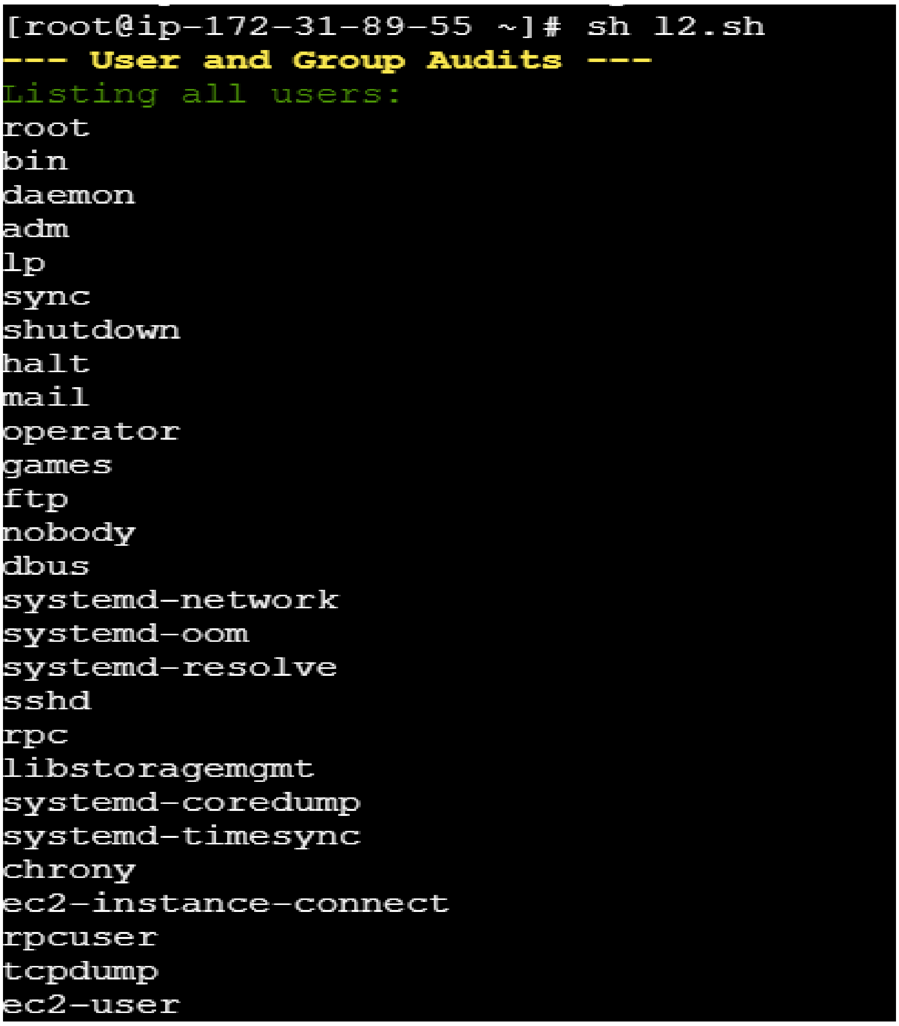
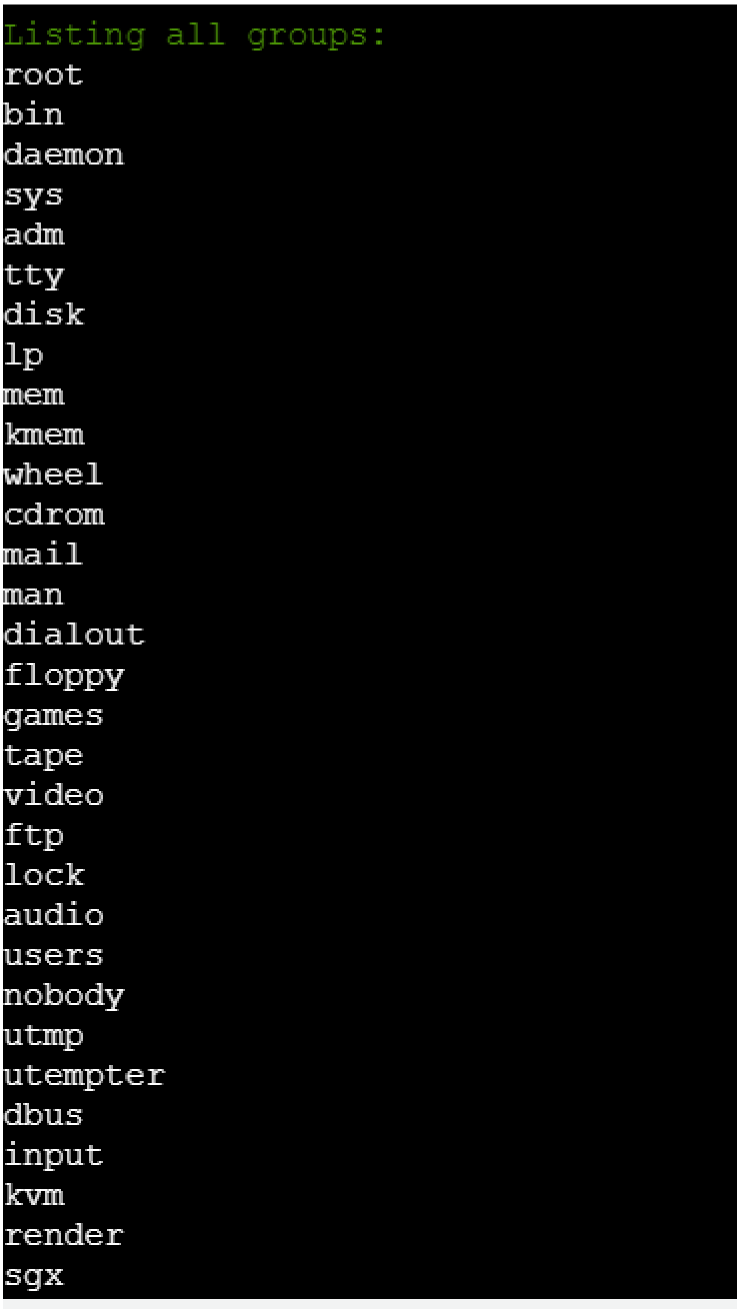
## Output:-

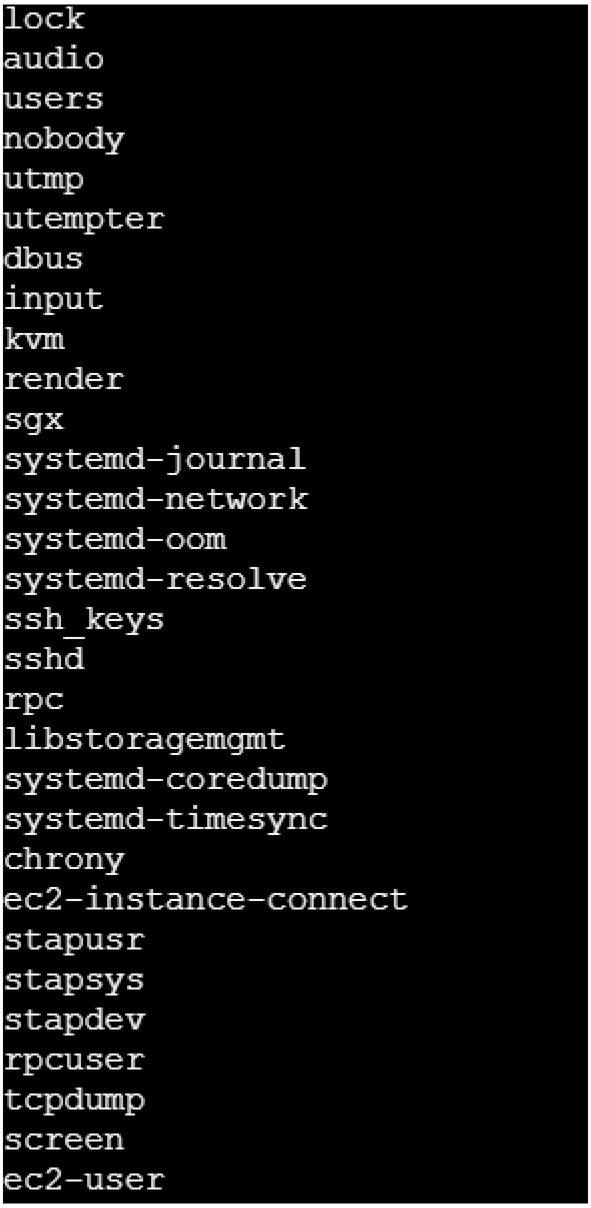
1. **User and Group Audits:**



```
[root@ip-172-31-89-55 ~]# sh 12.sh
--- User and Group Audits ---
Listing all users:
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
operator
games
ftp
nobody
dbus
systemd-network
systemd-oom
systemd-resolve
sshd
rpc
libstoragemgmt
systemd-coredump
systemd-timesync
chrony
ec2-instance-connect
rpcuser
tcpdump
ec2-user
```

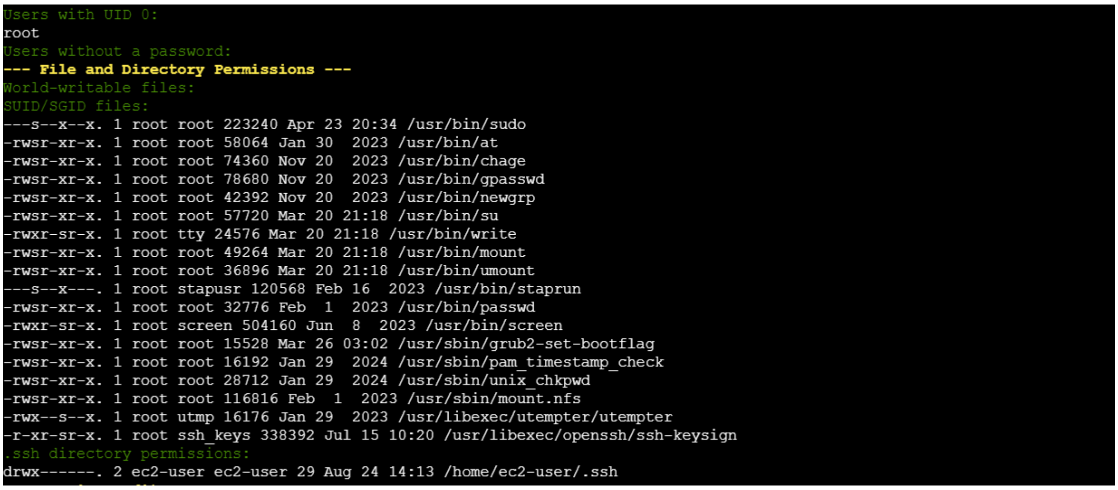


```
Listing all groups:
root
bin
daemon
sys
adm
tty
disk
lp
mem
kmem
wheel
cdrom
mail
man
dialout
floppy
games
tape
video
ftp
lock
audio
users
nobody
utmp
utempter
dbus
input
kvm
render
sgx
```



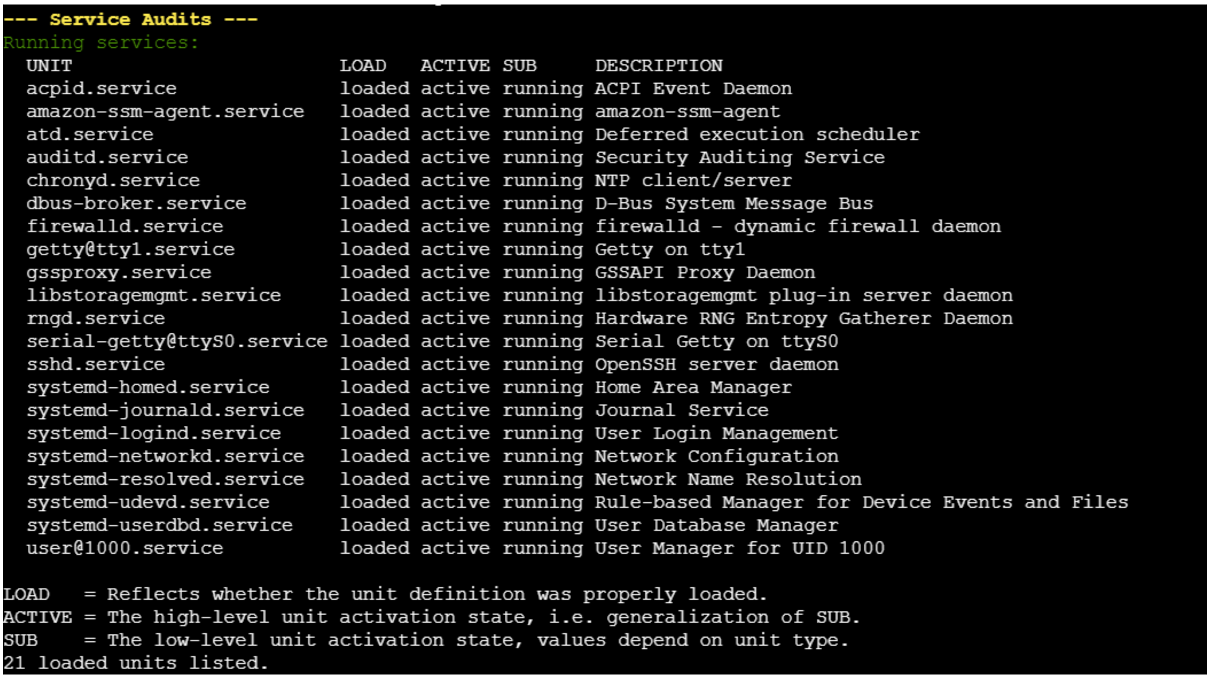
```
lock
audio
users
nobody
utmp
utempter
dbus
input
kvm
render
sgx
systemd-journal
systemd-network
systemd-oom
systemd-resolve
ssh_keys
sshd
rpc
libstoragemgmt
systemd-coredump
systemd-timesync
chrony
ec2-instance-connect
stapusr
stapsys
stapdev
rpcuser
tcpdump
screen
ec2-user
```

## 2..File and Directory Permissions:



```
Users with UID 0:
root
Users without a password:
--- File and Directory Permissions ---
World-writable files:
SUID/SGID files:
---s--x--x. 1 root root 223240 Apr 23 20:34 /usr/bin/sudo
-rwsr-xr-x. 1 root root 58064 Jan 30  2023 /usr/bin/at
-rwsr-xr-x. 1 root root 74360 Nov 20  2023 /usr/bin/chage
-rwsr-xr-x. 1 root root 78680 Nov 20  2023 /usr/bin/gpasswd
-rwsr-xr-x. 1 root root 42392 Nov 20  2023 /usr/bin/newgrp
-rwsr-xr-x. 1 root root 57720 Mar 20 21:18 /usr/bin/su
-rwxr-sr-x. 1 root tty 24576 Mar 20 21:18 /usr/bin/write
-rwsr-xr-x. 1 root root 49264 Mar 20 21:18 /usr/bin/mount
-rwsr-xr-x. 1 root root 36896 Mar 20 21:18 /usr/bin/umount
---s--x---. 1 root stapusr 120568 Feb 16  2023 /usr/bin/staprun
-rwsr-xr-x. 1 root root 32776 Feb  1  2023 /usr/bin/passwd
-rwxr-sr-x. 1 root screen 504160 Jun  8  2023 /usr/bin/screen
-rwsr-xr-x. 1 root root 15528 Mar 26 03:02 /usr/sbin/grub2-set-bootflag
-rwsr-xr-x. 1 root root 16192 Jan 29  2024 /usr/sbin/pam_timestamp_check
-rwsr-xr-x. 1 root root 28712 Jan 29  2024 /usr/sbin/unix_chkpwd
-rwsr-xr-x. 1 root root 116816 Feb  1  2023 /usr/sbin/mount.nfs
-rwx--s--x. 1 root utmp 16176 Jan 29  2023 /usr/libexec/utempter/utempter
-r-xr-sr-x. 1 root ssh_keys 338392 Jul 15 10:20 /usr/libexec/openssh/ssh-keysign
.ssh directory permissions:
drwx------. 2 ec2-user ec2-user 29 Aug 24 14:13 /home/ec2-user/.ssh
```

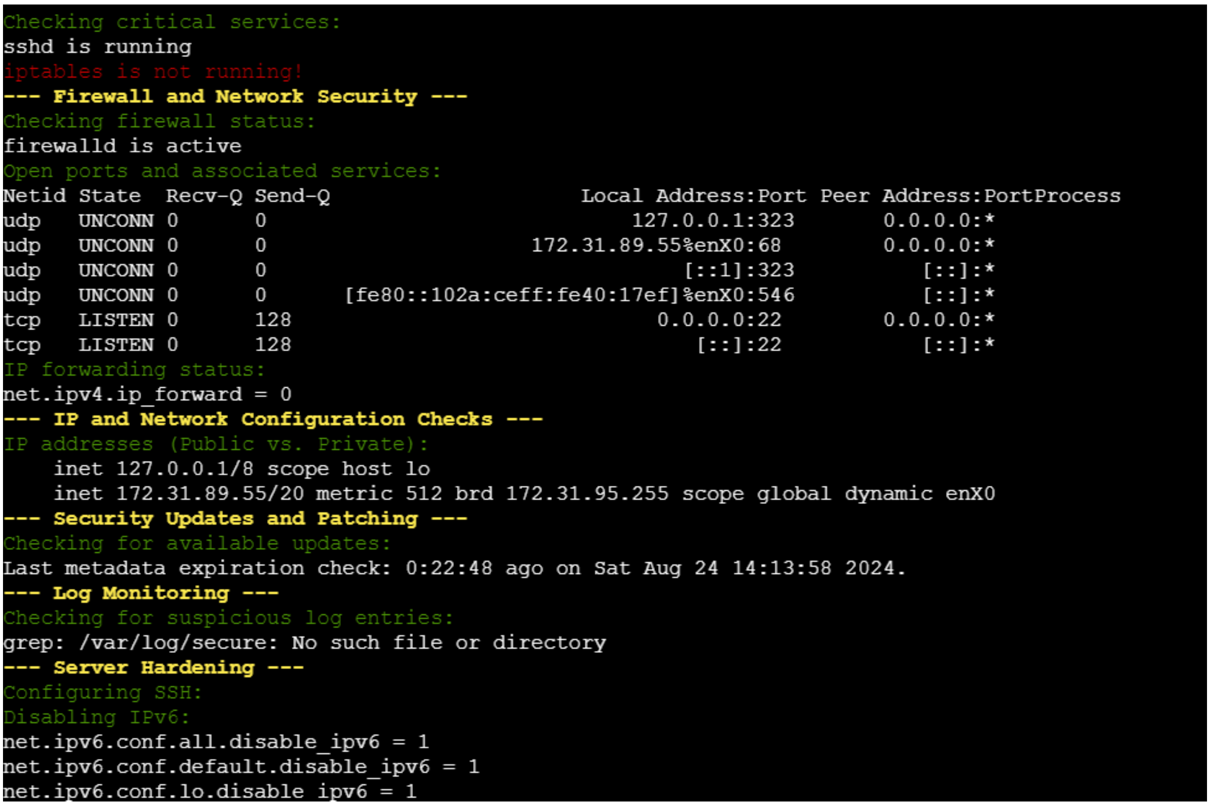
## 3.Service Audits:



```
--- Service Audits ---
Running services:
  UNIT                         LOAD   ACTIVE SUB     DESCRIPTION
  acpid.service                loaded active running ACPI Event Daemon
  amazon-ssm-agent.service     loaded active running amazon-ssm-agent
  atd.service                  loaded active running Deferred execution scheduler
  auditd.service               loaded active running Security Auditing Service
  chronyd.service              loaded active running NTP client/server
  dbus-broker.service          loaded active running D-Bus System Message Bus
  firewalld.service            loaded active running firewalld - dynamic firewall daemon
  getty@tty1.service           loaded active running Getty on tty1
  gssproxy.service             loaded active running GSSAPI Proxy Daemon
  libstoragemgmt.service       loaded active running libstoragemgmt plug-in server daemon
  rngd.service                 loaded active running Hardware RNG Entropy Gatherer Daemon
  serial-getty@ttyS0.service loaded active running Serial Getty on ttyS0
  sshd.service                 loaded active running OpenSSH server daemon
  systemd-homed.service        loaded active running Home Area Manager
  systemd-journald.service     loaded active running Journal Service
  systemd-logind.service       loaded active running User Login Management
  systemd-networkd.service     loaded active running Network Configuration
  systemd-resolved.service     loaded active running Network Name Resolution
  systemd-udevd.service        loaded active running Rule-based Manager for Device Events and Files
  systemd-userdbd.service      loaded active running User Database Manager
  user@1000.service            loaded active running User Manager for UID 1000

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
21 loaded units listed.
```

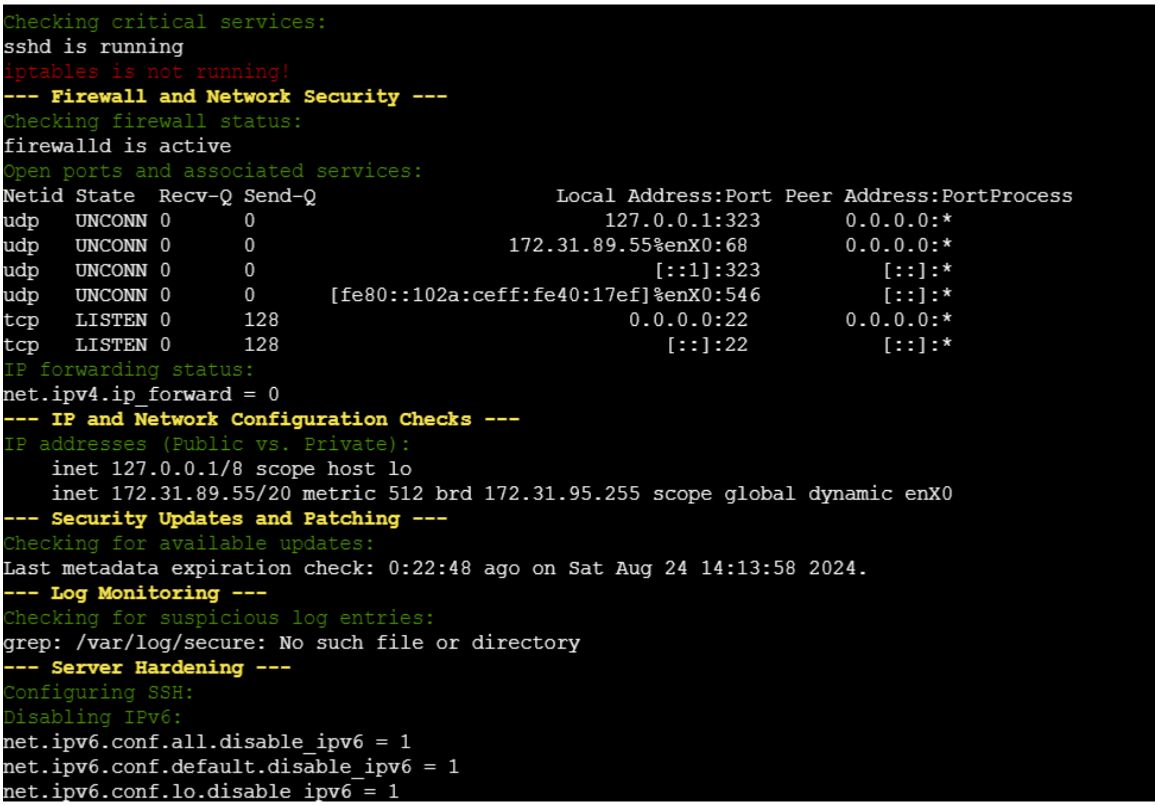
## 4. Firewall and Network Security:



```
Checking critical services:
sshd is running
iptables is not running!
--- Firewall and Network Security ---
Checking firewall status:
firewalld is active
Open ports and associated services:
Netid State  Recv-Q Send-Q                    Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0                             127.0.0.1:323       0.0.0.0:*
udp   UNCONN 0      0                     172.31.89.55%enX0:68        0.0.0.0:*
udp   UNCONN 0      0                                 [::1]:323          [::]:*
udp   UNCONN 0      0      [fe80::102a:ceff:fe40:17ef]%enX0:546          [::]:*
tcp   LISTEN 0      128                             0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128                                [::]:22           [::]:*
IP forwarding status:
net.ipv4.ip_forward = 0
--- IP and Network Configuration Checks ---
IP addresses (Public vs. Private):
    inet 127.0.0.1/8 scope host lo
    inet 172.31.89.55/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
--- Security Updates and Patching ---
Checking for available updates:
Last metadata expiration check: 0:22:48 ago on Sat Aug 24 14:13:58 2024.
--- Log Monitoring ---
Checking for suspicious log entries:
grep: /var/log/secure: No such file or directory
--- Server Hardening ---
Configuring SSH:
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

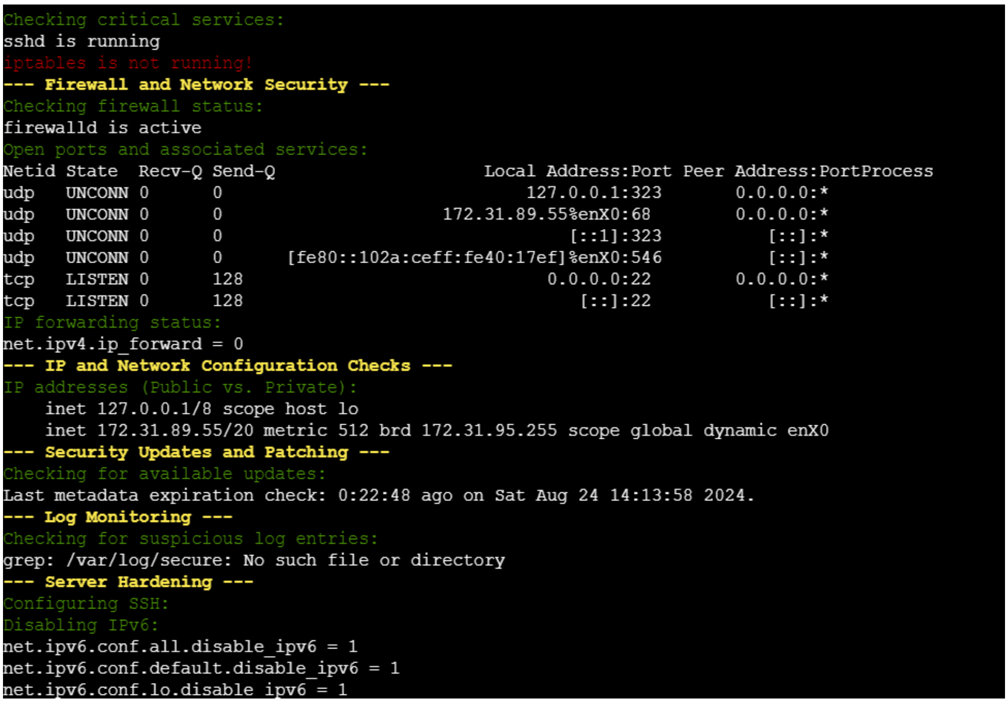
## 5. **IP and Network Configuration Checks:**

Public vs. Private IP Checks**:**



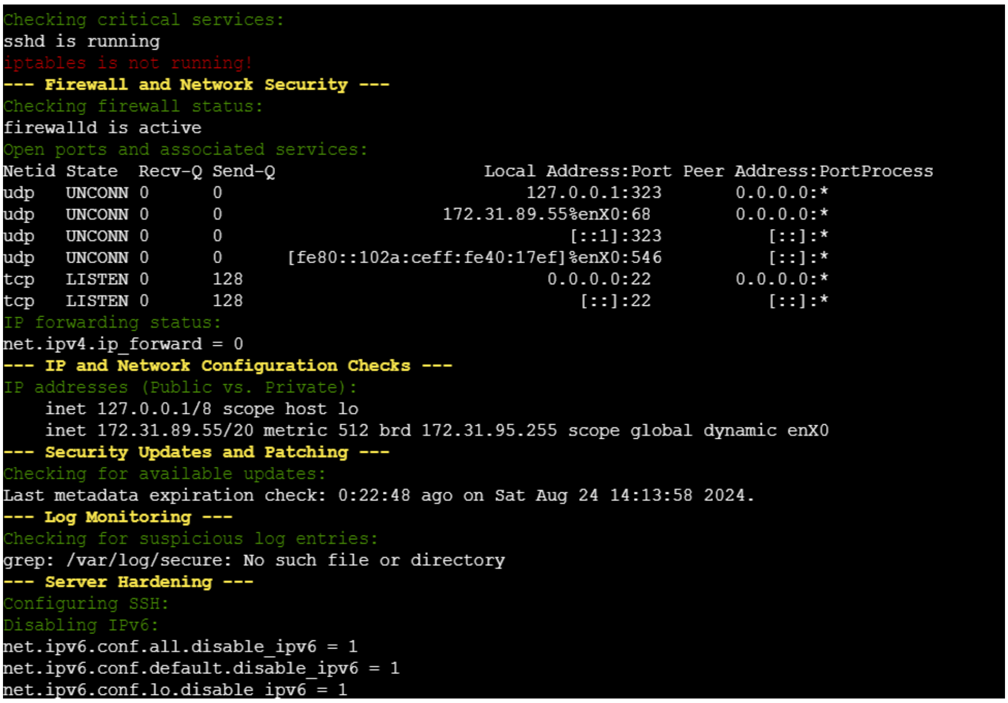
```
Checking critical services:
sshd is running
iptables is not running!
--- Firewall and Network Security ---
Checking firewall status:
firewalld is active
Open ports and associated services:
Netid State  Recv-Q Send-Q                    Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0                             127.0.0.1:323       0.0.0.0:*
udp   UNCONN 0      0                     172.31.89.55%enX0:68        0.0.0.0:*
udp   UNCONN 0      0                                 [::1]:323          [::]:*
udp   UNCONN 0      0      [fe80::102a:ceff:fe40:17ef]%enX0:546          [::]:*
tcp   LISTEN 0      128                             0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128                                [::]:22           [::]:*
IP forwarding status:
net.ipv4.ip_forward = 0
--- IP and Network Configuration Checks ---
IP addresses (Public vs. Private):
    inet 127.0.0.1/8 scope host lo
    inet 172.31.89.55/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
--- Security Updates and Patching ---
Checking for available updates:
Last metadata expiration check: 0:22:48 ago on Sat Aug 24 14:13:58 2024.
--- Log Monitoring ---
Checking for suspicious log entries:
grep: /var/log/secure: No such file or directory
--- Server Hardening ---
Configuring SSH:
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

## 6. **Security Updates and Patching:**



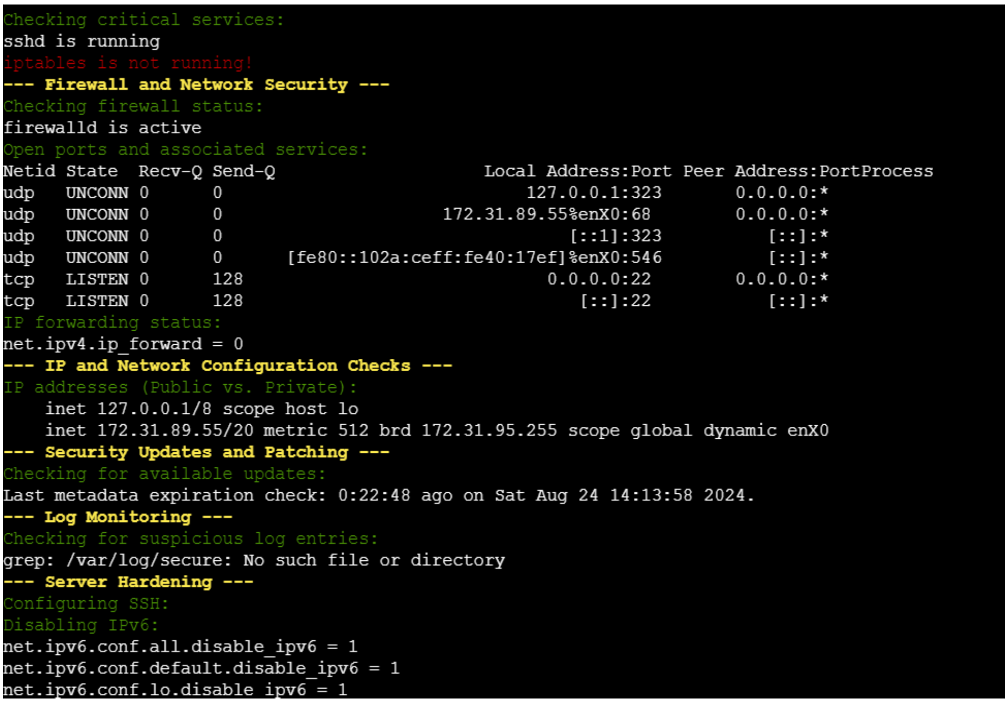
```
Checking critical services:
sshd is running
iptables is not running!
--- Firewall and Network Security ---
Checking firewall status:
firewalld is active
Open ports and associated services:
Netid State  Recv-Q Send-Q                    Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0                             127.0.0.1:323       0.0.0.0:*
udp   UNCONN 0      0                     172.31.89.55%enX0:68        0.0.0.0:*
udp   UNCONN 0      0                                 [::1]:323          [::]:*
udp   UNCONN 0      0      [fe80::102a:ceff:fe40:17ef]%enX0:546          [::]:*
tcp   LISTEN 0      128                             0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128                                [::]:22           [::]:*
IP forwarding status:
net.ipv4.ip_forward = 0
--- IP and Network Configuration Checks ---
IP addresses (Public vs. Private):
    inet 127.0.0.1/8 scope host lo
    inet 172.31.89.55/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
--- Security Updates and Patching ---
Checking for available updates:
Last metadata expiration check: 0:22:48 ago on Sat Aug 24 14:13:58 2024.
--- Log Monitoring ---
Checking for suspicious log entries:
grep: /var/log/secure: No such file or directory
--- Server Hardening ---
Configuring SSH:
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

## 7. **Log Monitoring:**



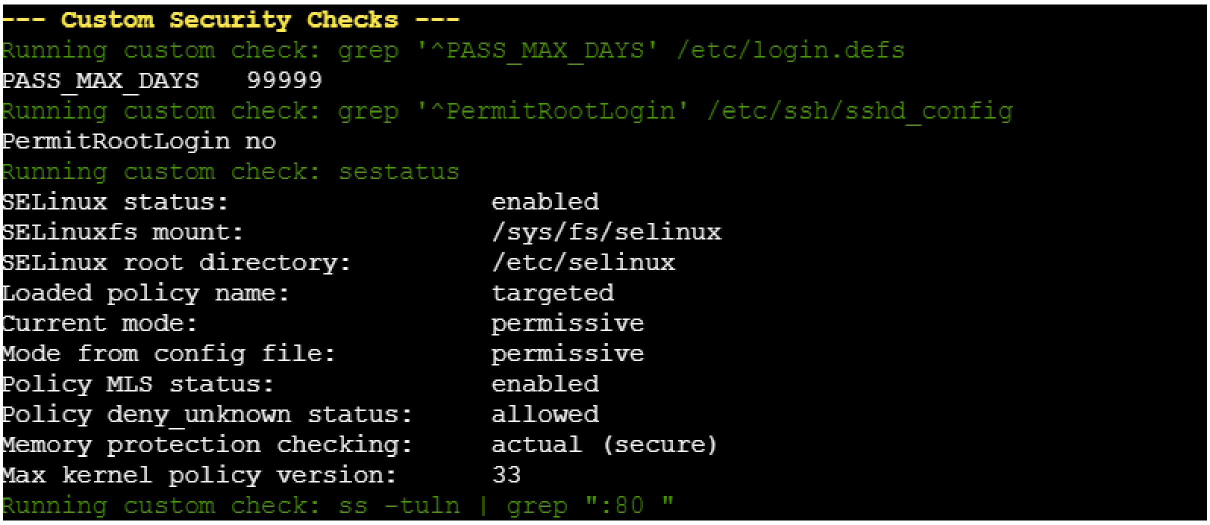
```
Checking critical services:
sshd is running
iptables is not running!
--- Firewall and Network Security ---
Checking firewall status:
firewalld is active
Open ports and associated services:
Netid State  Recv-Q Send-Q                    Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0                             127.0.0.1:323       0.0.0.0:*
udp   UNCONN 0      0                     172.31.89.55%enX0:68        0.0.0.0:*
udp   UNCONN 0      0                                 [::1]:323          [::]:*
udp   UNCONN 0      0      [fe80::102a:ceff:fe40:17ef]%enX0:546          [::]:*
tcp   LISTEN 0      128                             0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128                                [::]:22           [::]:*
IP forwarding status:
net.ipv4.ip_forward = 0
--- IP and Network Configuration Checks ---
IP addresses (Public vs. Private):
    inet 127.0.0.1/8 scope host lo
    inet 172.31.89.55/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
--- Security Updates and Patching ---
Checking for available updates:
Last metadata expiration check: 0:22:48 ago on Sat Aug 24 14:13:58 2024.
--- Log Monitoring ---
Checking for suspicious log entries:
grep: /var/log/secure: No such file or directory
--- Server Hardening ---
Configuring SSH:
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

## 8. **Server Hardening Steps:**



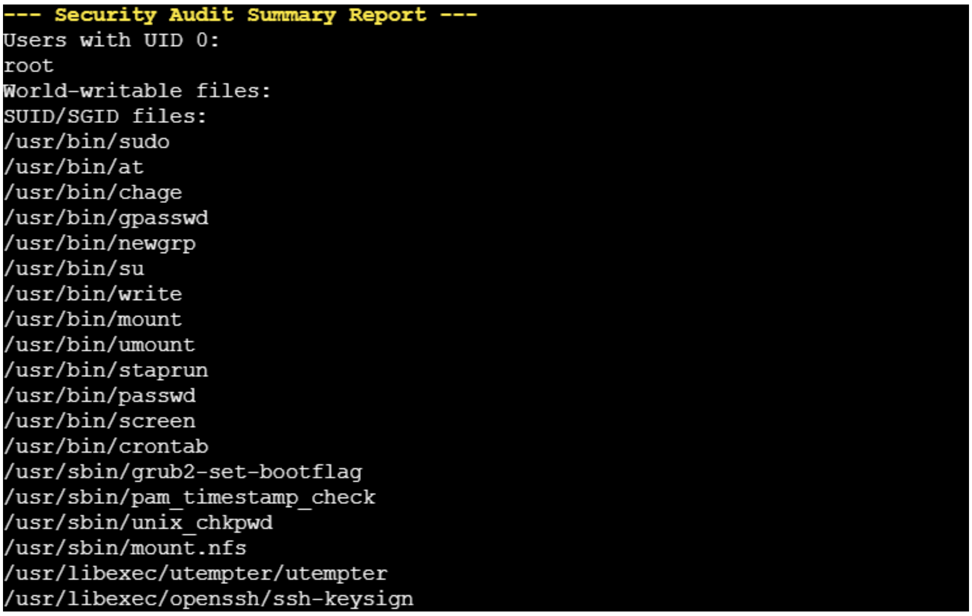
```
Checking critical services:
sshd is running
iptables is not running!
--- Firewall and Network Security ---
Checking firewall status:
firewalld is active
Open ports and associated services:
Netid State  Recv-Q Send-Q                    Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0                             127.0.0.1:323       0.0.0.0:*
udp   UNCONN 0      0                     172.31.89.55%enX0:68        0.0.0.0:*
udp   UNCONN 0      0                                 [::1]:323          [::]:*
udp   UNCONN 0      0      [fe80::102a:ceff:fe40:17ef]%enX0:546          [::]:*
tcp   LISTEN 0      128                             0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128                                [::]:22           [::]:*
IP forwarding status:
net.ipv4.ip_forward = 0
--- IP and Network Configuration Checks ---
IP addresses (Public vs. Private):
    inet 127.0.0.1/8 scope host lo
    inet 172.31.89.55/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
--- Security Updates and Patching ---
Checking for available updates:
Last metadata expiration check: 0:22:48 ago on Sat Aug 24 14:13:58 2024.
--- Log Monitoring ---
Checking for suspicious log entries:
grep: /var/log/secure: No such file or directory
--- Server Hardening ---
Configuring SSH:
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

## 9. **Custom Security Checks:**

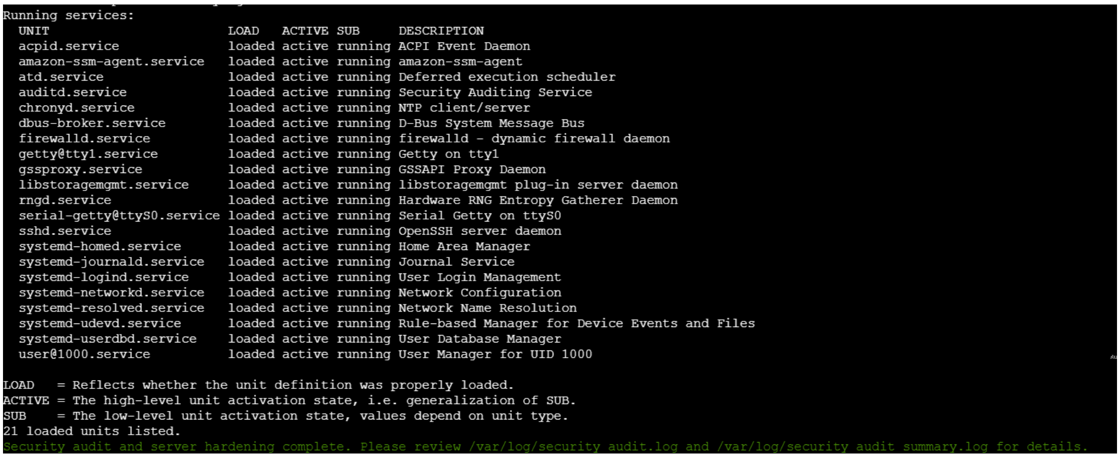


```
--- Custom Security Checks ---
Running custom check: grep '^PASS_MAX_DAYS' /etc/login.defs
PASS_MAX_DAYS   99999
Running custom check: grep '^PermitRootLogin' /etc/ssh/sshd_config
PermitRootLogin no
Running custom check: sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
Running custom check: ss -tuln | grep ":80 "
```

## 10. **Reporting and Alerting:**



```
--- Security Audit Summary Report ---
Users with UID 0:
root
World-writable files:
SUID/SGID files:
/usr/bin/sudo
/usr/bin/at
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/write
/usr/bin/mount
/usr/bin/umount
/usr/bin/staprun
/usr/bin/passwd
/usr/bin/screen
/usr/bin/crontab
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/libexec/utempter/utempter
/usr/libexec/openssh/ssh-keysign
```



```
Running services:
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  acpid.service                 loaded active running ACPI Event Daemon
  amazon-ssm-agent.service      loaded active running amazon-ssm-agent
  atd.service                   loaded active running Deferred execution scheduler
  auditd.service                loaded active running Security Auditing Service
  chronyd.service               loaded active running NTP client/server
  dbus-broker.service           loaded active running D-Bus System Message Bus
  firewalld.service             loaded active running firewalld - dynamic firewall daemon
  getty@tty1.service            loaded active running Getty on tty1
  gssproxy.service              loaded active running GSSAPI Proxy Daemon
  libstoragemgmt.service        loaded active running libstoragemgmt plug-in server daemon
  rngd.service                  loaded active running Hardware RNG Entropy Gatherer Daemon
  serial-getty@ttyS0.service    loaded active running Serial Getty on ttyS0
  sshd.service                  loaded active running OpenSSH server daemon
  systemd-homed.service         loaded active running Home Area Manager
  systemd-journald.service      loaded active running Journal Service
  systemd-logind.service        loaded active running User Login Management
  systemd-networkd.service      loaded active running Network Configuration
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-udevd.service         loaded active running Rule-based Manager for Device Events and Files
  systemd-userdbd.service       loaded active running User Database Manager
  user@1000.service             loaded active running User Manager for UID 1000

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
21 loaded units listed.
Security audit and server hardening complete. Please review /var/log/security audit.log and /var/log/security audit summary.log for details.
```