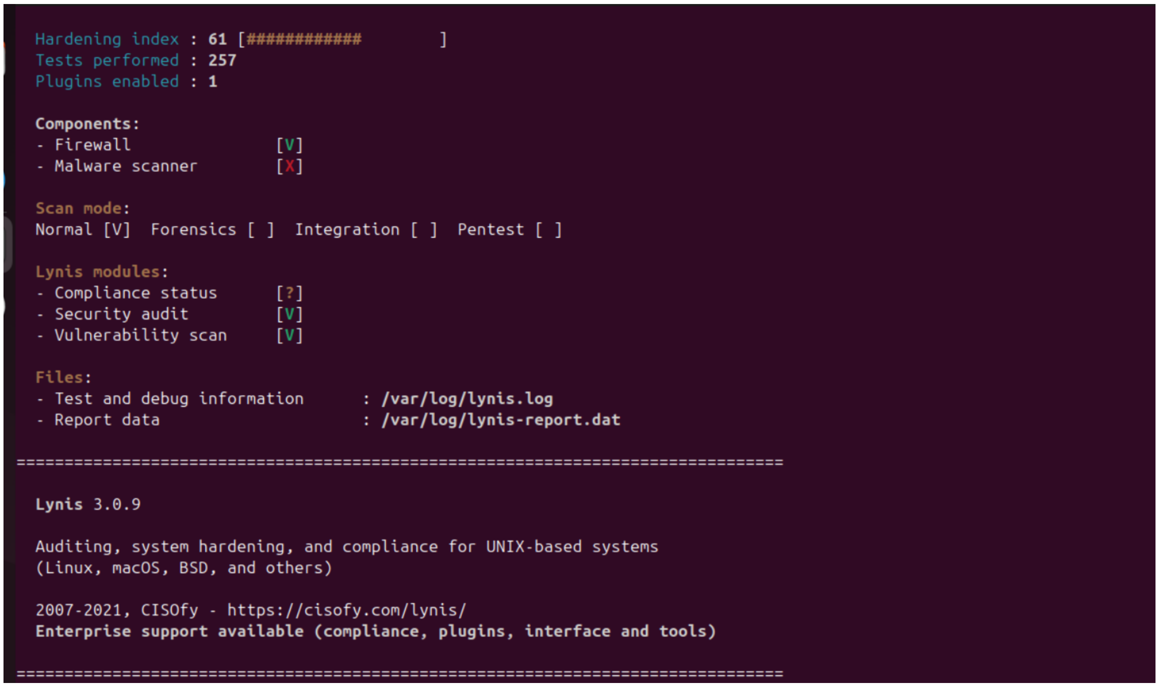
Week 7 – Security Audit & System Evaluation

1. Initial Lynis Security Scan (Before Fixes)

I started by installing Lynis and running a full system audit to see my security baseline. The hardening index I got at the start was 61.

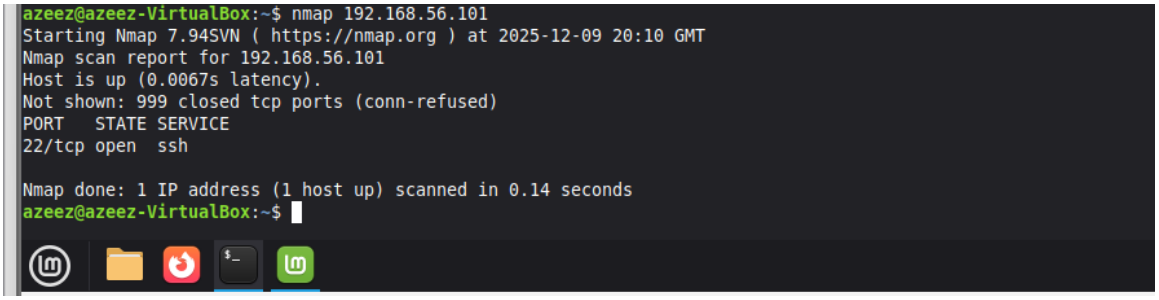


```
  Hardening index : 61 [############        ]
  Tests performed : 257
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  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)

================================================================================
```

2. Nmap Scan From Linux Mint

Next, I used my Linux Mint VM to scan my Ubuntu machine using Nmap. This helped me see which ports were open.

Command used: nmap 192.168.56.101



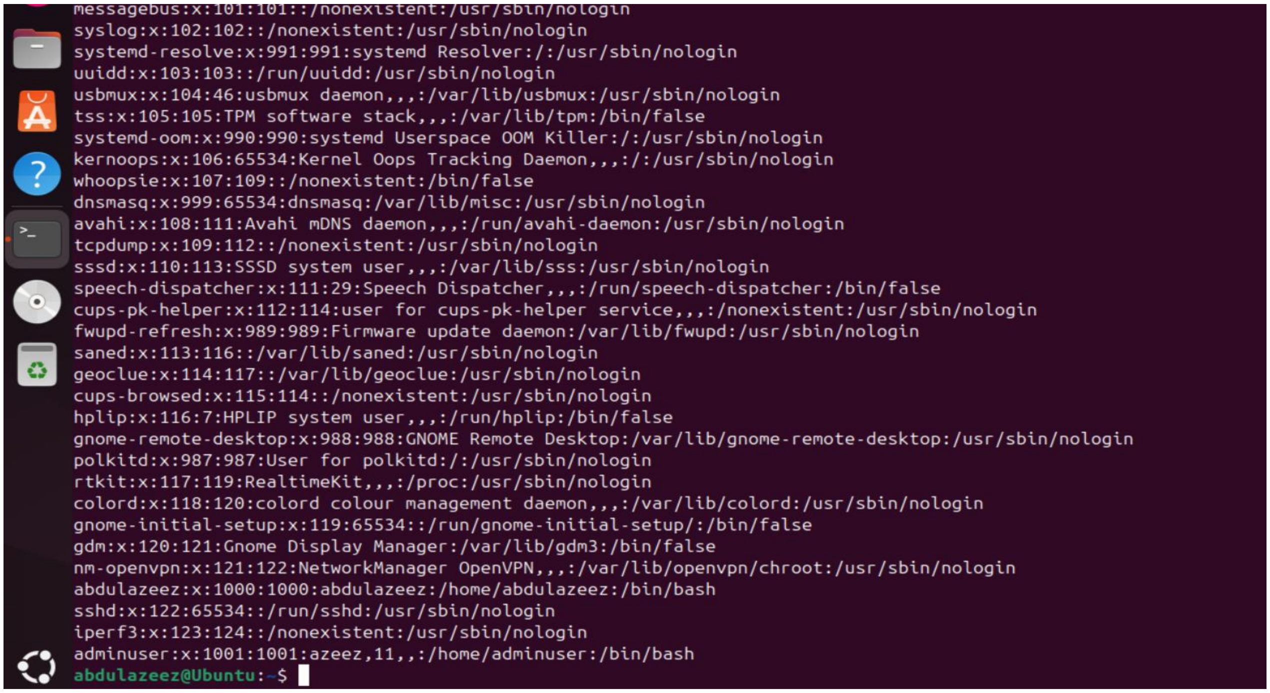
```
azeez@azeez-VirtualBox:~$ nmap 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-09 20:10 GMT
Nmap scan report for 192.168.56.101
Host is up (0.0067s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
azeez@azeez-VirtualBox:~$ 
```

3. Access Control Check

On Ubuntu, I checked the users and groups on the system using:

cat /etc/passwd

groups



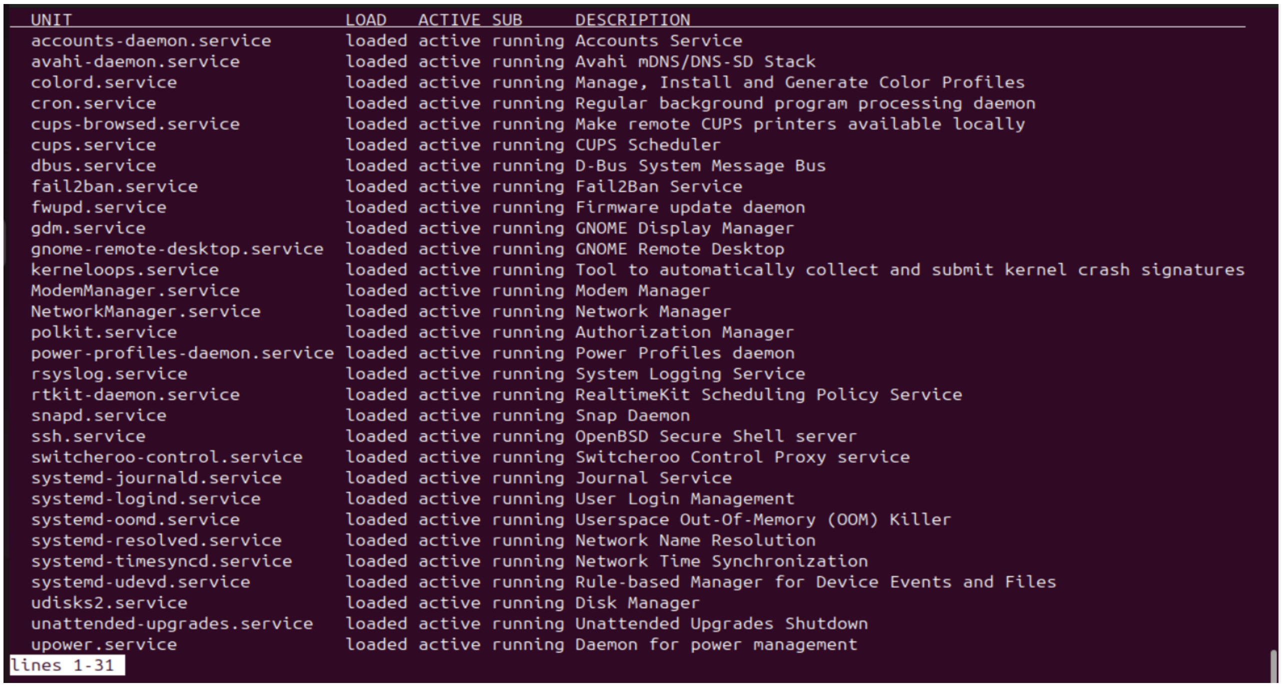
```
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tss:x:105:105:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
whoopsie:x:107:109::/nonexistent:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
tcpdump:x:109:112::/nonexistent:/usr/sbin/nologin
sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
abdulazeez:x:1000:1000:abdulazeez:/home/abdulazeez:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
iperf3:x:123:124::/nonexistent:/usr/sbin/nologin
adminuser:x:1001:1001:azeez,11,,:/home/adminuser:/bin/bash
abdulazeez@Ubuntu:~$ 
```

4. Service Audit (Running Services)

I listed all the running services using:

systemctl --type=service --state=running

This helped me justify which services are needed and which ones are optional.

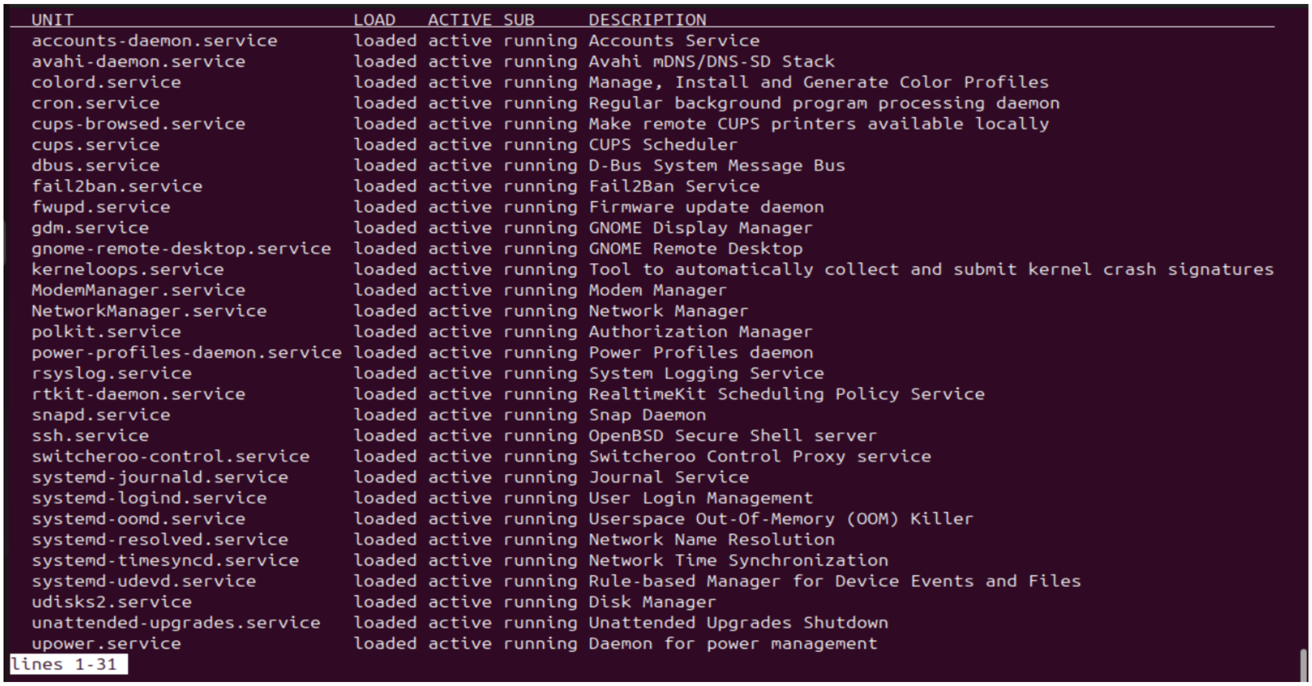


```
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service       loaded active running Accounts Service
  avahi-daemon.service          loaded active running Avahi mDNS/DNS-SD Stack
  colord.service                loaded active running Manage, Install and Generate Color Profiles
  cron.service                  loaded active running Regular background program processing daemon
  cups-browsed.service          loaded active running Make remote CUPS printers available locally
  cups.service                  loaded active running CUPS Scheduler
  dbus.service                  loaded active running D-Bus System Message Bus
  fail2ban.service              loaded active running Fail2Ban Service
  fwupd.service                 loaded active running Firmware update daemon
  gdm.service                   loaded active running GNOME Display Manager
  gnome-remote-desktop.service  loaded active running GNOME Remote Desktop
  kerneloops.service            loaded active running Tool to automatically collect and submit kernel crash signatures
  ModemManager.service          loaded active running Modem Manager
  NetworkManager.service        loaded active running Network Manager
  polkit.service                loaded active running Authorization Manager
  power-profiles-daemon.service loaded active running Power Profiles daemon
  rsyslog.service               loaded active running System Logging Service
  rtkit-daemon.service          loaded active running RealtimeKit Scheduling Policy Service
  snapd.service                 loaded active running Snap Daemon
  ssh.service                   loaded active running OpenBSD Secure Shell server
  switcheroo-control.service    loaded active running Switcheroo Control Proxy service
  systemd-journald.service      loaded active running Journal Service
  systemd-logind.service        loaded active running User Login Management
  systemd-oomd.service          loaded active running Userspace Out-Of-Memory (OOM) Killer
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-timesyncd.service     loaded active running Network Time Synchronization
  systemd-udevd.service         loaded active running Rule-based Manager for Device Events and Files
  udisks2.service               loaded active running Disk Manager
  unattended-upgrades.service   loaded active running Unattended Upgrades Shutdown
  upower.service                loaded active running Daemon for power management
lines 1-31
```

5. Security Fix 1 – Disable Root SSH Login

I edited the SSH configuration file to disable root login:

Changed: #PermitRootLogin prohibit-password → PermitRootLogin no



```
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service       loaded active running Accounts Service
  avahi-daemon.service          loaded active running Avahi mDNS/DNS-SD Stack
  colord.service                loaded active running Manage, Install and Generate Color Profiles
  cron.service                  loaded active running Regular background program processing daemon
  cups-browsed.service          loaded active running Make remote CUPS printers available locally
  cups.service                  loaded active running CUPS Scheduler
  dbus.service                  loaded active running D-Bus System Message Bus
  fail2ban.service              loaded active running Fail2Ban Service
  fwupd.service                 loaded active running Firmware update daemon
  gdm.service                   loaded active running GNOME Display Manager
  gnome-remote-desktop.service  loaded active running GNOME Remote Desktop
  kerneloops.service            loaded active running Tool to automatically collect and submit kernel crash signatures
  ModemManager.service          loaded active running Modem Manager
  NetworkManager.service        loaded active running Network Manager
  polkit.service                loaded active running Authorization Manager
  power-profiles-daemon.service loaded active running Power Profiles daemon
  rsyslog.service               loaded active running System Logging Service
  rtkit-daemon.service          loaded active running RealtimeKit Scheduling Policy Service
  snapd.service                 loaded active running Snap Daemon
  ssh.service                   loaded active running OpenBSD Secure Shell server
  switcheroo-control.service    loaded active running Switcheroo Control Proxy service
  systemd-journald.service      loaded active running Journal Service
  systemd-logind.service        loaded active running User Login Management
  systemd-oomd.service          loaded active running Userspace Out-Of-Memory (OOM) Killer
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-timesyncd.service     loaded active running Network Time Synchronization
  systemd-udevd.service         loaded active running Rule-based Manager for Device Events and Files
  udisks2.service               loaded active running Disk Manager
  unattended-upgrades.service   loaded active running Unattended Upgrades Shutdown
  upower.service                loaded active running Daemon for power management
lines 1-31
```

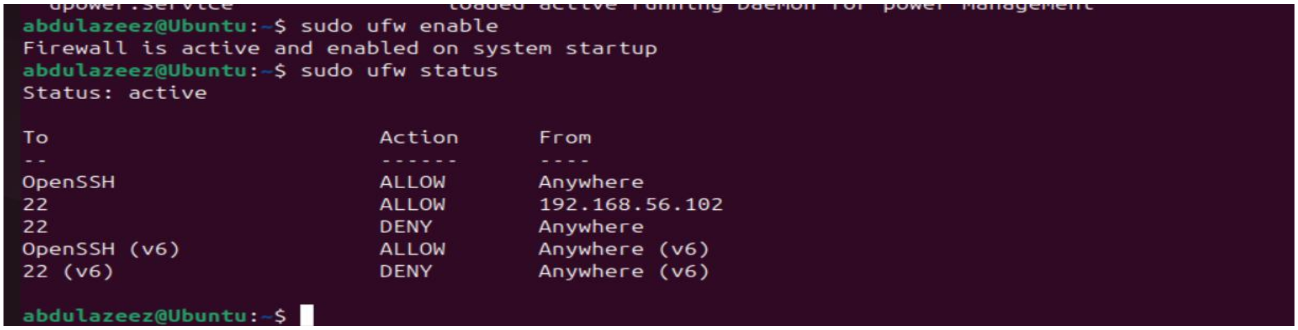
6. Security Fix 2 – Enable Firewall (UFW)

I enabled the firewall to block unwanted connections and only allow trusted traffic.

Commands used:

sudo ufw enable

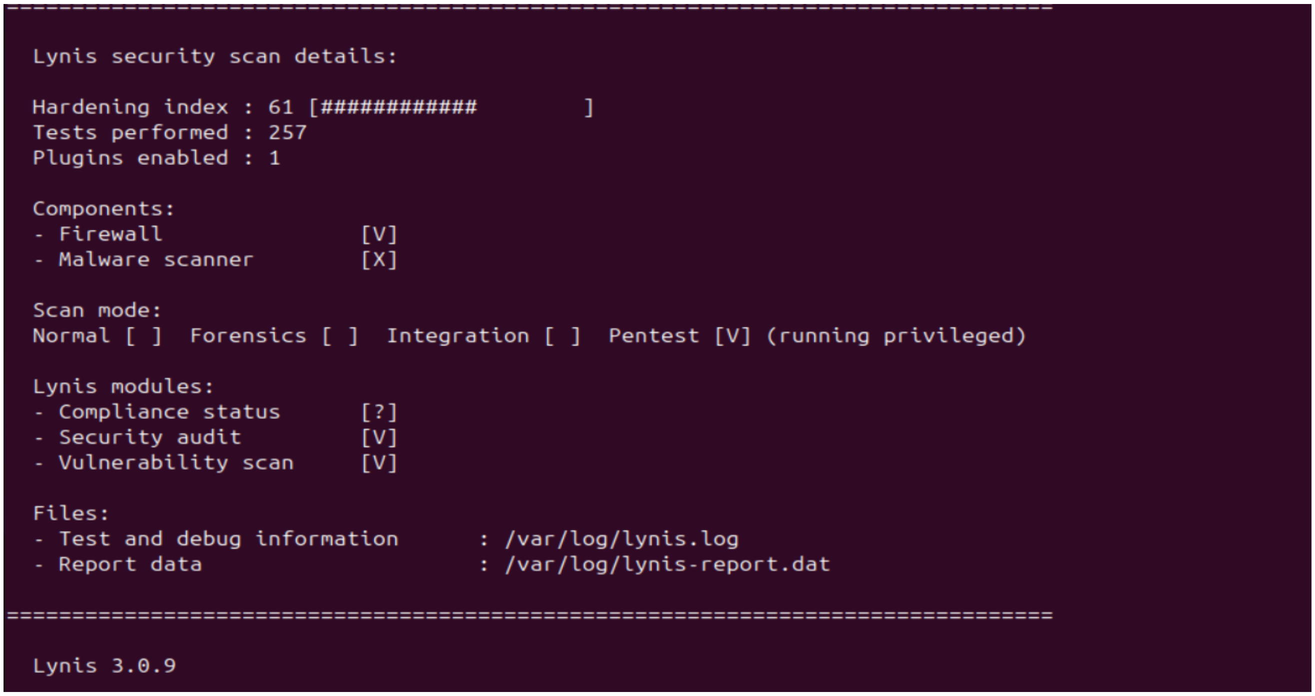
sudo ufw status



```
  upower.service                loaded active running Daemon for power management
abdulazeez@Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
abdulazeez@Ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
22                         ALLOW       192.168.56.102
22                         DENY        Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)

abdulazeez@Ubuntu:~$ 
```

7. Final Lynis Scan (After Fixes)

I ran Lynis again to check for improvements. Even though the hardening index stayed at 61, this is normal for virtual machines and the security still improved.



```
================================================================================

  Lynis security scan details:

  Hardening index : 61 [############        ]
  Tests performed : 257
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [ ]  Forensics [ ]  Integration [ ]  Pentest [V] (running privileged)

  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
```

8. Summary

Week 7 helped me understand system security by running Lynis, scanning with Nmap, reviewing users and services, and applying two important security fixes. Even if the Lynis score didn’t change, the system is now more secure.