Lab_9_Assignment

1. Write a bash script that monitors a sensitive directory (of your choice) for changes using inotifywait (Linux command). Use trap to handle SIGINT (Ctrl+C) to safely exit the script without leaving any processes running.

```
gedit:4877): tepl-WARNING **: 12:32:19.956: Default style scheme 'Kali-Dark'

gedit:4877): Gtk-WARNING **: 12:33:06.058: Calling org.xfce.Session.Manager.
bit"
┌──(kali㉿kali)-[~/Desktop/CYS]
└─$ ./pg_1.sh
onitoring directory: /home/kali/
etting up watches.  Beware: since -r was given, this may take a while!
atches established.
etected CREATE on /home/kali/.zsh_history.LOCK
etected DELETE on /home/kali/.zsh_history.LOCK
etected CREATE on /home/kali/new_file.txt
etected CREATE on /home/kali/.local/share/recently-used.xbel.TDH0W2
etected MODIFY on /home/kali/.local/share/recently-used.xbel.TDH0W2
etected MOVED_FROM on /home/kali/.local/share/recently-used.xbel.TDH0W2
etected MOVED_TO on /home/kali/.local/share/recently-used.xbel
etected MODIFY on /home/kali/.config/gedit/accels
etected CREATE on /home/kali/.local/share/recently-used.xbel.DUXDX2
etected MODIFY on /home/kali/.local/share/recently-used.xbel.DUXDX2
etected MOVED_FROM on /home/kali/.local/share/recently-used.xbel.DUXDX2
etected MOVED_TO on /home/kali/.local/share/recently-used.xbel
etected CREATE on /home/kali/.local/share/gedit/.goutputstream-6SPEX2
etected MODIFY on /home/kali/.local/share/gedit/.goutputstream-6SPEX2
etected MOVED_FROM on /home/kali/.local/share/gedit/.goutputstream-6SPEX2
etected MOVED_TO on /home/kali/.local/share/gedit/gedit-metadata.xml
CExiting ... Stopping directory monitoring.

┌──(kali㉿kali)-[~/Desktop/CYS]
└─$ gedit pg_1.sh
```

```
#!/bin/bash


DIR_TO_MONITOR="/home/kali/"


cleanup() {
    echo "Exiting ... Stopping directory monitoring."
    pkill -P $$  # Kills any child processes of this script
    exit 0
}

trap cleanup SIGINT


if ! command -v inotifywait &> /dev/null; then
    echo "inotifywait command not found. Please install inotify-tools."
    exit 1
fi

echo "Monitoring directory: $DIR_TO_MONITOR"
inotifywait -m -r -e modify,create,delete,move "$DIR_TO_MONITOR" |
while read -r path action file; do
    echo "Detected $action on $path$file"
done
```

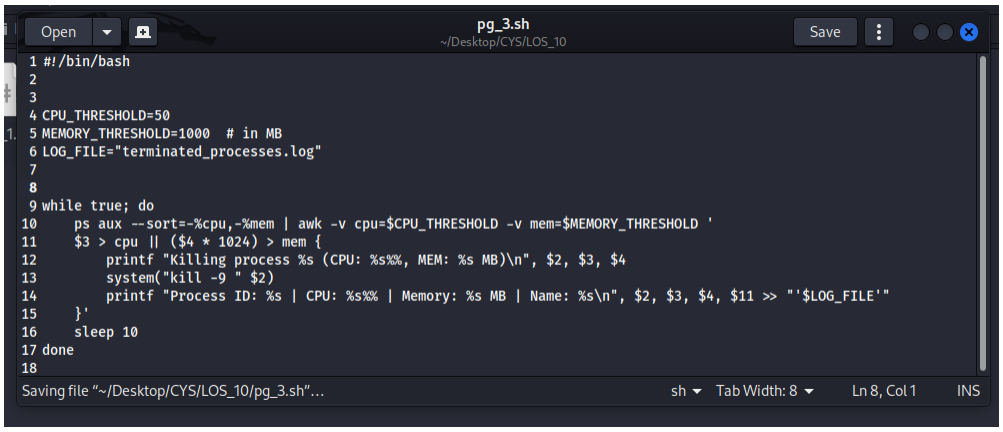
```
┌──(kali㉿kali)-[~]
└─$ gedit new_file.txt

(gedit:6099): tepl-WARNING **: 12:34:45.942: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.

(gedit:6099): tepl-WARNING **: 12:34:45.942: Default style scheme 'Kali-Dark' cannot be found, check your installation.

┌──(kali㉿kali)-[~]
└─$
```

2. Write a bash script that starts a background process (of your choice), and use trap to catch SIGINT and terminate the process cleanly.

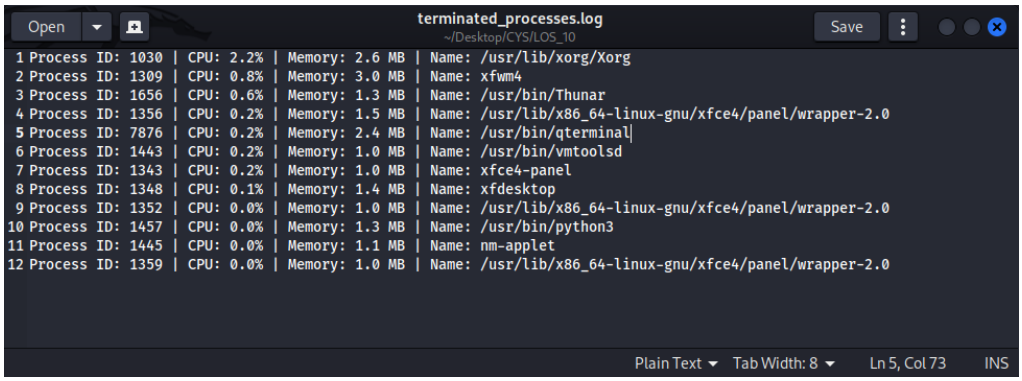
```
(gedit:9158): tepl-WARNING **: 12:40:48.886: Default style scheme 'Kali-Dark' cannot be found,

(gedit:9158): Gtk-WARNING **: 12:40:52.002: Calling org.xfce.Session.Manager.Inhibit failed: G
ibit"

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ ./pg_2.sh
PING google.com (142.250.196.46) 56(84) bytes of data.
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=1 ttl=128 time=62.5 ms

64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=2 ttl=128 time=117 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=3 ttl=128 time=140 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=4 ttl=128 time=126 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=5 ttl=128 time=83.1 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=6 ttl=128 time=133 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=7 ttl=128 time=127 ms
64 bytes from maa03s45-in-f14.1e100.net (142.250.196.46): icmp_seq=8 ttl=128 time=83.2 ms
^C
Terminating background process.
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 35041ms
rtt min/avg/max/mdev = 62.522/108.973/140.192/26.752 ms

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ gedit pg_2.sh

(gedit:9641): tepl-WARNING **: 12:41:45.755: Style scheme 'Kali-Dark' cannot be found, falling

(gedit:9641): tepl-WARNING **: 12:41:45.755: Default style scheme 'Kali-Dark' cannot be found,
```

```
#!/bin/bash


ping -i 5 google.com &
BG_PID=$!


cleanup() {
    echo "Terminating background process."
    kill $BG_PID
    exit 0
}


trap cleanup SIGINT


wait $BG_PID

```

3. Write a script that kills any process exceeding a defined CPU or memory usage limit or matching a list of malicious process names. The script should log the terminated process details for auditing purposes.

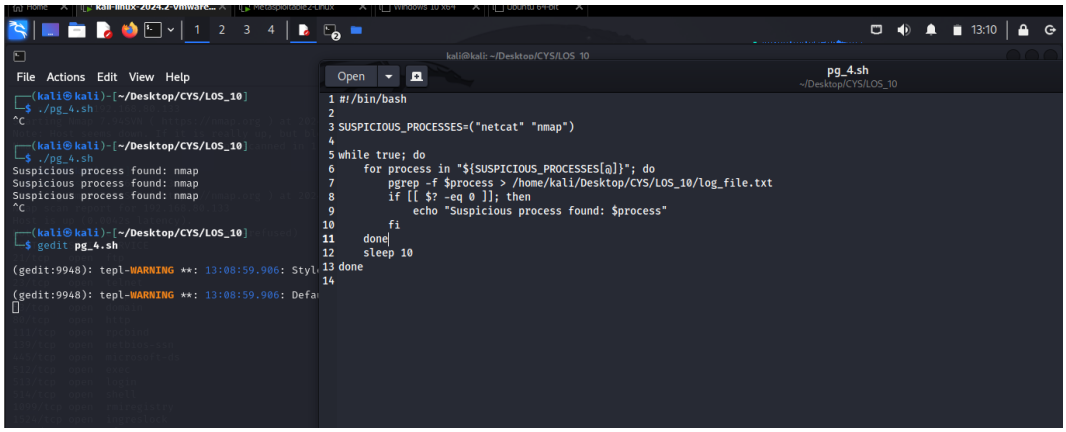



```
#!/bin/bash


CPU_THRESHOLD=50
MEMORY_THRESHOLD=1000  # in MB
LOG_FILE="terminated_processes.log"


while true; do
    ps aux --sort=-%cpu,-%mem | awk -v cpu=$CPU_THRESHOLD -v mem=$MEMORY_THRESHOLD '
    $3 > cpu || ($4 * 1024) > mem {
        printf "Killing process %s (CPU: %s%%, MEM: %s MB)\n", $2, $3, $4
        system("kill -9 " $2)
        printf "Process ID: %s | CPU: %s%% | Memory: %s MB | Name: %s\n", $2, $3, $4, $11 >> "'$LOG_FILE'"
    }'
    sleep 10
done

```

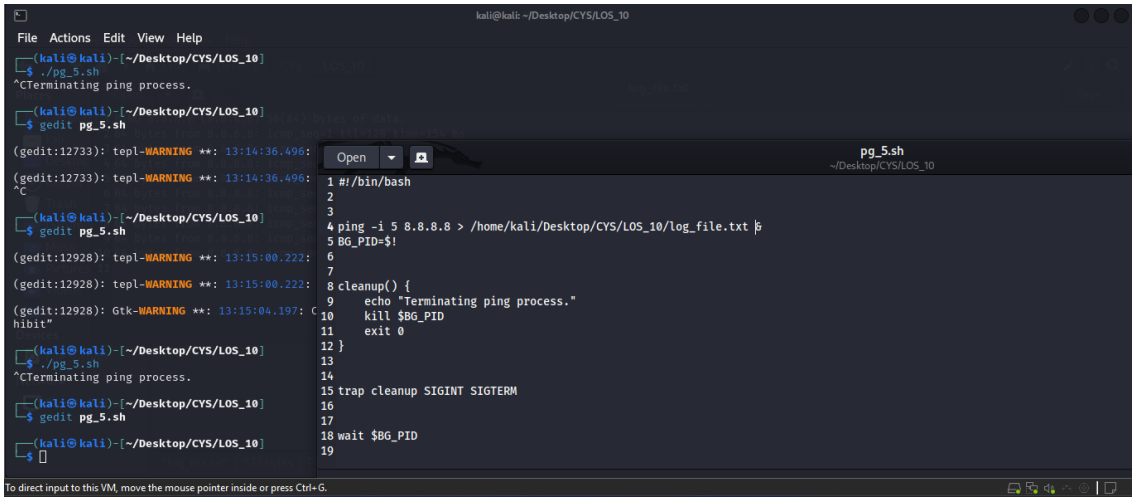


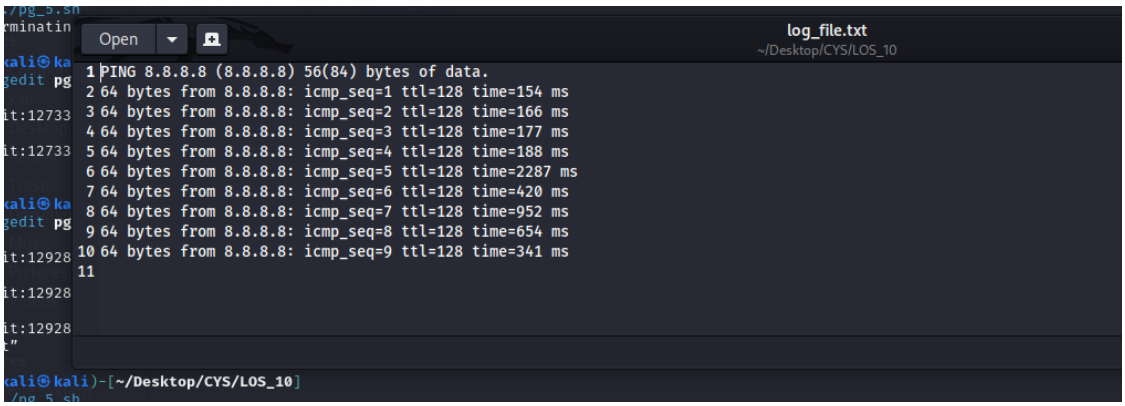

```
Process ID: 1030 | CPU: 2.2% | Memory: 2.6 MB | Name: /usr/lib/xorg/Xorg
Process ID: 1309 | CPU: 0.8% | Memory: 3.0 MB | Name: xfwm4
Process ID: 1656 | CPU: 0.6% | Memory: 1.3 MB | Name: /usr/bin/Thunar
Process ID: 1356 | CPU: 0.2% | Memory: 1.5 MB | Name: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Process ID: 7876 | CPU: 0.2% | Memory: 2.4 MB | Name: /usr/bin/qterminal
Process ID: 1443 | CPU: 0.2% | Memory: 1.0 MB | Name: /usr/bin/vmtoolsd
Process ID: 1343 | CPU: 0.2% | Memory: 1.0 MB | Name: xfce4-panel
Process ID: 1348 | CPU: 0.1% | Memory: 1.4 MB | Name: xfdesktop
Process ID: 1352 | CPU: 0.0% | Memory: 1.0 MB | Name: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Process ID: 1457 | CPU: 0.0% | Memory: 1.3 MB | Name: /usr/bin/python3
Process ID: 1445 | CPU: 0.0% | Memory: 1.1 MB | Name: nm-applet
Process ID: 1359 | CPU: 0.0% | Memory: 1.0 MB | Name: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
```

4. Write a script that monitors running processes and identifies any process that matches a list of known suspicious names (like netcat, nmap).

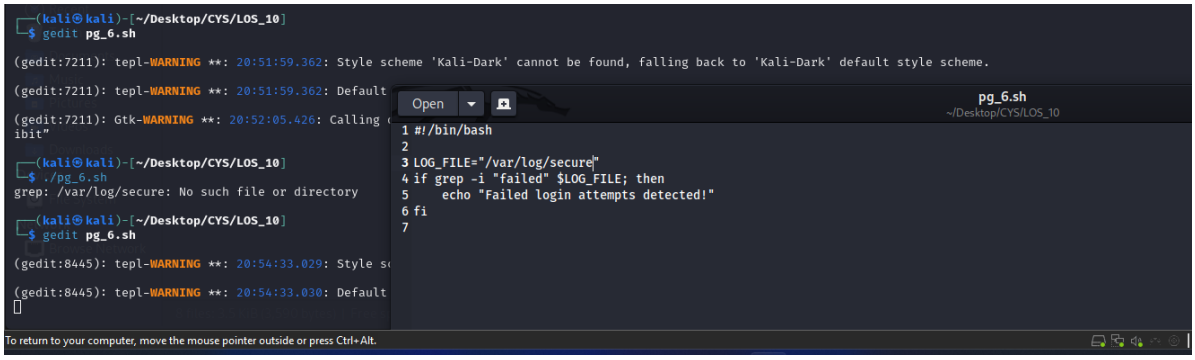


5. Create a script that runs a background process (such as a continuous ping to a specified IP address). Use trap to capture termination signals (SIGINT, SIGTERM) and ensure the background process is terminated safely when the script is interrupted.





6. Write a script that checks /var/log/auth.log for failed login attempts and sends notification if any are found. Schedule this script to run every 15 minutes using cron command.



Since there is no auth.log file, it is showing no such file.
It will show the Failed login attempts when run the program.

Scheduling with Cron:

To schedule the script to run every 15 minutes, follow these steps:

1. Open the crontab editor:

crontab -e

2. Add the following line to the crontab file:

***/15 * * * * /path/to/check_failed_logins.sh**

7. Write a script that removes all files older than 7 days from the /tmp directory, and use at to schedule the script to run at 2:00 AM the next day.

```
1 #!/bin/bash
2
3 TARGET_DIR="/tmp"
4 find $TARGET_DIR -type f -mtime +7 -exec rm -f {} \;
5 echo "Removed files older than 7 days from the Directory $TARGET_DIR"
6
```

```
┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ gedit pg_7.sh

(gedit:12475): tepl-WARNING **: 21:02:43.955: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default

(gedit:12475): tepl-WARNING **: 21:02:43.955: Default style scheme 'Kali-Dark' cannot be found, check your installation.

(gedit:12475): Gtk-WARNING **: 21:03:16.830: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.D
hibit"

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ ./pg_7.sh
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-haveged.service-gKAaLb': Permission denied
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-polkit.service-hfX0jP': Permission denied
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-systemd-logind.service-PpFBPZ': Permission denied
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-ModemManager.service-oiEPw9': Permission denied
find: '/tmp/vmware-root_609-3988556153': Permission denied
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-colord.service-dTzbqn': Permission denied
find: '/tmp/systemd-private-004cd9c9bbe846a08245c2916d624fea-upower.service-eNPLhN': Permission denied
Removed files older than 7 days from the Directory /tmp

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$
```

```
┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ echo "/home/kali/Desktop/CYS/LOS_10/pg_7.sh" | at 2:00 AM tomorrow

warning: commands will be executed using /bin/sh
job 1 at Tue Nov 12 02:00:00 2024

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$
```

8. Write a script to check if disk usage exceeds 10%, and use at to schedule it to run at a specific time.

```
┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ ./pg_8.sh

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ gedit pg_8.sh

(gedit:20866): tepl-WARNING **: 21:19:33.950: St

(gedit:20866): tepl-WARNING **: 21:19:33.950: De

(gedit:20866): Gtk-WARNING **: 21:20:53.662: Cal
hibit"

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ ./pg_8.sh
Warning: Disk usage has exceeded 10%.

┌──(kali㉿kali)-[~/Desktop/CYS/LOS_10]
└─$ gedit pg_8.sh

(gedit:21644): tepl-WARNING **: 21:21:08.934: St

(gedit:21644): tepl-WARNING **: 21:21:08.935: De
```

Open

pg_8.sh
~/Desktop/CYS/LOS_10

```
1 #!/bin/bash
2
3 THRESHOLD=10
4 USAGE=$(df / | grep / | awk '{ print $5}' | sed 's/%//g')
5
6 if [ "$USAGE" -gt "$THRESHOLD" ]; then
7     echo "Warning: Disk usage has exceeded $THRESHOLD%."
8 fi
9
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.