**UBUNTU CHECKLIST – CYBER PATRIOT**

1 Do forensics questions on Desktop

Lsof -i -P -n

Sudo ss -ln | grep tcp

Sudo lsof -i:<port>

2 Updates

Check for security updates

Daily updates

Run update (do this later)

3 Firewall config

ufw or gufw (gui version)

enable

incoming – reject

allow ssh – 22

disable 21 (depends on what the crucial service is)

4 Malware + Viruses

Optional, this may be included

Sudo apt install clamscan

Sudo clamav

5 Ssh permit root login no

Sudo nano /etc/ssh/sshd\_config

Sudo vi “ “ “ “

6 User accounts and admins administration

Remove unwanted accounts

Remove non approved admins

Make sure admins are admins

Change passwords to more secure passwords

7 Make the account and group required

Configurate everything

Password set with next login unless said otherwise

8 Update programs

Update ssh

Update firefox and more…

9 Uninstall “hacking tools” and unwanted apps

Games

Mail - postfix

Gaming apps etc.

10 Firefox blocks dangerous downloads + Firefox config

Preferences in firefox

Don’t save logins

Block pop up windows

Warn websites add ons

Block dangerous content

No cookies

11 PAM files

Cd /etc/pam.d

Sudo apt install libpam-cracklib

Sudo nano common-password

Change line with pan\_unix.so remember to 5 “remember=5”

Change line with pam\_unix.so minlen to 8

Add line with pam\_cracklib.so “ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1” to end of thine

Sudo nano ../login.defs

Scroll to PASS\_MAX\_DAYS 90

Set PASS\_MIN\_DAYS to 10

Set PASS\_WARN\_AGE to 7

Sudo nano common-auth

ADD THIS TO THE BOTTOM OF THE FILE >>

auth required pam\_tally2.so deny=5 onerr=fail unlock\_time=1800

deny sets failed login attempts

12 Look for media files and hidden files + unwanted files

Delete media files

locate \*.mp3

locate \*.jpg

locate \*.png, .mov, .mp4, .avi, .mpg, .mpeg, .flac, .m4a, .flv, .ogg, .gif, .jpeg

delete files called password.txt, members.txt, users.txt etc if it looks suspicious.

13 look for “hacking tools” (more) files in program files

Nmap

Metasploit

Netcat

Aircrack

Ophcrack

Wireshark

Hydra

Etc

14 Check the start-up apps

15 make sure the etc/passwd file isnt accessible without admin/root permission

16 Remove guest account

sudo nano /etc/lightdm/users.conf

“allow-guest=false”

Sudo service lightdm restart

17 Check and disable unwanted/non vital services

ftp

mysql

samba

filezilla

cp

telnet

apache

nginx

nv

found in /etc/

ftp = sudo apt-get remove pure-ftpd

18 Insecure file permissions

To the root of a server local file or passwd file

Chmod -w or -r or -x

W means write

R means read

X means executable

19 visudo

Only main user (you) can use sudo (or only specified accounts!)

20 Netcat

Sudo apt-get purge netcat nc netcat-\*

Removes all forms of netcat

21 Correct file permissions

Chmod -R 444 /var/log

Chmod 440 /etc/passwd

Chmod 440 /etc/shadow

Chmod 440 /etc/group

Chmod -R 444 /etc/ssh

22 Stop receiving bad cookies

Sysctl -n net.ipv4.tcp\_syncookies

23 Check the /etc/hosts file

Remove any other than 127.0.0.1 in ip category

Don’t touch ipv6

24 Use webmin to identify vulnerabilities

25 Check bad sources

Sudo nano /etc/apt/sources.list

Tips + Helpful commands

Systemctl - -type=service list-units

To find where an app is “whereis” so “whereis john” for example

Ctrl + alt + t opens a terminal window

-i ignores case

To find group members cat the /etc/group or type “groups”

ALT firewall

|  |
| --- |
| sudo apt-get install openssh-server |
|  | service ssh start |
|  | ifconfig |
|  | #to see the ip of the server |
|  | sudo apt install firewalld |
|  | #to open a port with firewalld |
|  | firewall-cmd --zone=public --add-port=\*\*\*\*/tcp --permanent |
|  | firewall-cmd --reload |
|  | cd /etc/ssh/ |
|  | sudo nano sshd\_config |
|  | port 2121 |
|  | service ssh restart |
|  | service ssh status |
|  |  |
|  | #check which ports open |
|  | firewall-cmd --list-all |
|  |  |
|  | #closing ports |
|  | firewall-cmd --remove-port=\*\*\*/tcp --permanent |
|  | firewall-cmd --reload |