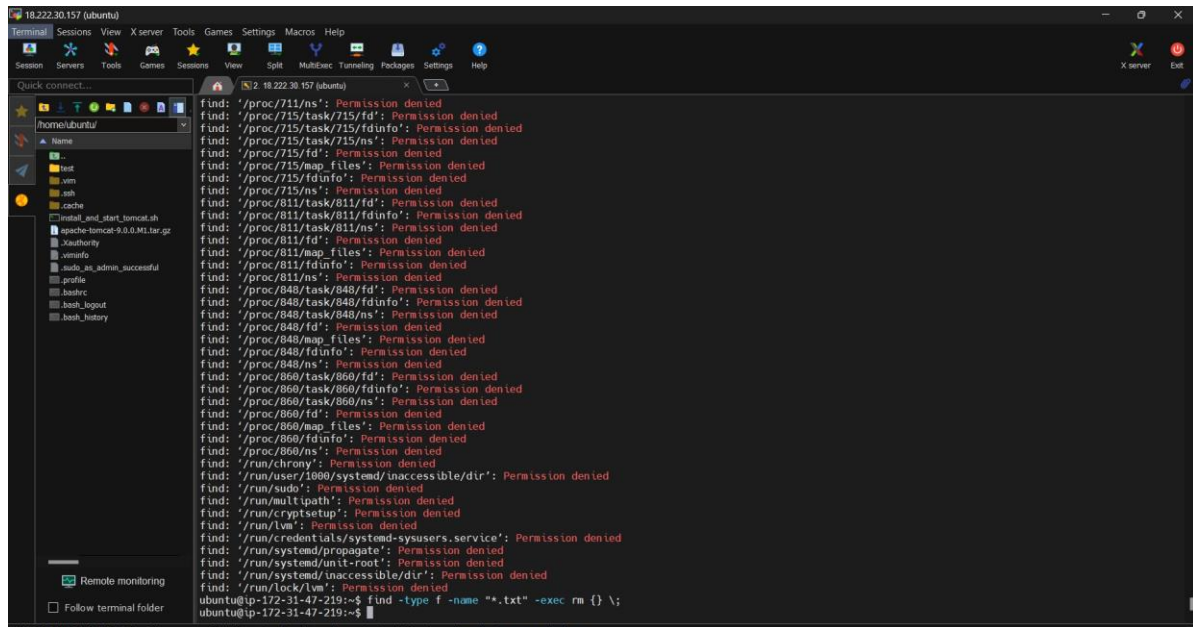


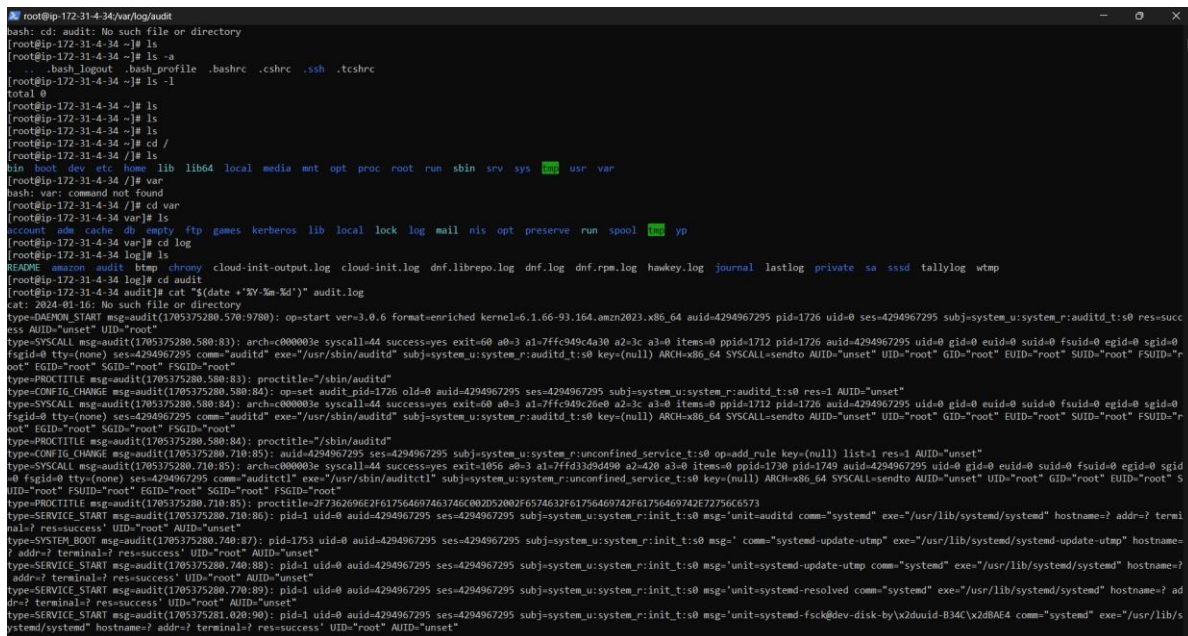
1) Find all files in entire machine ending with .txt and remove them



```
ubuntu@18.222.30.157:~$ find -type f -name "*.txt" -exec rm {} \;
```

The screenshot shows a terminal window with a file manager sidebar on the left displaying the contents of the home directory. The main terminal area shows the execution of a recursive find command to locate and remove all files ending in .txt across the entire system. The command is: `ubuntu@18.222.30.157:~$ find -type f -name "*.txt" -exec rm {} \;`

2) Find 10th record of var/log/audit/access-log file



```
root@ip-172-31-4-34:~# cd /var/log/audit
root@ip-172-31-4-34:~# ls
. .bash_logout .bash_profile .bashrc .chrc .ssh .tcshrc
total 0
root@ip-172-31-4-34:~# cd /
root@ip-172-31-4-34:~# cd /var
root@ip-172-31-4-34:~# cd /var/log
root@ip-172-31-4-34:~# cd /var/log/audit
root@ip-172-31-4-34:~# cat $(date +%Y-%m-%d) audit.log
cat: 2024-01-16: No such file or directory
type=DAEMON_START msg=audit(1705375280.570:9780): op=star ver=3.0.6 format=enriched kernel=6.1.66-93.164.amzn2023.x86_64 audit=4294967295 pid=1726 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=success AUID="unset" UID="root"
type=SYSCALL msg=audit(1705375280.580:83): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc949cda30 a2=3c a3=0 items=0 ppid=1712 pid=1726 audit=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditd" exe="/usr/sbin/auditd" subj=system_u:system_r:auditd_t:s0 key=(null) ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
type=PROCTITLE msg=audit(1705375280.580:83): proctitle="/sbin/auditd"
type=CONFIG_CHANGE msg=audit(1705375280.580:84): op=set audit_pid=1726 old=0 audit=4294967295 subj=system_u:system_r:auditd_t:s0 res=1 AUID="unset"
type=SYSCALL msg=audit(1705375280.580:84): arch=c000003e syscall=44 success=yes exit=1056 a0=3 a1=7ffc949cda30 a2=420 a3=0 items=0 ppid=1712 pid=1726 audit=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditd" exe="/usr/sbin/auditd" subj=system_u:system_r:auditd_t:s0 key=(null) ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
type=PROCTITLE msg=audit(1705375280.580:84): proctitle="/sbin/auditd"
type=CONFIG_CHANGE msg=audit(1705375280.710:85): audit=4294967295 subj=system_u:system_r:unconfined_service_t:s0 op=add_rule key=(null) list=1 res=1 AUID="unset"
type=SYSCALL msg=audit(1705375280.710:85): arch=c000003e syscall=44 success=yes exit=1056 a0=3 a1=7ffc949cda30 a2=420 a3=0 items=0 ppid=1730 pid=1749 audit=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditd" exe="/usr/sbin/auditd" subj=system_u:system_r:unconfined_service_t:s0 key=(null) ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
type=SYSTEM_BOOT msg=audit(1705375280.740:87): pid=1753 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success" UID="root" AUID="unset"
type=SYSTEM_BOOT msg=audit(1705375280.740:87): pid=1753 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=systemd-update-utmp exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success" UID="root" AUID="unset"
type=SYSTEM_BOOT msg=audit(1705375280.740:87): pid=1753 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=systemd-update-utmp exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success" UID="root" AUID="unset"
type=SYSTEM_BOOT msg=audit(1705375280.740:87): pid=1753 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=systemd-resolved comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success" UID="root" AUID="unset"
type=SERVICE_START msg=audit(1705375281.020:90): pid=1 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=systemd-fsck@dev-disk-by\x2duuid-B34C\x2dB4E4 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success" UID="root" AUID="unset"
```

The screenshot shows a terminal window where the user navigates to the `/var/log/audit` directory and uses the `cat` command to view the 10th record of the audit log. The command used is `cat $(date +%Y-%m-%d) audit.log`. The output shows several audit records, including system boot events and service start events.

3) Get only today's logs from access-log file

```
root@ip-172-31-4-34:/var/log/audit
[root@ip-172-31-4-34 /]# ls
bin boot dev etc home lib lib64 local media mnt opt proc root run sbin srv sys usr var
[root@ip-172-31-4-34 /]# cd var
[root@ip-172-31-4-34 var]# ls
account adm cache db empty ftp games kerberos lib local lock log mail nis opt preserve run spool yp
[root@ip-172-31-4-34 var]# cd log
[root@ip-172-31-4-34 log]# ls
sshdCDE amazon audit btmp chowny cloud-init-output.log cloud-init.log dnf.librepo.log dnf.log dnf.rpm.log hawkey.log journal lastlog private so sssd tallylog wtmp
[root@ip-172-31-4-34 log]# cd audit
[root@ip-172-31-4-34 audit]# ls
audit.log
[root@ip-172-31-4-34 audit]# cat 'NR=-10' audit.log
type=SERVICE_START msg=audit(1705375280.718:86): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
[root@ip-172-31-4-34 audit]#
```

4) Get all ports which are running (Occupied Ports)

```
root@ip-172-31-4-34-
[root@ip-172-31-4-34 ~]# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
udp        0      0 172.31.4.34:68         0.0.0.0:*
udp        0      0 172.31.4.34:323        0.0.0.0:*
udp6       0      0 fe80::7c:eff:febb:e:546 :::*
udp6       0      0 :::323                 :::*
```