**Cyber Centurion 2023**

1. Forensic Questions

* Lsof -i -P -n
* Sudo ss -ln | grep tcp
* Sudo lsof -i:<port>

1. Read me
2. Firewall

- sudo apt install gufw

1. Users - changing unsecure user passwords

* Sudo usermod –a –G groupname username

1. Firefox
2. Settings + Updates
3. Deleting stuff
4. Ssh root permit
5. Make sure the etc/passwd file isnt accessible without admin/root permission
6. PAM - 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 line

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

1. File Permissions

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

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

1. Remove Guest Account

* /etc/lightdm/users.conf

1. Malware

* Sudo apt install clamscan
* Sudo clamav

1. Check the /etc/hosts file

* Remove any other than 127.0.0.1 in ip category

// Unwanted/Non-vital services :

* ftp (( use command -> sudo apt-get remove pure-ftpd ))
* mysql
* samba
* filezilla
* cp
* telnet
* apache
* nginx
* Netcat
* John
* Nmap
* Metasploit
* Netcat (( to remove all forms of netcat -> Sudo apt-get purge netcat nc netcat-\* ))
* Aircrack
* Ophcrack
* Wireshark
* Hydra
* Mail – postfix
* Gaming apps