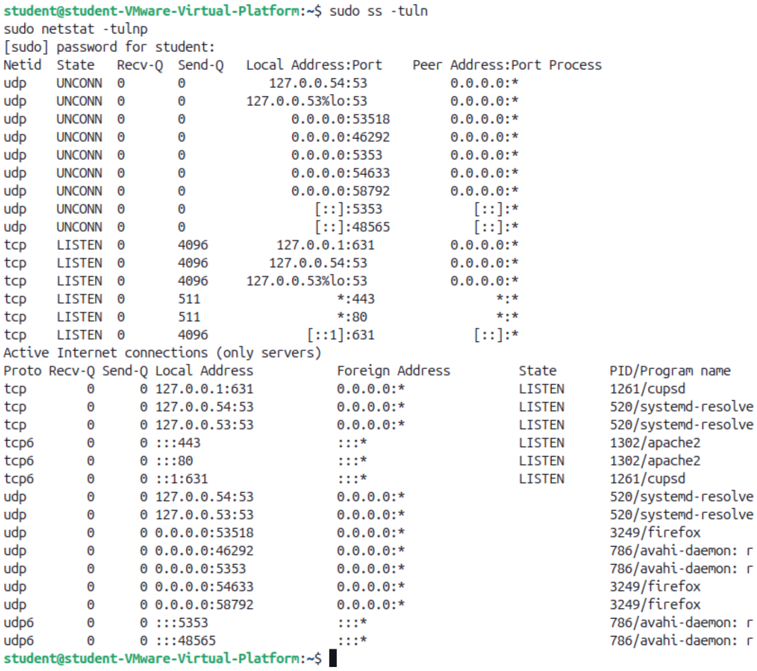
Step 1: Check Running Services & Open Ports

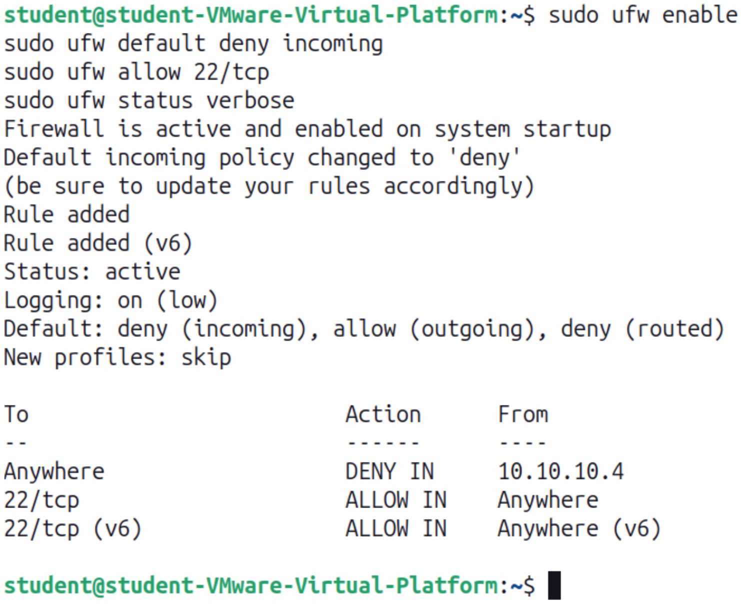
```
sudo ss -tuln
sudo netstat -tulnp
```



```
student@student-VMware-Virtual-Platform:~$ sudo ss -tuln
sudo netstat -tulnp
[sudo] password for student:
Netid  State   Recv-Q  Send-Q   Local Address:Port    Peer Address:Port Process
udp    UNCONN  0       0           127.0.0.54:53           0.0.0.0:*
udp    UNCONN  0       0        127.0.0.53%lo:53           0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:53518        0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:46292        0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:5353         0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:54633        0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:58792        0.0.0.0:*
udp    UNCONN  0       0                 [::]:5353            [::]:*
udp    UNCONN  0       0                 [::]:48565           [::]:*
tcp    LISTEN  0       4096         127.0.0.1:631          0.0.0.0:*
tcp    LISTEN  0       4096        127.0.0.54:53           0.0.0.0:*
tcp    LISTEN  0       4096     127.0.0.53%lo:53           0.0.0.0:*
tcp    LISTEN  0       511                  *:443                *:*
tcp    LISTEN  0       511                  *:80                 *:*
tcp    LISTEN  0       4096             [::1]:631             [::]:*
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1261/cupsd
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      520/systemd-resolve
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      520/systemd-resolve
tcp6       0      0 :::443                  :::*                    LISTEN      1302/apache2
tcp6       0      0 :::80                   :::*                    LISTEN      1302/apache2
tcp6       0      0 ::1:631                 :::*                    LISTEN      1261/cupsd
udp        0      0 127.0.0.54:53           0.0.0.0:*                           520/systemd-resolve
udp        0      0 127.0.0.53:53           0.0.0.0:*                           520/systemd-resolve
udp        0      0 0.0.0.0:53518           0.0.0.0:*                           3249/firefox
udp        0      0 0.0.0.0:46292           0.0.0.0:*                           786/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           786/avahi-daemon: r
udp        0      0 0.0.0.0:54633           0.0.0.0:*                           3249/firefox
udp        0      0 0.0.0.0:58792           0.0.0.0:*                           3249/firefox
udp6       0      0 :::5353                 :::*                                786/avahi-daemon: r
udp6       0      0 :::48565                :::*                                786/avahi-daemon: r
student@student-VMware-Virtual-Platform:~$
```

Step 2: Use UFW (Firewall)

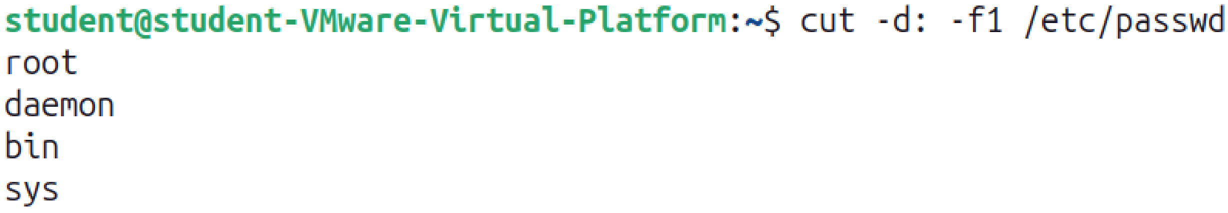
```
sudo ufw enable
sudo ufw default deny incoming
sudo ufw allow 22/tcp
sudo ufw status verbose
```



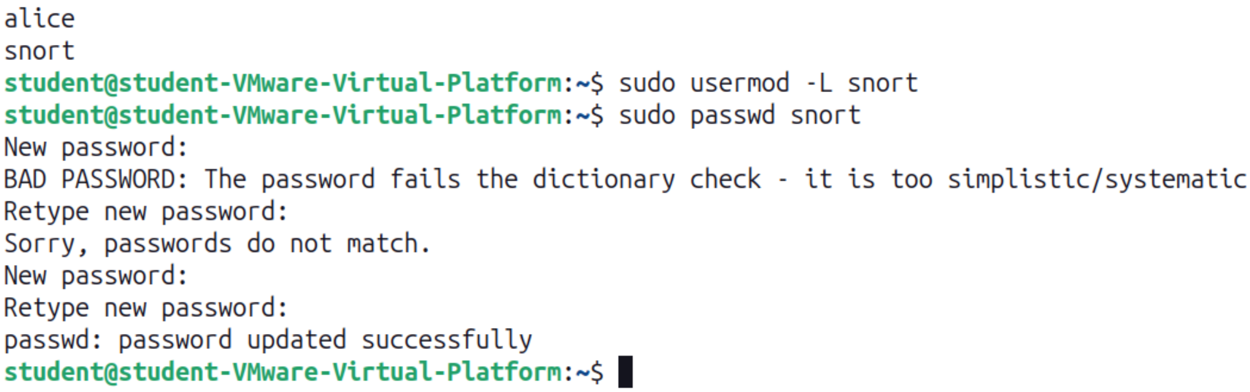
```
student@student-VMware-Virtual-Platform:~$ sudo ufw enable
sudo ufw default deny incoming
sudo ufw allow 22/tcp
sudo ufw status verbose
Firewall is active and enabled on system startup
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Rule added
Rule added (v6)
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
Anywhere                   DENY IN     10.10.10.4
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)

student@student-VMware-Virtual-Platform:~$
```

Step 3: Secure User Accounts

- Check users:
  cut -d: -f1 /etc/passwd
- Disable unused accounts:
  sudo usermod -L username   (Here you can delete Alice)
- Set strong passwords:
  sudo passwd username   (Use the password of Alice)



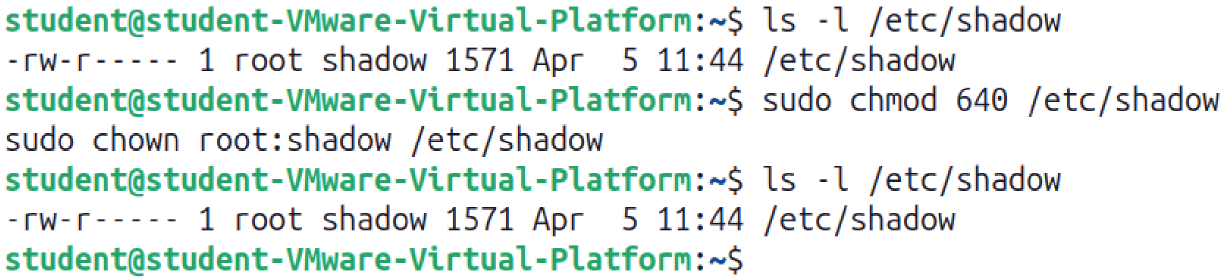
```
student@student-VMware-Virtual-Platform:~$ cut -d: -f1 /etc/passwd
root
daemon
bin
sys
```



```
alice
snort
student@student-VMware-Virtual-Platform:~$ sudo usermod -L snort
student@student-VMware-Virtual-Platform:~$ sudo passwd snort
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
student@student-VMware-Virtual-Platform:~$
```

Step 4: File and Directory Permissions

- View permissions:
  ls -l /etc/shadow
- Modify permissions:
  sudo chmod 640 /etc/shadow
  sudo chown root:shadow /etc/shadow

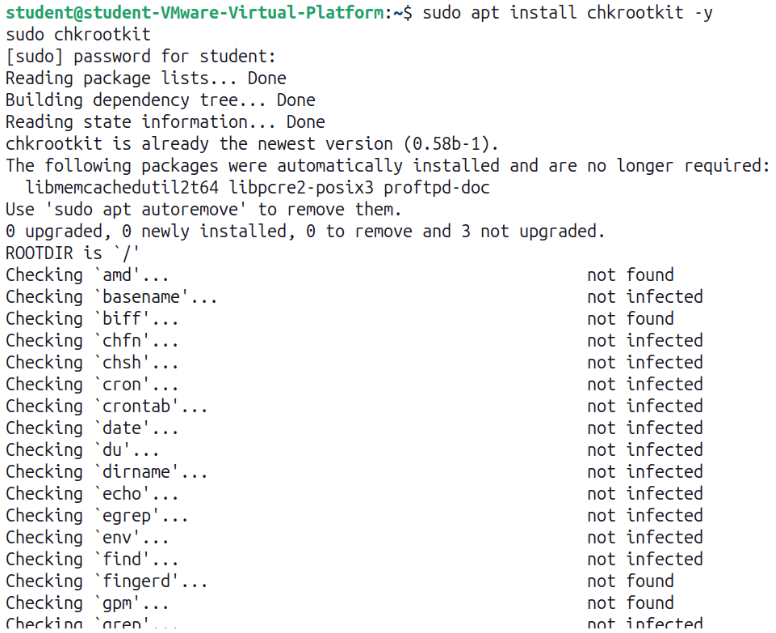


```
student@student-VMware-Virtual-Platform:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1571 Apr  5 11:44 /etc/shadow
student@student-VMware-Virtual-Platform:~$ sudo chmod 640 /etc/shadow
sudo chown root:shadow /etc/shadow
student@student-VMware-Virtual-Platform:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1571 Apr  5 11:44 /etc/shadow
student@student-VMware-Virtual-Platform:~$
```

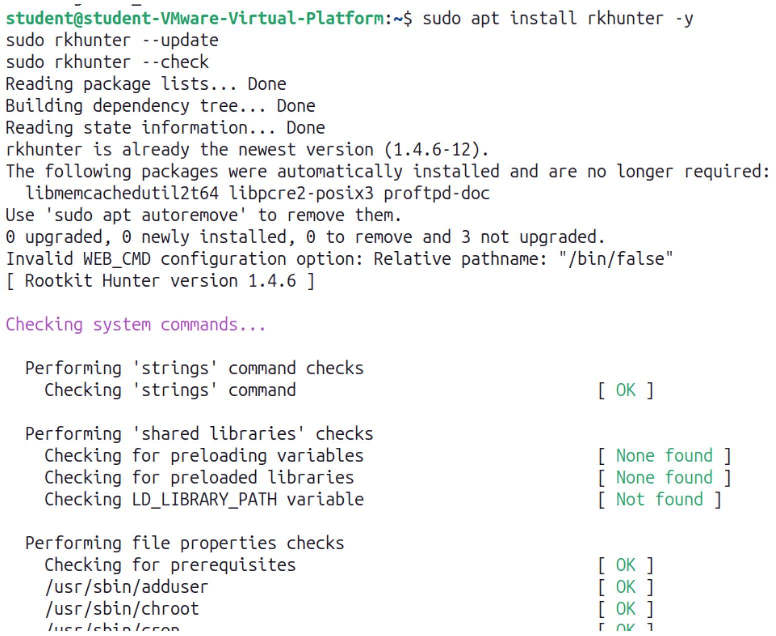
Step 5: Rootkit Detection

sudo chkrootkit

sudo rkhunter --check



```
student@student-VMware-Virtual-Platform:~$ sudo apt install chkrootkit -y
sudo chkrootkit
[sudo] password for student:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
chkrootkit is already the newest version (0.58b-1).
The following packages were automatically installed and are no longer required:
  libmemcachedutil2t64 libpcre2-posix3 proftpd-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
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
```

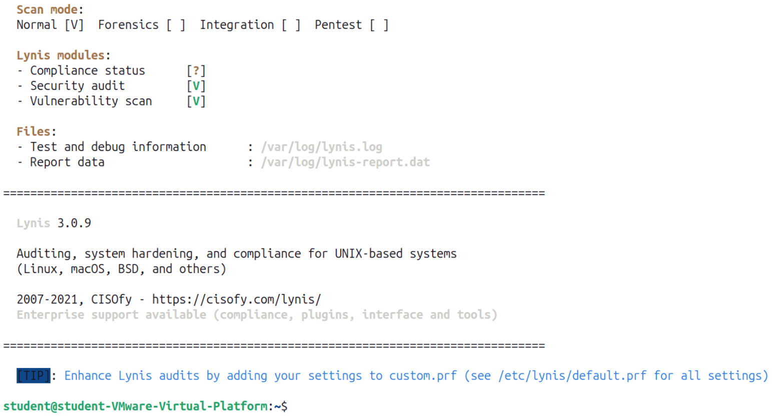


```
student@student-VMware-Virtual-Platform:~$ sudo apt install rkhunter -y
sudo rkhunter --update
sudo rkhunter --check
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rkhunter is already the newest version (1.4.6-12).
The following packages were automatically installed and are no longer required:
  libmemcachedutil2t64 libpcre2-posix3 proftpd-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Invalid WEB_CMD configuration option: Relative pathname: "/bin/false"
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                           [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                    [ None found ]
    Checking for preloaded libraries                     [ None found ]
    Checking LD_LIBRARY_PATH variable                    [ Not found ]

  Performing file properties checks
    Checking for prerequisites                           [ OK ]
    /usr/sbin/adduser                                    [ OK ]
    /usr/sbin/chroot                                     [ OK ]
    /usr/sbin/cron                                       [ OK ]
```

Step 6: Perform Security Audit with Lynis

sudo lynis audit system

Review suggestions at the end of the audit.



```
  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

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

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

student@student-VMware-Virtual-Platform:~$
```

Step 7: Configure System Logging and Auditing

sudo auditctl -e 1

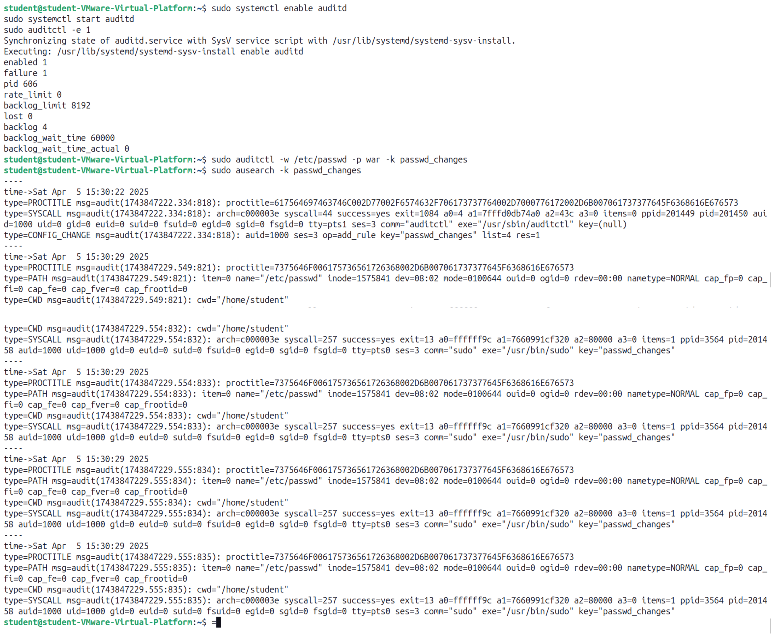
sudo systemctl enable auditd

To monitor file:

sudo auditctl -w /etc/passwd -p war -k passwd_changes

To view logs:

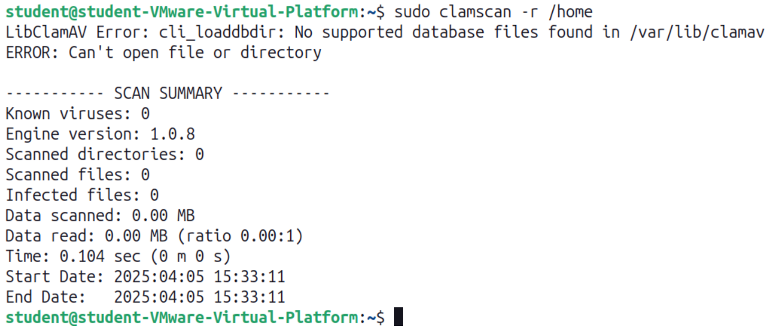
sudo ausearch -k passwd_changes



```
student@student-VMware-Virtual-Platform:~$ sudo systemctl enable auditd
sudo systemctl start auditd
sudo auditctl -e 1
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
enabled 1
failure 1
pid 606
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 60000
backlog_wait_time_actual 0
student@student-VMware-Virtual-Platform:~$ sudo auditctl -w /etc/passwd -p war -k passwd_changes
student@student-VMware-Virtual-Platform:~$ sudo ausearch -k passwd_changes
----
time->Sat Apr  5 15:30:22 2025
type=PROCTITLE msg=audit(1743847222.334:818): proctitle=617564697463746C002D77002F6574632F706173737764002D7000776172002D6B007061737377645F6368616E676573
type=SYSCALL msg=audit(1743847222.334:818): arch=c000003e syscall=44 success=yes exit=1084 a0=4 a1=7fffd0db74a0 a2=43c a3=0 items=0 ppid=201449 pid=201450 aui
d=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="auditctl" exe="/usr/sbin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1743847222.334:818): auid=1000 ses=3 op=add_rule key="passwd_changes" list=4 res=1
----
time->Sat Apr  5 15:30:29 2025
type=PROCTITLE msg=audit(1743847229.549:821): proctitle=7375646F00617573656172636800 2D6B007061737377645F6368616E676573
type=PATH msg=audit(1743847229.549:821): item=0 name="/etc/passwd" inode=1575841 dev=08:02 mode=0100644 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=CWD msg=audit(1743847229.549:821): cwd="/home/student"

type=CWD msg=audit(1743847229.554:832): cwd="/home/student"
type=SYSCALL msg=audit(1743847229.554:832): arch=c000003e syscall=257 success=yes exit=13 a0=ffffff9c a1=7660991cf320 a2=80000 a3=0 items=1 ppid=3564 pid=2014
58 auid=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" key="passwd_changes"
----
time->Sat Apr  5 15:30:29 2025
type=PROCTITLE msg=audit(1743847229.554:833): proctitle=7375646F0061757365617263680002D6B007061737377645F6368616E676573
type=PATH msg=audit(1743847229.554:833): item=0 name="/etc/passwd" inode=1575841 dev=08:02 mode=0100644 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=CWD msg=audit(1743847229.554:833): cwd="/home/student"
type=SYSCALL msg=audit(1743847229.554:833): arch=c000003e syscall=257 success=yes exit=13 a0=ffffff9c a1=7660991cf320 a2=80000 a3=0 items=1 ppid=3564 pid=2014
58 auid=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" key="passwd_changes"
----
time->Sat Apr  5 15:30:29 2025
type=PROCTITLE msg=audit(1743847229.555:834): proctitle=7375646F0061757365617263680002D6B007061737377645F6368616E676573
type=PATH msg=audit(1743847229.555:834): item=0 name="/etc/passwd" inode=1575841 dev=08:02 mode=0100644 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=CWD msg=audit(1743847229.555:834): cwd="/home/student"
type=SYSCALL msg=audit(1743847229.555:834): arch=c000003e syscall=257 success=yes exit=13 a0=ffffff9c a1=7660991cf320 a2=80000 a3=0 items=1 ppid=3564 pid=2014
58 auid=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" key="passwd_changes"
----
time->Sat Apr  5 15:30:29 2025
type=PROCTITLE msg=audit(1743847229.555:835): proctitle=7375646F0061757365617263680002D6B007061737377645F6368616E676573
type=PATH msg=audit(1743847229.555:835): item=0 name="/etc/passwd" inode=1575841 dev=08:02 mode=0100644 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=CWD msg=audit(1743847229.555:835): cwd="/home/student"
type=SYSCALL msg=audit(1743847229.555:835): arch=c000003e syscall=257 success=yes exit=13 a0=ffffff9c a1=7660991cf320 a2=80000 a3=0 items=1 ppid=3564 pid=2014
58 auid=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" key="passwd_changes"
student@student-VMware-Virtual-Platform:~$ =
```

Step 8: Install and Scan with ClamAV Antivirus

```
sudo freshclam
sudo clamscan -r /home
```



```
student@student-VMware-Virtual-Platform:~$ sudo clamscan -r /home
LibClamAV Error: cli_loaddbdir: No supported database files found in /var/lib/clamav
ERROR: Can't open file or directory

----------- SCAN SUMMARY -----------
Known viruses: 0
Engine version: 1.0.8
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.104 sec (0 m 0 s)
Start Date: 2025:04:05 15:33:11
End Date:   2025:04:05 15:33:11
student@student-VMware-Virtual-Platform:~$
```