Linux

Swashbucklers



**Important Notes**

* Always use “ls -al” because they have used files with no name

**Forensics Question**

* First thing to do
* Should be free points never miss these
* Anything you find on these that shouldn’t be there is to be deleted after getting points for the question

**Readme**

* Anything written here is a potential vulnerability
* Take note of EVERYTHING

**Updates**

* First thing is check apt sources
  + /etc/apt/sources.list
  + /etc/apt/sources.list.d/
  + System Settings > Software and Updates > Other Software
* Install updates once sources are confirmed
  + apt-get update
  + apt-get dist-upgrade
  + apt-get autoremove
* Other apt settings are easiest done through GUI when not using a script
  + System Settings > Software and Updates > Updates
    - Check important security updates
    - Automatically check for updates daily
    - Download and install security updates automatically

**User Auditing**

* Files to check
  + /etc/passwd
    - Fake root (UID 0)
    - Unnecessary users
    - Necessary users
  + /etc/shadow
    - Locked out users have a ‘!’
  + /etc/group
    - Sudo group is the admin group
    - Unnecessary groups
  + /etc/sudoers
    - Anything sketchy
  + /etc/sudoers.d/
    - Anything sketchy
* Change passwords to all users once users are confirmed
  + cut -d: -f1 /etc/passwd | sed 's/$/:Cyb3rp4tr!0t\_RBR!/' | chpasswd
* Fix login screen
  + /etc/lightdm/lightdm.conf
    - allow-guest=false
  + /usr/share/lightdm/lightdm.conf/50-ubuntu-conf
    - greeter-show-manual-login=true
    - greeter-hide-users=true
* Check path variable
  + Echo $PATH
* Search for media files/hacking tools
  + Install tree package
  + tree -a /home/

**Network**

* Install and configure the firewall
  + apt-get install ufw
  + ufw enable
  + ufw default deny incoming
  + ufw default allow outgoing
  + ufw logging on
  + service ufw restart
* Check ports and close all unnecessary ports by removing unnecessary services
  + netstat -tulpen
  + lsof -i :*port*
  + whereis *program*
  + dpkg -S *location*
  + If package
    - apt-get purge package
  + If program
    - rm *location* && killall -9 program
* The hosts file contains any redirects, cypat loves using this file for forensics
  + /etc/hosts
* Check DNS
  + /etc/resolv.conf
* Sysctl handles networking configuration
  + /etc/sysctl.conf
    - Disable ipv6
      * net.ipv6.conf.all.disable\_ipv6 = 1
      * net.ipv6.conf.default.disable\_ipv6 = 1
      * net.ipv6.conf.lo.disable\_ipv6 = 1
      * sysctl -p reload config
    - Configure ipv6
      * net.ipv4.ip\_forward = 0
      * net.ipv4.conf.default.accept\_source\_route = 0
      * net.ipv4.tcp\_syncookies = 1
      * net.ipv4.conf.all.send\_redirects = 0
      * net.ipv4.conf.default.send\_redirects = 0
      * net.ipv4.conf.all.log\_martians = 1
      * net.ipv4.conf.default.secure\_redirects = 1
      * net.ipv4.icmp\_echo\_ifnore\_broadcasts = 1
      * net.ipv4.conf.all.rp\_filter = 1
      * net.ipv4.conf.default.rp\_filter = 1

**Policy**

* Password aging settings
  + /etc/login.defs
    - PASS\_MAX\_DAYS 90
    - PASS\_MIN\_DAYS 10
    - PASS\_WARN\_DAYS 7
* Enable encryption
  + /etc/login.defs
    - ENCRYPT\_METHOD SHA512
    - Comment ROUNDS lines
* PAM (be careful, make sure you set passwords before you do this)
  + Install libpam-cracklib, it helps you make sure this doesn’t backfire
    - apt-get install libpam-cracklib
  + Configure common-password to enforce password complexity
    - /etc/pam.d/common-password
      * password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
      * Password requisite pam\_pwhistory.so use\_authtok remember=24 enforce\_for\_root
  + Configure common-auth to enforce a lockout policy **(be careful)**
    - /etc/pam.d/common-auth
      * auth required pam\_tally2.so deny=5 onerr=fail unlock\_time=1800
    - Configure su to enforce a su policy
      * /etc/pam.d/su
        + auth required pam\_wheel.so
* Secure grub
  + Grub-md5-sum
* System Settings
  + Personal file sharing
  + Remote desktop
  + Record file and application usage
* Audit
  + apt-get install auditd
  + auditctl -e 1

**Bad Things**

* There are a bunch of tools you can use to find malicious files/configuration on the system
  + Lynis
    - apt-get install lynis
    - lynis audit system
  + RKHunter
    - apt install rkhunter
    - rkhunter --propupd
    - rkhunter --checkall
  + ChkRootkit
    - apt install chkrootkit
    - chkrootkit -q
* Check for malicious/unnecessary packages and files
  + Packages
    - dpkg -l | grep *pattern*
  + Files
    - find / -iname *pattern*
  + Apt logs
    - /var/log/apt/history.log
* Check startup files
  + Startup applications
  + Install bum to check startup services
    - apt-get install bum
  + /root/
  + /etc/profile and /etc/profile.d/
    - Don't worry about vte file
  + /etc/bash.bashrc
  + ~/.profile and /root/.profile
  + ~/.bashrc and root/.bashrc
  + ~/.bash\_logout and root/.bash\_logout
  + /etc/rc.local
    - Should be empty
  + /etc/rc[0-6].d/
    - Go through each and clean
    - ls | grep -r \*.sh
* Check cron jobs
  + crontab -l -u root
  + crontab -l -u *user*
  + /etc/crontab
  + /etc/cron.d/\*
  + /etc/crond.hourly, daily, weekly, monthly
  + /var/spool/cron
  + /var/spool/cron/crontabs