Q3)
cd Download/
touch test.txt touch test.log
sudo apt install auditd

```
saroj@ubuntu:~/Downloads$ sudo apt install auditd
[sudo] password for saroj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 84 not upgraded.
Need to get 246 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libauparse0 amd64 1:2.8.5-2ubuntu6 [49.8 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/main amd64 auditd amd64 1:2.8.5-2ubuntu6 [196 kB]
Fetched 246 kB in 13s (19.0 kB/s)
```

sudo service auditd start
sudo service auditd status

```
saroj@ubuntu:~/Downloads$ sudo service auditd status
● auditd.service - Security Auditing Service
     Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2021-11-27 07:19:58 PST; 47s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 2505 (auditd)
      Tasks: 2 (limit: 2260)
     Memory: 376.0K
     CGroup: /system.slice/auditd.service
             └─2505 /sbin/auditd

Nov 27 07:19:58 ubuntu augenrules[2519]: backlog_wait_time 15000
Nov 27 07:19:58 ubuntu augenrules[2519]: enabled 1
Nov 27 07:19:58 ubuntu augenrules[2519]: failure 1
Nov 27 07:19:58 ubuntu augenrules[2519]: pid 2505
Nov 27 07:19:58 ubuntu augenrules[2519]: rate_limit 0
Nov 27 07:19:58 ubuntu augenrules[2519]: backlog_limit 8192
Nov 27 07:19:58 ubuntu augenrules[2519]: lost 0
Nov 27 07:19:58 ubuntu augenrules[2519]: backlog 4
Nov 27 07:19:58 ubuntu augenrules[2519]: backlog_wait_time 0
Nov 27 07:19:58 ubuntu systemd[1]: Started Security Auditing Service.
```

sudo auditctl -l
sudo auditctl -s
auditctl -w /home/saroj/Downloads/test.txt -p rwx -k /home/saroj/Downloads/test.log
sudo auditctl -w /home/saroj/Downloads/test.txt -p rwx -k /home/saroj/Downloads/test.log
sudo auditctl -l
sudo ausearch -k /home/saroj/Downloads/test.log
cat test.txt
sudo ausearch -k /home/saroj/Downloads/test.log

```
saroj@ubuntu:~/Downloads$ cat test.txt
aple
ball
cat
dog
egg
fish
saroj@ubuntu:~/Downloads$ sudo ausearch -k /home/saroj/Downloads/test.log
----
time->Sat Nov 27 07:24:39 2021
type=PROCTITLE msg=audit(1638026679.280:92): proctitle=617564697463746C002D77002F686F6D652F7361726F6A2F446F776E6C6F6164732F746573742E747874002D7000727778002D6B002F686F6D652F7361726F6A2F446F776E6C6F6164732F746573742E6C6F67
type=SYSCALL msg=audit(1638026679.280:92): arch=c000003e syscall=44 success=yes exit=1116 a0=4 a1=7ffe5341d830 a2=45c a3=0 items=0 ppid=3387 pid=3388 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=5 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1638026679.280:92): auid=1000 ses=5 subj=unconfined op=add_rule key="/home/saroj/Downloads/test.log" list=4 res=1
----
time->Sat Nov 27 07:26:47 2021
type=PROCTITLE msg=audit(1638026807.737:108): proctitle=6361740074657374742E747874
type=PATH msg=audit(1638026807.737:108): item=0 name="test.txt" inode=1586463 dev=08:05 mode=0100664 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(1638026807.737:108): cwd="/home/saroj/Downloads"
type=SYSCALL msg=audit(1638026807.737:108): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=7fff9b2ed6bf a2=0 a3=0 items=1 ppid=2311 pid=3421 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=5 comm="cat" exe="/usr/bin/cat" subj=unconfined key="/home/saroj/Downloads/test.log"
```