13-3822 FusRoDah!!1

http://cypat.guru/index.php/Linux_Hardening

- **Forensics**
- **Updates**
    - Open “software and updates”
    - Check all for “Ubuntu software” and “other software”
    - Select important and recommended updates in “updates”
    - Select most frequent option in “updates”
    - Use “software updater” to update
- **Users**
    - USERS: sudo nano /etc/passwd
    - Disable/enable user (including root)
        - DISABLE: sudo passwd -l [user]
            - Alternatives:
            - In /etc/passwd change /bin/bash to /bin/nologin
            - In /etc/passwd add * or ! before x
            - Use chage -E [date prior to today] [user]
        - ENABLE: sudo passwd -u [user]
        - DELETE ROOT: passwd -d root
    - Remove unauthorized users and delete their files using GUI
    - Disable guest user
        - sudo nano /etc/lightdm/lightdm.conf
        - ADD AT END: allow-guest=false
        - sudo restart lightdm OR sudo service lightdm restart
    - Edit sudoers
        - sudo nano /etc/sudoers
        - [group/user] FROM_WHERE=(AS_WHO) CAN_RUN_WHAT
        - ALIASES: [type]_Alias [NAME] = [item], [item]...
        - /etc/sudoers.d directory exists. Bad command -> ALL ALL = NOPASSWD: ALL
    - Add Notes Later: Dangerous Sudoers File
    - Groups
        - /etc/group
        - May have hidden users
        - Everyone should have unique UID and only root has UID 0
        - Admins in admin (admin != adm?) and sudo group
- **Password Policy**
    - Complexity
        - sudo nano /etc/pam.d/common-password
        - password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5 minlen=14
        - sudo apt-get install libpam-pwquality
        - password requisite pam_pwquality.so retry=3 retry=3 minlen=12 maxrepeat=3 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 reject_username enforce_for_root

  - sudo nano /etc/pam.d/common-auth
    - auth [success=1 default=ignore] pam_unix.so nullok_secure onerr=fail deny=5 unlock_time=1800
  - Disable auto login
    - sudo nano /etc/lightdm/lightdm.conf
    - Remove autologin line
    - Restart to take effect
  - Expiration
    - sudo nano /etc/login.defs
    - Aging controls (for new users)
      - PASS_MAX_DAYS 30
      - PASS_MIN_DAYS 0
      - PASS_WARN_AGE 7
    - Aging controls (existing users)
      - sudo chage [option] <days> <username>
  - Change password to $3cureP@ssword2020: sudo passwd [user]
- **Files**
  - Find Non-Work Media Files
    - find . -type f -name "*.[extension]"
    - grep -n -R [string to search within files] .
    - /home
    - png, jpg, jpeg, mov, gif, mp3, mp4, wav, avi
    - Open with xdg-open [file]
  - Secure Permissions
    - r=4, w=2, x=1
    - Secure permissions for these files/directories:
      - chmod 700 /root
      - chmod 700 /var/log/audit
      - chmod 740 /etc/rc.d/init.d/iptables
      - chmod 740 /sbin/iptables
      - chmod -R 700 /etc/skel
      - chmod 600 /etc/rsyslog.conf
      - chmod 640 /etc/security/access.conf
      - chmod 600 /etc/sysctl.conf
    - chmod 755 /home
    - chmod 644 /etc/passwd AND chown root:root passwd
    - chmod 600 /etc/shadow AND chown root:[root/admin group] shadow
    - Add Notes Later: Verify SSL Certificate Checksum Binary Files
- **Programs**
  - apt-cache for info on available packages, apt-get to manage packages
  - Check installed packages: sudo dpkg --get-selections
  - Check installed services (kernel modules):
    - service --status-all
    - systemctl -r --type service --all

    - ls /etc/init.d
  - List startup services: initctl list
  - Uninstall software: sudo apt-get purge --auto-remove [software]
  - List running processes:
    - LIST: ps -aux | less
    - DYNAMIC LIST: top
    - TREE: pstree
    - SEARCH BY NAME: pgrep [name]
  - Kill Process: kill(all) -9 [id OR name]
  - Update Linux: sudo apt-get update THEN sudo apt-get upgrade
  - **sudo netstat -tulpn**
  - **Sudo apt list --installed**
    - **apt-get remove ftp cups apache samba avahi**
    - **Surround w/ ***
  - **Ubuntu Software**
- **Malware**
  - Rootkits
    - sudo apt-get install chkrootkit
    - sudo chkrootkit
  - Malware
    - Install ISPProtect:
      - sudo apt-get install php-cli
      - sudo mkdir -p /usr/local/ispprotect
      - sudo chown -R root:root /usr/local/ispprotect
      - sudo chmod -R 750 /usr/local/ispprotect
      - sudo cd /usr/local/ispprotect
      - sudo wget http://www.ispprotect.com/download/ispp_scan.tar.gz
      - sudo tar xzf ispp_scan.tar.gz
      - sudo rm -f ispp_scan.tar.gz
      - sudo ln -s /usr/local/ispprotect/ispp_scan /usr/local/bin/ispp_scan
    - sudo ispp_scan
  - Backdoors
    - apt-get remove [netcat, nc, netcat-openbsd, openbsd]
- **Firewall (ufw)**
  - sudo ufw enable
  - INFO: sudo ufw status verbose && sudo ufw show raw
  - RULES: sudo ufw [delete (optional-deletes rule)] [allow/deny] [port]/[protocol (optional)]
    - ALLOW: ssh, http, https
  - SERVICE RULES
    - LIST: less /etc/services
    - sudo ufw [allow/deny] [service]
  - sudo ufw logging full
  - sudo ufw default deny incoming

    - sudo ufw default allow outgoing
- **Bash History**
    - Clear history:
        - history -c
        - history -w
    - Don’t write to history:
        - echo “HISTFILESIZE=0” >> ~/.bash_profile
        - echo 'set +o history' >> /etc/profile
- **Firefox**
    - “Strict” setting
    - “Do not track” = always
    - Check Delete cookies and site data when Firefox is closed
    - Never remember history
    - Clear history
    - Uncheck all in “Address bar”
    - Block everything in “Permissions”
    - Uncheck everything in “Firefox data collection and Use”
    - Check all in “Security”
    - Ask for certificates every time and check OCSP
    - Make firefox default browser
    - Update firefox
    - Manage addons
    - about:config in address bar
        - Browser.privatebrowsing.autostart = true
        - Browser.safebrowsing.phishing.enabled = false
        - Browser.safebrowsing.malware.enabled = false
        - Browser.startup.homepage = startpage.com
        - Browser.startup.page = 0
        - datareporting.healthreport.uploadEnabled = false
        - dom.event.clipboardevents.enabled = false
        - dom.storage.enabled = false
        - Geo.enabled = false
        - Media.peerconnection.enabled = false
        - network.cookie.cookieBehavior = 1
        - network.cookie.lifetimePolicy = 2
        - network.dns.disablePrefetch = true
        - network.http.sendRefererHeader = 0
        - network.http.sendSecureXSiteReferrer = false
        - Network.prefetch-next = false
        - Privacy.donottrackheader.enabled = true
        - Privacy.donottrackheader.value = 1
        - Privacy.trackingprotection.enabled = true
        - Toolkit.telemetry.enabled = false
- **SSH**

  - /etc/ssh/sshd_config
    - PermitRootLogin no
    - DenyUsers root
    - AllowGroups admin (if normal users don’t need to ssh)
- **Sysctl**
  - Load with “sudo sysctl -p /etc/sysctl.conf”
- **Auditing (Audit Daemon / auditd)**
  - apt-get install auditd audispd-plugins
  - List rules: sudo auditctl -l
  - Make rule: sudo auditctl -a exit,always -F path=[file path to audit] -F perm=[r,w,x (execute),a (attribute change)]
  - Check file events: ausearch -f [file path to check]
    - Check what the syscall means: ausyscall [architecture using uname -m] [call #]
  - sudo nano /etc/audit/audit.rules
    - -b 1024
    - -a exit,always -S unlink -S rmdir
    - -a exit,always -S stime.*
    - -a exit,always -S setrlimit.*
    - -w /var/www -p wa
    - -w /etc/group -p wa
    - -w /etc/passwd -p wa
    - -w /etc/shadow -p wa
    - -w /etc/sudoers -p wa
    - -e 2
- **Random tips (not required)**
  - Reset password
    - Hold shift on boot to access grub menu
    - Boot in recovery mode and select root
    - Get write access: mount -rw -o remount /
    - passwd [user]
    - Exit and select resume in recovery menu
  - Disable IPv6
    - sudo nano /etc/sysctl.conf
    - Add at bottom:
      - net.ipv6.conf.all.disable_ipv6 = 1
      - net.ipv6.conf.default.disable_ipv6 = 1
      - net.ipv6.conf.lo.disable_ipv6 = 1
  - /etc/hosts is like DNS; can block websites using 127.0.0.1 as address