Windows 10 Checklist

Account Policies	
Enforce password history	5
Maximum password age	90
Minimum password age	30
Minimum password length	14
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account lockout duration	30
Account lockout threshold	5
Reset account lockout counter after	30
Local Policies	
Audit account logon events	Success, failure
Audit account management	Success, failure
Audit directory service access	Success, failure
Audit logon events	Success, failure
Audit object access	Success, failure
Audit policy change	Success, failure
Audit privilege use	Success, failure
Audit process tracking	Success, failure
Audit system events	Success, failure
Access Credential Manager as a trusted caller	Default
Access this computer from the network	Users and administrators
Act as part of the operating system	Trusted users
Add workstations to domain	Authorized member of IT team

Adjust memory quotas for a process	Only users who could adjust memory quotas
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Allow log on through Terminal Services	Default
Back up files and directories	Disabled
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Default
Create a token object	Not Defined
Create global objects	Disabled
Create permanent shared objects	Disabled
Create symbolic links	Not Defined
Debug programs	Only to trusted users/administrators
Deny access to this computer from the network	Default
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Deny log on through Terminal Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined/Admin.
Force shutdown from a remote system	Default
Generate security audits	localservice/Network service
Impersonate a client after authentication	Default
Increase a process working set	Users

Increase scheduling priority	Default Value
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Default Value
Log on as a service	Minimize list of google accounts
Manage auditing and security log	Admins.
Modify an object label	Disabled
Modify firmware environment values	Default
Obtain an impersonation token for another user in the same session	Default
Perform volume maintenance tasks	Admins.
Profile single process	Default
Profile system performance	Admins.
Remove computer from a docking station	Default
Replace a process level token	Not Defined
Restore files and directories	Default
Shut down the system	Default
Synchronize directory service data	Not Defined
Take ownership of files or other objects	Admins.
Security Options	
Administrator account status	Default
Block Microsoft Accounts	Default
Guest account status	Disabled
Limit local use of blank passwords to console logon only	Enabled
Rename administrator account	Enabled
Rename guest account	Enabled

Audit the access of global system objects	Disabled
Audit the use of Backup and Restore Privilege	Disabled
Force audit policy subcategory settings	Enabled
Shutdown system immediately if unable to log security	Disabled
Devices	
Allow undock without having to logon	Disabled
Allowed to format and eject removable media	Administrators
Prevent users from installing printer drivers	Enabled
Restrict CD ROM access	Enabled
Restrict floppy access	Disabled
Domain controller	
Allow server operators to schedule tasks	Dependent
LDAP server signing requirements	Require signature
Refuse machine account password changes	Disabled
Domain member	
Digitally encrypt or sign secure channel data (always)	Enabled
Digitally encrypt secure channel data (when possible)	Enabled
Digitally sign secure channel data (when possible)	Enabled
Disable machine account password changes	Disabled
Maximum machine account password age	30 days
Require strong session key	Enabled
Interactive logon	
Display user information when session is locked	Not Defined
Do not display last user name	Disabled
Do not require CTRL+ALT+DEL	Disabled

Machine account lockout threshold	Disabled
Machine inactivity limit	Disabled
Message text for users attempting to log on	Restricted to authorized users
Message title for users attempting to log on	Authorized users
Number of previous logons to cache	Do not change
Prompt user to change password before expiration	5 days
Require Domain Controller authentication to unlock	Enabled
Require smart card	Require smart card
Smart card removal behavior	Lock Worksation
Microsoft network client	
Digitally sign communications (always)	Enabled
Digitally sign communications (if server agrees)	Enabled
Send unencrypted password to third party smb servers	Disabled
Microsoft network server	
Amount of idle time required before suspending session	15 minutes or less
Attempt S4U2Self to obtain claim information	Not Defined
Digitally sign communications (always)	Disabled
Digitially sign communications (if server agrees)	Enabled
Disconnect clients when logon hours expire	Enabled
Server SPN target name validation level	Off
Network access	
Allow anonymous SID/name translation	Disabled
Do not allow enumeration of SAM accounts	Disabled
Do not allow anonymous enumeration of SAM accounts and shares	Enabled/Not Defined

Do not allow storage of passwords and credentials (for network authentication)	Disabled
Let Everyone permissions apply to anonymous users	Disabled
Named Pipes that can be accessed anonymously	Null value (enabled but no info)
Remote accesible registry paths	Null value (enabled but no info)
Remote accesible registry paths and sub paths	Null value (enabled but no info)
Restrict anonymous access to named pipes and shares	Enabled
Shares can be accessed anonymously	Null value (enabled but no info)
Sharing and security model for local accounts	Classic - local users authenticate as themselves.
Network security	
Allow Local System to use computer identity for NTLM	Not Defined
Allow Local System NULL session fallback	Default
Allow PKU2U authentication requests to this computer	Disabled/do not configure the policy
Configure encryption types allowed for Kerberos	Not Defined
Do not store LAN manager hash value on next password change	Enabled
Force logoff when logon hours expire	Disabled
LAN manager authentication level	Not Defined
LDAP client signing requirements	Require Signature
Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Add remote server exceptions	Not Defined
Add server exceptions in this domain	Not Defined
Audit incoming NTLM traffic	Not Defined

Audit NTLM authentication in this domain	Not Defined
Incoming NTLM traffic	Not Defined
NTLM authentication in this domain	Not Configured
Other	
Allow automatic administrative logon	Disabled
Allow floppy copy and access to all drives and all folders	Disabled
Allow system to be shutdown without having to logon	If server, disabled - if client, enabled
Clear virtual memory page file	Enabled
Force strong key protection for user keys stored on computer	User must enter password each time key is used
Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
Require case insensitivity for non windows subsystems	Enabled
Strengthen default permissions of internal system objects	Enabled
Optional subsystems	Null value
Use certificate rules on windows executables	Enabled
User Account Control	
Admin Approval Mode for the Built-in Administrator account	Disabled
Allow UIAccess applications to prompt for elevation	Disabled
Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows Binaries
Behavior of the elevation prompt for standard users	Prompt for credentials
Detect application installations and prompt for elevation	Disabled
Only elevate executables that are signed	Disabled
Only elevate UIAccess applications that are installed in secure locations	Enabled

Run all administrators in Admin Approval Mode	Enabled
Switch to secure desktop when prompting for elevation	Enabled
Virtualize file and registry write failures to per-user locations	Enabled

- Automatic services - Windows Firewall, Windows Update, Windows Defender
- Disabled services - IP Helper, SNMP Trap, a lot of remote services =
- Remove unnecessary sharing
- Delete media files and sketchy txt files
- Firefox should be our default browser unless said otherwise

General Windows Hardening

Key: items marked with (s) are covered by a script; everything under them is covered too

Password for all users: **superCyberPatriot123!**

Users:

- ☐ Disable default administrator account (s)
  - Open Command Prompt → “net user administrator /active:no”
- ☐ Make sure each user on the system is supposed to be there. (s)
  - ☐ Delete users if necessary (keep files).
  - ☐ Add users if the ReadME says so or if you can’t find a user in the system, but they are supposed to be.
- ☐ Make sure that each user has the right privileges (standard or administrator) (s)
- ☐ Make sure that each user is password protected, and that all users have secure passwords. (s)
- ☐ Create or add users to groups if instructed by ReadME **(not scripted)**

Local Security Policy:

Search → secpol.msc

- ☐ Ensure the following for passwords: (s)
  - ☐ Minimum Password Age: 30

- ☐ Maximum Password age: 90
- ☐ Enforce Password History: 24
- ☐ Password Length: 12
- ☐ Passwords meet complexity requirements = ENABLED.
- ☐ Passwords are not stored using reversible encryption.
- ☐ Relax minimum password length limits = DISABLED
- ☐ Minimum password length audit = 12

☐ Ensure the following for account lockout: (S)

- ☐ Duration: 30 minutes
- ☐ Threshold: 5
- ☐ Reset account counter after: 30 minutes

☐ Auditing: (S)

- ☐ Set Advanced Audit Policy Configurations
- Advanced Audit Policy Config → System Audit Policy → audit everything under dropdown options
- ☐ Make sure each policy is set to both “Success, Failure.” (Audit everything)
- Security Settings -> Local Policies -> Audit Policies

☐ Security Settings → Local Policies → Security Options: **(not scripted)**

- ☐ Guest accounts disabled
- ☐ Limit local use of blank passwords to console only = enabled
- ☐ Do not allow anonymous enumeration of SAM accounts = enabled
- ☐ Set “User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode” to “Prompt for consent on secure desktop”
- ☐ Set “User Account Control: Behavior of the elevation prompt for standard users” to “prompt for credentials”

☐ Security Settings → Local Policies → User Rights Assignment: (S)

- ☐ Remove “Everyone” group from “May access this computer from the network” option
- ☐ Remove any non-default & non-admin groups from “Create global objects” policy

☐ Miscellaneous (S)

- ☐ Require CTRL-ALT-DELETE = enabled
  - Run → netplwiz → Advanced tab → check box “Require ctrl alt delete”

Group Policy:

Run → gpedit.msc

- ☐ Disable Let everyone permissions apply to anonymous users (S)
  - Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options
- ☐ Disable AutoPlay for all users (S)
  - Computer Configuration → Administrative Templates → Windows Components → AutoPlay Policies → Set “Turn off AutoPlay” to “Enabled”
- ☐ Enable Windows Defender SmartScreen (S)
  - Computer Configuration → Administrative Templates → Windows Components → Windows Defender SmartScreen → Explorer → Set “Configure Windows Defender SmartScreen” to “Enabled” and put the setting on “Warn”
- ☐ Enable Digitally sign communications for Microsoft Network Server (both versions) (S)
  - Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Updates:

- ☐ Make sure Windows is running on the latest version
- ☐ Make sure the required applications for the machine are updated (Open them to check)
- ☐ Enable automatic updates

Firefox/Chrome Settings:

- ☐ Update to latest version
- ☐ Turn on automatic updates
- ☐ Firefox/Chrome should have strict protection.
- ☐ Block pop-up windows.
- ☐ Websites should warn you when they try to install add-ons.
- ☐ Block dangerous content and downloads.
- ☐ HTTPS only
- ☐ DNS protection

Prohibited Files/Software: (CHECK THE README)

- ☐ Delete all hacking tools, games, and other unnecessary applications via RevoUnistaller.
- ☐ Delete all suspicious files that are referenced in readme or forensics questions
- ☐ Delete all mp3, mp4, and mov files (unless required by the machine) & check for hidden files.
- ☐ Delete all pictures unless told not to.

Firewall: (s)

- ☐ Make sure that the Windows Defender Firewall is on.
- ☐ If stated in the ReadME, add or delete inbound or outbound rules.

Malware:

- ☐ Enable Windows Defender (s)
  - ☐ Ensure that no exceptions are configured (pathway or file type exceptions)
  - Gpedit.msc → Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus → Exclusions. Set to “Not Configured”
- ☐ Follow Windows Security Recommendations in Settings **(not scripted)**
- ☐ Install a secondary antivirus software (MalwareByte) and perform a scan → remove any viruses found **(not scripted)**
- ☐ Check Task Manager for suspicious process running **(not scripted)**
  - Task Manager → Details

Applications:

- ☐ Based on the ReadME, you may have to install required applications. If you need to, install the latest, stable version of the application.

User Access Control:

- ☐ Make sure that the UAC is turned all the way up.

Services: (s)

- ☐ Disable unnecessary services (s)
  - Search → Services.msc → stop service & disable startup
  - ☐ Telnet (TlntSvr)
  - ☐ FTP (ftpsvc) (Windows FTP Service)

- ☐ RDP (TermService)
- ☐ Windows Remote Management (WinRM)
- ☐ Internet Information Services (IIS)
- ☐ Word Wide Web Publishing

☐ Enable any required service (instructed in ReadME) (S)

Ensure the following are enabled:

- ☐ Windows Update service
- ☐ Windows Event Log service

Network Sharing & Remote Connections:

Disable unless instructed in the ReadME

☐ Disable Remote Desktop (RDP) (S)

- Settings → search “Remote Desktop” → uncheck “Allow remote connections to my computer”

☐ Disable Printer & File sharing (S)

- Control Panel → Network & Internet → View network status and tasks under Network and Sharing Center → “Change advanced sharing setting” on left side → select “Turn off file and printer sharing” on bottom

☐ Disable Universal Plug & Play Framework (UpNp) (S)

- Search →services.msc →disable “UpNp Device Host”

☐ Disable Remote Assistance (S)

- ☐ Control Panel → System & Security → under “System” click “Allow remote access” →click Remote tab uncheck “Allow Remote Assistance connection to this computer”

☐ Stop Sharing Shared Folders (S)

- fsmgmt.msc → shares → right click & select “stop sharing” to all *non-default* folders
- Default shares: C$, ADMIN$, and IPC$
  - Note: Folders that end in *$* are considered hidden shares

☐ Configure RDP (only if listed under ReadME as a critical service)

- ☐ Enable network level authentication
- Settings → System → Remote Desktop → Advanced Settings → Select “Require computers to use Network Level Authentication to connect”
- ☐ Set RDP Security Layer to SSL
- gpedit.msc → Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security → Double click

“Require use of specific security layer for remote connections” → set to “Enabled” and set the security layer to SSL

Network Security

- Control Panel → Internet Options:
  - Under Security Tab:
    - ☐ Set security level to high
  - Under Privacy Tab:
    - ☐ Block All Cookies
    - ☐ Never allow websites to request your physical location
    - ☐ Turn on Pop-up Blocker
    - ☐ Disable toolbars and extensions when InPrivate Browsing starts

Action Center

Action center is a place where you can view all of Windows security issues and recommended fixes for them

- Control Panel → System & Security → Action Center

☐ Enable all Action Center recommendations

☐ Enable File History

Tasks Manager & Scheduler

☐ Check Task Manager for any suspicious or unresponsive tasks & end them

☐ Check Task Scheduler and remove any suspicious tasks

☐ Enable monitoring on Resource Monitor

- Open Task Manager → Performance tab → Open Resource Monitor (bottom left) → Monitor (top right) → Start Monitoring

Forensics:

☐ Answered forensic #1

☐ Answered forensic #2

☐ Answered forensic #3W

☐

Windows Server 2022 Hardening

Server Message Block (SMB) Configuration

SMB is a protocol that allows for file sharing across devices of different operating systems, it is a security risk if not configured correctly

- ☐ Disable SMB V1
    - Search → Windows Features →Uncheck “SMB 1.0”
- ☐ Set Encrypt Data to True
- How to view all current SMB Configurations:
    - PowerShell → “Get-SmbServerConfiguration”
- How to change an SMB configuration:
    - PowerShell → “Set-SmbServerConfiguration -SettingName $Value -force” (*-force will skip setup step*)

Internet Information Services Configuration (IIS)

IIS is a service that allows you to host web servers on a Windows machine; it should be disabled unless the ReadME says it’s a critical service. This section is on how to configure IIS if it is required.

- ☐ Enable IIS Sub-Features to make IIS Manager accessible
    - Search → “Windows Features” → Check all the boxes & sub-boxes under Internet Information Services besides FTP

IIS Manager will now be accessible through Search

Active Directory Configuration

Active Directory is a Windows Server tool that allows you to manage your server by organizing it in a hierarchical structure with organizational units (OUs) at the bottom, Domains, Trees, and Forests on top

- To Access AD Tools:
    - ☐ Enable Activity Directory Domain Services role
    - ☐ Install Group Policy Management feature
- AD Config Tools:
    - Group Policy Management Console (Run → gpmc.msc)
    - ☐ Configure Settings
    - ☐ Configure Permissions
    - DSA.msc: Allows you to view all users and objects in AD

Firewall Configuration

- ☐ Configure Windows Firewall to allow only necessary inbound/outbound traffic
- Search → Windows Firewall → Advanced Settings → Windows Firewall Defender Properties:

    - Block Inbound Connections
    - Allows Outbound Connections
- ☐ Check for & disable suspicious inbound & outbound rules

Feature and Role Configuration

- ☐ Install and configure roles relevant to the competition scenario
    - Server Manager → Add Roles or Features
- ☐ Remove or disable unnecessary services and roles
- ☐ Install Windows Defender role
- ☐ Instal WSUS (Windows Server Update Service) role

Services

- ☐ Disable DNS Server service (if not required)
- ☐ Disable other general windows services mentioned above (FTP, Telnet, etc.)
- ☐ Ensure important services listed above are enabled (Event Log, Windows Update)

Server Manager Tools

- ☐ Check Task Scheduler for harmful tasks
    - Server Manager → Tools → Task Scheduler
- ☐ Follow Best Practices Analyzer (BPA)
    - Server Manager → Dashboard → “BPA results” under the server name