1 Forensics

1 and 2 maybe a 3rd one

Lsof -i -P -n

2 Updates

Check for security updates

Daily updates

Run update

3 firewall

ufw or gufw (gui version)

status on

incoming – reject

allow ssh – 22

disable 21

4 malware + virus

Sudo apt install clamscan

Sudo clamav

5 ssh permit root login no

Sudo nano /etc/ssh/sshd\_config

Sudo vi “ “ “ “

6 User accounts

Remove unwanted accounts

Remove not admins

Make sure admins are admins

Change passwords

7 make the account and group required

Config everything

Password set with next login unless said otherwise

8 update programs

Update ssh

Update firefox

9 Uninstall “hacking tools” and unwanted apps

Games

Mail

Gaming stuff etc

10 firefox blocks dangerous downloads

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

Delete media files

Cd ..

Cd ..

locate \*.mp3

locate \*.jpg

locate \*.png

13 look for SUS files in program files

Nmap

Metasploit

Netcat

Aircrack

Ophcrack

Wireshark

Hydra

Etc

14 check startup apps

15 make sure passwd files aren’t accessible without admin

16 remove guest account

sudo nano /etc/lightdm/users.conf

“allow-guest=false”

Add that |

17

18

19

20

21