Attacking & Defending Test Exercise

-Daniel Sheehan

Introduction

In this skills demo I will begin by installing Ubuntu desktop along with an antivirus software (ClamAV), anti-rootkit software (Chkrootkit) and a system auditing software (Lynis audit system), I will also be using Security Onion to log in as an analyst and check the alerts to see if there is any suspicious activity. If there is I will create a new case and escalate any alerts needed.

Setting up and installing software

I started up my virtual machine and used the sudo apt update command to check all installed software, ensuring everything was up to date.	`root@ub1:~# sudo apt update`
	`Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease`
	`Hit:2 http://ie.archive.ubuntu.com/ubuntu jammy InRelease`
	`Get:3 http://ie.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]`
	`Hit:4 http://ie.archive.ubuntu.com/ubuntu jammy-backports InRelease`
	`Fetched 119 kB in 1s (188 kB/s)`
	`Reading package lists... Done`
	`Building dependency tree... Done`
	`Reading state information... Done`
	`2 packages can be upgraded. Run 'apt list --upgradable' to see them.`
	`root@ub1:~#`

I then installed clamav on my Ubuntu machine using the sudo apt install command	`root@ub1:~# sudo apt install clamav`
	`Reading package lists... Done`
	`Building dependency tree... Done`
	`Reading state information... Done`
	`clamav is already the newest version (0.103.9+dfsg-0ubuntu0.22.04.1).`
	`0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.`
	`root@ub1:~#`

Once clamav was installed I used sudo apt install again to install chkrootkit.	`clamav is already the newest version (0.103.9+dfsg-0ubuntu0.22.04.1).`
	`0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.`
	`root@ub1:~# sudo apt install chkrootkit`
	`Reading package lists... Done`
	`Building dependency tree... Done`
	`Reading state information... Done`
	`chkrootkit is already the newest version (0.55-4).`
	`0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.`
	`root@ub1:~#`

Lastly, I installed Lynis auditing system using sudo apt install, this will run a full scan of my system and show improvements I could make security wise.	`root@ub1:~# sudo apt install lynis`
	`Reading package lists... Done`
	`Building dependency tree... Done`
	`Reading state information... Done`
	`lynis is already the newest version (3.0.7-1).`
	`0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.`
	`root@ub1:~#`

Demonstration of ClamAV

Using the terminal, I cd'd into the home directory and used the clamscan command to run a quick scan of my ubuntu machine and check for Malware that could potentially harm it. Before installing and using the service I ran a "sudo apt update" command to ensure that all packages are up to date.

| **I took this a step further and used the command:** sudo service clamav-daemon status. This told me that clamav was successfully up and running. | ```
---------- SCAN SUMMARY ----------
Known viruses: 8679785
Engine version: 0.103.9
Scanned directories: 22
Scanned files: 9
Infected files: 0
Data scanned: 0.04 MB
Data read: 0.02 MB (ratio 2.00:1)
Time: 19.285 sec (0 m 19 s)
Start Date: 2023:11:30 13:28:28
End Date:   2023:11:30 13:28:48
root@ub1:~# sudo service clamav-daemon status
● clamav-daemon.service - Clam AntiVirus userspace daemon
     Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
    Drop-In: /etc/systemd/system/clamav-daemon.service.d
             └─extend.conf
     Active: active (running) since Thu 2023-11-30 09:45:30 GMT; 3h 45min ago
       Docs: man:clamd(8)
             man:clamd.conf(5)
             https://docs.clamav.net/
   Main PID: 675 (clamd)
      Tasks: 2 (limit: 9202)
     Memory: 1.4G
        CPU: 20.287s
     CGroup: /system.slice/clamav-daemon.service
             └─675 /usr/sbin/clamd --foreground=true

Nov 30 09:46:12 ub1 clamd[675]: Thu Nov 30 09:46:12 2023 -> Self checking every 3600 seconds.
Nov 30 10:46:12 ub1 clamd[675]: Thu Nov 30 10:46:12 2023 -> SelfCheck: Database status OK.
Nov 30 11:30:55 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 11:30:55 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 11:30:56 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 11:30:56 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 11:46:12 ub1 clamd[675]: Thu Nov 30 11:46:12 2023 -> SelfCheck: Database status OK.
Nov 30 12:41:17 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 12:41:17 ub1 systemd[1]: /lib/systemd/system/clamav-daemon.service:12: Standard output type syslog is obsolete, automatically updating to journal. Please update your unit file, and consider
Nov 30 12:46:12 ub1 clamd[675]: Thu Nov 30 12:46:12 2023 -> SelfCheck: Database status OK.
Lines 1-25/25 (END)
```| |
| Once in the correct directory I entered “clamscan” into the CLI in order to run a scan using Clam AV of my system | ```
root@ub1:~# clamscan
clamscan -r
/root/.profile: OK
/root/.sudo_as_admin_successful: Empty file
/root/lynis-30-11-23.txt: OK
/root/.lesshst: OK
/root/.bash_history: OK
/root/.bashrc: OK

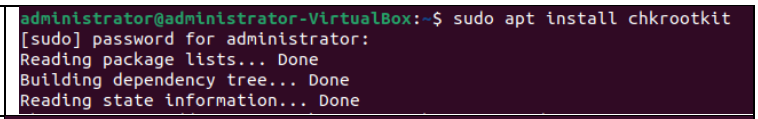
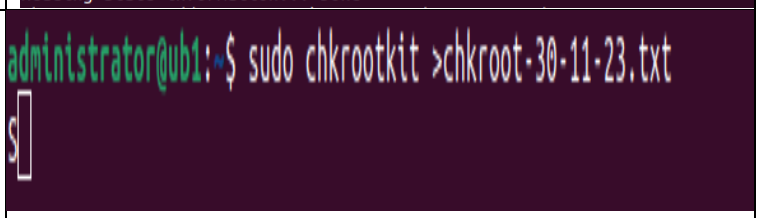
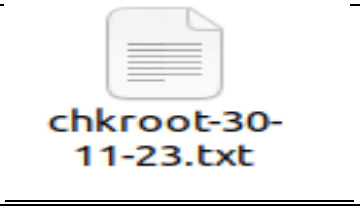
----------- SCAN SUMMARY -----------
Known viruses: 8679785
Engine version: 0.103.9
Scanned directories: 1
Scanned files: 5
Infected files: 0
Data scanned: 0.04 MB
Data read: 0.02 MB (ratio 2.00:1)
Time: 18.876 sec (0 m 18 s)
Start Date: 2023:11:30 13:28:09
End Date:   2023:11:30 13:28:28
root@ub1:~# clamscan -r
```| |
| Using the command: clamscan >scan-30-11-23.txt I redirected the results of this scan into a text file in my home directory providing us with easy access to the scan results. | ```
administrator@ub1:~$ clamscan >scan-30-11-23.txt
```| |
| I have successfully managed to put the results of my scan into a text file for convenience. |  scan-30-11-23.txt | |
```

Below you will find results of this scan in raw text (Clamscan)

```
/home/administrator/cv2.txt: Empty file
/home/administrator/scan-30-11-23.txt: OK
/home/administrator/.profile: OK
/home/administrator/.sudo_as_admin_successful: Empty file
/home/administrator/.vboxclient-vmsvga-session-tty2-control.pid: OK
/home/administrator/cv.txt: OK
/home/administrator/.bash_logout: OK
/home/administrator/.vboxclient-clipboard-tty2-service.pid: OK
/home/administrator/.vboxclient-draganddrop-tty2-control.pid: OK
/home/administrator/.vboxclient-hostversion-tty2-control.pid: OK
/home/administrator/.vboxclient-clipboard-tty2-control.pid: OK
/home/administrator/.bash_history: OK
/home/administrator/.vboxclient-seamless-tty2-control.pid: OK
/home/administrator/csf.tgz: OK
/home/administrator/.bashrc: OK
/home/administrator/.vboxclient-seamless-tty2-service.pid: OK
/home/administrator/.vboxclient-draganddrop-tty2-service.pid: OK
/home/administrator/.vboxclient-vmsvga-session-tty2-service.pid: OK

----------- SCAN SUMMARY -----------
Known viruses: 8679785
Engine version: 0.103.9
Scanned directories: 1
Scanned files: 16
Infected files: 0
Data scanned: 20.24 MB
Data read: 2.18 MB (ratio 9.27:1)
Time: 22.857 sec (0 m 22 s)
Start Date: 2023:11:30 13:37:30
End Date: 2023:11:30 13:37:53
```

Demonstration of chkrootkit

Using sudo chkrootkit >chkroot-30-11-23.txt I successfully saved the results of my rootkit scan to a text file under the name of chkroot-30-11-23.txt in a similar process to my ClamAV scan.

I installed chkrootkit on my system using the command: Sudo apt install chkrootkit	
I will run chkrootkit and redirect the results of my scan to a text file and name it chkroot-30-11-23.txt for easy access and convenience. The data will be scored as plain text.	
I have successfully saved the results of my scan to my text file.	

Below you will find results of this scan in raw text (chkrootkit)

```
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not found
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not found
Checking `mingetty'... not found
Checking `netstat'... not found
not found
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not found
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not found
Checking `sshd'... not infected
Checking `syslogd'... not tested
Checking `tar'... not infected
Checking `tcpd'... not found
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not found
Checking `timed'... not found
Checking `traceroute'... not found
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for rootkit HiDrootkit's default files... nothing found
Searching for rootkit t0rn's default files... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for rootkit Lion's default files... nothing found
Searching for rootkit RSHA's default files... nothing found
Searching for rootkit RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following suspicious files and directories Ire found:
/usr/lib/debug/.build-id
/usr/lib/modules/6.2.0-36-generic/vdso/.build-id
/usr/lib/modules/6.2.0-37-generic/vdso/.build-id
/usr/lib/libreoffice/share/.registry
```

```
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for OBSD rk v1... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for Linux/Ebury - Operation Windigo ssh... nothing found
Searching for 64-bit Linux Rootkit ... nothing found
Searching for 64-bit Linux Rootkit modules... nothing found
Searching for Mumblehard Linux ... nothing found
Searching for Backdoor.Linux.Mokes.a ... nothing found
Searching for Malicious TinyDNS ... nothing found
Searching for Linux.Xor.DDoS ... nothing found
Searching for Linux.Proxy.1.0 ... nothing found
Searching for CrossRAT ... nothing found
Searching for Hidden Cobra ... nothing found
Searching for Rocke Miner ... nothing found
Searching for PWNLNX4 lkm... nothing found
Searching for PWNLNX6 lkm... nothing found
Searching for Umbreon lrk... nothing found
Searching for Kinsing.a backdoor... nothing found
Searching for RotaJakiro backdoor... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[641], /usr/sbin/NetworkManager[641])
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... user administrator deleted or never logged from lastlog!
Checking `chkutmp'... The tty of the following process(es) was not found in /var/run/utmp:
! RUID PID TTY CMD
! adminis+ 113302 pts/0 bash
! adminis+ 114324 pts/0 sudo chkrootkit
chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not tested
```

Demonstration of Lynis

I will now install Lynis audit system to run an audit on my machine. Install using the following command: Sudo apt install lynis	administrator@ub1: ~ administrator@ub1:~$ sudo apt install lynis Reading package lists... Done Building dependency tree... Done Reading state information... Done lynis is already the newest version (3.0.7-1). 0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded. administrator@ub1:~$
I will scan my system by running Lynis I will then redirect the results of my Lynis scan to a text file and call it "lynis-30-11-23.txt" for convenience and easy accessibility.	administrator@ub1:~$ sudo lynis audit system >lynis-30-11-23.txt
As I can see I have successfully stored the results of my scan in then text file.	lynis-30-11-23.txt

Below you will find results of this scan in raw text (Lynis audit system)

```
[1;37m[ Lynis 3.0.7 ][0m

################################################################################
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
Ilcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] [1;33mInitializing program[0m
------------------------------------


[1;31mWarning[0m: [1;37mPID file exists, probably another Lynis process is running.[0m
--------------------------------------------------------------------------------
If you are unsure if another Lynis process is running currently, you are advised
to stop the current process and check the process list first. If you cancelled
a previous instance (by using CTRL+C), you can ignore this message.

You are advised to check for temporary files after program completion.
--------------------------------------------------------------------------------

[1;33mNote: [1;37mCancelling the program can leave temporary files behind[0m
[2C- Detecting OS... [41C [ [1;32mDONE[0m ]
[2C- Checking profiles...[37C [ [1;32mDONE[0m ]

---------------------------------------------------
Program version: 3.0.7
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
Kernel version: 6.2.0
Hardware platform: x86_64
Hostname: ub1
---------------------------------------------------
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
---------------------------------------------------
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
---------------------------------------------------
[2C- Program update status... [32C [ [1;32mNO UPDATE[0m ]

[+] [1;33mSystem tools[0m
------------------------------------
[2C- Scanning available tools...[30C
[2C- Checking system binaries...[30C

[+] [1;35mPlugins (phase 1)[0m
------------------------------------
[0CNote: plugins have more extensive tests and may take several minutes to complete[0C
[0C [0C
[2C- [0;36mPlugin[0m: [1;37mdebian[0m[21C
[
[+] [1;33mDebian Tests[0m
------------------------------------
[2C- Checking for system binaries that are required by Debian Tests...[0C
[4C- Checking /bin... [38C [ [1;32mFOUND[0m ]
[4C- Checking /sbin... [37C [ [1;32mFOUND[0m ]
[4C- Checking /usr/bin... [34C [ [1;32mFOUND[0m ]
[4C- Checking /usr/sbin... [33C [ [1;32mFOUND[0m ]
[4C- Checking /usr/local/bin... [28C [ [1;32mFOUND[0m ]
```

```
[4C- Checking /usr/local/sbin... [27C [ [1;32mFOUND[0m ]
[2C- Authentication:[42C
[4C- PAM (Pluggable Authentication Modules):[16C
[6C- libpam-tmpdir[40C [ [1;31mNot Installed[0m ]
[2C- File System Checks:[38C
[4C- DM-Crypt, Cryptsetup & Cryptmount:[21C
[2C- Software:[48C
[4C- apt-listbugs[43C [ [1;31mNot Installed[0m ]
[4C- apt-listchanges[40C [ [1;31mNot Installed[0m ]
[4C- needrestart[44C [ [1;31mNot Installed[0m ]
[4C- fail2ban[47C [ [1;31mNot Installed[0m ]
]

[+] [1;33mBoot and services[0m
------------------------------------
[2C- Service Manager[42C [ [1;32msystemd[0m ]
[2C- Checking UEFI boot[39C [ [1;37mDISABLED[0m ]
[2C- Checking presence GRUB2[34C [ [1;32mFOUND[0m ]
[4C- Checking for password protection[23C [ [1;31mNONE[0m ]
[2C- Check running services (systemctl)[23C [ [1;32mDONE[0m ]
[8CResult: found 37 running services[20C
[2C- Check enabled services at boot (systemctl)[15C [ [1;32mDONE[0m ]
[8CResult: found 58 enabled services[20C
[2C- Check startup files (permissions)[24C [ [1;32mOK[0m ]
[2C- Running 'systemd-analyze security'[23C
[8C- ModemManager.service:[30C [ [1;37mMEDIUM[0m ]
[8C- NetworkManager.service:[28C [ [1;33mEXPOSED[0m ]
[8C- accounts-daemon.service:[27C [ [1;37mMEDIUM[0m ]
[8C- acpid.service:[37C [ [1;31mUNSAFE[0m ]
[8C- alsa-state.service:[32C [ [1;31mUNSAFE[0m ]
[8C- anacron.service:[35C [ [1;31mUNSAFE[0m ]
[8C- apport.service:[36C [ [1;31mUNSAFE[0m ]
[8C- avahi-daemon.service:[30C [ [1;31mUNSAFE[0m ]
[8C- clamav-daemon.service:[29C [ [1;31mUNSAFE[0m ]
[8C- clamav-freshclam.service:[26C [ [1;31mUNSAFE[0m ]
[8C- colord.service:[36C [ [1;33mEXPOSED[0m ]
[8C- cron.service:[38C [ [1;31mUNSAFE[0m ]
[8C- cups-browsed.service:[30C [ [1;31mUNSAFE[0m ]
[8C- cups.service:[38C [ [1;31mUNSAFE[0m ]
[8C- dbus.service:[38C [ [1;31mUNSAFE[0m ]
[8C- dmesg.service:[37C [ [1;31mUNSAFE[0m ]
[8C- emergency.service:[33C [ [1;31mUNSAFE[0m ]
[8C- gdm.service:[39C [ [1;31mUNSAFE[0m ]
[8C- getty@tty1.service:[32C [ [1;31mUNSAFE[0m ]
[8C- irqbalance.service:[32C [ [1;37mMEDIUM[0m ]
[8C- kerneloops.service:[32C [ [1;31mUNSAFE[0m ]
[8C- lfd.service:[39C [ [1;31mUNSAFE[0m ]
[8C- lynis.service:[37C [ [1;31mUNSAFE[0m ]
[8C- networkd-dispatcher.service:[23C [ [1;31mUNSAFE[0m ]
[8C- nginx.service:[37C [ [1;31mUNSAFE[0m ]
[8C- open-vm-tools.service:[29C [ [1;31mUNSAFE[0m ]
[8C- packagekit.service:[32C [ [1;31mUNSAFE[0m ]
[8C- plymouth-start.service:[28C [ [1;31mUNSAFE[0m ]
[8C- polkit.service:[36C [ [1;31mUNSAFE[0m ]
[8C- poIr-profiles-daemon.service:[21C [ [1;33mEXPOSED[0m ]
[8C- rc-local.service:[34C [ [1;31mUNSAFE[0m ]
[8C- rescue.service:[36C [ [1;31mUNSAFE[0m ]
[8C- rsyslog.service:[35C [ [1;31mUNSAFE[0m ]
[8C- rtkit-daemon.service:[30C [ [1;37mMEDIUM[0m ]
[8C- snapd.aa-prompt-listener.service:[18C [ [1;31mUNSAFE[0m ]
[8C- snapd.service:[37C [ [1;31mUNSAFE[0m ]
[8C- ssh.service:[39C [ [1;31mUNSAFE[0m ]
[8C- switcheroo-control.service:[24C [ [1;33mEXPOSED[0m ]
[8C- systemd-ask-password-console.service:[14C [ [1;31mUNSAFE[0m ]
[8C- systemd-ask-password-plymouth.service:[13C [ [1;31mUNSAFE[0m ]
[8C- systemd-ask-password-wall.service:[17C [ [1;31mUNSAFE[0m ]
[8C- systemd-fsckd.service:[29C [ [1;31mUNSAFE[0m ]
[8C- systemd-initctl.service:[27C [ [1;31mUNSAFE[0m ]
[8C- systemd-jmynald.service:[26C [ [1;32mPROTECTED[0m ]
[8C- systemd-logind.service:[28C [ [1;32mPROTECTED[0m ]
[8C- systemd-networkd.service:[26C [ [1;32mPROTECTED[0m ]
[8C- systemd-oomd.service:[30C [ [1;32mPROTECTED[0m ]
[8C- systemd-resolved.service:[26C [ [1;32mPROTECTED[0m ]
[8C- systemd-rfkill.service:[28C [ [1;31mUNSAFE[0m ]
[8C- systemd-timesyncd.service:[25C [ [1;32mPROTECTED[0m ]
```

```
[8C- systemd-udevd.service:[29C [ [1;37mMEDIUM[0m ]
[8C- thermald.service:[34C [ [1;31mUNSAFE[0m ]
[8C- ubuntu-advantage.service:[26C [ [1;31mUNSAFE[0m ]
[8C- udisks2.service:[35C [ [1;31mUNSAFE[0m ]
[8C- unattended-upgrades.service:[23C [ [1;31mUNSAFE[0m ]
[8C- upolr.service:[36C [ [1;32mPROTECTED[0m ]
[8C- user@1000.service:[33C [ [1;31mUNSAFE[0m ]
[8C- uuidd.service:[37C [ [1;32mPROTECTED[0m ]
[8C- vboxadd-service.service:[27C [ [1;31mUNSAFE[0m ]
[8C- vgauth.service:[36C [ [1;31mUNSAFE[0m ]
[8C- whoopsie.service:[34C [ [1;31mUNSAFE[0m ]
[8C- wpa_supplicant.service:[28C [ [1;31mUNSAFE[0m ]

[+] [1;33mKernel[0m
------------------------------------
[2C- Checking default run level[31C [ [1;32mRUNLEVEL 5[0m ]
[2C- Checking CPU support (NX/PAE)[28C
[4CCPU support: PAE and/or NoeXecute supported[14C [ [1;32mFOUND[0m ]
[2C- Checking kernel version and release[22C [ [1;32mDONE[0m ]
[2C- Checking kernel type[37C [ [1;32mDONE[0m ]
[2C- Checking loaded kernel modules[27C [ [1;32mDONE[0m ]
[6CFound 102 active modules[31C
[2C- Checking Linux kernel configuration file[17C [ [1;32mFOUND[0m ]
[2C- Checking default I/O kernel scheduler[20C [ [1;37mNOT FOUND[0m ]
[2C- Checking for available kernel update[21C [ [1;32mOK[0m ]
[2C- Checking core dumps configuration[24C
[4C- configuration in systemd conf files[20C [ [1;37mDEFAULT[0m ]
[4C- configuration in etc/profile[27C [ [1;37mDEFAULT[0m ]
[4C- 'hard' configuration in security/limits.conf[11C [ [1;37mDEFAULT[0m ]
[4C- 'soft' configuration in security/limits.conf[11C [ [1;37mDEFAULT[0m ]
[4C- Checking setuid core dumps configuration[15C [ [1;37mPROTECTED[0m ]
[2C- Check if reboot is needed[32C [ [1;32mNO[0m ]

[+] [1;33mMemory and Processes[0m
------------------------------------
[2C- Checking /proc/meminfo[35C [ [1;32mFOUND[0m ]
[2C- Searching for dead/zombie processes[22C [ [1;31mFOUND[0m ]
[2C- Searching for IO waiting processes[23C [ [1;31mFOUND[0m ]
[2C- Search prelink tooling[35C [ [1;32mNOT FOUND[0m ]

[+] [1;33mUsers, Groups and Authentication[0m
------------------------------------
[2C- Administrator accounts[35C [ [1;32mOK[0m ]
[2C- Unique UIDs[46C [ [1;32mOK[0m ]
[2C- Consistency of group files (grpck)[23C [ [1;32mOK[0m ]
[2C- Unique group IDs[41C [ [1;32mOK[0m ]
[2C- Unique group names[39C [ [1;32mOK[0m ]
[2C- Password file consistency[32C [ [1;32mOK[0m ]
[2C- Password hashing methods[33C [ [1;32mOK[0m ]
[2C- Checking password hashing rounds[25C [ [1;33mDISABLED[0m ]
[2C- Query system users (non daemons)[25C [ [1;32mDONE[0m ]
[2C- NIS+ authentication support[30C [ [1;37mNOT ENABLED[0m ]
[2C- NIS authentication support[31C [ [1;37mNOT ENABLED[0m ]
[2C- Sudoers file(s)[42C [ [1;32mFOUND[0m ]
[4C- Permissions for directory: /etc/sudoers.d[14C [ [1;31mWARNING[0m ]
[4C- Permissions for: /etc/sudoers[26C [ [1;32mOK[0m ]
[4C- Permissions for: /etc/sudoers.d/README[17C [ [1;32mOK[0m ]
[2C- PAM password strength tools[30C [ [1;32mOK[0m ]
[2C- PAM configuration files (pam.conf)[23C [ [1;32mFOUND[0m ]
[2C- PAM configuration files (pam.d)[26C [ [1;32mFOUND[0m ]
[2C- PAM modules[46C [ [1;32mFOUND[0m ]
[2C- LDAP module in PAM[39C [ [1;37mNOT FOUND[0m ]
[2C- Accounts without expire date[29C [ [1;33mSUGGESTION[0m ]
[2C- Accounts without password[32C [ [1;32mOK[0m ]
[2C- Locked accounts[42C [ [1;32mOK[0m ]
[2C- Checking user password aging (minimum)[19C [ [1;33mDISABLED[0m ]
[2C- User password aging (maximum)[28C [ [1;33mDISABLED[0m ]
[2C- Checking expired passwords[31C [ [1;32mOK[0m ]
[2C- Checking Linux single user mode authentication[11C [ [1;32mOK[0m ]
[2C- Determining default umask[32C
[4C- umask (/etc/profile)[35C [ [1;33mNOT FOUND[0m ]
[4C- umask (/etc/login.defs)[32C [ [1;33mSUGGESTION[0m ]
[2C- LDAP authentication support[30C [ [1;37mNOT ENABLED[0m ]
[2C- Logging failed login attempts[28C [ [1;32mENABLED[0m ]
```

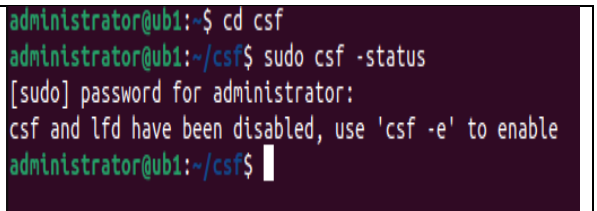
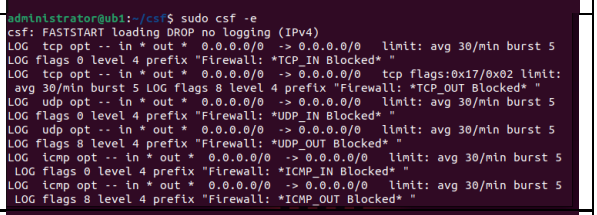
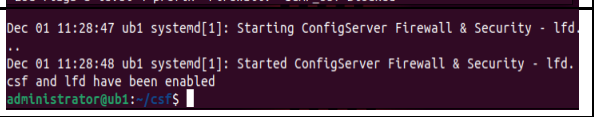
```
[+] [1;33mShells[0m
------------------------------------
[2C- Checking shells from /etc/shells[25C
[4CResult: found 11 shells (valid shells: 11).[14C
[4C- Session timeout settings/tools[25C [ [1;33mNONE[0m ]
[2C- Checking default umask values[28C
[4C- Checking default umask in /etc/bash.bashrc[13C [ [1;33mNONE[0m ]
[4C- Checking default umask in /etc/profile[17C [ [1;33mNONE[0m ]

[+] [1;33mFile systems[0m
------------------------------------
[2C- Checking mount points[36C
[4C- Checking /home mount point[29C [ [1;33mSUGGESTION[0m ]
[4C- Checking /tmp mount point[30C [ [1;33mSUGGESTION[0m ]
[4C- Checking /var mount point[30C [ [1;33mSUGGESTION[0m ]
[2C- Query swap partitions (fstab)[28C [ [1;32mOK[0m ]
[2C- Testing swap partitions[34C [ [1;32mOK[0m ]
[2C- Checking for old files in /tmp[27C [ [1;32mOK[0m ]
[2C- Checking /tmp sticky bit[33C [ [1;32mOK[0m ]
[2C- Checking /var/tmp sticky bit[29C [ [1;32mOK[0m ]
[2C- ACL support root file system[29C [ [1;32mENABLED[0m ]
[2C- Mount options of /[39C [ [1;33mNON DEFAULT[0m ]
[2C- Mount options of /dev[36C [ [1;33mPARTIALLY HARDENED[0m ]
[2C- Mount options of /dev/shm[32C [ [1;33mPARTIALLY HARDENED[0m ]
[2C- Mount options of /run[36C [ [1;32mHARDENED[0m ]
[2C- Total without nodev:10 noexec:31 nosuid:26 ro or noexec (W^X): 12 of total 49[0C
[2C- Disable kernel support of some filesystems[15C

[+] [1;33mUSB Devices[0m
------------------------------------
[2C- Checking usb-storage driver (modprobe config)[12C [ [1;37mNOT DISABLED[0m ]
[2C- Checking USB devices authorization[23C [ [1;33mENABLED[0m ]
[2C- Checking USBGuard[40C [ [1;37mNOT FOUND[0m ]

[+] [1;33mStorage[0m
------------------------------------
[2C- Checking firewire ohci driver (modprobe config)[10C [ [1;32mDISABLED[0m ]

[+] [1;33mNFS[0m
------------------------------------
[2C- Check running NFS daemon[33C [ [1;37mNOT FOUND[0m ]

[+] [1;33mName services[0m
------------------------------------
[2C- Checking search domains[34C [ [1;32mFOUND[0m ]
[2C- Checking /etc/resolv.conf options[24C [ [1;32mFOUND[0m ]
[2C- Searching DNS domain name[32C [ [1;33mUNKNOWN[0m ]
[2C- Checking /etc/hosts[38C
[4C- Duplicate entries in hosts file[24C [ [1;32mNONE[0m ]
[4C- Presence of configured hostname in /etc/hosts[10C [ [1;32mFOUND[0m ]
[4C- Hostname mapped to localhost[27C [ [1;32mNOT FOUND[0m ]
[4C- Localhost mapping to IP address[24C [ [1;32mOK[0m ]

[+] [1;33mPorts and packages[0m
------------------------------------
[2C- Searching package managers[31C
[4C- Searching dpkg package manager[25C [ [1;32mFOUND[0m ]
[6C- Querying package manager[29C
[4C- Query unpurged packages[32C [ [1;33mFOUND[0m ]
[2C- Checking security repository in smyces.list file[8C [ [1;32mOK[0m ]
[2C- Checking APT package database[28C [ [1;32mOK[0m ]
[2C- Checking vulnerable packages[29C [ [1;32mOK[0m ]
[2C- Checking upgradeable packages[28C [ [1;37mSKIPPED[0m ]
[2C- Checking package audit tool[30C [ [1;32mINSTALLED[0m ]
[4CFound: apt-check[41C
[2C- Toolkit for automatic upgrades (unattended-upgrade)[6C [ [1;32mFOUND[0m ]

[+] [1;33mNetworking[0m
------------------------------------
[2C- Checking IPv6 configuration[30C [ [1;37mENABLED[0m ]
[6CConfiguration method[35C [ [1;37mAUTO[0m ]
[6CIPv6 only[46C [ [1;37mNO[0m ]
[2C- Checking configured nameservers[26C
[4C- Testing nameservers[36C
[8CNameserver: 127.0.0.53[31C [ [1;32mOK[0m ]
```

```
[4C- DNSSEC supported (systemd-resolved)[20C [ [1;33mNO[0m ]
[2C- Getting listening ports (TCP/UDP)[24C [ [1;32mDONE[0m ]
[2C- Checking promiscuous interfaces[26C [ [1;32mOK[0m ]
[2C- Checking status DHCP client[30C
[2C- Checking for ARP monitoring software[21C [ [1;33mNOT FOUND[0m ]
[2C- Uncommon network protocols[31C [ [1;33m0[0m ]

[+] [1;33mPrinters and Spools[0m
------------------------------------
[2C- Checking cups daemon[37C [ [1;32mRUNNING[0m ]
[2C- Checking CUPS configuration file[25C [ [1;32mOK[0m ]
[4C- File permissions[39C [ [1;31mWARNING[0m ]
[2C- Checking CUPS addresses/sockets[26C [ [1;32mFOUND[0m ]
[2C- Checking lp daemon[39C [ [1;37mNOT RUNNING[0m ]

[+] [1;33mSoftware: e-mail and messaging[0m
------------------------------------

[+] [1;33mSoftware: firewalls[0m
------------------------------------
[2C- Checking iptables kernel module[26C [ [1;32mFOUND[0m ]
[4C- Checking iptables policies of chains[19C [ [1;32mFOUND[0m ]
[4C- Checking for empty ruleset[29C [ [1;32mOK[0m ]
[4C- Checking for unused rules[30C [ [1;33mFOUND[0m ]
[2C- Checking CSF status (configuration file)[17C [ [1;32mFOUND[0m ]
[4C- Check if CSF testing mode is disabled[18C [ [1;32mOK[0m ]
[4C- Check if CSF is running[32C [ [1;32mOK[0m ]
[2C- Checking host based firewall[29C [ [1;32mACTIVE[0m ]

[+] [1;33mSoftware: Ibserver[0m
------------------------------------
[2C- Checking Apache[42C [ [1;37mNOT FOUND[0m ]
[2C- Checking nginx[43C [ [1;32mFOUND[0m ]
[4C- Searching nginx configuration file[21C [ [1;32mFOUND[0m ]
[6C- Found nginx includes[33C [ [1;32m8 FOUND[0m ]
[4C- Parsing configuration options[26C
[8C- /etc/nginx/nginx.conf[30C
[8C- /etc/nginx/modules-enabled/50-mod-http-geoip2.conf[1C
[8C- /etc/nginx/modules-enabled/50-mod-http-image-filter.conf[0C
[8C- /etc/nginx/modules-enabled/50-mod-http-xslt-filter.conf[0C
[8C- /etc/nginx/modules-enabled/50-mod-mail.conf[8C
[8C- /etc/nginx/modules-enabled/50-mod-stream.conf[6C
[8C- /etc/nginx/modules-enabled/70-mod-stream-geoip2.conf[0C
[8C- /etc/nginx/sites-enabled/default[19C
[6C- SSL configured[39C [ [1;31mNO[0m ]
[6C- Checking log file configuration[22C
[8C- Missing log files (access_log)[21C [ [1;32mNO[0m ]
[8C- Disabled access logging[28C [ [1;32mNO[0m ]
[8C- Missing log files (error_log)[22C [ [1;32mNO[0m ]
[8C- Debugging mode on error_log[24C [ [1;32mNO[0m ]

[+] [1;33mSSH Support[0m
------------------------------------
[2C- Checking running SSH daemon[30C [ [1;32mFOUND[0m ]
[4C- Searching SSH configuration[28C [ [1;32mFOUND[0m ]
[4C- OpenSSH option: AllowTcpForwarding[21C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: ClientAliveCountMax[20C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: ClientAliveInterval[20C [ [1;32mOK[0m ]
[4C- OpenSSH option: Compression[28C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: FingerprintHash[24C [ [1;32mOK[0m ]
[4C- OpenSSH option: GatewayPorts[27C [ [1;32mOK[0m ]
[4C- OpenSSH option: IgnoreRhosts[27C [ [1;32mOK[0m ]
[4C- OpenSSH option: LoginGraceTime[25C [ [1;32mOK[0m ]
[4C- OpenSSH option: LogLevel[31C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: MaxAuthTries[27C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: MaxSessions[28C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: PermitRootLogin[24C [ [1;32mOK[0m ]
[4C- OpenSSH option: PermitUserEnvironment[18C [ [1;32mOK[0m ]
[4C- OpenSSH option: PermitTunnel[27C [ [1;32mOK[0m ]
[4C- OpenSSH option: Port[35C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: PrintLastLog[27C [ [1;32mOK[0m ]
[4C- OpenSSH option: StrictModes[28C [ [1;32mOK[0m ]
[4C- OpenSSH option: TCPKeepAlive[27C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: UseDNS[33C [ [1;32mOK[0m ]
[4C- OpenSSH option: X11Forwarding[26C [ [1;33mSUGGESTION[0m ]
```

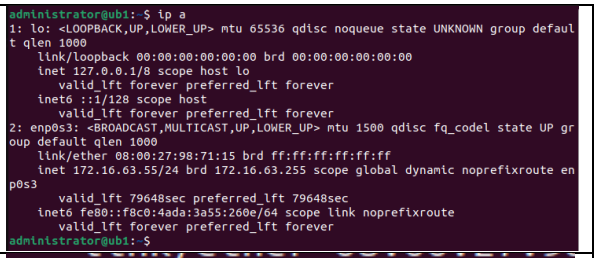
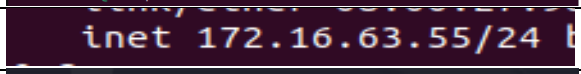
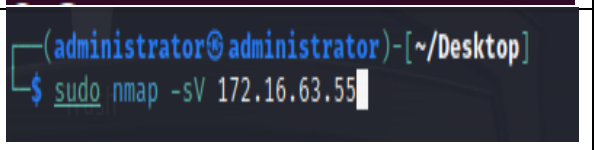
```
[4C- OpenSSH option: AllowAgentForwarding[19C [ [1;33mSUGGESTION[0m ]
[4C- OpenSSH option: AllowUsers[29C [ [1;37mNOT FOUND[0m ]
[4C- OpenSSH option: AllowGroups[28C [ [1;37mNOT FOUND[0m ]

[+] [1;33mSNMP Support[0m
------------------------------------
[2C- Checking running SNMP daemon[29C [ [1;37mNOT FOUND[0m ]

[+] [1;33mDatabases[0m
------------------------------------
[4CNo database engines found[32C

[+] [1;33mLDAP Services[0m
------------------------------------
[2C- Checking OpenLDAP instance[31C [ [1;37mNOT FOUND[0m ]

[+] [1;33mPHP[0m
------------------------------------
[2C- Checking PHP[45C [ [1;37mNOT FOUND[0m ]

[+] [1;33mSquid Support[0m
------------------------------------
[2C- Checking running Squid daemon[28C [ [1;37mNOT FOUND[0m ]

[+] [1;33mLogging and files[0m
------------------------------------
[2C- Checking for a running log daemon[24C [ [1;32mOK[0m ]
[4C- Checking Syslog-NG status[30C [ [1;37mNOT FOUND[0m ]
[4C- Checking systemd jmynal status[24C [ [1;32mFOUND[0m ]
[4C- Checking Metalog status[32C [ [1;37mNOT FOUND[0m ]
[4C- Checking RSyslog status[32C [ [1;32mFOUND[0m ]
[4C- Checking RFC 3195 daemon status[24C [ [1;37mNOT FOUND[0m ]
[4C- Checking minilogd instances[28C [ [1;37mNOT FOUND[0m ]
[2C- Checking logrotate presence[30C [ [1;32mOK[0m ]
[2C- Checking remote logging[34C [ [1;33mNOT ENABLED[0m ]
[2C- Checking log directories (static list)[19C [ [1;32mDONE[0m ]
[2C- Checking open log files[34C [ [1;32mDONE[0m ]
[2C- Checking deleted files in use[28C [ [1;33mFILES FOUND[0m ]

[+] [1;33mInsecure services[0m
------------------------------------
[2C- Installed inetd package[34C [ [1;32mNOT FOUND[0m ]
[2C- Installed xinetd package[33C [ [1;32mOK[0m ]
[4C- xinetd status[42C
[2C- Installed rsh client package[29C [ [1;32mOK[0m ]
[2C- Installed rsh server package[29C [ [1;32mOK[0m ]
[2C- Installed telnet client package[26C [ [1;32mOK[0m ]
[2C- Installed telnet server package[26C [ [1;32mNOT FOUND[0m ]
[2C- Checking NIS client installation[25C [ [1;32mOK[0m ]
[2C- Checking NIS server installation[25C [ [1;32mOK[0m ]
[2C- Checking TFTP client installation[24C [ [1;32mOK[0m ]
[2C- Checking TFTP server installation[24C [ [1;32mOK[0m ]

[+] [1;33mBanners and identification[0m
------------------------------------
[2C- /etc/issue[47C [ [1;32mFOUND[0m ]
[4C- /etc/issue contents[36C [ [1;33mIAK[0m ]
[2C- /etc/issue.net[43C [ [1;32mFOUND[0m ]
[4C- /etc/issue.net contents[32C [ [1;33mIAK[0m ]

[+] [1;33mScheduled tasks[0m
------------------------------------
[2C- Checking crontab and cronjob files[23C [ [1;31mWARNING[0m ]

[+] [1;33mAccounting[0m
------------------------------------
[2C- Checking accounting information[26C [ [1;33mNOT FOUND[0m ]
[2C- Checking sysstat accounting data[25C [ [1;33mNOT FOUND[0m ]
[2C- Checking auditd[42C [ [1;37mNOT FOUND[0m ]
[+] [1;33mTime and Synchronization[0m
------------------------------------
[2C- NTP daemon found: systemd (timesyncd)[20C [ [1;32mFOUND[0m ]
[2C- Checking for a running NTP daemon or client[14C [ [1;32mOK[0m ]
[2C- Last time synchronization[32C [ [1;32m505s[0m ]
[+] [1;33mCryptography[0m
```

NMAP

For my partner to run an NMAP scan I will have to enable csf

I began by entering the csf directory and using sudo csf -status. This told me that csf is currently disabled	
I then used sudo csf -e to enable csf	
I can now see that csf is enabled meaning I are ready to run an NMAP scan with my partner on their Kali machine.	

Now that CSF is installed and enabled I will run an NMAP scan

On my Ubuntu desktop machine I used the ip a command to check the IP of this machine, this is essential to run the NMAP scan.	
This told me that my IP address is 172.16.63.55	
On my partners Kali machine I opened the terminal and ran the command: **sudo nmap -sV** followed by my Ubuntu machines IP address, This ran a n NMAP scan of my machine	

NMAP SCAN

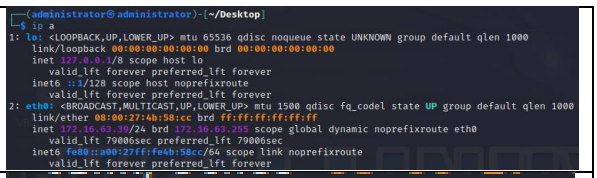
```
┌──(administrator㉿administrator)-[~/Desktop]
└─$ sudo nmap -sV 172.16.63.55
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 11:56 GMT
Nmap scan report for 172.16.63.55
Host is up (0.00046s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT    STATE  SERVICE    VERSION
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
25/tcp  closed smtp
53/tcp  closed domain
80/tcp  closed http
110/tcp closed pop3
143/tcp closed imap
443/tcp closed https
465/tcp closed smtps
587/tcp closed submission
993/tcp closed imaps
995/tcp closed pop3s
MAC Address: 08:00:27:98:71:15 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
```

As I can see my partner's Kali machine successfully managed to run an NMAP scan on my Ubuntu machine showing us that CSF alongside NMAP are up and running. This shows us that SSH is open on port 22.

Blocking IP

Now that I can see that they are able to successfully scan my machine I are going to attempt to block their IP address meaning they should no longer be able to scan my machine.

To do this my partner will run an ip a command in their kali terminal so that I can obtain their IP address, this is the address that I will be blocking.

Ip a scan results:	
I can see my partners IP address is: 172.16.63.39	

Now that I have obtained my partners IP address I will navigate to csf.deny on my Ubuntu machine in order to block their machine from running an NMAP scan.

Navigating to directory of csf.deny

In order to get to my csf.deny file I must cd into the etc file by using cd/etc, I follow this up by typing sudo su and entering my administrator password, this gives us permission to cd into the csf directory.

```
administrator@ub1:~$ cd /etc
administrator@ub1:/etc$ sudo su
[sudo] password for administrator:
root@ub1:/etc# cd csf
root@ub1:/etc/csf#
```

In my csf directory I can check the contents of the directory by typing ls:

```
root@ub1:/etc/csf# ls
alerts          csf.logfiles    csf.smtpauth      messenger
changelog.txt   csf.logignore   csf.suignore      pt_deleted_action.pl
csf.allow       csf.mignore     csf.syslogs       readme.txt
csf.blocklists  csf.pignore     csf.syslogusers   regex.custom.pm
csf.cloudflare  csf.pl          csftest.pl        remove_apf_bfd.sh
csf.conf        csf.rblconf     csf.uidignore     ui
csf.deny        csf.redirect    csfwebmin.tgz     uninstall.sh
csf.dirwatch    csf.resellers   downloadservers   version.txt
csf.dyndns      csf.rignore     install.txt       webmin
csf.fignore     csf.signore     lfd.pl
csf.ignore      csf.sips        license.txt
root@ub1:/etc/csf#
```

I can now see the csf.deny file that I need to add my partners IP address to

I will now open this file and edit it using: nano csf.deny

```
root@ub1:/etc/csf# nano csf.deny
```

Now that I are in the empty csf.deny file I are going to add my partner's IP address at the end of the file	GNU nano 6.2 csf.deny # # Copyright 2006-2018, Way to the Web Limited # URL: http://www.configserver.com # Email: sales@waytotheweb.com # # The following IP addresses will be blocked in iptables # One IP address per line # CIDR addressing allowed with a quaded IP (e.g. 192.168.254.0/24) # Only list IP addresses, not domain names (they will be ignored) # # Note: If you add the text "do not delete" to the comments of an entry then # DENY_IP_LIMIT will ignore those entries and not remove them # # Advanced port+ip filtering allowed with the following format # tcp/udp|in/out|s/d=port,port,...|s/d=ip # # See readme.txt for more information regarding advanced port filtering #
Now that I have added their IP to the csf.deny file I need to save and exit by pressing ctrl s and ctrl x	GNU nano 6.2 csf.deny # # Copyright 2006-2018, Way to the Web Limited # URL: http://www.configserver.com # Email: sales@waytotheweb.com # # The following IP addresses will be blocked in iptables # One IP address per line # CIDR addressing allowed with a quaded IP (e.g. 192.168.254.0/24) # Only list IP addresses, not domain names (they will be ignored) # # Note: If you add the text "do not delete" to the comments of an entry then # DENY_IP_LIMIT will ignore those entries and not remove them # # Advanced port+ip filtering allowed with the following format # tcp/udp|in/out|s/d=port,port,...|s/d=ip # # See readme.txt for more information regarding advanced port filtering # 172.16.63.39
For the block to successfully take place I must now reload the csf file by using the command sudo csf -r	root@ub1:/etc/csf# sudo csf -r

NMAP scan attempt with blocked IP

Results:

```
┌──(administrator㉿administrator)-[~/Desktop]
└─$ sudo nmap -sV 172.16.63.55
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 12:02 GMT
Nmap scan report for 172.16.63.55
Host is up (0.00028s latency).
All 1000 scanned ports on 172.16.63.55 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:98:71:15 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
```

As I can see in the screenshot above the Kali machine was unable to successfully run an NMAP scan as I blocked their IP address

Removing Blocked IP from csf.deny

Now that I have blocked my partners machine I will navigate back to the csf.deny file and remove their IP from the block list to allow them to attempt the next step.

```
  GNU nano 6.2                                                                                    csf.deny
################################################################################
# Copyright 2006-2018, Way to the Web Limited
# URL: http://www.configserver.com
# Email: sales@waytotheweb.com
################################################################################
# The following IP addresses will be blocked in iptables
# One IP address per line
# CIDR addressing allowed with a quaded IP (e.g. 192.168.254.0/24)
# Only list IP addresses, not domain names (they will be ignored)
#
# Note: If you add the text "do not delete" to the comments of an entry then
# DENY_IP_LIMIT will ignore those entries and not remove them
#
# Advanced port+ip filtering allowed with the following format
# tcp/udp|in/out|s/d=port,port,...|s/d=ip
#
# See readme.txt for more information regarding advanced port filtering
#
```

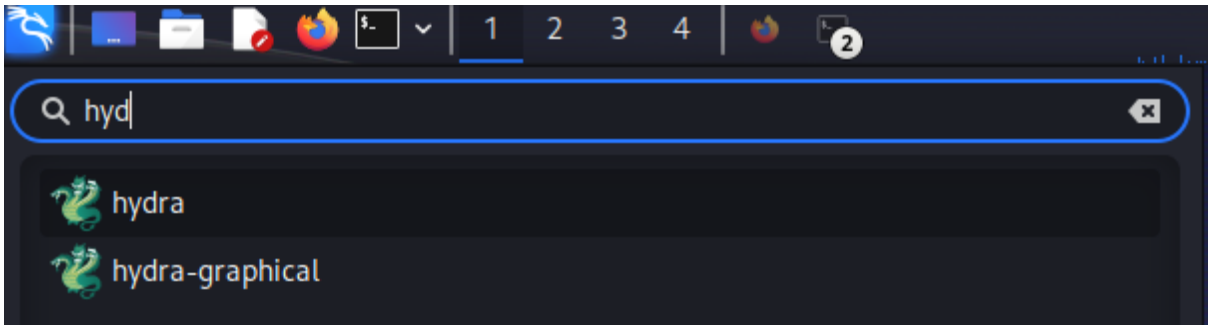
Now that I have removed their IP I can save and exit by using cntrl s and cntrl x.

DO NOT FORGET TO USE sudo csf -r to reload the file!!!!

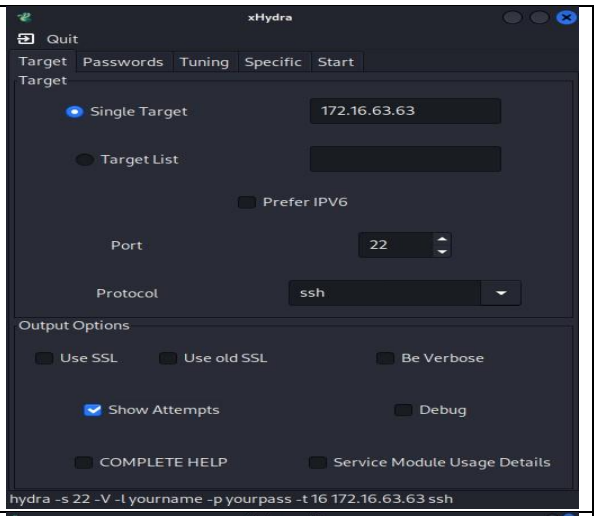
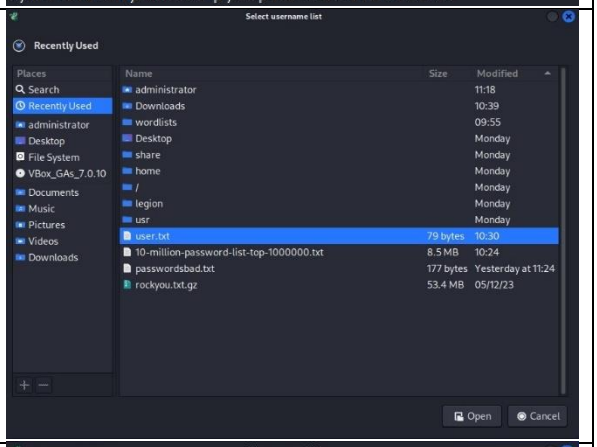
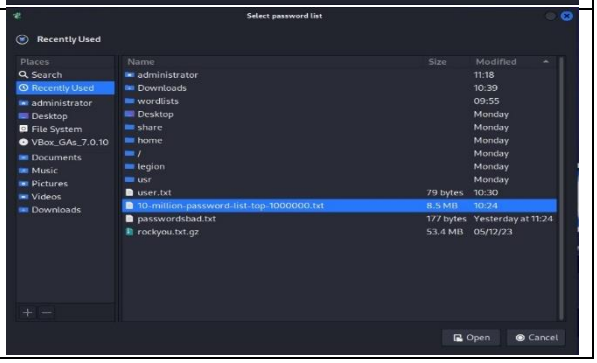
```
ACCEPT  all opt -- in lo out *  0.0.0.0/0  -> 0.0.0.0/0
ACCEPT  all opt -- in * out lo  0.0.0.0/0  -> 0.0.0.0/0
LOGDROPOUT  all opt -- in * out !lo  0.0.0.0/0  -> 0.0.0.0/0
LOGDROPIN  all opt -- in !lo out *  0.0.0.0/0  -> 0.0.0.0/0
csf: FASTSTART loading DNS (IPv4)
LOCALOUTPUT  all opt -- in * out !lo  0.0.0.0/0  -> 0.0.0.0/0
LOCALINPUT  all opt -- in !lo out *  0.0.0.0/0  -> 0.0.0.0/0
*WARNING* Binary location for [SENDMAIL] [/usr/sbin/sendmail] in /etc/csf/csf.conf i
*WARNING* Missing or incorrect binary locations will break csf and lfd functionality

*WARNING* RESTRICT_SYSLOG is disabled. See SECURITY WARNING in /etc/csf/csf.conf.
root@ub1:/etc/csf#
```

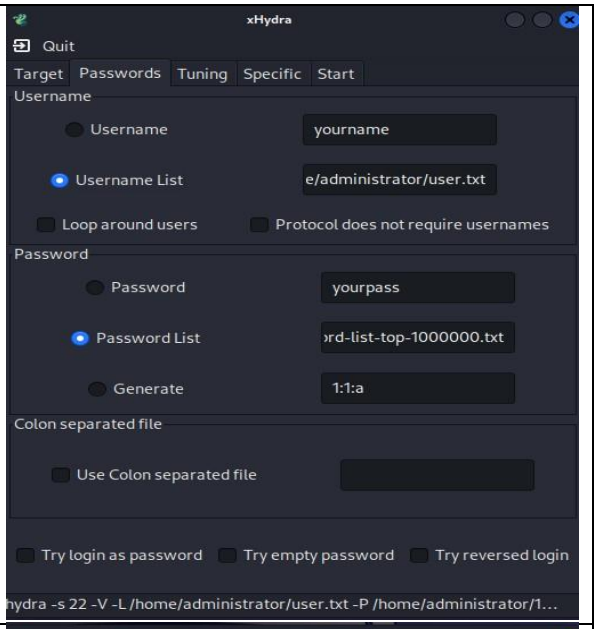
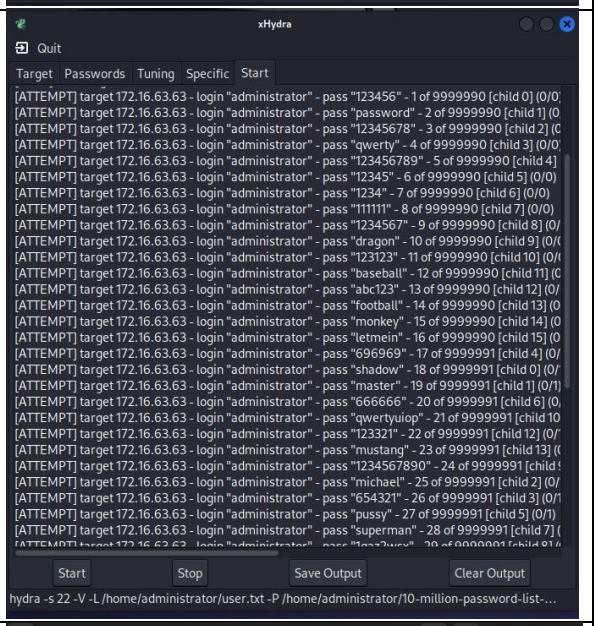
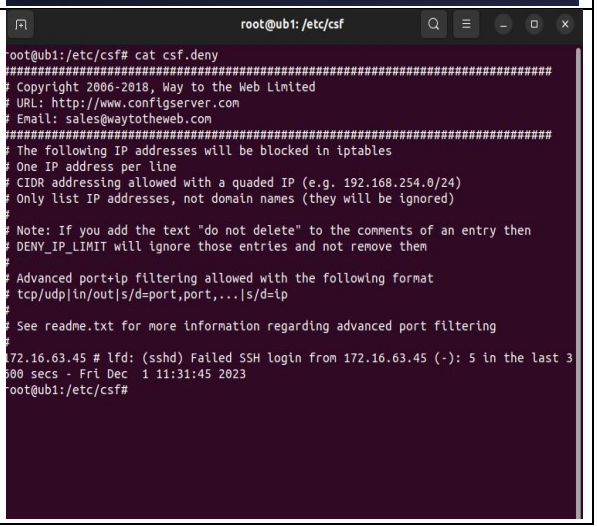
Hydra Brute Force attack

Now that my partner's address is unblocked, I can proceed to the next step where they will attempt a Hydra brute force attack on my Ubuntu machine.

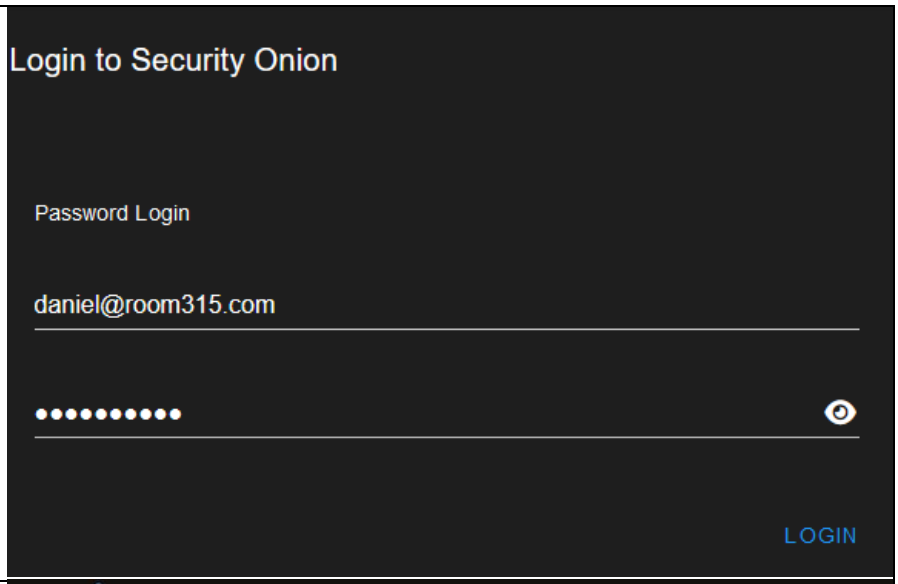
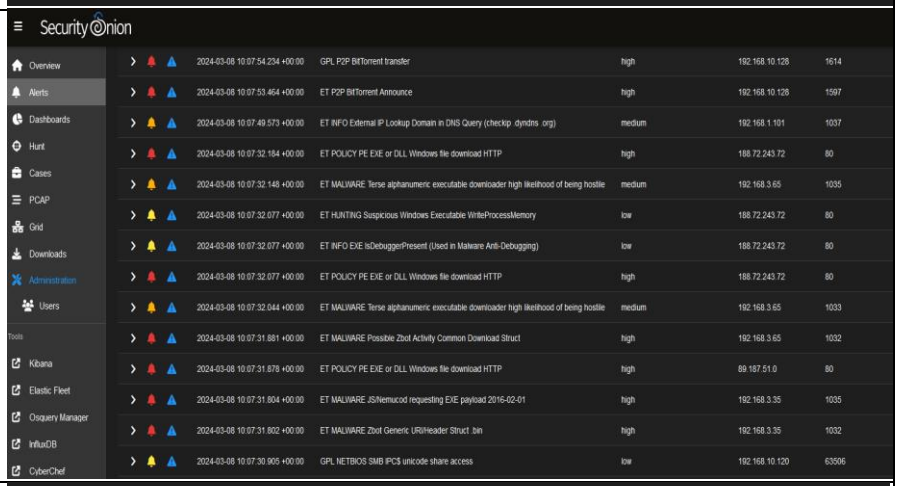
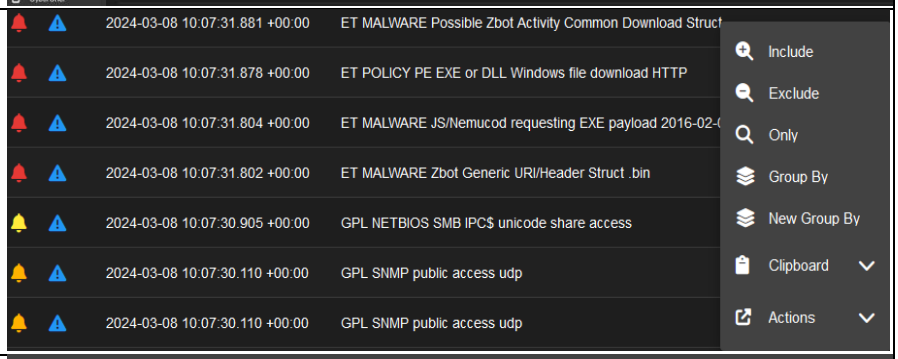
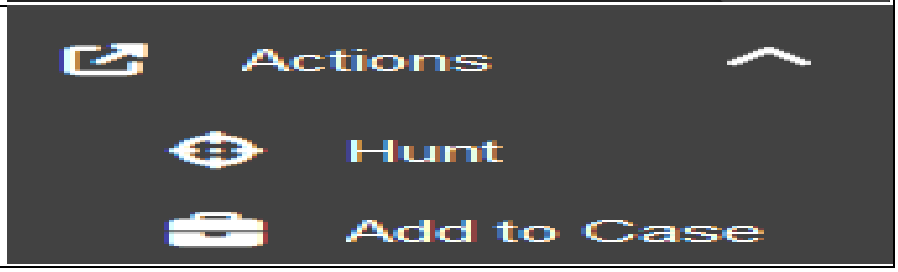


They will be using hydra graphical for this experiment.

My partner will be targeting my Ubuntu machine's IP address: 172.16.63.63 They will be targeting port 22 with an ssh protocol.	
They will use a list of possible user logins during this brute force penetration test to help automate the process and help them get into my system.	
Alongside this my partner will use a password list containing 10 million potential passwords to help them break into my system.	

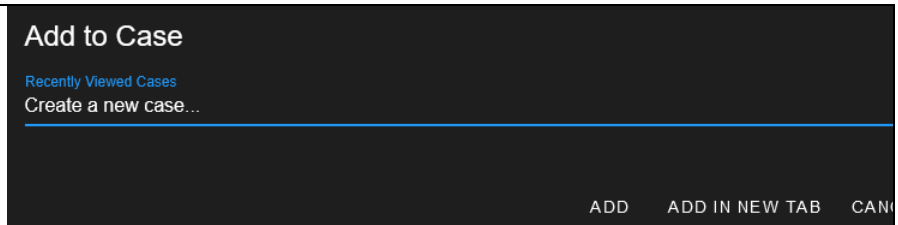
My partner will set up these lists and begin the scan when ready:	
My partner will now have to wait in order to see if their username and password list is successful in breaching my machine, sitting through a long list of attempts.	
I will now Cat scan the csf.deny file on my Ubuntu desktop machine where I can see a list of failed login attempts from my partner's Kali Linux machine:	

Using Security Onion

I navigated to Security Onion and logged into my server using the following login: daniel@room315.com Pass: Password01	
I then navigated to the alerts tab and selected an alert to write a case about, The alert that I selected was to do with possible Zbot activity.	
I clicked on the Zbot case that I selected and clicked on the actions heading	
Under the actions heading I selected "add to Case" in order to start creating a new case.	

I then created a new case and selected:

Add in new tab



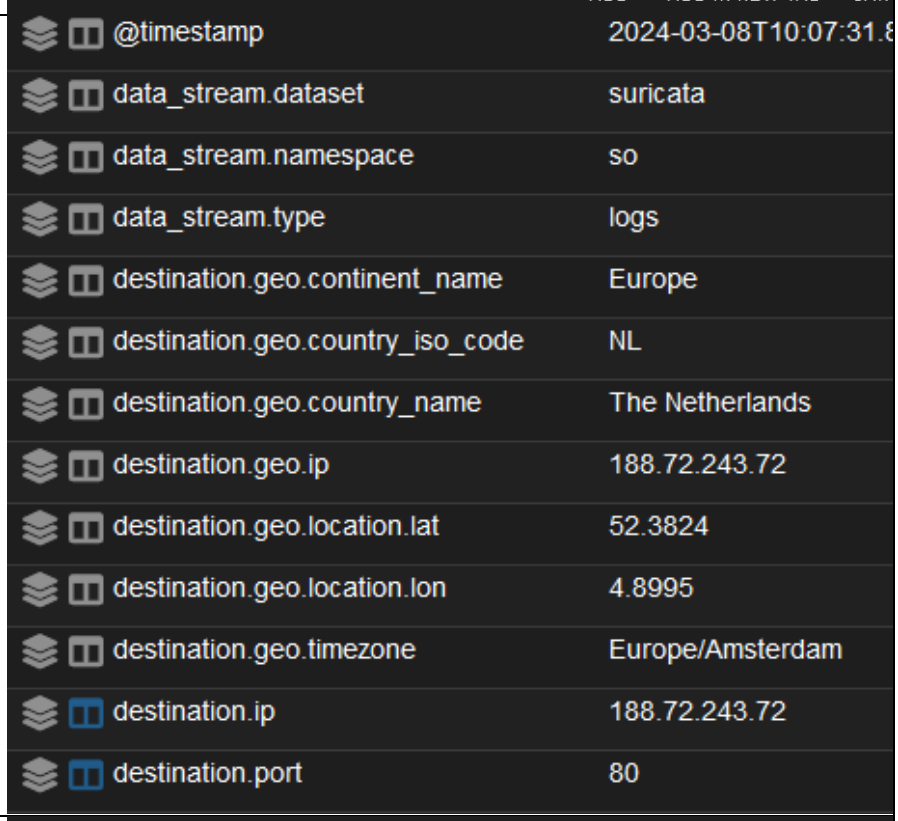
I used the drill down option on the case in order to analyse the information surrounding it.

I was presented information such as:

IP: 188.72.243.72

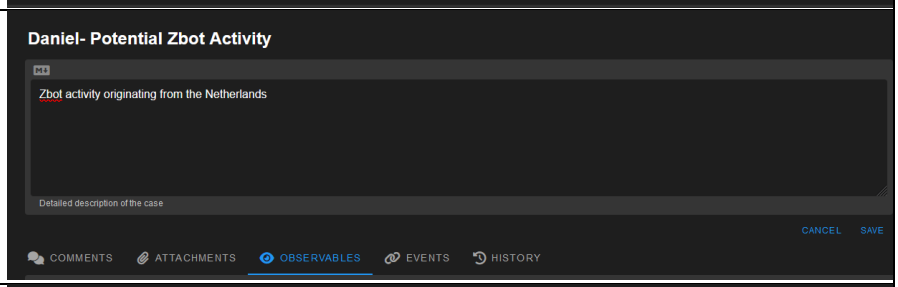
Geolocation/Origin: Amsterdam, Netherlands

Destination port: 80

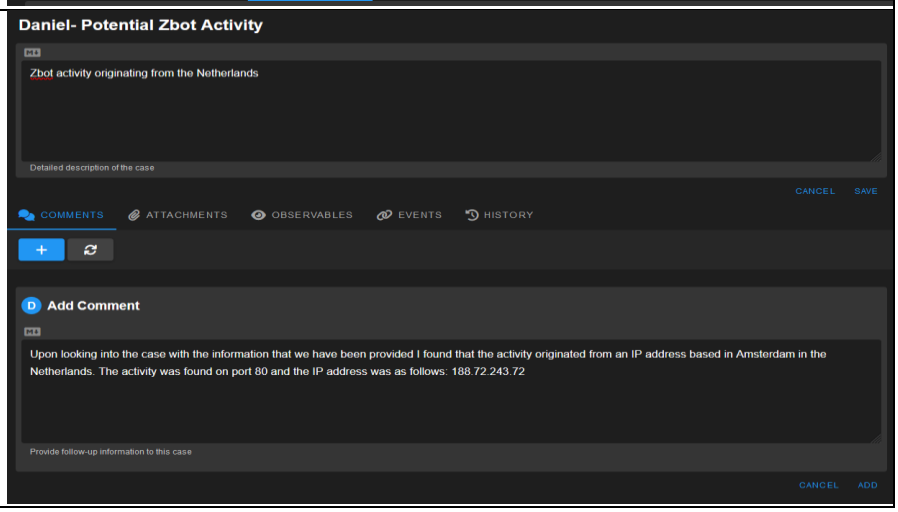


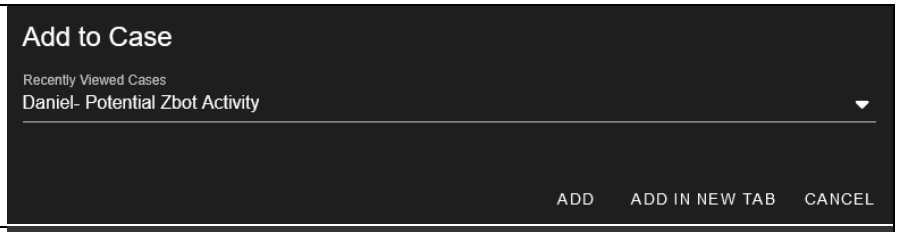
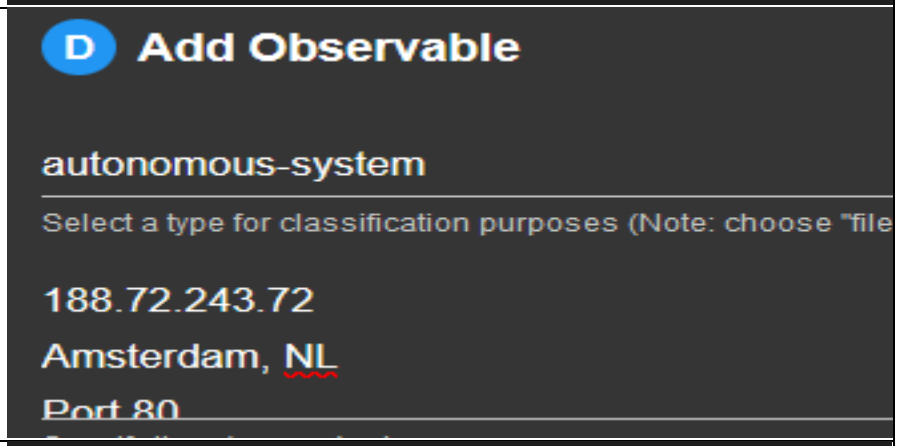
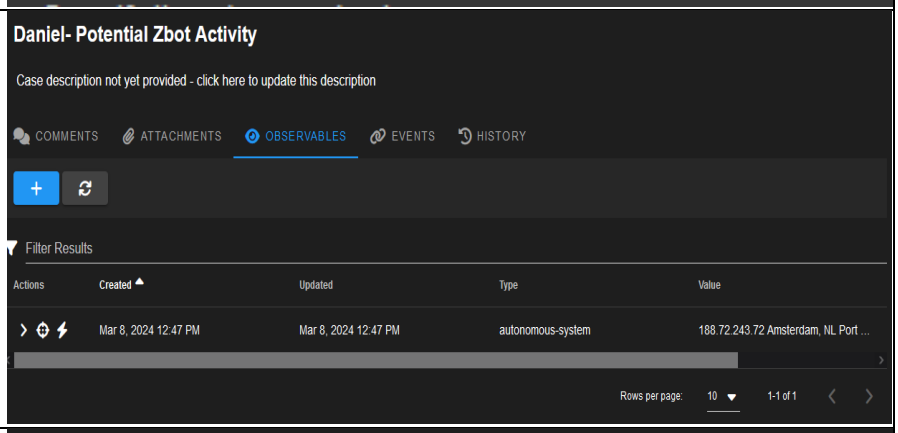
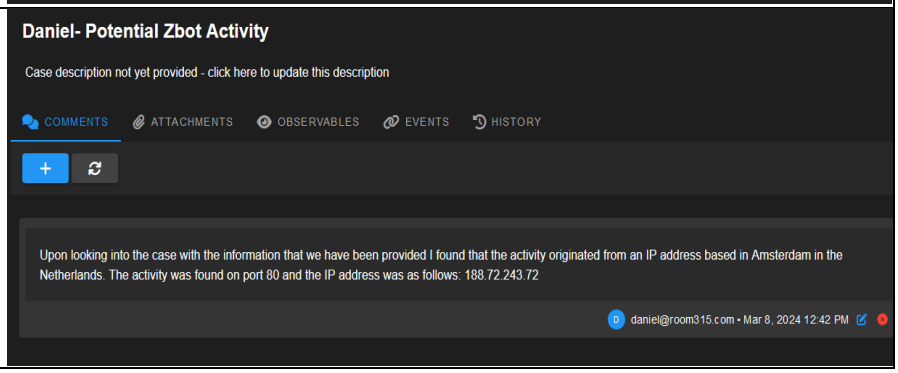
@timestamp	2024-03-08T10:07:31.8
data_stream.dataset	suricata
data_stream.namespace	so
data_stream.type	logs
destination.geo.continent_name	Europe
destination.geo.country_iso_code	NL
destination.geo.country_name	The Netherlands
destination.geo.ip	188.72.243.72
destination.geo.location.lat	52.3824
destination.geo.location.lon	4.8995
destination.geo.timezone	Europe/Amsterdam
destination.ip	188.72.243.72
destination.port	80

I wrote up a report/description on this activity in order to notify any higher ups about this issue.



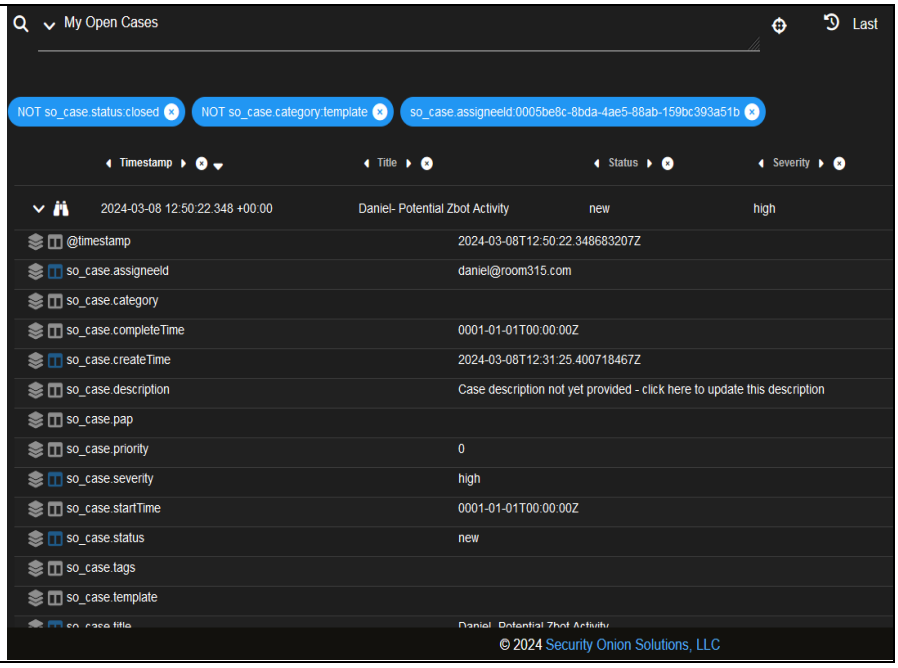
I wrote up a comment expanding on the issue and clicked add to publish it so that my superiors could stay updated and informed on the case



I navigated back to the list and selected my case to add a list of Observables	
I then typed a list of observables to the case that I gathered. Once I was finished, I scrolled down and clicked add to make sure these Ire added to the case	
Observables:	
Comments:	

I then navigated back to the list of open cases and filtered the results to my own username in the “raised by” category.

Here I can see a detailed breakdown of the case that I have made surrounding the alert.



With this I have successfully logged into Security Onion as an analyst, checked alerts for suspicious activity and created a case and escalated it.

Conclusion

After all of these steps have been completed I can confirm that I have completed all steps required to complete this skills demo. I have successfully demonstrated how to install Ubuntu Desktop alongside setting up and using security software such as ClamAV, Chkrootkit and Lynis along with how to use nmap scans and detect security vulnerabilities. I also used security onion to analyse and identify suspicious activity on my network so I could escalate the issue and create a case to investigate the problem