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)