  - Drive redirection.
  - LPT port redirection.
  - Plug and Play device redirection.

10.3 Limit who can connect via RDP

- Ensure "Remote Desktop Users" group contains only approved accounts.
- Deny RDP to Guests and any non-approved users through user rights assignment or group membership.

10.4 Remove other remote control tools
- Make sure tools like TightVNC, remote admin tools, or unauthorized remote agents are removed unless the README specifically requires them.

==========
11. SERVICES AND FEATURES
==========

Goal: Disable unnecessary services, keep required services running.

11.1 Enumerate services
- Command:
  - Get-Service | Sort-Object Status,Name
- Log the list to a CSV for later comparison.

11.2 Disable unnecessary services while keeping core roles
- Candidate services to disable if not required:
  - RemoteRegistry
  - Telnet
  - FTP services (if present)
  - SNMP (if not used)
  - Any third-party services that are clearly not part of the scenario.
- Use:
  - Set-Service -Name <ServiceName> -StartupType Disabled
  - Stop-Service -Name <ServiceName> -Force

11.3 Ensure required services are running
- For example:
  - DNS (if domain controller).
  - Active Directory Domain Services (NTDS).
  - File and Printer Sharing (LanmanServer) if file server.
- Start them if they are stopped:
  - Start-Service <ServiceName>

==========
12. FORENSICS PROTECTION
==========

Goal: Do not destroy evidence needed to answer Forensics Questions.

12.1 Read all Forensics Questions before script changes
- Manually open each Forensics file on the Desktop.
- Write answers down as required by the problem statement.
- Only after answering, allow your script to touch files or settings that might change evidence.

12.2 Script should avoid wiping suspicious folders until forensics is done
- Your script can include variables like:
  - $ForensicsCompleted = $false
- Only run destructive cleanup tasks if $ForensicsCompleted is set to $true by user input.

==========
13. FINAL VALIDATION AND SELF-CHECK
==========

Goal: Confirm that your script has hit all scoring points and not broken the server.

13.1 Re-enumerate users, groups, shares, and policies
- Rerun:
  - Get-LocalUser | Export-Csv C:\HardeningLogs\LocalUsers-After.csv
  - Get-LocalGroupMember "Administrators"
  - Get-SmbShare
  - auditpol /get /category:* > C:\HardeningLogs\auditpol-after.txt

13.2 Manual checklist pass for key points
- Unauthorized users removed.
- Admin group fixed.
- Exec SMB Users group created and filled correctly.
- SMBv1 disabled.
- Private$ share disabled if required.
- Exec SMB share configured with correct share and NTFS permissions.
- Password policy and lockout policy match hardened settings.
- LimitBlankPasswordUse enabled.
- Windows automatically checks for updates.
- Notepad++ and Wireshark updated (or handled correctly).
- Plain-text passwords file removed or secured.
- TightVNC and netcat removed (or not present if not part of scenario).
- Audit File Share success enabled.

13.3 Save and stop transcript
- End logging:
  - Stop-Transcript
- Zip up C:\HardeningLogs for future review and training.

==========

END OF SERVER 2022 SCRIPTING CHECKLIST
==========