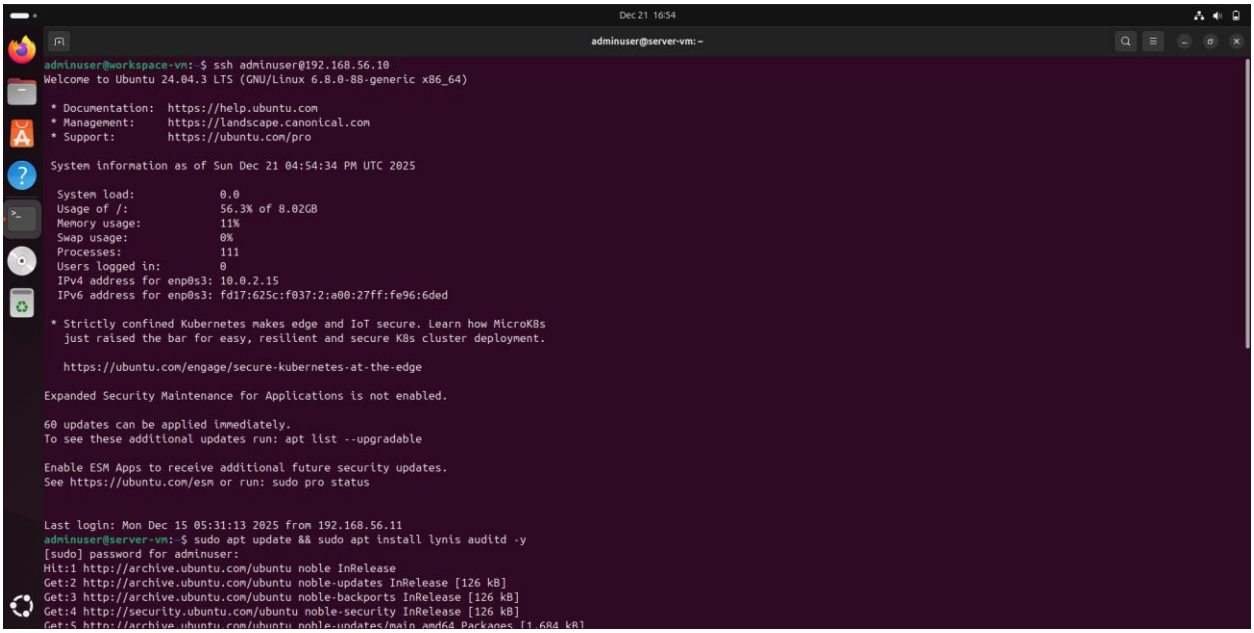
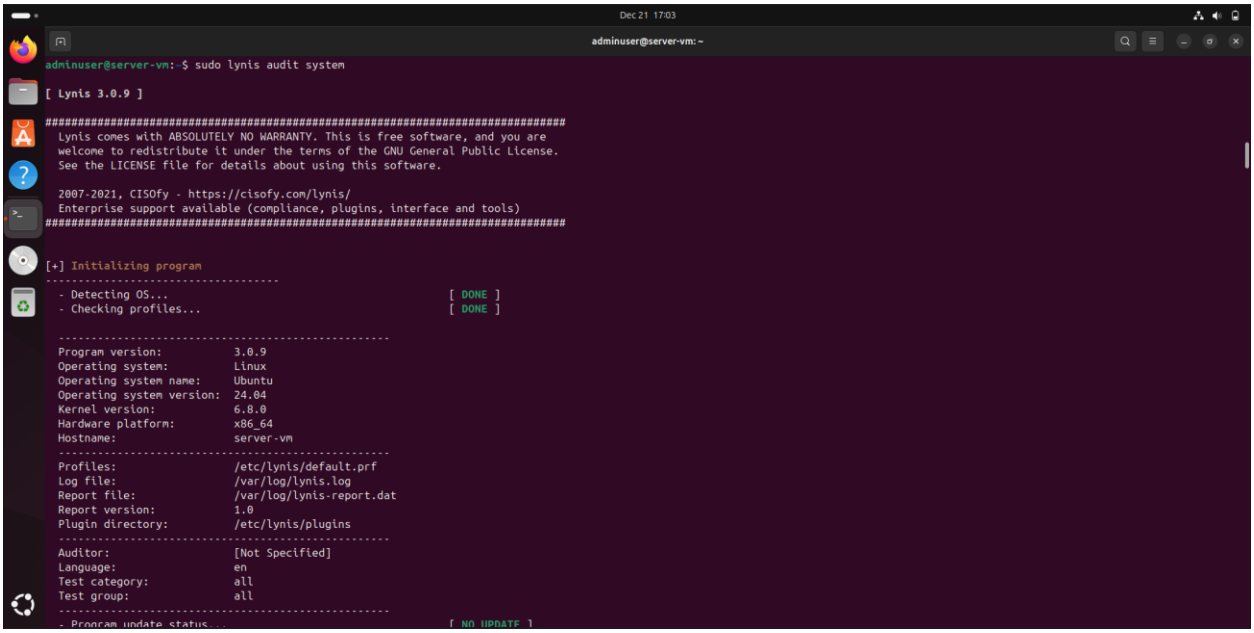
Security scanning with Lynis

Before starting scanning, we should install tools.

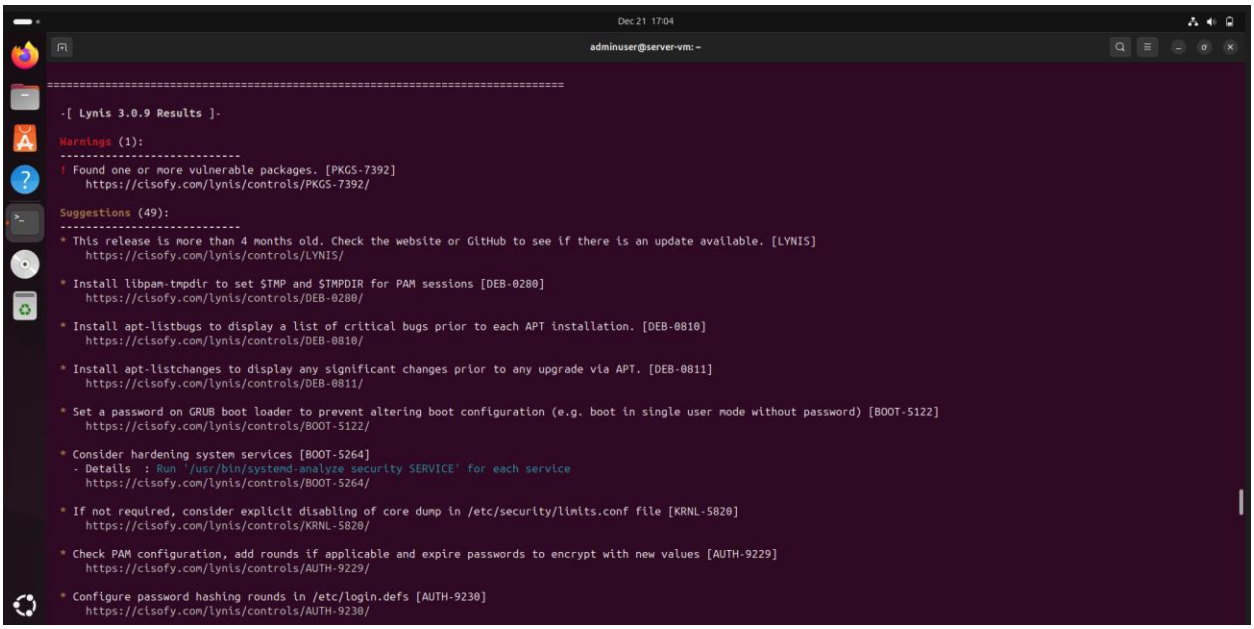
Install Audit Tools: *sudo apt update && sudo apt install lynis auditd –y*

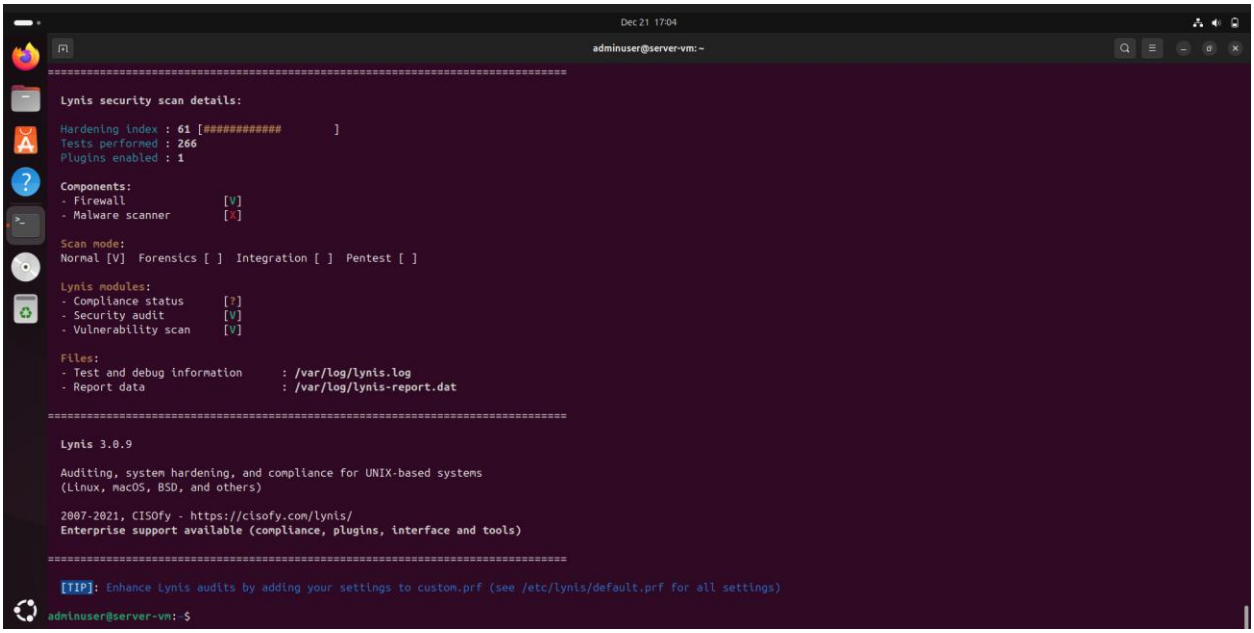


Run Lynis with the command *sudo lynis audit system*.



Before changes:

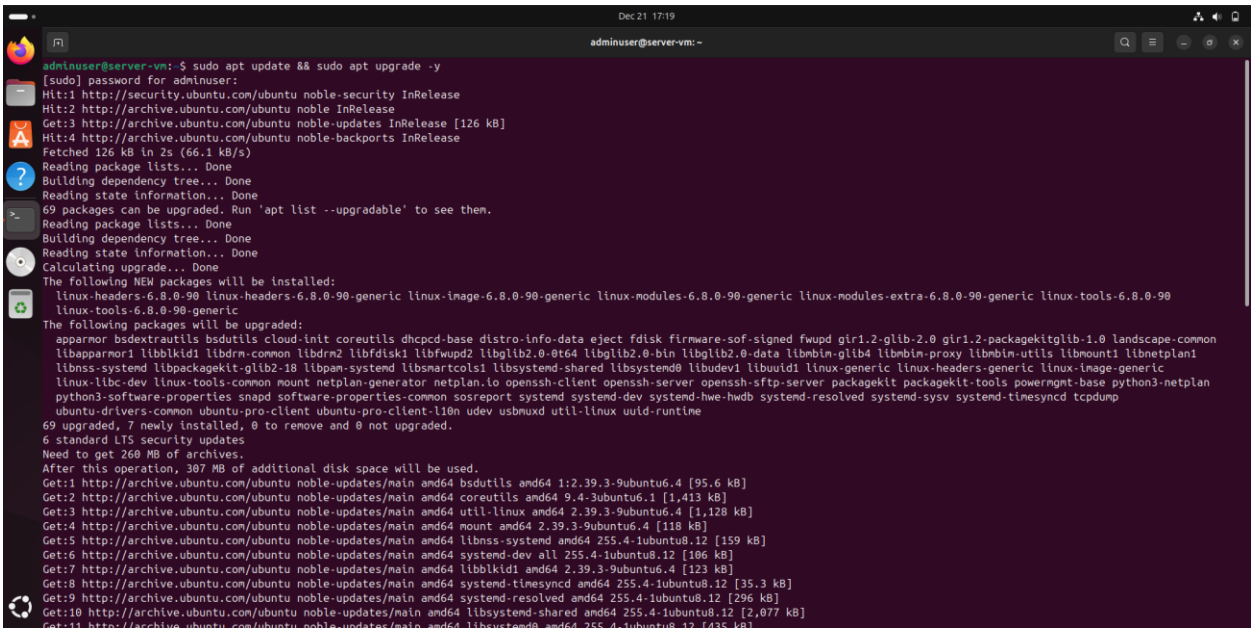




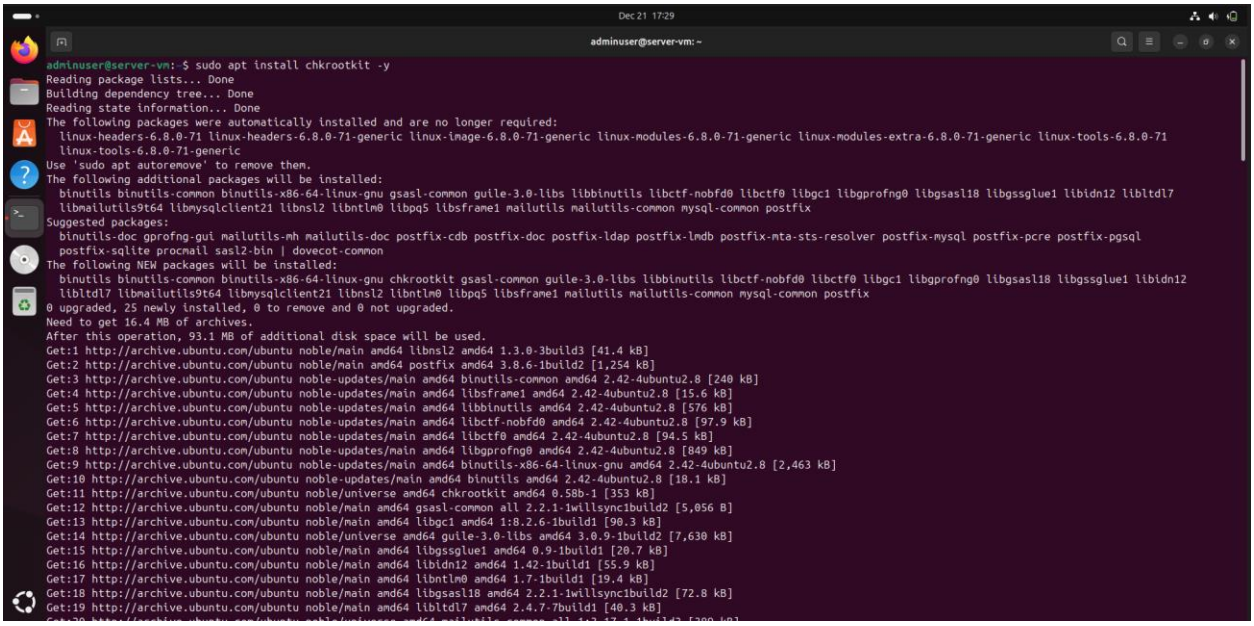
Metric	Initial Score
Hardening Index	61
Warnings	1
Suggestions	49

Key Findings & Remediations:

1. Found one or more vulnerable packages. [PKGS-7392]
   Fix: *sudo apt update && sudo apt upgrade –y*



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

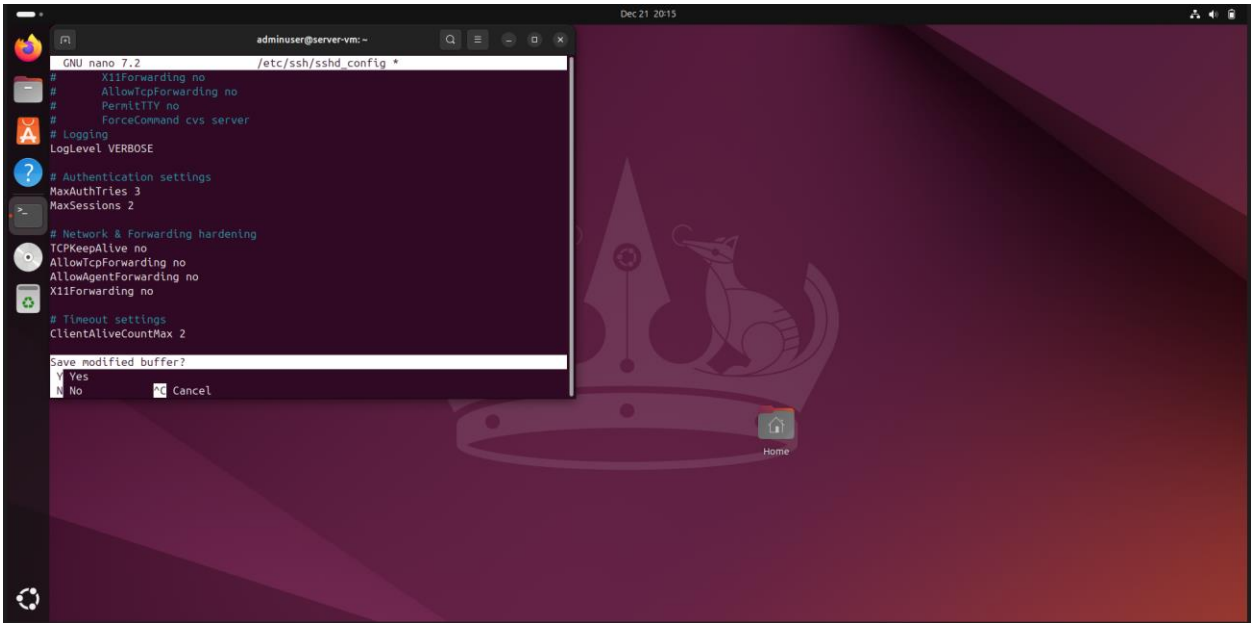


3. Consider hardening SSH configuration [SSH-7408]
   a. AllowTcpForwarding (set YES to NO)
   b. ClientAliveCountMax (set 3 to 2)
   c. LogLevel (set INFO to VERBOSE)
   d. MaxAuthTries (set 6 to 3)
   e. MaxSessions (set 10 to 2)

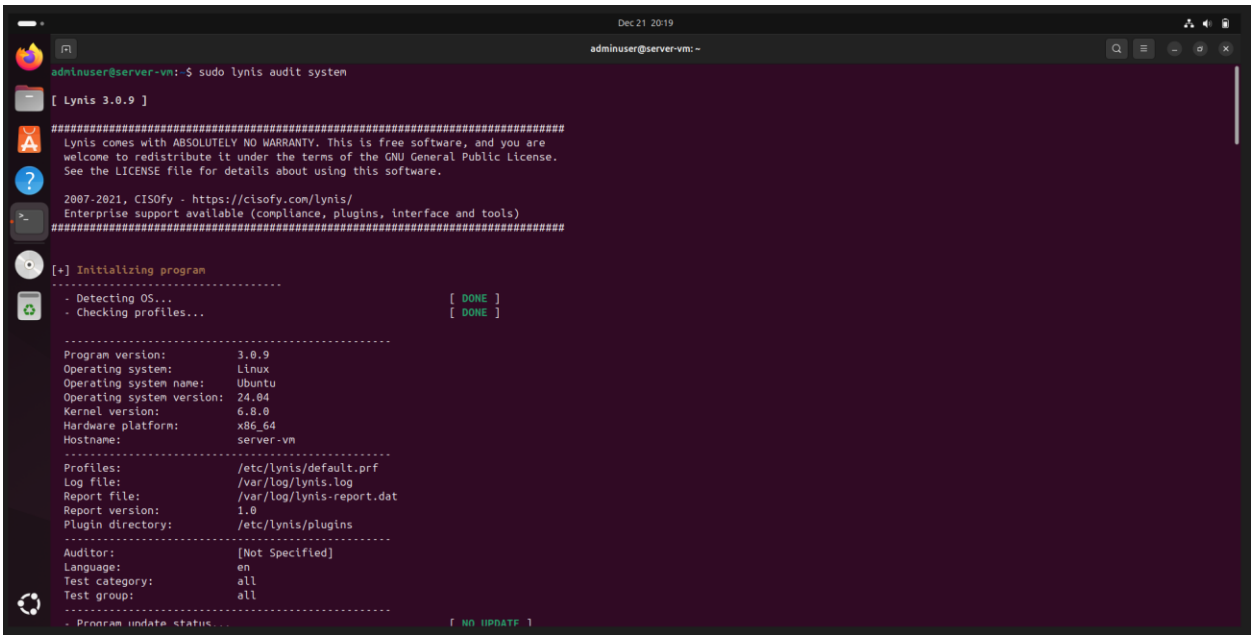
f. TCPKeepAlive (set YES to NO)
g. X11Forwarding (set YES to NO)
h. AllowAgentForwarding (set YES to NO)

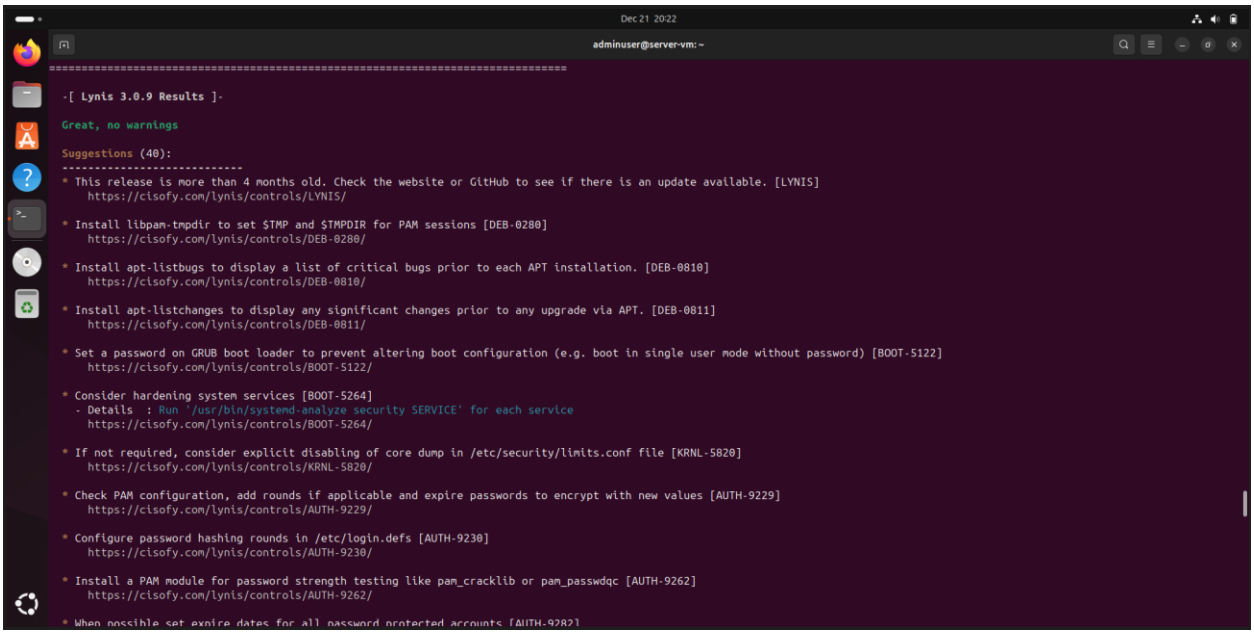
Fix: Update sshd_config

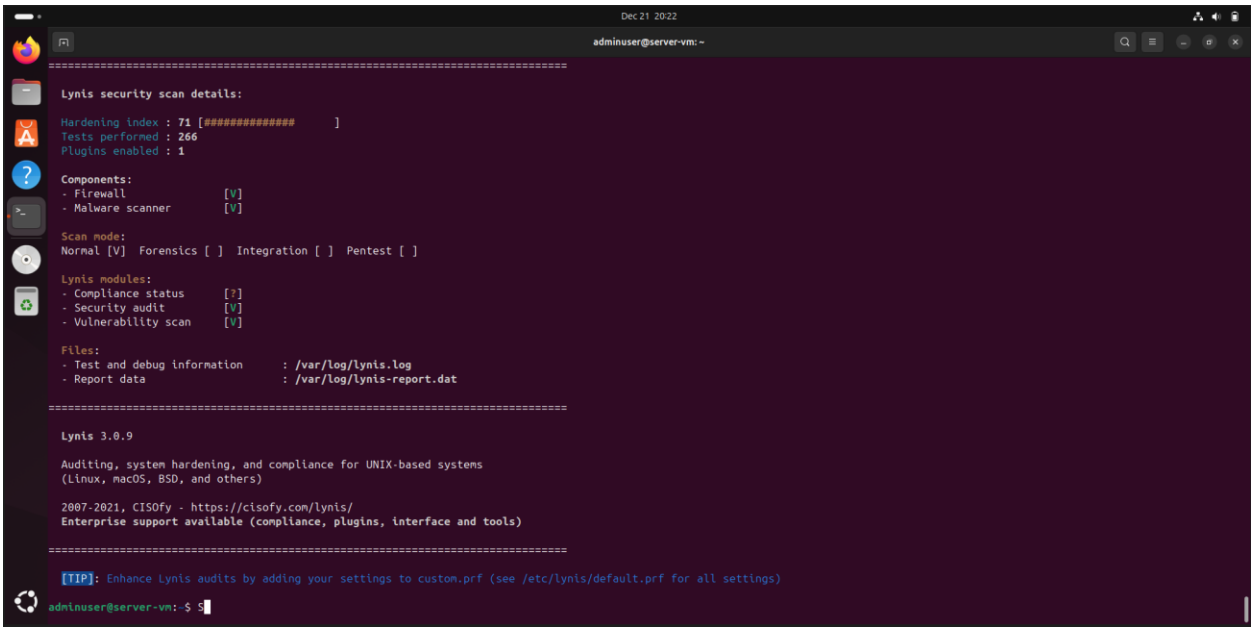
```
# Logging
LogLevel VERBOSE

# 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 20:19
adminuser@server-vm: ~
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 UPDATE]


Dec 21 20:22
adminuser@server-vm: ~
-[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 libpam-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]

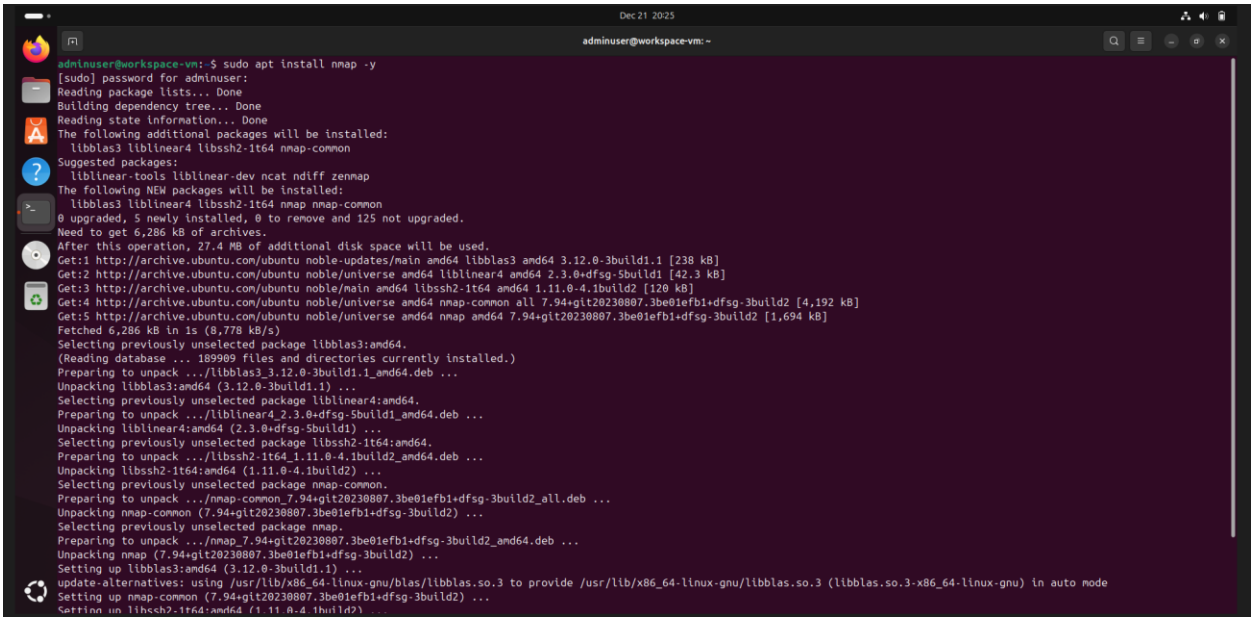


Metric	Initial Score	Final Score
Hardening Index	61	71
Warnings	1	0
Suggestions	49	40

Network Security Assessment (Nmap)

Install Network security tools: sudo apt install nmap -y

Command: nmap -sV 192.168.56.10




```
adminuser@workspace-vm:~$ 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).

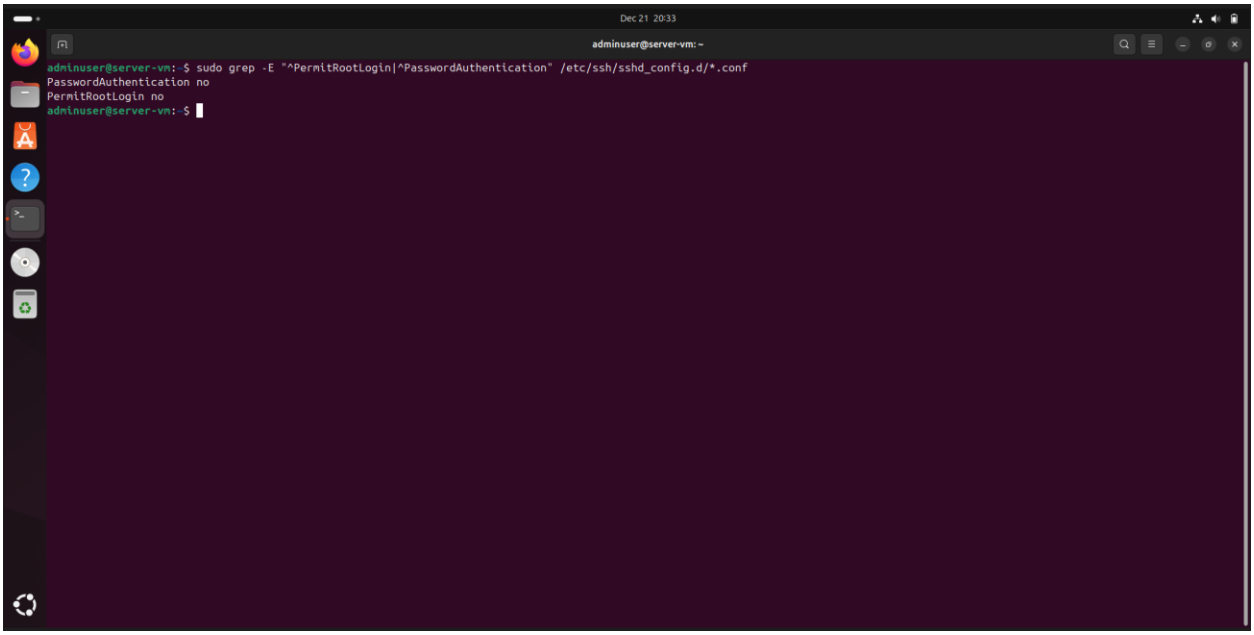
Access Control Verification

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

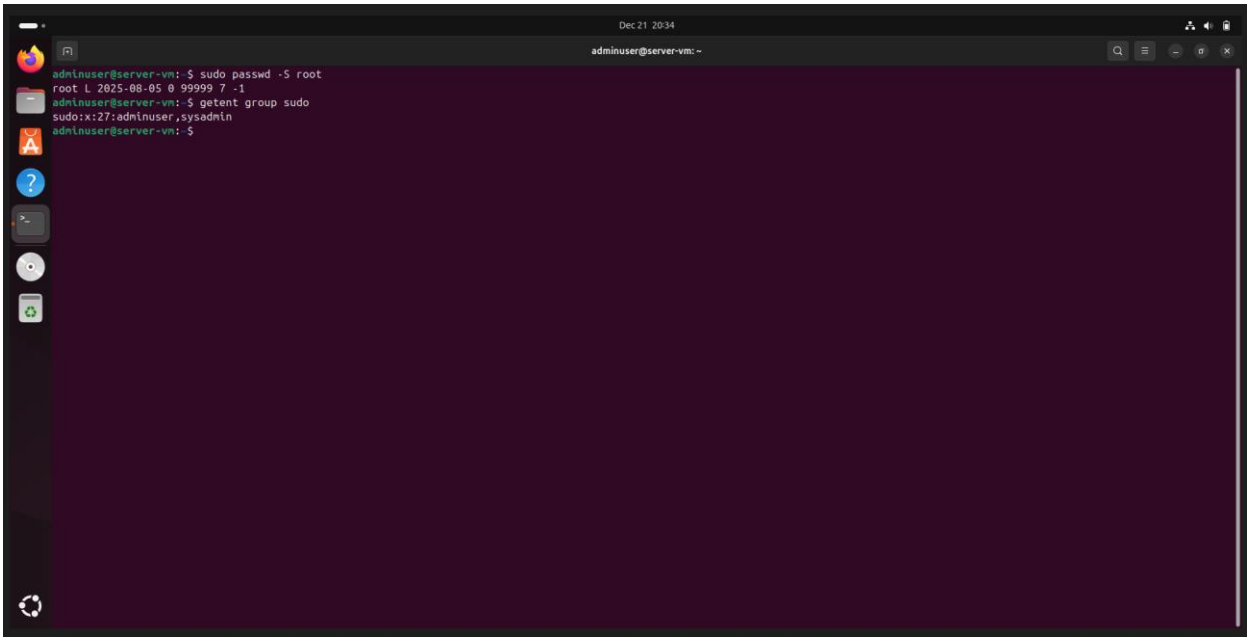


2. User & Sudo Privileges: sudo passwd -S root and getent group sudo

• Root Account: Locked

• Admin User: adminuser, sysadmin are the only member of the sudo group.

• Verification Command: getent group sudo

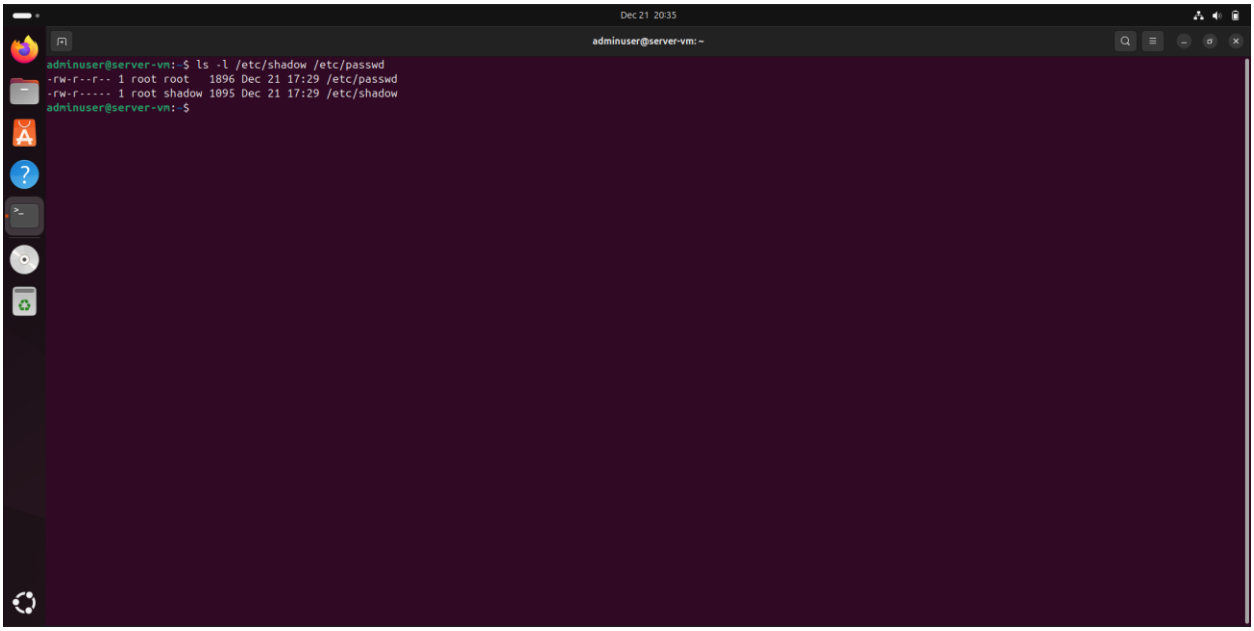


3. File Permission Checks: ls -l /etc/shadow /etc/passwd

Check critical file permissions to prevent unauthorized modification.

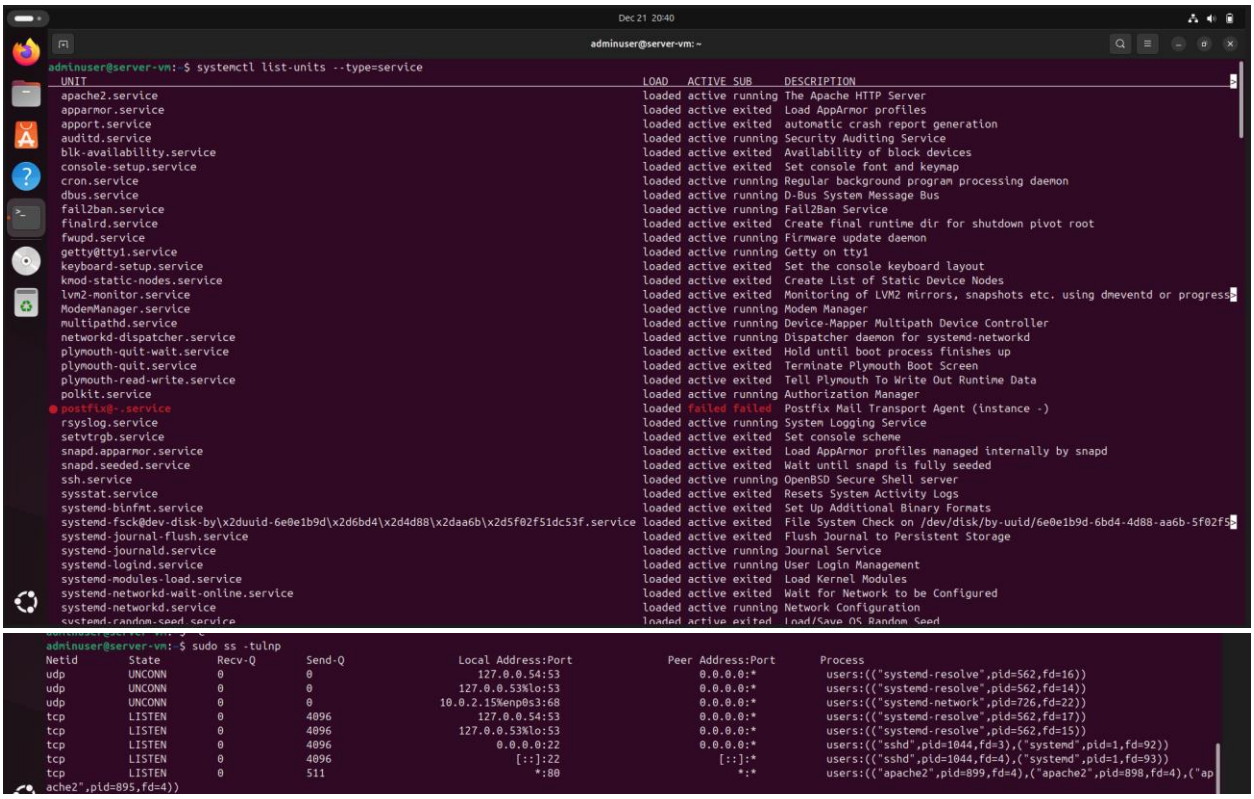
• /etc/shadow: Owned by root:shadow, permissions 640.

• /etc/passwd: Owned by root:root, permissions 644.



Service Audit & Justification

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



System Configuration Review

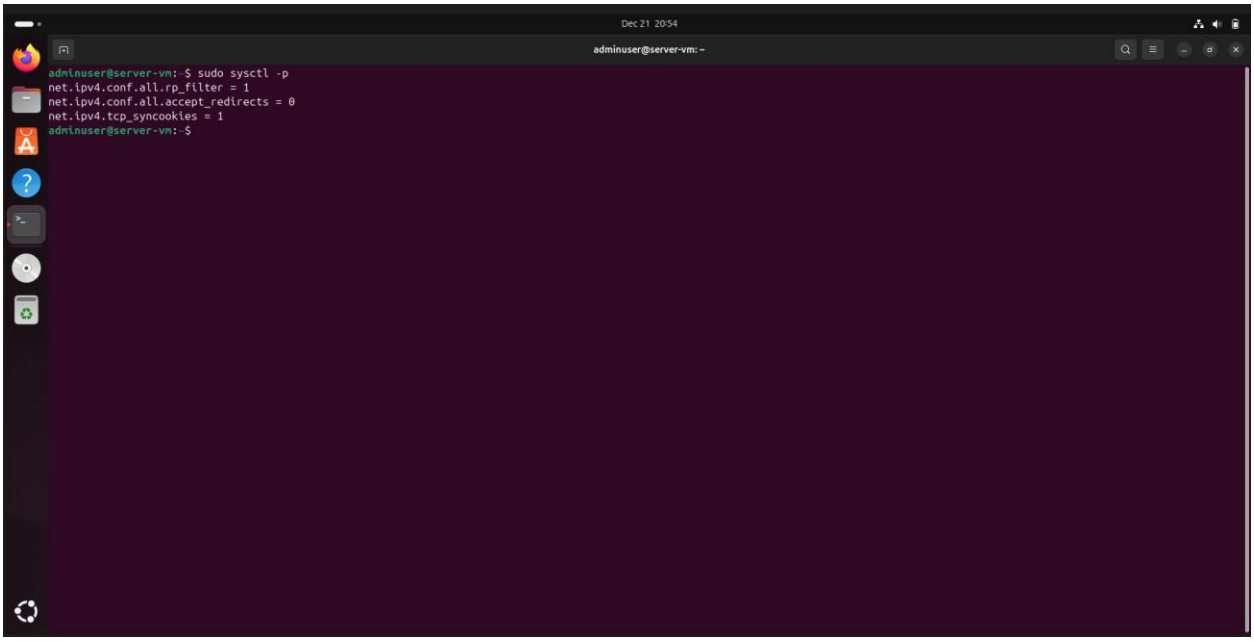
1. Kernel Hardening (sysctl)

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).

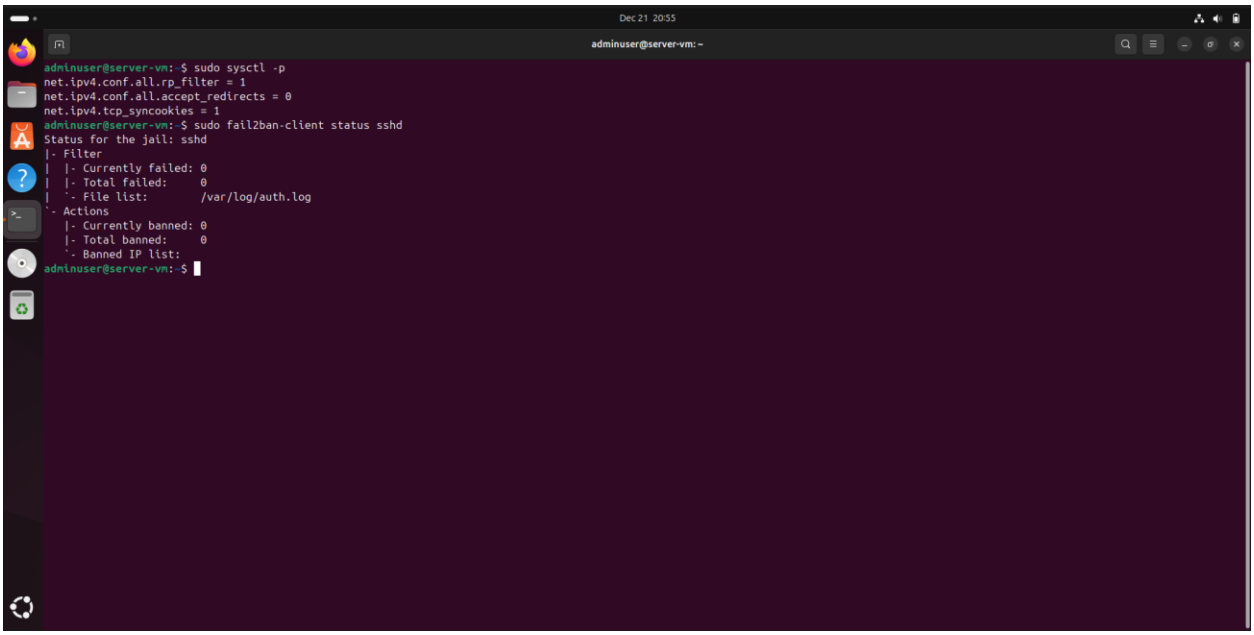
• SYN Cookies: Enabled (Protects against SYN Flood DoS attacks).



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.



3. Automatic Updates

• Tool: unattended-upgrades package installed.

• Configuration: Configured to automatically install security updates to maintain system integrity.