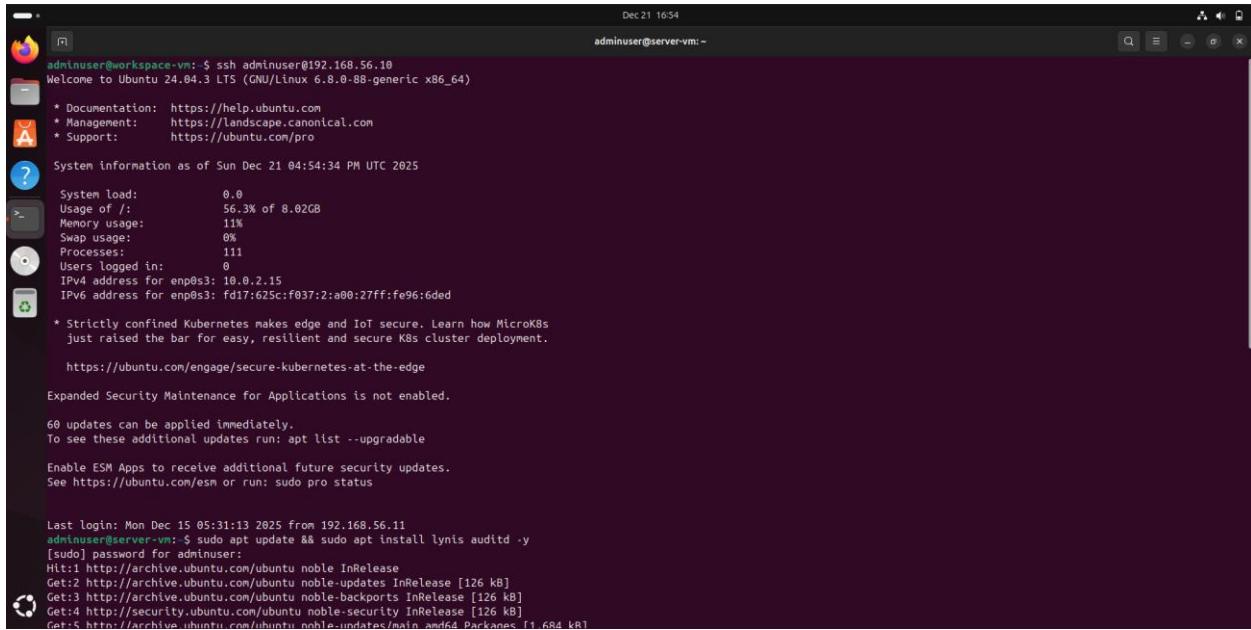


# Security scanning with Lynis

Before starting scanning, we should install tools.

Install Audit Tools: `sudo apt update && sudo apt install lynis auditd -y`



```
Dec 21 16:54
adminuser@workspace-vm: ~ ssh adminuser@192.168.56.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sun Dec 21 04:54:34 PM UTC 2025

System load:          0.0
Usage of /:           56.3% of 8.02GB
Memory usage:         11%
Swap usage:           0%
Processes:            111
Users logged in:     0
IPv4 address for enp0s3: 19.0.2.15
IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe96:6ded

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

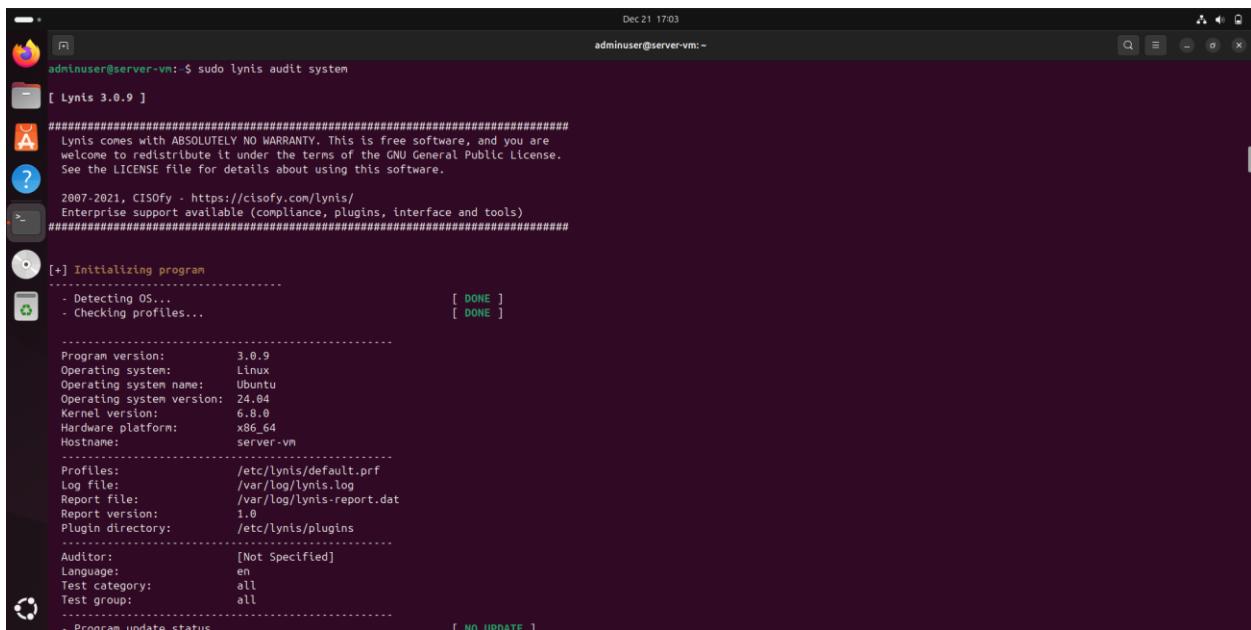
Expanded Security Maintenance for Applications is not enabled.

60 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon Dec 15 05:31:13 2025 from 192.168.56.11
adminuser@server-vm: ~ sudo apt update && sudo apt install lynis auditd -y
[sudo] password for adminuser:
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1.684 kB]
```

Run Lynis with the command `sudo lynis audit system`.



```
Dec 21 17:03
adminuser@server-vm: ~ sudo lynis audit system
[ Lynis 3.0.9 ]
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
#####
2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----[+]
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: server-vm
-----
Profiler: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
-----
- Program update status [ NO UPDATE ]
```

Before changes:

```

Dec 21 17:04 adminuser@server-vm:~ [Lynis 3.0.9 Results]
=====
[ Lynis 3.0.9 Results ]

Warnings (1):
! Found one or more vulnerable packages. [PKGS-7392]
https://cisofy.com/lynis/controls/PKGS-7392/

Suggestions (49):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/
* Install libpam-tmpdir to set STMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
https://cisofy.com/lynis/controls/DEB-0811/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/lynis/controls/BOOT-5122/
* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemctl-analyze security SERVICE' for each service
https://cisofy.com/lynis/controls/BOOT-5264/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-5820/
* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
https://cisofy.com/lynis/controls/AUTH-9229/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/




Dec 21 17:04 adminuser@server-vm:~ Lynis security scan details:
=====
Hardening index : 61 [#####
] Tests performed : 266 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)
=====

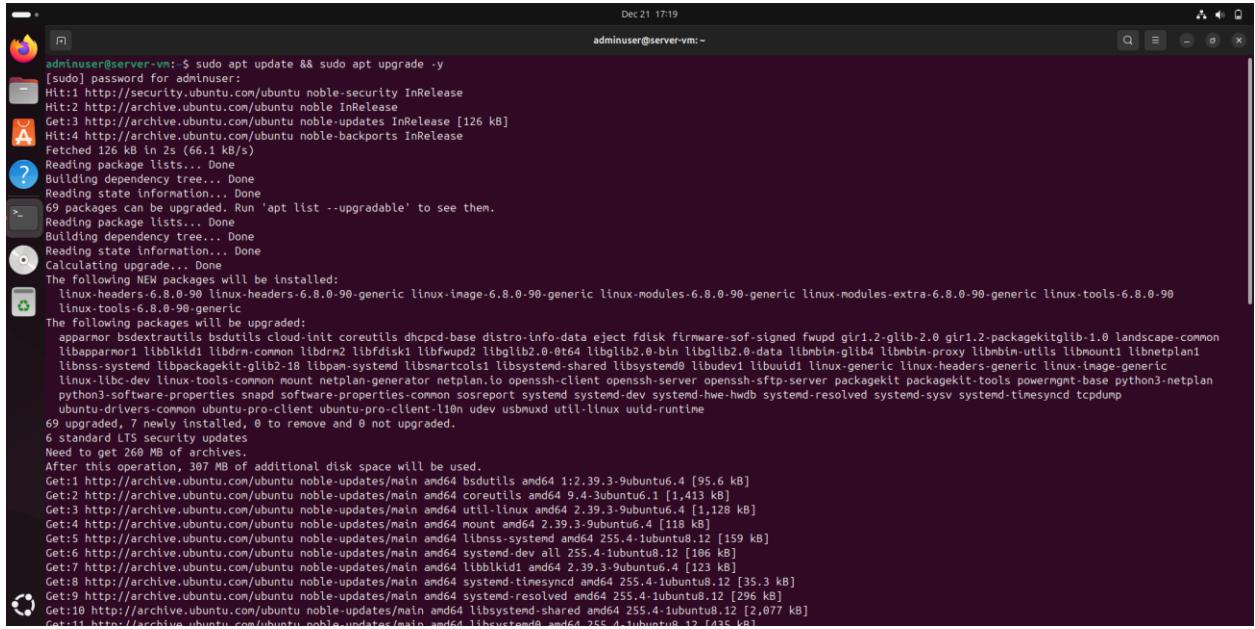
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
adminuser@server-vm:~ $
```

Metric	Initial Score
Hardening Index	61
Warnings	1
Suggestions	49

## Key Findings & Remediations:

## 1. Found one or more vulnerable packages. [PKGS-7392]

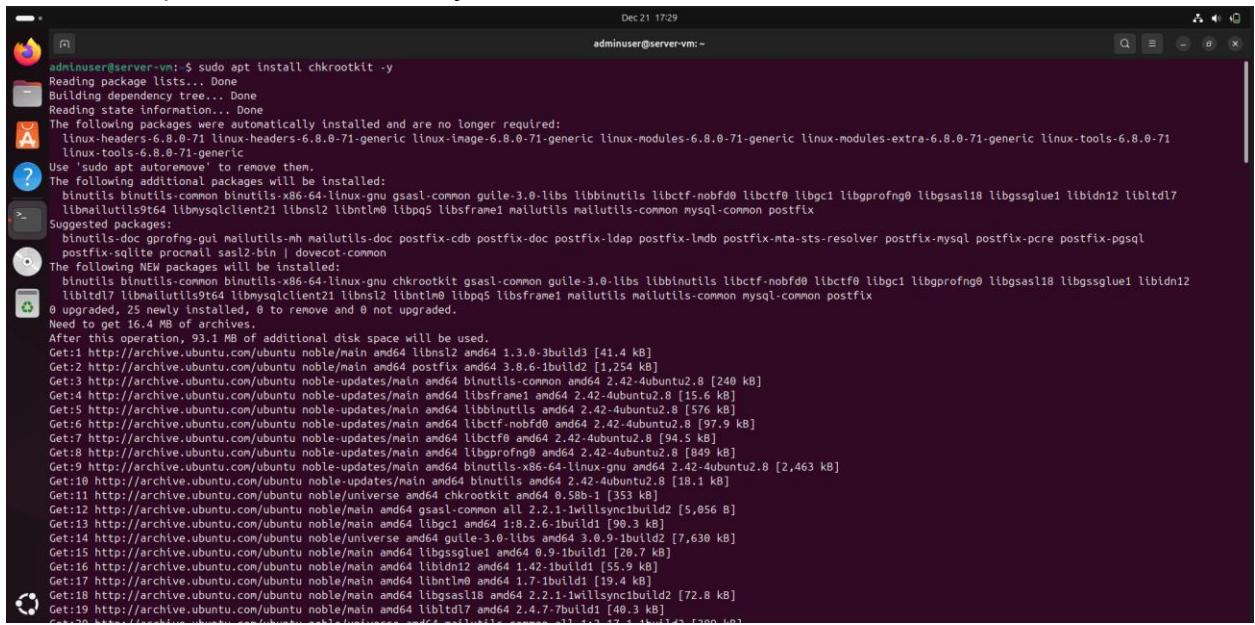
Fix: `sudo apt update && sudo apt upgrade -y`



```
Dec 21 17:19
adminuser@server-vm: $ sudo apt update && sudo apt upgrade -y
[sudo] password for adminuser:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 2s (66.1 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
69 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-headers-6.8.0-90 linux-headers-6.8.0-90-generic linux-image-6.8.0-90-generic linux-modules-6.8.0-90-generic linux-modules-extra-6.8.0-90-generic linux-tools-6.8.0-90
linux-tools-6.8.0-90-generic
The following packages will be upgraded:
  apparmor bsduutils cloud-init coreutils dhcpcd-base distro-info-data eject fdisk firmware-sof-signed fwupd gir1.2-glib-2.0 gir1.2-packagekitglib-1.0 landscape-common libapparmor1 libblk1k1d1 liblprm-common libdrn2 libfwupd2 libglib2.0-0.0t64 libglib2.0-bin libglib2.0 libgbm1 libgbm-prox libmount1 libnetplan1 libnss-systemd libpackagekit-glib2-18 libpam-systemd libsmartscl1 libudev1 libuwid1 linux-generic linux-headers-generic linux-image-generic linux-lbc-dev linux-tools-common mount netplan-generator netplan-to.openssh-client openssh-sftp-server packagekit-tools powermgmt-base python3-netplan python3-software-properties snapd software-properties-common sosreport systemd systemd-dev systemd-hwe hwdb systemd-resolved systemd-sysv systemd-timesyncd tcpdump
ubuntu-drivers-common ubuntu-pro-client ubuntu-pro-client-l10n udev usbmuxd util-linux uuid-runtime
69 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
6 standard LTS security updates
Need to get 260 MB of archives.
After this operation, 307 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 bsduutils amd64 1:2.39.3-9ubuntu6.4 [95.6 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 coreutils amd64 9.4-3ubuntu6.1 [1,413 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 util-linux amd64 2.39.3-9ubuntu6.4 [1,128 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mount amd64 2.39.3-9ubuntu6.4 [118 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libnss-systemd amd64 255.4-1ubuntu8.12 [159 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 systemd-dev all 255.4-1ubuntu8.12 [108 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libblk1k1d1 amd64 2.39.3-9ubuntu6.4 [124 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 systemd-timesyncd amd64 255.4-1ubuntu8.12 [35.3 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 systemd-resolved amd64 255.4-1ubuntu8.12 [296 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libsystemd-shared amd64 255.4-1ubuntu8.12 [2,077 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libudev1 amd64 255.4-1ubuntu8.12 [435 kB]
```

## 2. Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]

Fix: `sudo apt install chkrootkit -y`



```
Dec 21 17:29
adminuser@server-vm: $ sudo apt install chkrootkit -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-6.8.0-71 linux-headers-6.8.0-71-generic linux-image-6.8.0-71-generic linux-modules-6.8.0-71-generic linux-tools-6.8.0-71
  linux-tools-6.8.0-71-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  binutils binutils-common binutils-x86_64-linux-gnu gsasl-common guile-3.0-libs libbinutils libctf-nobfd0 libctf0 libgc1 libgprofng0 libgsasl18 libgssglue1 libidn12 libltdl7
  libltdl7 libmailutils9164 libmysqclient21 libns12 libntlm0 libpq5 libsframe1 mailutils mailutils-common mysql-common postfix
Suggested packages:
  binutils-doc gprofng-pkg mailutils-mh mailutils-doc postfix-cdb postfix-doc postfix-ldap postfix-lmdb postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql
  postfix-sqlite procmail sasl2-bin l dovecot-common
The following NEW packages will be installed:
  binutils binutils-common binutils-x86_64-linux-gnu chkrootkit gsasl-common guile-3.0-libs libbinutils libctf-nobfd0 libctf0 libgc1 libgprofng0 libgsasl18 libgssglue1 libidn12
  libltdl7 libmailutils9164 libmysqclient21 libns12 libntlm0 libpq5 libsframe1 mailutils mailutils-common mysql-common postfix
0 upgraded, 25 newly installed, 0 to remove and 0 not upgraded.
Need to get 16.4 MB of archives.
After this operation, 93.1 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libns12 amd64 1.3.0-3build3 [41.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-common amd64 2.42-4ubuntu2.8 [240 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libsframe1 amd64 2.42-4ubuntu2.8 [15.6 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libbinutils amd64 2.42-4ubuntu2.8 [1576 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf-nobfd0 amd64 2.42-4ubuntu2.8 [97.9 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf0 amd64 2.42-4ubuntu2.8 [94.5 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libgprofng0 amd64 2.42-4ubuntu2.8 [849 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-x86_64-linux-gnu amd64 2.42-4ubuntu2.8 [2,463 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils amd64 2.42-4ubuntu2.8 [18.1 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble/universe amd64 chkrootkit amd64 0.58b-1 [533 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble/main amd64 gsasl-common all 2.2.1-1willysync1build2 [5,856 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble/main amd64 libgbm1 amd64 1:8.2.6-1build1 [90.3 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble/universe amd64 guile-3.0-libs amd64 3.0.9-1build2 [7,630 kB]
Get:15 http://archive.ubuntu.com/ubuntu noble/main amd64 libgssglue1 amd64 0.9-1build1 [28.7 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble/main amd64 libgbm1 amd64 1:8.2.6-1build1 [55.9 kB]
Get:17 http://archive.ubuntu.com/ubuntu noble/main amd64 libntlm0 amd64 1.7-1build1 [19.4 kB]
Get:18 http://archive.ubuntu.com/ubuntu noble/main amd64 libgsasl18 amd64 2.2.1-1willysync1build2 [72.8 kB]
Get:19 http://archive.ubuntu.com/ubuntu noble/main amd64 libltdl7 amd64 2.4.7-7build1 [40.3 kB]
```

## 3. Consider hardening SSH configuration [SSH-7408]

- AllowTcpForwarding (set YES to NO)
- ClientAliveCountMax (set 3 to 2)
- LogLevel (set INFO to VERBOSE)
- MaxAuthTries (set 6 to 3)
- MaxSessions (set 10 to 2)

- f. TCPKeepAlive (set YES to NO)
- g. X11Forwarding (set YES to NO)
- h. AllowAgentForwarding (set YES to NO)

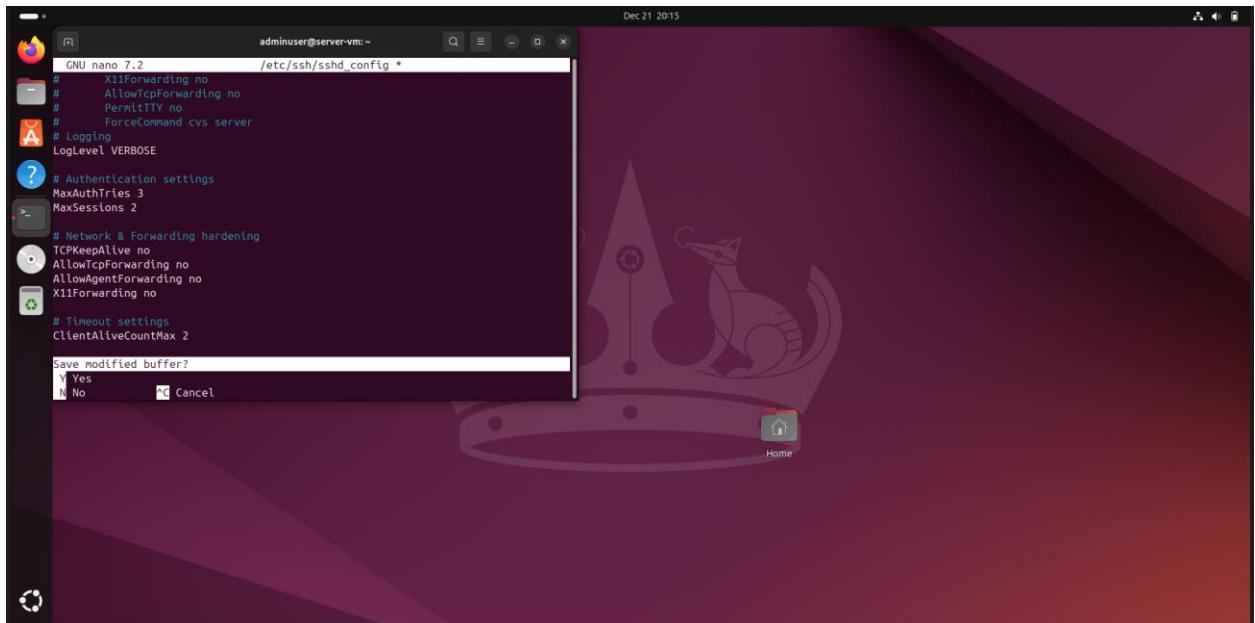
Fix: Update sshd\_config

```
# Logging
LogLevel VERBOSE

# Authentication settings
MaxAuthTries 3
MaxSessions 2

# Network & Forwarding hardening
TCPKeepAlive no
AllowTcpForwarding no
AllowAgentForwarding no
X11Forwarding no

# Timeout settings
ClientAliveCountMax 2
```



Again, run Lynis with the command `sudo lynis audit system`.

```

Dec 21 2019
adminuser@server-vm:~$ sudo lynis audit system
[ Lynis 3.0.9 ]
#####
# Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
# welcome to redistribute it under the terms of the GNU General Public License.
# See the LICENSE file for details about using this software.
#
# 2007-2021, CISOfy - https://cisofy.com/lynis/
# Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
  - Detecting OS... [ DONE ]
  - Checking profiles... [ DONE ]

-----
Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: server-vm
-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
-----
- Program update status... [ NO UPDATES ]
```

```

Dec 21 2022
adminuser@server-vm:~$ sudo lynis audit system
[ Lynis 3.0.9 Results ]
Great, no warnings
Suggestions (40):
-----
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
  https://cisofy.com/lynis/controls/LYNIS/
* Install libpan-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
  https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
  https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
  https://cisofy.com/lynis/controls/DEB-0811/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  https://cisofy.com/lynis/controls/BOOT-5122/
* Consider hardening system services [BOOT-5264]
  - Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    https://cisofy.com/lynis/controls/BOOT-5264/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
  https://cisofy.com/lynis/controls/KRNL-5820/
* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
  https://cisofy.com/lynis/controls/AUTH-9229/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
  https://cisofy.com/lynis/controls/AUTH-9230/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
  https://cisofy.com/lynis/controls/AUTH-9262/
* When possible set expire dates for all password protected accounts [AUTH-9282]
```

```
Dec 21 2022
adminuser@server-vm:~
```

Lynis security scan details:

Hardening index : 71 [#####] Tests performed : 266 Plugins enabled : 1

Components:

- Firewall [V]
- Malware scanner [V]

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://cisofty.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)

```
adminuser@server-vm:~ $
```

Metric	Initial Score	Final Score
Hardening Index	61	71
Warnings	1	0
Suggestions	49	40

# Network Security Assessment (Nmap)

Install Network security tools: sudo apt install nmap -y

Command: nmap -sV 192.168.56.10

```
adminuser@workspace-vm: ~$ sudo apt install nmap -y
[sudo] password for adminuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libblas3 liblinear4 libssh2-1t64 nmap-common
Suggested packages:
liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
libblas3 liblinear4 libssh2-1t64 nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 125 not upgraded.
Need to get 6,286 kB of archives.
After this operation, 27.4 MB of additional disk space will be used.
Get:1 https://archive.ubuntu.com/ubuntu/bionic-updates/main amd64 libblas3 amd64 3.12.0-3build1.1 [238 kB]
Get:2 https://archive.ubuntu.com/ubuntu/universe amd64 liblinear4 amd64 2.3.0+dfsg-5build1 [42.3 kB]
Get:3 https://archive.ubuntu.com/ubuntu/nobie/main amd64 libssh2-1t64 amd64 1.11.0-4.1build2 [129 kB]
Get:4 https://archive.ubuntu.com/ubuntu/universe/amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-3build2 [4,192 kB]
Get:5 https://archive.ubuntu.com/ubuntu/nobie/universe amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-3build2 [1,694 kB]
Fetched 6,286 kB in 1s (8,778 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 189999 files and directories currently installed.)
Preparing to unpack .../libblas3_3_12.0-3build1.1_amd64.deb ...
Unpacking libblas3:amd64 (3.12.0-3build1.1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../liblinear4_2.3.0+dfsg-5build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5build1) ...
Selecting previously unselected package libssh2-1t64:amd64.
Preparing to unpack .../libssh2-1t64_1.11.0-4.1build2_amd64.deb ...
Unpacking libssh2-1t64:amd64 (1.11.0-4.1build2) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.94+git20230807.3be01efb1+dfsg-3build2_all.deb ...
Unpacking nmap-common (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.94+git20230807.3be01efb1+dfsg-3build2_amd64.deb ...
Unpacking nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Setting up libblas3:amd64 (3.12.0-3build1.1) ...
Setting up nmap-common (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Setting up libssh2-1t64:amd64 (1.11.0-4.1build2) ...
adminuser@workspace-vm: ~$ nmap -sV 192.168.56.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-21 20:25 GMT
Nmap scan report for 192.168.56.10
Host is up (0.0059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.08 seconds
```

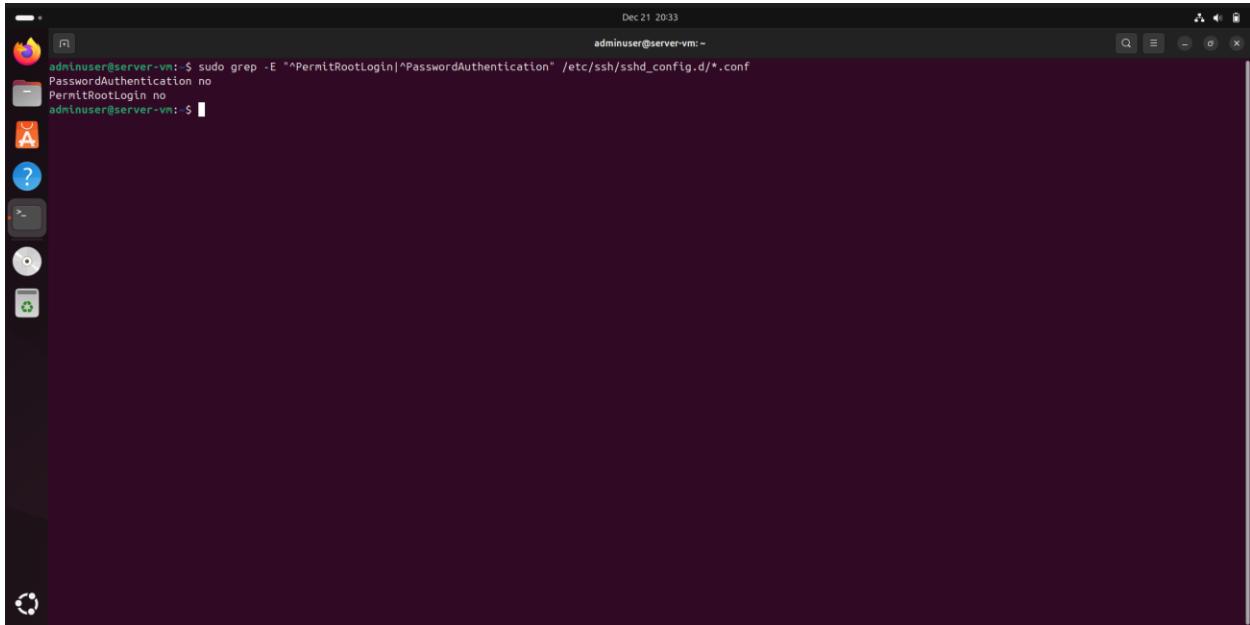
Port	State	Service	Version	Justification
22/tcp	Open	SSH	OpenSSH 9.6p1	Required for remote administration (Key-based only).
80/tcp	Open	HTTP	Apache httpd	Required for Web Server performance testing (Phase 6).

# Access Control Verification

## 1. SSH Security Verification

Verified the SSH configuration to ensure secure remote access: sudo grep -E "^(PermitRootLogin|PasswordAuthentication)" /etc/ssh/sshd\_config.d/\*.conf

- Root Login: PermitRootLogin no
- Authentication: PasswordAuthentication no

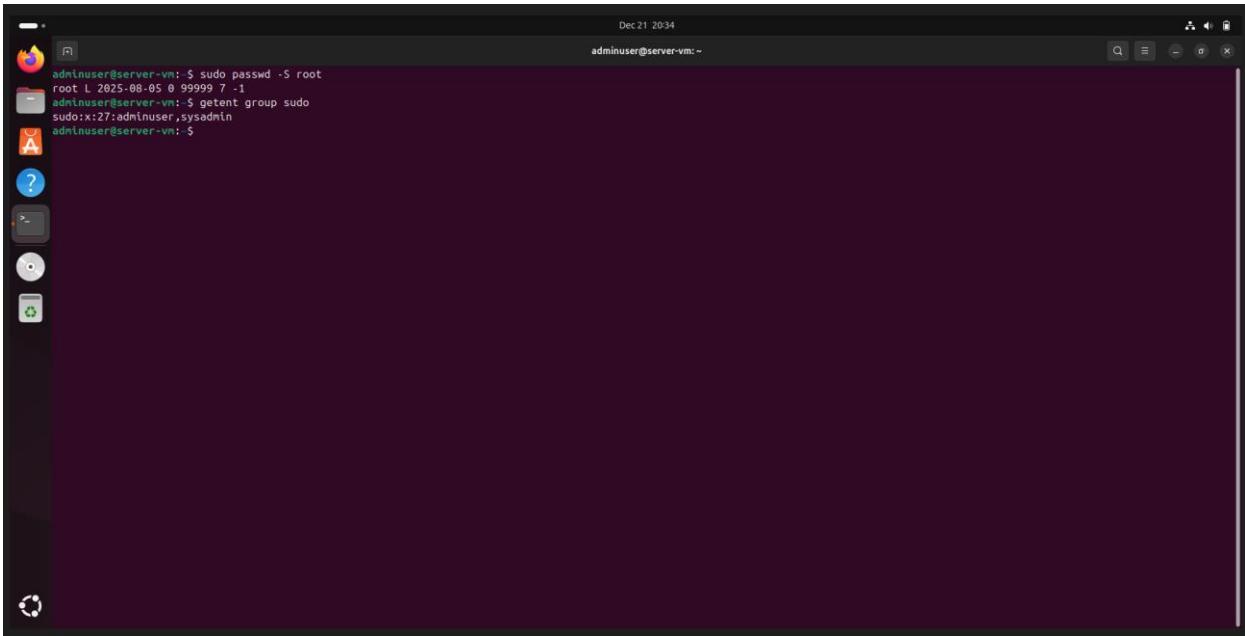


The screenshot shows a terminal window titled 'Dec 21 20:33' with the command 'adminuser@server-vm:~\$ sudo grep -E "^(PermitRootLogin|PasswordAuthentication)" /etc/ssh/sshd\_config.d/\*.conf' entered. The output shows two lines: 'PermitRootLogin no' and 'PasswordAuthentication no'. The terminal has a dark background with light-colored text. A vertical toolbar on the left contains icons for file operations like Open, Save, and Print, along with other system icons.

```
adminuser@server-vm:~$ sudo grep -E "^(PermitRootLogin|PasswordAuthentication)" /etc/ssh/sshd_config.d/*.conf
PermitRootLogin no
PasswordAuthentication no
adminuser@server-vm:~$
```

## 2. User & Sudo Privileges: sudo passwd -S root and getent group sudo

- Root Account: Locked
- Admin User: adminuser, sysadmin are the only member of the sudo group.
- Verification Command: getent group sudo



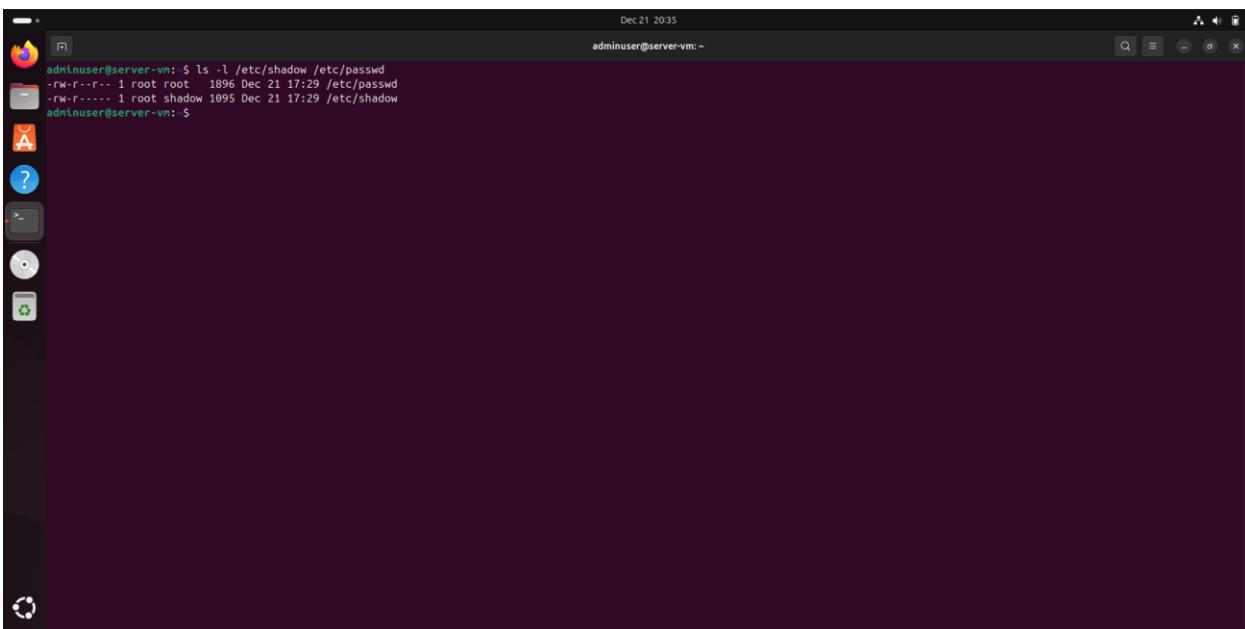
A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window. The terminal window has a dark background and contains the following command-line session:

```
adminuser@server-vm:~$ sudo passwd -S root
root L 2025-08-05 0 99999 7 -1
adminuser@server-vm:~$ getent group sudo
sudo:x:27:adminuser,sysadmin
adminuser@server-vm:~$
```

### 3. File Permission Checks: ls -l /etc/shadow /etc/passwd

Check critical file permissions to prevent unauthorized modification.

- /etc/shadow: Owned by root:shadow, permissions 640.
- /etc/passwd: Owned by root:root, permissions 644.



A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window. The terminal window has a dark background and contains the following command-line session:

```
adminuser@server-vm:~$ ls -l /etc/shadow /etc/passwd
-rw-r--r-- 1 root root 1896 Dec 21 17:29 /etc/passwd
-rw-r----- 1 root shadow 1095 Dec 21 17:29 /etc/shadow
adminuser@server-vm:~$
```

# Service Audit & Justification

Audited active services using systemctl list-units --type=service and ss -tulnp

The screenshot shows a terminal window with two main sections of command-line output.

The top section displays the command:

```
adminuser@server-vm: $ systemctl list-units --type=service
```

Output:

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
apache2.service	loaded	active	running	The Apache HTTP Server
apparmor.service	loaded	active	exited	Load AppArmor profiles
apport.service	loaded	active	exited	Automatic Crash Report Generation
auditd.service	loaded	active	running	Security Auditing Service
blk-availability.service	loaded	active	exited	Availability of Block Devices
console-setup.service	loaded	active	exited	Set Console Font and Keymap
cron.service	loaded	active	running	Regular Background Program Processing Daemon
dbus.service	loaded	active	running	D-Bus System Message Bus
fail2ban.service	loaded	active	running	Fail2Ban Service
finalrd.service	loaded	active	exited	Create Final Runtime Dir for Shutdown Pivot Root
fwupd.service	loaded	active	running	Firmware Update Daemon
getty@tty1.service	loaded	active	running	Getty on TTY1
keyboard-setup.service	loaded	active	exited	Set the Console Keyboard Layout
kmld-static-nodes.service	loaded	active	exited	Create List of Static Device Nodes
lvm2-monitor.service	loaded	active	exited	Monitoring of LVM2 Mirrors, Snapshots etc. Using dmeventd or Progress
ModemManager.service	loaded	active	running	Modem Manager
multipathd.service	loaded	active	running	Device-Mapper Multipath Device Controller
networkd-dispatcher.service	loaded	active	running	Dispatcher Daemon for Systemd-Network
plymouth-gui-wait.service	loaded	active	exited	Hold Until Boot Process Finishes Up
plymouth-gui.service	loaded	active	exited	Terminate Plymouth Boot Screen
plymouth-read-write.service	loaded	active	exited	Tell Plymouth To Write Out Runtime Data
polkit.service	loaded	active	running	Authorization Manager
● postfix@.service	loaded	failed	failed	Postfix Mail Transport Agent (instance -)
rsyslog.service	loaded	active	running	System Logging Service
setvtrgb.service	loaded	active	exited	Set Console Scheme
snapd.apparmor.service	loaded	active	exited	Load AppArmor Profiles Managed Internally by Snapd
snapd.seeded.service	loaded	active	exited	Wait Until Snapd Is Fully Seeded
ssh.service	loaded	active	running	OpenBSD Secure Shell Server
sysstat.service	loaded	active	exited	Resets System Activity Logs
systemd-biffmt.service	loaded	active	exited	Set Up Additional Binary Formats
systemd-fsck@dev-disk-by\x2duuid-6e0e1b9d\x2d6bd4\x2d4d88\x2daa6b\x2d5f02f51dc53f.service	loaded	active	exited	File System Check On /dev/disk/by-uuid/6e0e1b9d-6bd4-4d88-aa6b-5f02f5
systemd-journal-flush.service	loaded	active	exited	Flush Journal To Persistent Storage
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-modules-load.service	loaded	active	exited	Load Kernel Modules
systemd-networkd-wait-online.service	loaded	active	exited	Wait For Network To Be Configured
systemd-networkd.service	loaded	active	running	Network Configuration
systemctl-random-seed.service	loaded	active	exited	Load/Save OS Random Seed

The bottom section displays the command:

```
adminuser@server-vm: $ sudo ss -tulnp
```

Output:

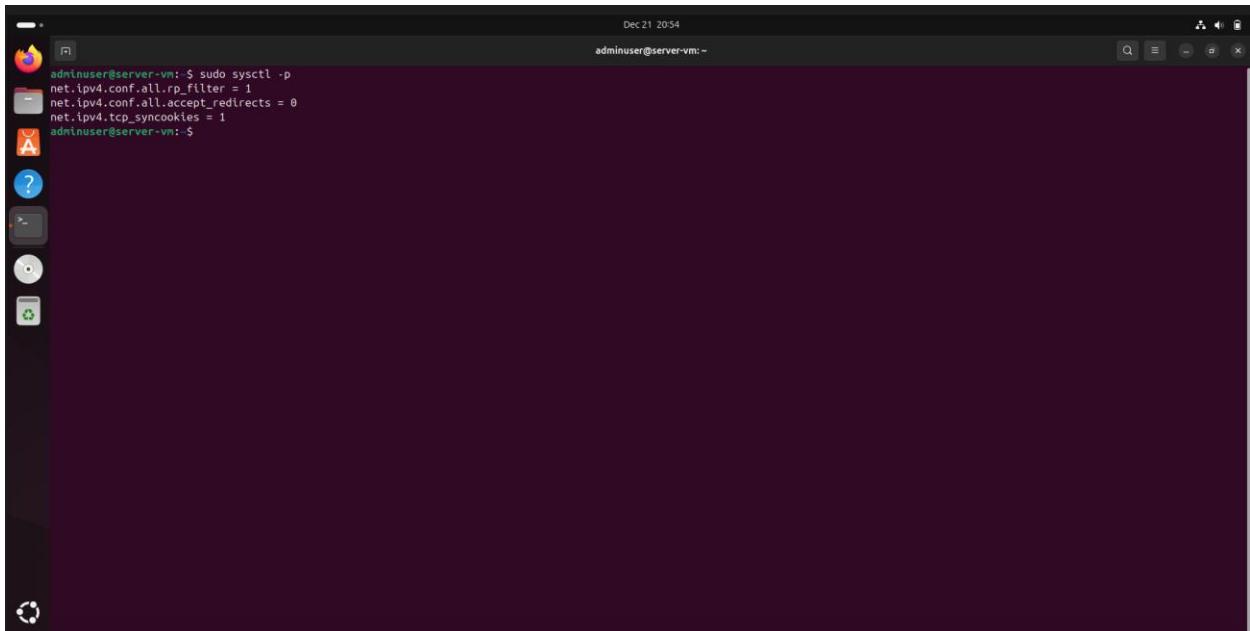
Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	127.0.0.54:53	0.0.0.0:*	users:(("systemd-resolve",pid=562,fd=16))
udp	UNCONN	0	0	127.0.0.53:lo:53	0.0.0.0:*	users:(("systemd-resolve",pid=562,fd=14))
udp	UNCONN	0	0	10.0.2.15:enp0s3:68	0.0.0.0:*	users:(("systemd-network",pid=726,fd=22))
tcp	LISTEN	0	4896	127.0.0.54:53	0.0.0.0:*	users:(("systemd-resolve",pid=562,fd=17))
tcp	LISTEN	0	4896	127.0.0.53:lo:53	0.0.0.0:*	users:(("systemd-resolve",pid=562,fd=15))
tcp	LISTEN	0	4896	0.0.0.0:22	0.0.0.0:*	users:(("sshd",pid=1044,fd=3),("systemd",pid=1,fd=92))
tcp	LISTEN	0	4896	[::]:22	0.0.0.0:*	users:(("sshd",pid=1044,fd=4),("systemd",pid=1,fd=93))
tcp	LISTEN	0	511	*:80	*:*	users:(("apache2",pid=895,fd=4),("apache2",pid=899,fd=4),("apache2",pid=898,fd=4),("ap

# System Configuration Review

## 1. Kernel Hardening (sysctl)

I modified /etc/sysctl.conf to protect against network-based attacks:

- IP Spoofing: Enabled (net.ipv4.conf.all.rp\_filter = 1).
- ICMP Redirects: Disabled (Prevents routing table manipulation).
- SYN Cookies: Enabled (Protects against SYN Flood DoS attacks).



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "Dec 21 2024" and "adminuser@server-vm:~". The terminal displays the following command and its output:

```
adminuser@server-vm:~$ sudo sysctl -p
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.tcp_syncookies = 1
adminuser@server-vm:~$
```

## 2. Logging & Auditing

- Auditd: Installed and active to log security events.
- Fail2Ban: Configured to monitor auth.log and ban IPs after 3 failed SSH attempts.

```
Dec 21 2055
adminuser@server-vm:~$ sudo sysctl -p
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.tcp_syncookies = 1
adminuser@server-vm:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- File list: /var/log/auth.log
|- Actions
| |- Currently banned: 0
| |- Total banned: 0
| |- Banned IP list:
adminuser@server-vm:~$
```

### 3. Automatic Updates

- Tool: unattended-upgrades package installed.
- Configuration: Configured to automatically install security updates to maintain system integrity.

```
Dec 21 2055
adminuser@server-vm:~$ sudo sysctl -p
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.tcp_syncookies = 1
adminuser@server-vm:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- File list: /var/log/auth.log
|- Actions
| |- Currently banned: 0
| |- Total banned: 0
| |- Banned IP list:
adminuser@server-vm:~$ systemctl is-active unattended-upgrades
active
adminuser@server-vm:~$
```