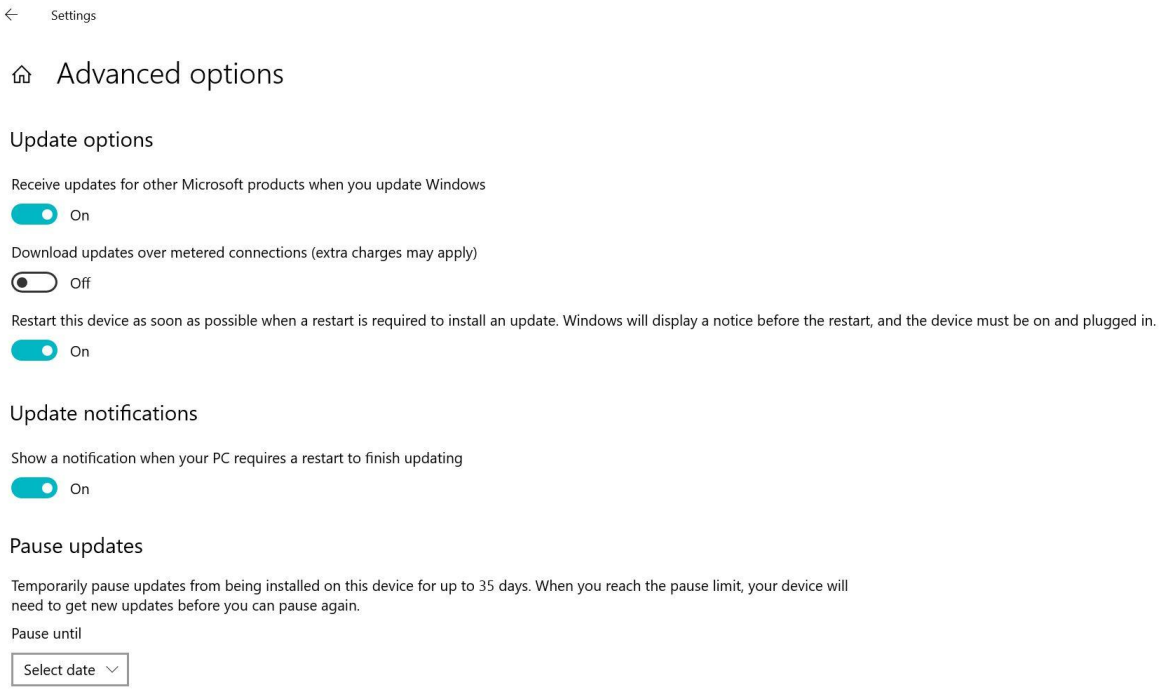
Windows Checklist

MAKE NOTES

- Read the Readme
- Forensics Questions
- Windows Settings
    - Updates (if Readme Allows)
        - Settings\Updates+Security\Windows Update
        - Check for updates



    - Users (settings and control panel)
        - Account type correct
        - Passwords exist?
        - Groups (if specified in Readme)
        - Passwords length/complexity/strength
            - If not replace with ‘ CyberPatriot21 ’
    - Hidden Files

        - Update and security\for developers
        - (or type “show hidden files” in windows search)
        - click show hidden files, folders, and drives
    - Malware + Virus
        - Windows Security\Virus + threat protection
            - Quick scan
            - Check for updates
    - Remote Desktop Settings
        - Settings\update and security\for developers
            - Disable RDS by unchecking all Remote desktop boxes (Unless specified in readme to keep enabled)
        - System properties\remote
            - Uncheck remote assistance
            - Don’t allow remote connections
- Control Panel
    - Users (settings and control panel)
        - Account type correct
        - Passwords exist?
        - Groups (if specified in Readme)
        - Passwords length/complexity/strength
            - If not replace with ‘ CyberPatriot21 ’
    - Firewall
        - Windows Defender Firewall (in Control Panel)
        - Make sure its on (private and public)
        - Restore default settings if needed
    - Programs/Suspicious apps (in file explorer and control panel)
        - Control panel\Programs\programs and features
            - Check for suspicious programs/hacking tools/ non work related files
            - CHECK README
- Computer Management
    - Shared files
        - Computer management\system tools\shared folders\shares
            - Stop share for Admin$, C$, IPC$ (right click)

- File Explorer
    - Programs/Hidden Files
        - AFTER YOU HAVE SHOWN HIDDEN FILES IN SETTINGS
        - In file explorer search *.mp3
            - .mp3, .mp4, .avi, .mov, .jpeg, .png, etc
            - You can right click file to open file location then delete
        - Check C drive for program files/ suspicious files
            - HashCat, Wireshark, TeamViewer, Steam, iTunes, CCleaner, (hacking tools)
- Program Updates
    - README
    - Notepad++, Firefox, sometimes edge or other web browser
    - Firefox options
        - Don't save logins
        - Check for updates
        - Auto install updates
        - In Privacy and Security switch to Standard or Strict
        - Do Not Track → Always
        - Clear cookies and delete cookies when closed
        - Disable autofill logins + psswds
        - Enable block popup windows
        - Enable Warn when try to install add ons
        - Enable block dangerous + deceptive content
- Password Policy
    - Type "sec pol" in windows search → security policy
    - Account policies\password policy
        - Password history → 7 days
        - Max password age → 90 days
        - Min password age → 15 days
        - Min password length → 10 characters
        - Complexity requirements → enabled
        - Store psswd w/reversible encryption → disable
    - Account policies\account lockout policy
        - Lockout threshold usually between 5-10

    - Local policies\audit policy
        - Audit all w/success + failure checked
        - If you lose points → uncheck it :)
    - Local policies\user rights assignment
        - Disable guest

- Examples.xlsx = Mini checklist made by Coach Jake

Linux Ubuntu Checklist

MAKE NOTES

- Read the Readme
- Forensics Questions
- Updates
    - Gear on upper right\system settings\software+updates
    - Update tab
        - Important updates + recommended updates checked
        - Check updates → Daily
        - When updates → Download + install automatically
- Firewall
    - Gear\system settings\firewall configuration
    - (if not installed)
        - Sudo apt install gufw
        - gufw
    - reject incoming
    - status → on
    - profile → home
    - outgoing → allow
- Malware + Virus
    - Cmdln
        - Sudo apt install clamscan (or clamav)
        - clamscan
- Users
    - Account type correct
    - Passwords exist?
    - Groups (if specified in Readme)
    - Passwords length/complexity/strength
        - If not replace with ‘ CyberPatriot21 ’
- Software updates(Firefox)

- Settings in firefox\ updates + security
  - Don’t save logins
  - Check for updates
  - Auto install updates
  - In Privacy and Security switch to Standard or Strict
  - Do Not Track → Always
  - Clear cookies and delete cookies when closed
  - Disable autofill logins + psswds
  - Enable block popup windows
  - Enable Warn when try to install add ons
  - Enable block dangerous + deceptive content
- PAM files
  - Cmdln
    - Cd etc/pam.d/
    - sudo apt install libpam-cracklib
    - sudo nano common-password
      - after line w/”pam_unix.so”)
        - remember = 5
        - minlen=8
      - at end of line w/”pam_cracklib.so”
        - ucredit = -1
        - lcredit = -1
        - dcredit = -1
        - ocredit = -1
      - ctrl + o
      - ctrl + x
    - sudo nano ../login.defs
      - scroll all the way down to…
      - PASS_MAX_DAYS → 90
      - PASS_MIN_DAYS → 10
      - PASS_WARN_AGE → 7
      - Ctrl + o
      - Ctrl + x
- Account policy

    - Cmdln (in etc/pam.d)
        - Sudo nano common-auth
        - Add to end of file
        - Auth required pam_tally2.so deny = 5 onerr = fail unlock_time = 1800
        - Ctrl + o
        - Ctrl + x
- Media/Hidden Files
    - Hidden files → cmdln in etc/pam.d/
    - Ls -la
    - Cd ../..
    - Locate *.mp3
        - . mp3, .mp4, .avi, .mov, .jpeg, .png, etc
- Software
    - Synaptic
        - Cmdln
            - sudo add-apt-repository universe
            - sudo apt update
            - sudo apt install synaptic
        - View software and snap files, delete unwanted files
    - Cmdln
        - apt list –installed
        - snap list
        - flatpal list
        - sudo apt-get install PackageNameHere (for updating software)
        - CHECK README
- OS Updates
    - Cmdln
    - Use ssh to login (`ssh user@server-name`)
        - sudo apt-get update
        - sudo apt-get upgrade
        - sudo reboot
- Bum
    - Cmdln in home directory

        - sudo apt install bum
        - sudo bum (any hacker tools checked?)
- Remove Guest Account
    - Cmdln
    - Gedit /etc/lightdm/lightdm.conf
    - Add ‘ allow-guest = false ‘ to the end of the file
    - Ctrl + o
    - Ctrl + x

Linux Services

man → manual

In command line: →service –status-all

Or systemctl

netstat → network status (whats listening)

Server

SRV 2019 State	Category	
Forensics 1	Forensics	
Forensics 2	Forensics	
Forensics 3	Forensics	
unauth user	User audit	
unauth user	User audit	
user not an admin	User audit	
user has pw	User audit	
user pw expires	User audit	
insecure pw	User audit	
min pw length	Acct policy	
secure acct lockout	Acct policy	
Windows updates	OS updates	
removed 3 tools	Unwanted software	
audit sensitive priv use	Local Policy	
3	Local Policy	
mailenable updated	App updates	
1	uncategorized OS settings	remote assistance, remote desktop, printer sharing
IIS SSL Cert	application security	likely this
IIS Logging	application security	likely this
mailenable (readme)	application security	likely this
mailenable (readme)	application security	likely this
mailenable (readme)	application security	likely this
mailenable (readme)	application security	likely this
1	application security	
1	defensive countermeasures	likely firewall settings
2	Malware	Probably not in add/remove programs
2	Prohibited files	could be related to forensic questions
2	Service auditing	Services should have been stopped

- **READ THE READ ME**

- Take notes
- Look at Forensics Questions
- Don’t spend too long, watch the time
- Check all User Folder for exe folders

- Look at Users through Computer Management

-Double check everything

- Change all passwords

Admin services

-Computer management

Look at what’s running and not running

Examples.xlsx = A mini checklist made by Coach Jake