3. Create a file in your system. Whenever someone performs some action(read, write, execute) on that file, the event should be logged somewhere.

To watch the file, we should need tools like

- **iwatch**
- **auditd, etc**

Installing auditd tool

sudo apt install auditd

sudo service start auditd

To see if auditd is active

sudo systemctl status auditd.service

```
bibek@bibek-LfTech:~$ sudo systemctl status auditd.service
● auditd.service - Security Auditing Service
     Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: e
     Active: active (running) since Sat 2021-11-27 20:47:45 +0545; 34s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 7063 (auditd)
      Tasks: 2 (limit: 2946)
     Memory: 384.0K
     CGroup: /system.slice/auditd.service
             └─7063 /sbin/auditd

नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: backlog_wait_time 15000
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: enabled 1
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: failure 1
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: pid 7063
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: rate_limit 0
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: backlog_limit 8192
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: lost 0
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: backlog 4
नव ह्बर  27  20:47:45     bibek-LfTech augenrules[7077]: backlog_wait_time 0
नव ह्बर  27  20:47:45     bibek-LfTech systemd[1]: Started Security Auditing Service.
```

To show the rules

sudo auditctl -l

```
bibek@bibek-LfTech:~$ sudo auditctl -l
No rules
```

At first no rules are written

Creating a bash script file

vi echo.sh

```
#!/bin/bash
echo "Log of leapfrog"
```

Creating echo.log to store logs

touch echo.log

To write rule using auditd

sudo auditctl -w /home/bibek/assignment/auditd/echo.sh -p rwx -k /home/bibek/assignment/auditd/echo.log

Here during writing log,

- **-w represent path to the file**
- **-p represent permission such as r(read), w(write), x(execute),a(change in the file's attribute)**
- **-k represent the file for storing logs**

Now doing cat action on echo.sh file

cat echo.sh

```
bibek@bibek-LfTech:~/assignment/auditd$ cat echo.sh
#!/bin/bash
echo "Log of leapfrog"
bibek@bibek-LfTech:~/assignment/auditd$
```

Checking the log file

sudo ausearch -k echo.log

```
time->Sat Nov 27 21:13:05 2021
type=PROCTITLE msg=audit(1638026885.704:172): proctitle=636174006563686F2E7368
type=PATH msg=audit(1638026885.704:172): item=0 name="echo.sh" inode=532249 dev=08:
05 mode=0100775 ouid=1000 ogid=1000 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 ca
p_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1638026885.704:172): cwd="/home/bibek/assignment/auditd"
type=SYSCALL msg=audit(1638026885.704:172): arch=c000003e syscall=257 success=yes e
xit=3 a0=ffffff9c a1=7fff41fa66ac a2=0 a3=0 items=1 ppid=5399 pid=8008 auid=1000 ui
d=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=p
ts1 ses=9 comm="cat" exe="/usr/bin/cat" subj=unconfined key="/home/bibek/assignment
/auditd/echo.log"
bibek@bibek-LfTech:~/assignment/auditd$
```

Now running script echo.sh

./echo.sh

```
bibek@bibek-LfTech:~/assignment/auditd$ ./echo.sh
Log of leapfrog
bibek@bibek-LfTech:~/assignment/auditd$
```

Again viewing the log

sudo ausearch -k echo.log

```
ts1 ses=9 comm="cat" exe="/usr/bin/cat" subj=unconfined key="/home/bibek/assignment
/auditd/echo.log"
----
time->Sat Nov 27 21:16:00 2021
type=PROCTITLE msg=audit(1638027060.803:179): proctitle=2F62696E2F62617368002E2F656
3686F2E7368
type=PATH msg=audit(1638027060.803:179): item=2 name="/lib64/ld-linux-x86-64.so.2"
inode=661064 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp
=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1638027060.803:179): item=1 name="/bin/bash" inode=655452 dev=0
8:05 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe
=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1638027060.803:179): item=0 name="./echo.sh" inode=532249 dev=0
8:05 mode=0100775 ouid=1000 ogid=1000 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0
cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1638027060.803:179): cwd="/home/bibek/assignment/auditd"
type=EXECVE msg=audit(1638027060.803:179): argc=2 a0="/bin/bash" a1="./echo.sh"
type=SYSCALL msg=audit(1638027060.803:179): arch=c000003e syscall=59 success=yes ex
it=0 a0=5605df6fe720 a1=5605df70e730 a2=5605df6fb7b0 a3=8 items=3 ppid=5399 pid=803
0 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fs
gid=1000 tty=pts1 ses=9 comm="echo.sh" exe="/usr/bin/bash" subj=unconfined key="/ho
me/bibek/assignment/auditd/echo.log"
```

With iwatch

Installing iwatch

sudo apt install iwatch

Creating leapfrog.sh file and for storing log creating leapfrog.log

vi leapfrog.sh

```
#!/bin/bash
echo "IWATCH logs
```

touch leapfrog.log

Watching log of leapfrog file

iwatch -e access,close_nowrite,close_write,open leapfrog.sh

- **-e represents events access, close_nowrite(opened in read-only mode), close_write(opened in writable mode),open,etc**

```
bibek@bibek-LfTech:~/assignment/iwatch$ iwatch -e access,close_nowrite,close_write,
open leapfrog.sh
Wide character in print at /usr/bin/iwatch line 359.
[27/  नव ह्बर /2021    21:32:11]      IN_OPEN leapfrog.sh
Wide character in print at /usr/bin/iwatch line 359.
[27/  नव ह्बर /2021    21:32:11]      IN_CLOSE_NOWRITE leapfrog.sh
Wide character in print at /usr/bin/iwatch line 359.
[27/  नव ह्बर /2021    21:32:11]      IN_OPEN leapfrog.sh
Wide character in print at /usr/bin/iwatch line 359.
[27/  नव ह्बर /2021    21:32:11]      IN_ACCESS leapfrog.sh
Wide character in print at /usr/bin/iwatch line 359.
[27/  नव ह्बर /2021    21:32:11]      IN_CLOSE_NOWRITE leapfrog.sh
```

While appending log to leapfrog.log

iwatch -e access,close_nowrite,close_write,open leapfrog.sh &>> leapfrog.log

```
bibek@bibek-LfTech:~/assignment/iwatch$ cat leapfrog.log
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
bibek@bibek-LfTech:~/assignment/iwatch$
```

Only this message comes, the actual message was not appended

I personally found auditd tool best over iwatch