**LINUX:**

* LIGHTDM
* sudo apt-get install lightdm
  + edit /etc/lightdm/lightdm.conf
    - add allow-guest=false line at the end
    - sudo restart lightdm
* Updates
  + apt-get update
  + apt-get upgrade
  + apt-get dist-upgrade
* Firewall
  + Apt-get install ufw (only if not installed, check first)
  + ufw enable
  + ufw status
* **Users**
* remove unauthorized users
* Add any needed users
* **Passwords**
* Set complex password for all accounts(make them the same)(Cyb3rPatr!0t$)
* Edit /etc/login.defs
  + FAILLOG\_ENAB YES
  + LOG\_UNKFAIL\_ENAB YES
  + SYSLOG\_SU\_ENAB YES
  + SYSLOG\_SG\_ENAB YES
  + PASS\_MAX\_DAYS 90
  + PASS\_MIN\_DAYS 10
  + PASS\_WARN\_AGE 7
  + Edit /etc/pam.d/common-password
    - password required pam\_cracklib.so retry=3 minlen=12 difok=5 lcredit=0 ucredit=1 dcredit=1 ocredit2
    - password required pam\_unix.so md5 use\_authtok
    - (Reference <https://deer-run.com/users/hal/sysadmin/pam_cracklib.html)>
  + /etc/pam.d/common-auth add deny=5 unlock\_time=1800 to the end of line with pam\_tally2.so
* Check /etc/passwd file
  + Look for repeating UID or GID
  + Make sure no programs have a /bin/sh or bin/bash
  + Only root should have UID and GID of 0
* Check /etc/group file
  + Add all admins to sudo and adm group
* Disable root accounts
* Passwd –l root
* Secure ssh(only if in readme)
  + Edit /ect/ssh/sshd\_config
    - LoginGraceTime 60
    - PermitRootLogin no
    - Protocol 2
    - PermitEmptyPasswords no
    - PasswordAuthentication yes
    - X11Fowarding no
    - UsePAM yes
    - UsePrivilegeSeparation yes
* find ssh authorized keys
  + find / -name authorized\_keys
* User history files
  + find / -name .“history” | grep null
* Secure /etc/shadow
  + Chmod 640 /etc/shadow
* Look for bad prorgams
  + Dpkg-query –l | grep {PACKAGE}(add grep if you want to filter)
* Check sudoers file
  + Check /etc/sudoers
  + Or .etc/sudoers.d
  + Make sure there are no NOPASSWD values
    - Change all to ALL=(ALL:ALL) ALL
* Check user groups
* IF not booting to GUI
  + Check runlevel *runlevel*
  + *RunLEVELS*
    - 0-system halt
    - 1-single user
    - 2-multiuser no filesystem
    - 3 multiuser commandline only
    - 4 userdefineable
    - 5 multi-users GUI
    - 6-REBOOT
    - To change level *Telinit {level}*
* Write down/delete bad files
  + Find [options] [path] [expression]
  + Ex:find [search directory] -type f –name ‘\*.pdf\*’
  + If confused reference <https://linuxize.com/post/how-to-find-files-in-linux-using-the-command-line/>
* Disable unecessary services(top , kill)
* Check open ports
* top command- check for high cpu/ram usage
* ps -auxf
* check open network ports
  + netstat -nalp
  + netstat -plant
* still running binaries
  + ls -alR /proc/”/exe 2> /dev/null | grep deleted

MORE PROCESS stuf

* process running in tmp and dev dirs.
  + ls -alR /proc/”/cwd 2> /dev/null | grep tmp
  + ls -alR /proc/”/cwd 2> /dev/null | grep dev

CHECK THESE dirs.

* /tmp
* /var/tmp
* /dev/shm
* /var/run
* /var/spool
* each users home directories
* CHECK crontabs or other scheduled tasks
* anacron -l/cron
  + crontab -u [user] to specify user
  + /etc/crontab and /etc/cron.d to find system cronjobs
  + limit cro use to admins
  + crontab -e as well

LOGS

* check for zero log sizes
  + ls -al /var/log/\*
* find binary logs
  + grep [[:cntrl:]] /var/log/\* .log

at end if stuck

<https://cdn.ttgtmedia.com/rms/security/Malware%20Forensics%20Field%20Guide%20for%20Linux%20Systems_Ch3.pdf>

CIS document in drive

install and configure auditd

not needed services:

* DCCP(208)
* SCTP
* RDS
* TIPC
* FTP
* SMTP
* DHCP
* LDAP
* DNS
* HTTP
* Samba
* snmp server
* telnet

configure PAM(check CIS documents)

make sure group for root account is GID 0

ensure sudo is installed and requires password

ss -ln to list open ports

service --status-all

install fail2ban