==========
ULTIMATE CYBERPATRIOT SERVER CHECKLIST (WINDOWS SERVER 2019/2022)
==========

SCOPE:
- Windows Server 2019 and Windows Server 2022
- Domain Controller or Member Server
- CyberPatriot scoring + best practices from CIS/STIG-style hardening

IMPORTANT GENERAL RULES:
- Always obey the README. If it says a service/software/role is required, keep it.
- Fix Forensics FIRST whenever possible so you don't delete evidence.
- For domain controllers, be careful with DNS/AD roles and IPv6 (don't kill the domain).
- Document changes in a text file: C:\Hardening-Notes.txt

PHASE 0 – INITIAL RECON & FORENSICS

0.1 Identify server role
- Open "Server Manager".
- Check:
  - Dashboard: see if "Active Directory Domain Services", "DNS", "File and Storage Services", "IIS", etc. are installed.
  - If AD DS + DNS present: this is a Domain Controller.
  - Note installed roles and features in your notes.

0.2 Read README and Forensics docs
- On Desktop:
  - Open README file. Write down:
    - Allowed local users.
    - Allowed domain users and groups.
    - Required applications and services.
    - Critical roles (DNS, IIS, file shares, etc.).
    - Any explicitly allowed "hacking tools" or utilities.
  - Open each "Forensics Question X" document and read fully.

0.3 Answer Forensics Questions before breaking evidence
Common patterns:

0.3.1 Shared folder path (e.g., greybeard share)
- Win + R → type: fsmgmt.msc → Enter (Shared Folders).
- Click "Shares".
- Double-click suspicious share (e.g., greybeard, NTDSdump, Private$).

- Copy full “Folder path” into the Forensics answer.
- Save and close the Forensics file.

0.3.2 Hash of a file (e.g., jarlsberg.png)
- Shift + right-click on Desktop → “Open PowerShell window here”.
- Run:
  Get-FileHash -Algorithm SHA256 .\filename.ext
- Copy the Hash value into the Forensics answer file.

0.3.3 Credentials or paths in text/log/pcap
- If given a pcap:
  - Open in Wireshark (if present).
  - Filter (e.g., http, ftp, smtp) to find usernames/passwords, hostnames, or IPs.
- If given a log file / OSForensics hint:
  - Use search (Ctrl+F) inside the log viewer or Notepad to locate requested string.
- Paste answers exactly in the requested format.

0.3.4 Multi-part forensics (e.g., multiple usernames)
- Answer each line exactly as instructed (no extra spaces or punctuation).
- Save all Forensics docs before continuing.

PHASE 1 – USER / GROUP AUDIT (LOCAL + DOMAIN)

1.1 Local Users and Groups (member server)
- Win + R → lusrmgr.msc → Enter.
- Click “Users”.
- Compare all accounts vs README:
  - Delete unauthorized users:
    - Right-click user → Delete → Yes.
  - For suspicious “service” users not in README:
    - Check if tied to required software; if not, delete or disable.

1.2 Local group membership
- In lusrmgr.msc → “Groups”:
  - Open each of these at minimum:
    - Administrators
    - Remote Desktop Users
    - Backup Operators
    - Users
    - IIS_IUSRS (if IIS installed)
  - Remove any user/group not explicitly allowed by README or expected roles.
  - Ensure:

- Only approved admins in “Administrators”.
- Only allowed RDP users in “Remote Desktop Users”.
- “Guests” group only contains the Guest account if Guest is used at all.

1.3 Domain Users and Groups (Domain Controller)
- Server Manager → Tools → “Active Directory Users and Computers” (dsa.msc).
- Check:
  - “Users” container and any OUs with user accounts.
- For each unauthorized domain user (names from README or answer keys):
  - Right-click user → Disable or Delete (based on README expectations).
- Admin groups:
  - Right-click “Domain Admins” → Properties → Members.
    - Remove anyone not on the approved list.
  - Right-click “Enterprise Admins” (if present) → Members → remove unauthorized accounts.
  - Check other powerful groups:
    - “Schema Admins”
    - “DnsAdmins”
    - Any custom admin groups.
  - Remove “Domain Users” or large catch-all groups from powerful roles like DnsAdmins.

1.4 Ensure password expiration for normal users
- For each non-service user:
  - In lusrmgr.msc or ADUC (domain):
    - Right-click user → Properties.
    - Make sure:
      - “Password never expires” is unchecked unless user is explicitly a service account.
      - If image requires “user X must change password at next logon”, check that box.

PHASE 2 – ACCOUNT & PASSWORD POLICIES

2.1 Local Security Policy
- Win + R → secpol.msc → Enter.
- Go to:
  - Security Settings → Account Policies → Password Policy.

2.2 Password Policy
Set these (server-safe values that match CIS + CP patterns):

- Enforce password history:
  - 24 passwords remembered (or at least 12; do not leave at 0).
- Maximum password age:
  - 60–90 days.

- Minimum password age:
  - ≥ 1 day.
- Minimum password length:
  - 14 characters (if competition seems to use 10, at least 10; 14 is CIS-friendly).
- Password must meet complexity requirements:
  - Enabled.
- Store passwords using reversible encryption:
  - Disabled.

2.3 Account Lockout Policy
- Security Settings → Account Policies → Account Lockout Policy.
- Set:
  - Account lockout threshold:
    - 5–10 invalid logon attempts (never 0, never < 5).
  - Account lockout duration:
    - At least 15 minutes.
  - Reset account lockout counter after:
    - 15 minutes or more.
- This hits “secure lockout threshold” and “account lockout duration” scoring.

2.4 Kerberos Policy (Domain Controller)
- Security Settings → Account Policies → Kerberos Policy.
- Configure:
  - Enforce user logon restrictions:
    - Enabled.
  - Maximum lifetime for user ticket:
    - 10 hours.
  - Maximum lifetime for service ticket:
    - 600 minutes.
  - Maximum lifetime for user ticket renewal:
    - 7 days.
  - Maximum tolerance for computer clock synchronization:
    - 5 minutes.
- In Group Policy (if exposed):
  - Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos.
  - For “Configure encryption types allowed for Kerberos”:
    - Select AES-based options only (disable RC4, DES).

PHASE 3 – SECURITY OPTIONS (LOCAL POLICIES)

3.1 Accounts options

- secpol.msc → Security Settings → Local Policies → Security Options.
Configure:

- Accounts: Guest account status:
  - Disabled (for servers, unless README says otherwise).
- Accounts: Limit local account use of blank passwords to console logon only:
  - Enabled.
- Accounts: Rename administrator account:
  - Rename “Administrator” to a non-obvious name, unless README defines the name.
- Accounts: Rename guest account:
  - Rename or disable as above.
- Accounts: Block Microsoft accounts:
  - “Users can’t add or log on with Microsoft accounts” (if present).

3.2 Audit-related options
- Audit: Force audit policy subcategory settings to override category settings:
  - Enabled (allows Advanced Audit Policy to take effect).
- Audit: Shut down system immediately if unable to log security audits:
  - Disabled (avoid accidental DoS in competition).

3.3 Network security and anonymous access
Configure all of these as hardened:

- Network access: Do not allow anonymous enumeration of SAM accounts:
  - Enabled.
- Network access: Do not allow anonymous enumeration of SAM accounts and shares:
  - Enabled, if present.
- Network access: Let Everyone permissions apply to anonymous users:
  - Disabled.
- Network access: Restrict anonymous access to Named Pipes and Shares:
  - Enabled (or “No access without explicit permissions”).
- Network access: Shares that can be accessed anonymously:
  - Empty (no extra shares).
- Network security: LAN Manager authentication level:
  - “Send NTLMv2 response only. Refuse LM & NTLM.”
- Network security: Minimum session security for NTLM SSP based clients:
  - Require 128-bit encryption.
- Network security: Minimum session security for NTLM SSP based servers:
  - Require 128-bit encryption.
- LDAP client signing requirements:
  - Require signing.

3.4 Interactive logon
- Interactive logon: Do not require CTRL+ALT+DEL:

  - Disabled (so CTRL+ALT+DEL **is** required).
- Interactive logon: Message title for users attempting to log on:
  - “Authorized Use Only” (or similar).
- Interactive logon: Message text for users attempting to log on:
  - Add standard legal banner text (warning about monitoring, prosecution, etc.).
- Interactive logon: Machine inactivity limit:
  - 900 seconds (15 minutes) or less.
- Interactive logon: Number of previous logons to cache:
  - 4 or fewer (or default recommended by CIS).

3.5 Domain controller-specific options
- Domain controller: LDAP server signing requirements:
  - Require signing.
- Domain controller: Refuse machine account password changes:
  - Disabled.
- Domain controller: Allow server operators to schedule tasks:
  - Disabled.

3.6 Other critical Security Options
- Recovery console: Allow automatic administrative logon:
  - Disabled.
- Clear virtual memory pagefile:
  - Enabled (forces pagefile wipe at shutdown).
- Strengthen default permissions of internal system objects:
  - Enabled.
- Optional subsystems:
  - Null (empty).
- Require case insensitivity for non-Windows subsystems:
  - Enabled.
- Use certificate rules on Windows executables for Software Restriction Policies:
  - Enabled (if policy is in use).
- Allow system to be shut down without having to log on:
  - For servers: Disabled.

3.7 UAC (User Account Control)
- Control Panel → User Accounts → Change User Account Control settings:
  - Drag slider to the **highest** level (“Always notify”).
- In Security Options / from Mega Checklist:
  - Run all administrators in Admin Approval Mode:
    - Enabled.
  - Switch to the secure desktop when prompting for elevation:
    - Enabled.
  - Behavior of the elevation prompt for administrators:
    - Prompt for consent on the secure desktop (or “Prompt for credentials”).

- Behavior of the elevation prompt for standard users:
  - Prompt for credentials.
- Only elevate UIAccess applications that are installed in secure locations:
  - Enabled.
- Virtualize file and registry write failures to per-user locations:
  - Enabled.

PHASE 4 – ADVANCED AUDIT POLICY

4.1 Basic Audit Policy

- secpol.msc → Security Settings → Local Policies → Audit Policy:
  - Audit account logon events: Success, Failure.
  - Audit logon events: Success, Failure.
  - Audit account management: Success, Failure.
  - Audit directory service access (for DCs): Success, Failure.
  - Audit policy change: Success, Failure.
  - Audit privilege use: Failure (and Success if you can handle more logs).
  - Audit system events: Success, Failure.

4.2 Advanced Audit Policy Configuration

- secpol.msc → Advanced Audit Policy Configuration → System Audit Policies.
- Ensure at least:
  - Account Management:
    - User Account Management: Success, Failure.
  - Authentication Policy Change:
    - Authentication Policy Change: Success.
  - Logon/Logoff:
    - Logon: Success, Failure.
    - Account Lockout: Success.
  - System:
    - System Integrity: Success, Failure.
  - Object Access:
    - File Share: Success (for file servers).

4.3 DNS auditing (Domain Controller)

- Open PowerShell as Administrator:
  - Set-DnsServerDiagnostics -EventLogLevel 3
- This enables “Audit DNS events” and is explicitly scored.

PHASE 5 – USER RIGHTS ASSIGNMENT

5.1 Open User Rights Assignment
- secpol.msc → Security Settings → Local Policies → User Rights Assignment.

5.2 Lock down dangerous rights
For each right, set to minimal safe groups:

- Access this computer from the network:
  - Domain Controller: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.
  - Member Server: Administrators, Authenticated Users.
  - Remove “Everyone”.
- Allow log on locally:
  - Administrators (and backup operators if required).
  - Remove Guests or unnecessary groups.
- Allow log on through Remote Desktop Services:
  - Administrators and the specific Remote Desktop Users group (if RDP required).
  - Remove broad groups like “Users” or “Everyone”.

- Back up files and directories:
  - Administrators.
- Restore files and directories:
  - Administrators.
- Change the system time/zone:
  - Administrators, LOCAL SERVICE.
- Force shutdown from a remote system:
  - Administrators only.
- Shut down the system:
  - Administrators only.
- Load and unload device drivers:
  - Administrators only.
- Take ownership of files or other objects:
  - Administrators only.
- Debug programs:
  - Administrators only.
- Enable computer and user accounts to be trusted for delegation:
  - Domain Admins or NO ONE (depending on domain policy).
  - Ensure “Everyone” is NOT here.

Deny rights:
- Deny access to this computer from the network:
  - Guests, Local account (and local accounts of member servers if using domain policies).
- Deny log on locally:
  - Guests.

- Deny log on through Remote Desktop Services:
  - Guests, Local account.

Service-related rights:
- Generate security audits:
  - LOCAL SERVICE, NETWORK SERVICE.
- Impersonate a client after authentication:
  - Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE, IIS_IUSRS (if IIS).
- Log on as a batch job:
  - Only necessary service accounts (or Administrators if needed).
- Access Credential Manager as a trusted caller:
  - No One.

PHASE 6 – NETWORK ADAPTER & PROTOCOL HARDENING

6.1 Network adapter properties (member servers / non-AD critical machines)
- Control Panel → Network and Sharing Center → Change adapter settings.
- Right-click primary adapter → Properties.
- For CyberPatriot workstation-style servers where safe (NOT critical DC dependencies):
  - Consider unchecking:
    - Client for Microsoft Networks (only if not joining domain / not sharing).
    - File and Printer Sharing for Microsoft Networks (if file sharing not needed).
    - QoS Packet Scheduler (if not needed).
    - LLDP and Link Layer Topology Discovery Mapper/Responder (if not used).
  - Always leave:
    - IPv4 enabled (critical).
- For domain controllers / file servers:
  - Leave Client for Microsoft Networks and File and Printer Sharing enabled.
  - Focus on DNS / WINS tweaks instead of unchecking core protocols.

6.2 IPv4 advanced settings
- In adapter Properties:
  - Select “Internet Protocol Version 4 (TCP/IPv4)” → Properties → Advanced.
  - DNS tab:
    - Uncheck “Register this connection’s addresses in DNS” if server should not auto-register.
  - WINS tab:
    - Select “Disable NetBIOS over TCP/IP” unless NetBIOS is required.

6.3 IPv6
- For pure member servers not using AD over IPv6:
  - You may uncheck IPv6 if safe and consistent with README.
- For domain controllers or complex environments:

- Leave IPv6 enabled to avoid breaking AD/DC behavior.

6.4 Disable UPnP (port 1900)
- Registry (only if you're comfortable):
  - Win + R → regedit.
  - Navigate to:
    - HKLM\Software\Microsoft\DirectPlayNATHelp\DPNHUPnP
  - Right-click right pane → New → DWORD (32-bit) Value:
    - Name: UPnPMode
    - Value: 2
  - This hardens UPnP behavior.

PHASE 7 – FIREWALL & DEFENSIVE TOOLS

7.1 Turn on Windows Defender Firewall for all profiles
- Control Panel → Windows Defender Firewall.
- Ensure:
  - Domain network: On.
  - Private network: On.
  - Public network: On.

7.2 Harden inbound rules
- Click "Advanced settings" → Windows Defender Firewall with Advanced Security.
- Inbound Rules:
  - Disable or delete rules for:
    - Consumer apps (Microsoft Edge inbound, MSN apps, Xbox, etc.) if present.
    - Any inbound rules for games or random apps.
  - Keep or configure rules only for:
    - DNS (if server is DNS server).
    - File & printer sharing (if file server).
    - IIS HTTP/HTTPS (if web server).
    - RDP (if allowed by README).
- Outbound Rules:
  - Default allow is usually fine.
  - Disable obviously malicious or unnecessary outbound rules (e.g., weird remote tools).

7.3 Windows Defender / AV
- Open "Windows Security".
- Virus & threat protection:
  - Ensure real-time protection is ON.
  - Cloud-delivered protection ON.
  - Automatic sample submission ON.

PHASE 8 – REMOTE ACCESS: RDP, REMOTE ASSISTANCE, WINRM

8.1 Remote Desktop
- This depends on README:
  - If RDP should be allowed:
    - System Properties → Remote tab.
    - Enable “Allow remote connections to this computer”.
    - Require “Network Level Authentication”.
    - Add ONLY allowed users to “Remote Desktop Users” group.
  - If RDP should be disabled:
    - gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections.
      - “Allow users to connect remotely by using Remote Desktop Services” = Disabled.

8.2 Remote Assistance
- System Properties → Remote tab.
- Uncheck “Allow Remote Assistance connections to this computer”.
- This is commonly scored as a defensive countermeasure.

8.3 Windows Remote Management (WinRM)
- gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Windows Remote Management (WinRM) → WinRM Service.
- “Allow unencrypted traffic”:
  - Disabled.

PHASE 9 – SHARES, NTFS PERMISSIONS, SMB CONFIG

9.1 Review shared folders
- Win + R → fsmgmt.msc → Enter.
- Click “Shares”.
- Only default administrative shares should be there unless README says otherwise:
  - ADMIN$
  - C$
  - IPC$
- For non-default shares:
  - If NOT in README and not required:
    - Right-click → Stop Sharing → Yes.

9.2 SYSVOL and NTDS

- Ensure:
  - “Everyone” does NOT have full share or NTFS permissions to SYSVOL.
  - NTDS dump shares are disabled:
    - Remove any share pointing to NTDS files.
  - Domain Users are not granted access to NTDS folders.

9.3 File share permissions
- For each legitimate share:
  - Right-click share → Properties → Share Permissions:
    - Remove “Everyone” with full control.
    - Limit to specific groups (e.g., Exec SMB Users for an Exec share).
  - Check NTFS permissions:
    - Right-click folder → Properties → Security.
    - Ensure only necessary groups have modify/full control.

9.4 SMB version and encryption
- Disable SMBv1:
  - Control Panel → Programs → Turn Windows features on or off.
  - Uncheck “SMB 1.0/CIFS File Sharing Support”.
- PowerShell for SMB server settings:
  - PowerShell (Admin):
    - Get-SmbServerConfiguration
  - Look for:
    - EnableSMB1Protocol = False.
    - EncryptData = True (for sensitive shares).
  - To enable encryption by default:
    - Set-SmbServerConfiguration -EncryptData $true -Force

PHASE 10 – SERVICES, ROLES, AND FEATURES

10.1 Services console
- Win + R → services.msc → Enter.
- Scan list and change Startup type and status as follows, unless README says otherwise:

Disable/Stop if not required:
- Telnet
- FTP services (Microsoft FTP or third party) unless image is an FTP server.
- SNMP, SNMP Trap.
- Simple TCP/IP Services.
- Remote Registry.
- UPnP Device Host.
- Any third-party remote desktop (TightVNC, etc., if not required).

- XAMPP / FileZilla Server, if not part of intended web stack.
- Game or media services (Teamspeak, Jellyfin, etc.).

Ensure Running / Automatic:
- Event Log services.
- Windows Update.
- DNS Server (on DNS servers).
- Active Directory Domain Services (on DCs).
- Windows Defender services.
- Any required roles (IIS, file services) as indicated by README.

10.2 Windows Features
- Control Panel → Programs → Turn Windows features on or off.
- Turn off:
  - Telnet Client/Server.
  - SNMP (unless explicitly required).
  - RIP Listener.
  - Client for NFS.
  - Unneeded IIS / Web services if server is not a web server.
- Turn on only what the scenario requires (e.g., required IIS components).

10.3 DNS service hardening (Domain Controller)
- If competition docs mention reverse TCP DLL or DNS plugin:
  - Stop DNS:
    - sc.exe stop dns
  - Remove malicious DLL:
    - Remove-Item "C:\Windows\System32\DNS\ipv6_dnsapi.dll" -Force (example path; adjust if different)
  - Remove “ServerLevelPluginDll” registry entry:
    - HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters
  - Start DNS:
    - sc.exe start dns
- Configure DNS service restart on failure:
  - sc.exe failure DNS reset= 10 actions= restart/10000/restart/10000/restart/10000
- Disable dynamic updates on sensitive zones if required.
- Apply SIGRed workaround if described in README/keys (e.g., setting maximum UDP packet size for DNS or installing patches).

10.4 Server roles
- Server Manager → Manage → Remove Roles and Features:
  - Remove roles not required by scenario (e.g., Web Server, if not specified).
- Install necessary security roles:
  - Windows Defender features.
  - WSUS (if scenario revolves around patch management).

- Run Best Practices Analyzer:
  - In Server Manager → Dashboard → under server name → BPA results.
  - Resolve high/medium-severity issues that don't conflict with README.

PHASE 11 – IIS / WEB SERVER HARDENING (IF REQUIRED)

11.1 Confirm IIS is required
- If README or scenario does NOT mention hosting a website:
  - Consider removing IIS role completely.
- If IIS is required (e.g., for Skynet, Exec portal, WordPress, etc.):

11.2 Enable necessary IIS sub-features
- Turn Windows features on or off → Internet Information Services.
- Check needed subfeatures (Web Management Tools, World Wide Web Services, etc.), avoid FTP unless needed.

11.3 IIS Manager configuration
- Open "Internet Information Services (IIS) Manager".
- For each site (e.g., Default Web Site, Skynet, WordPress):
  - Logging:
    - Enable logging; ensure log file directory is valid.
  - Error Pages:
    - For remote requests, do NOT use "Detailed":
      - Use "Detailed local only, custom error for remote" or equivalent.
  - HTTP Response Headers:
    - Remove or minimize "Server" header if configuration allows.
  - SSL:
    - Require HTTPS for login/admin pages or the whole site if scenario expects SSL requirement:
      - Set binding for HTTPS.
      - Rewrite HTTP → HTTPS if necessary.

11.4 Remove test files and backdoors
- Inside the web root (e.g., C:\inetpub\wwwroot or custom):
  - Delete:
    - phpinfo.php.
    - Sample/test pages not needed.
    - Known backdoor scripts (php web shells, test .aspx, reverse shell scripts) as indicated by notes/keys.
  - For apps like WordPress:
    - Ensure debug flags are off in wp-config.php.
    - Remove leftover install/upgrade directories.

11.5 PHP configuration
- Edit php.ini (location depends on install):
  - expose_php = Off
  - display_errors = Off
  - log_errors = On (direct errors to logs instead of output).

PHASE 12 – OS & APPLICATION UPDATES

12.1 Windows Updates
- Settings → Update & Security → Windows Update:
  - Click “Check for updates”.
  - Install available security/quality updates.
- Configure automatic updates:
  - gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Windows Update → Configure Automatic Updates.
  - Enable with a regular schedule (e.g., auto download and install).

12.2 Application updates
For each allowed application in README:

- Firefox:
  - Menu → Help → About Firefox → let it update fully.
- Chrome / Chromium:
  - Settings → About → let updates apply.
- Notepad++:
  - Help → Update Notepad++ (or reinstall from official installer).
- Wireshark:
  - If allowed, update; if not required, uninstall via Programs and Features.
- Other allowed apps (LibreOffice, 7-Zip, etc.):
  - Use built-in updater or download latest version.

12.3 Remove old or insecure versions
- Control Panel → Programs and Features:
  - Uninstall old versions of browsers, scripting tools, or frameworks that are replaced by updated versions.
  - Make sure applications stay installed in default directories when competition expects that (some keys penalize moving program folders).

PHASE 13 – UNWANTED SOFTWARE, BACKDOORS, FILE CLEANUP

13.1 Remove hacking tools and unwanted software (unless allowed)
- Programs and Features:
  - Uninstall:
    - Password crackers, exploit kits, dsniff-style tools.
    - Netcat (if it is a backdoor, distinct from OS binaries).
    - Teamspeak, games, media players not in README.
    - TightVNC Server or other remote control tools if not required.
- Common directories:
  - C:\Users\Public\Downloads
  - C:\Users\<user>\Downloads
  - C:\Program Files and C:\Program Files (x86)
  - Delete archives and installers for hacking tools and malware.

13.2 Scheduled tasks
- Task Scheduler:
  - Server Manager → Tools → Task Scheduler.
  - Look under:
    - Task Scheduler Library and subfolders.
  - Delete suspicious tasks:
    - Reverse shells.
    - Strange names pointing to scripts in Temp/AppData.
  - Keep tasks clearly related to Windows or required roles.

13.3 Prohibited files
- Search for forbidden file types/content:
  - Use File Explorer search:
    - *.mp3, *.avi, *.mp4, etc. in user areas if README says no media.
  - Search for “password”, “creds”, or similar keywords in Documents/Desktop.
  - Delete:
    - Plaintext credential files.
    - Prohibited music/media files.
    - Screenshots with sensitive info if README forbids them.

13.4 NTFS permissions on sensitive directories
- For SYSVOL, NTDS, DNS directories, and web roots:
  - Right-click folder → Properties → Security.
  - Ensure:
    - Access is limited to SYSTEM, Administrators, and appropriate service accounts/groups.
    - Domain Users do not have read/write to NTDS or other sensitive directories.
- For Exec SMB share or similar:
  - Confirm only Exec SMB Users (or scenario-specified group) has access.

PHASE 14 – BROWSER, INTERNET OPTIONS, ACTION CENTER

14.1 Internet Options (if IE/Edge settings still used)
- Control Panel → Internet Options.
- Security tab:
  - Set zone security level to “High” for Internet.
- Privacy tab:
  - Block all cookies or use high privacy.
  - Never allow websites to request physical location.
  - Turn on Pop-up Blocker.
  - Disable toolbars and extensions when InPrivate Browsing starts.

14.2 Action Center / Security & Maintenance
- Control Panel → System and Security → Security and Maintenance (Action Center).
- Make sure:
  - All security messages are enabled (Windows Update, Firewall, AV).
  - Turn on File History if appropriate.

PHASE 15 – MONITORING, RESOURCE TOOLS, FINAL PASS

15.1 Resource Monitor
- Task Manager → Performance tab → Open Resource Monitor.
- Start monitoring:
  - Look for suspicious high-CPU or network processes.
  - Investigate unknown processes, especially those listening on unusual ports.

15.2 Final category checklist (quick mental run-through)
Check each CyberPatriot category:

- Account Policies:
  - Password length, age, history, complexity set.
  - Lockout threshold, duration, reset set.

- Local Policy:
  - Security Options hardened (anonymous, UAC, interactive logon, NTLM).
  - User Rights Assignment cleaned.

- User Auditing:
  - Unauthorized users removed.
  - Group memberships cleaned (Admins, DnsAdmins, Exec groups).
  - Guest/Administrator appropriately renamed/disabled.

  - Password expiration enforced where needed.

- Application Security:
  - Required services (DNS, IIS, SMB) running and configured securely.
  - Insecure services (FTP, Telnet, random servers) disabled.
  - IIS/HTTP/PHP hardened if present.

- Application Updates:
  - Firefox/Chrome/Notepad++/Wireshark/etc. updated.

- Operating System Updates:
  - Windows Updates installed or majority installed.
  - Automatic updates configured.

- Defensive Countermeasures:
  - Firewall enabled on all profiles.
  - AV/Windows Defender actively protecting.
  - Remote Assistance disabled; RDP secured or disabled per README.

- Prohibited Files:
  - MP3/media removed if forbidden.
  - Plaintext passwords and sensitive docs removed if not required.

- Unwanted Software / Malware:
  - Hacking tools, games, remote-control software removed unless explicitly allowed.
  - Backdoors, cryptominers, RATs, suspicious scheduled tasks removed.

- Service Auditing:
  - Services console checked; unneeded services disabled.
  - DNS, AD DS, and other core roles verified working and hardened.

- Uncategorized OS Settings:
  - Screen lock timeout set.
  - Shares and NTFS permissions hardened.
  - Network adapter security (DNS registration, NetBIOS, UPnP) addressed.

==========
END OF ULTIMATE SERVER CHECKLIST
==========