Set 2: Script for Automating Security Audits and Server Hardening on Linux Servers

Task Description:

You are required to create a Bash script that automates both the security audit and the hardening process of Linux servers. The script should be reusable and modular, allowing it to be easily deployed across multiple servers to ensure they meet stringent security standards. The script should include checks for common security vulnerabilities, IPv4/IPv6 configurations, public vs. private IP identification, and the implementation of hardening measures as outlined in the provided document. The final script should be uploaded to a GitHub repository with comprehensive documentation.

Requirements:

1. **User and Group Audits:**
   - **List all users and groups on the server.**
   - **Check for users with UID 0 (root privileges) and report any non-standard users.**
   - **Identify and report any users without passwords or with weak passwords.**
2. **File and Directory Permissions:**
   - **Scan for files and directories with world-writable permissions.**
   - **Check for the presence of .ssh directories and ensure they have secure permissions.**
   - **Report any files with SUID or SGID bits set, particularly on executables.**
3. **Service Audits:**
   - **List all running services and check for any unnecessary or unauthorized services.**
   - **Ensure that critical services (e.g., sshd, iptables) are running and properly configured.**
   - **Check that no services are listening on non-standard or insecure ports.**
4. **Firewall and Network Security:**
   - **Verify that a firewall (e.g., iptables, ufw) is active and configured to block unauthorized access.**
   - **Report any open ports and their associated services.**
   - **Check for and report any IP forwarding or other insecure network configurations.**
5. **IP and Network Configuration Checks:**
   - **Public vs. Private IP Checks:**
     - **Identify whether the server's IP addresses are public or private.**
     - **Provide a summary of all IP addresses assigned to the server, specifying which are public and which are private.**
     - **Ensure that sensitive services (e.g., SSH) are not exposed on public IPs unless required.**

6. **Security Updates and Patching:**
   - **Check for and report any available security updates or patches.**
   - **Ensure that the server is configured to receive and install security updates regularly.**
7. **Log Monitoring:**
   - **Check for any recent suspicious log entries that may indicate a security breach, such as too many login attempts on SSH.**
8. **Server Hardening Steps:**
   - **SSH Configuration:**
     - **Implement SSH key-based authentication and disable password-based login for root.**
     - **Ensure that SSH keys are securely stored and used.**
   - **Disabling IPv6 (if not required):**
     - **Disable IPv6 if it is not in use, following the provided guidelines.**
     - **Update services like SafeSquid to listen on the correct IPv4 addresses after disabling IPv6.**
   - **Securing the Bootloader:**
     - **Set a password for the GRUB bootloader to prevent unauthorized changes to boot parameters.**
   - **Firewall Configuration:**
     - **Implement the recommended iptables rules, including default policies, loopback interface acceptance, and specific port allowances.**
   - **Automatic Updates:**
     - **Configure unattended-upgrades to automatically apply security updates and remove unused packages, following the provided guidelines.**
9. **Custom Security Checks:**
   - **Allow the script to be easily extended with custom security checks based on specific organizational policies or requirements.**
   - **Include a configuration file where custom checks can be defined and managed.**
10. **Reporting and Alerting:**
    - **Generate a summary report of the security audit and hardening process, highlighting any issues that need attention.**
    - **Optionally, configure the script to send email alerts or notifications if critical vulnerabilities or misconfigurations are found.**

Ans :

1. First launch a server (configuration here – t2.micro free-tier) from AWS management console. Now, using keypair file login server, SSH using Putty. Enable required ports 22, 80.
2. In putty shell, first update Package Manager
   - ⇨ sudo yum update -y
3. Create a directory where we can create shell script files
   - ⇨ mkdir task
   - ⇨ cd task
4. After getting inside our created directory, create a file with extension of sh
   - ⇨ nano TaskB-FileA.sh

now, make a script that will help to monitor all resources

TaskB-FileA.sh

```
#!/bin/bash


# Function to log output to /var/log/security_audit.log
log() {
  echo "$1" | tee -a /var/log/security_audit.log
}


# Ensure the script is run as root
if [[ "$(id -u)" -ne 0 ]]; then
  log "This script must be run as root"
  exit 1
fi


log "Starting security audit..."


# Listing all users and groups
log "Listing all users and groups:"
cut -d: -f1 /etc/passwd
cut -d: -f1 /etc/group
```

```
# Users with UID 0
log "Users with UID 0:"
awk -F: '$3 == 0 {print $1}' /etc/passwd


# Users without passwords
log "Users without passwords:"
awk -F: '($2 == "" && $1 != "root") {print $1}' /etc/shadow


# World-writable files and directories
log "World-writable files and directories:"
find / -xdev -type d -perm -0007 -exec ls -ld {} \;


# Checking .ssh directory permissions
log "Checking .ssh directory permissions:"
find /home -type d -name ".ssh" -exec ls -ld {} \;


# Files with SUID or SGID bits set
log "Files with SUID or SGID bits set:"
find / -xdev \( -perm -4000 -o -perm -2000 \) -type f -exec ls -l {} \;


# Listing all running services
log "Listing all running services:"
systemctl list-units --type=service --state=running


# Ensuring critical services are running
log "Ensuring critical services are running:"
for service in acpid amazon-ssm-agent atd auditd chronyd dbus-broker getty@tty1 gssproxy
libstoragemgmt rngd serial-getty@ttyS0 sshd systemd-homed systemd-journald systemd-logind
systemd-networkd systemd-resolved systemd-udevd systemd-userdbd; do
  systemctl is-active --quiet "$service" && log "$service is running" || log "$service is not running"
done


# Checking for firewall configuration
```

```
if command -v firewall-cmd &> /dev/null; then
    log "Listing firewalld rules:"
    firewall-cmd --list-all
else
    log "firewalld not found. Skipping firewall configuration."
fi

# Checking IP forwarding
log "Checking IP forwarding:"
sysctl net.ipv4.ip_forward

# Checking IP addresses
log "Checking IP addresses:"
ip addr show

# Checking for security updates
log "Checking for security updates:"
if command -v yum &> /dev/null; then
    yum check-update
elif command -v dnf &> /dev/null; then
    dnf check-update
else
    log "No package manager found for security updates."
fi

# Checking SSH configuration
log "Updating SSH configuration:"
grep -E '^PermitRootLogin|^PasswordAuthentication|^AllowUsers|^DenyUsers' /etc/ssh/sshd_config

# Disabling IPv6
log "Disabling IPv6:"
sysctl net.ipv6.conf.all.disable_ipv6
```

```
# Setting GRUB password

log "Setting GRUB password: (This is a placeholder action)"

# Implementation depends on specific system setup


log "Security audit completed. Check /var/log/security_audit.log for details."
```

Now, save this file (ctrl+x & enter)

5. Now give execution permission to this file
   - ⇨ sudo chmod +x TaskB-FileA.sh

6. Now, execute the file
   - ⇨ sudo .\TaskB-FileA.sh

OutPut:

```
[ec2-user@ip-172-31-84-224 task] $ sudo ./TaskB-FileA.sh

Starting security audit...

Listing all users and groups:

root

bin

daemon

adm

lp

sync

shutdown

halt

mail

operator

games

ftp
```

Set 2

```
nobody
dbus
systemd-network
systemd-oom
systemd-resolve
sshd
rpc
libstoragemgmt
systemd-coredump
systemd-timesync
chrony
ec2-instance-connect
rpcuser
tcpdump
ec2-user
nginx
root
bin
daemon
sys
adm
tty
disk
lp
mem
kmem
wheel
cdrom
mail
man
dialout
floppy
```

Set 2

```
games
tape
video
ftp
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
```

- Arti Bhatlawande

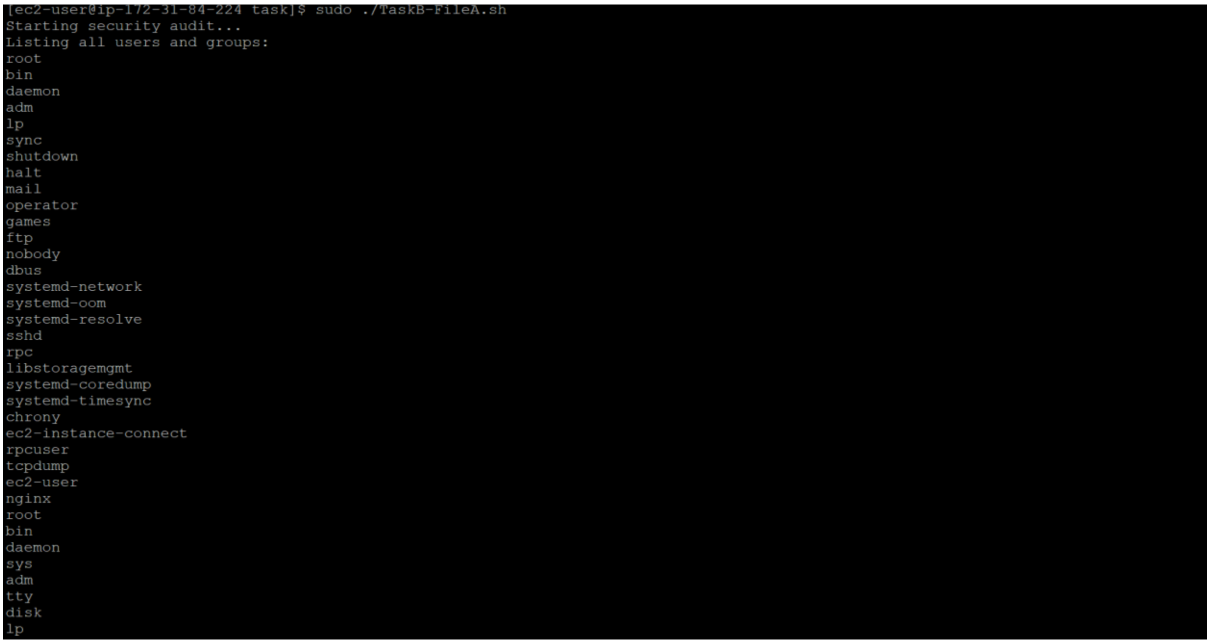
```
screen

ec2-user

nginx

Users with UID 0:

root

Users without passwords:

World-writable files and directories:

drwxrwxrwt. 13 root root 260 Aug 25 10:25 /tmp

drwxrwxrwt. 9 root root 16384 Aug 25 10:25 /var/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/cloud-init

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-resolved.service-efY04w/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-policy-routes@enX0.service-XynM1r/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-logind.service-QdGbQo/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-dbus-broker.service-jmHmb1/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-nginx.service-ktBcPo/tmp

drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-chronyd.service-In5z01/tmp

Checking .ssh directory permissions:

drwx------. 2 ec2-user ec2-user 111 Aug 25 08:41 /home/ec2-user/.ssh

Files with SUID or SGID bits set:

---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
Listing all 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
  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
  nginx.service             loaded active running The nginx HTTP and reverse proxy server
  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
```

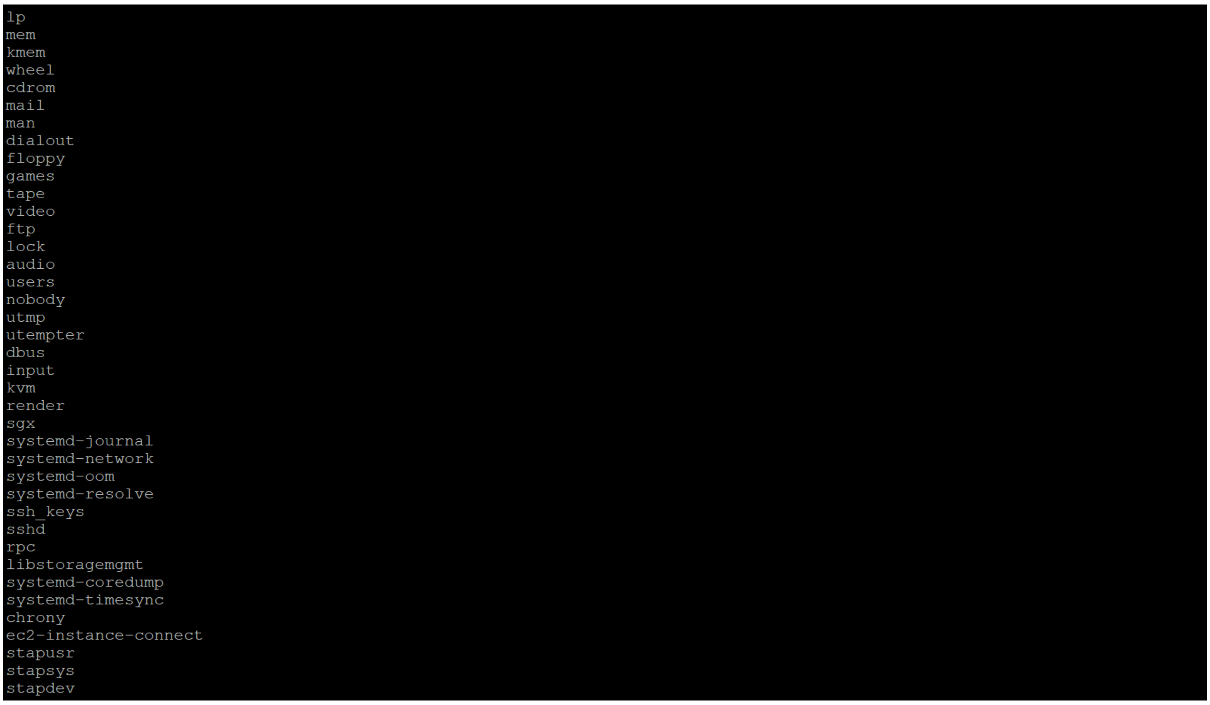
```
LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
21 loaded units listed.
Ensuring critical services are running:
acpid is running
amazon-ssm-agent is running
atd is running
auditd is running
chronyd is running
dbus-broker is running
getty@tty1 is running
gssproxy is running
libstoragemgmt is running
rngd is running
serial-getty@ttyS0 is running
sshd is running
systemd-homed is running
systemd-journald is running
systemd-logind is running
systemd-networkd is running
systemd-resolved is running
systemd-udevd is running
systemd-userdbd is running
firewalld not found. Skipping firewall configuration.
Checking IP forwarding:
net.ipv4.ip_forward = 0
Checking IP addresses:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
```

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen
1000
    link/ether 12:f5:77:86:8a:05 brd ff:ff:ff:ff:ff:ff
    altname eni-0ef3ff4e2cf674c7b
    altname device-number-0.0
    inet 172.31.84.224/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 3092sec preferred_lft 3092sec
    inet6 fe80::10f5:77ff:fe86:8a05/64 scope link
       valid_lft forever preferred_lft forever
Checking for security updates:
Last metadata expiration check: 18:17:13 ago on Sat Aug 24 16:08:48 2024.
Updating SSH configuration:
PermitRootLogin no
PasswordAuthentication no
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 0
Setting GRUB password: (This is a placeholder action)
Security audit completed. Check /var/log/security_audit.log for details.
```

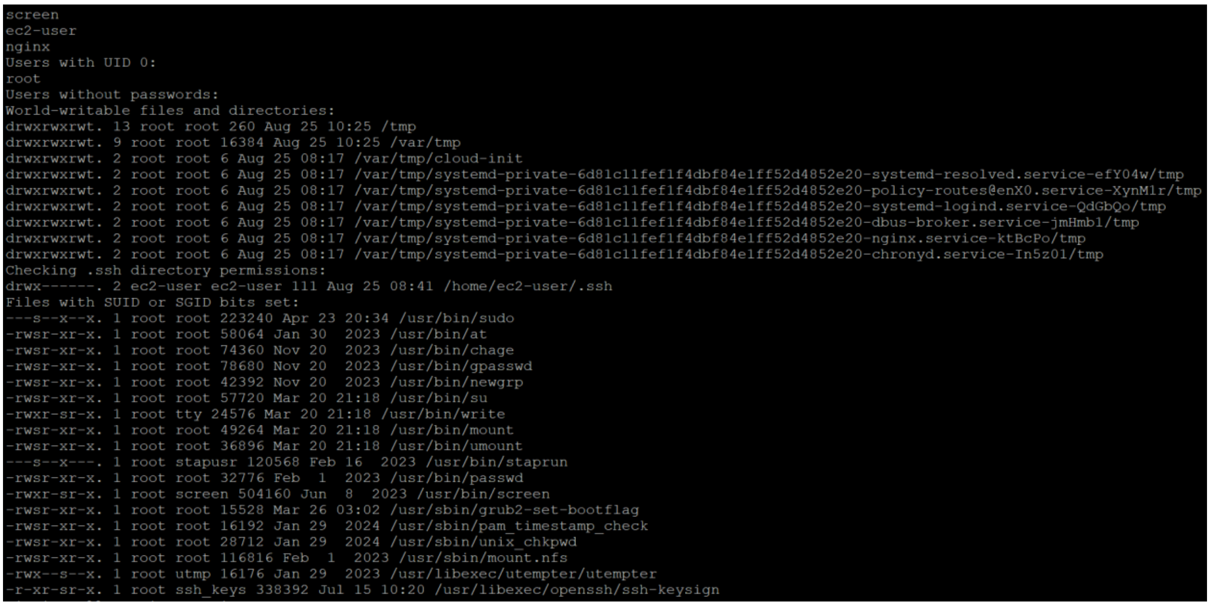
Here output obtained is as following:



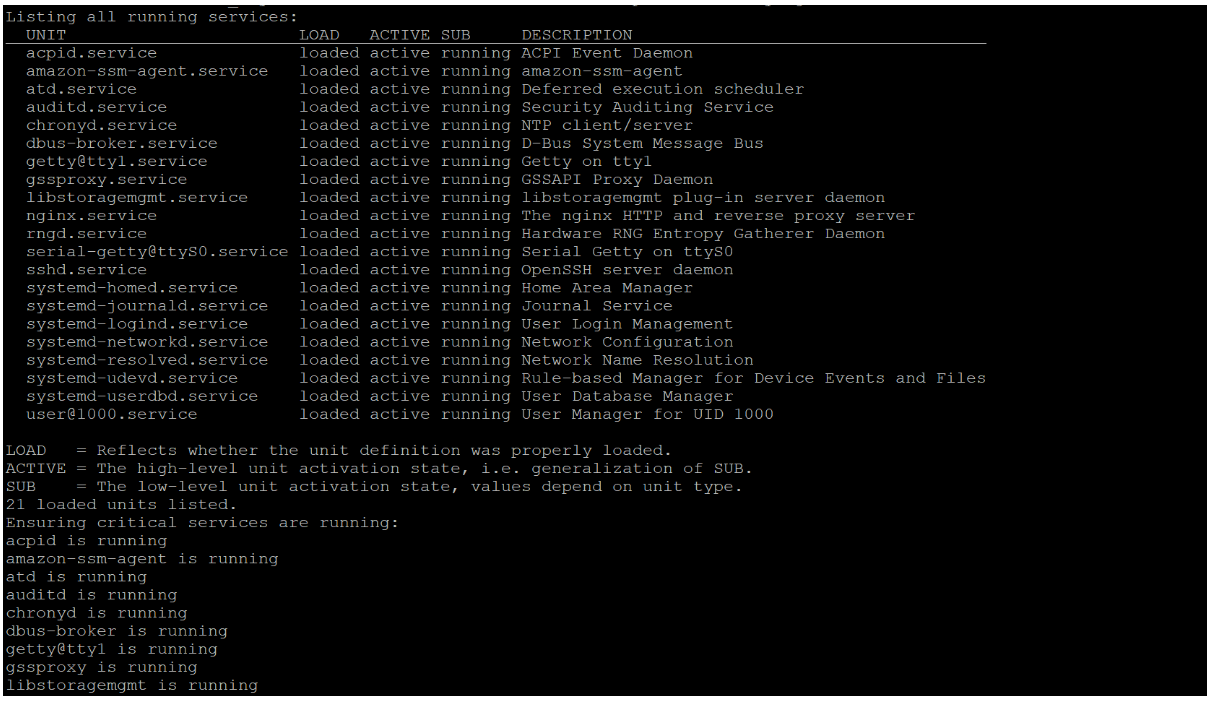
```
[ec2-user@ip-172-31-84-224 task]$ sudo ./TaskB-FileA.sh
Starting security audit...
Listing all users and groups:
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
operator
games
ftp
nobody
dbus
systemd-network
systemd-oom
systemd-resolve
sshd
rpc
libstoragemgmt
systemd-coredump
systemd-timesync
chrony
ec2-instance-connect
rpcuser
tcpdump
ec2-user
nginx
root
bin
daemon
sys
adm
tty
disk
lp
```



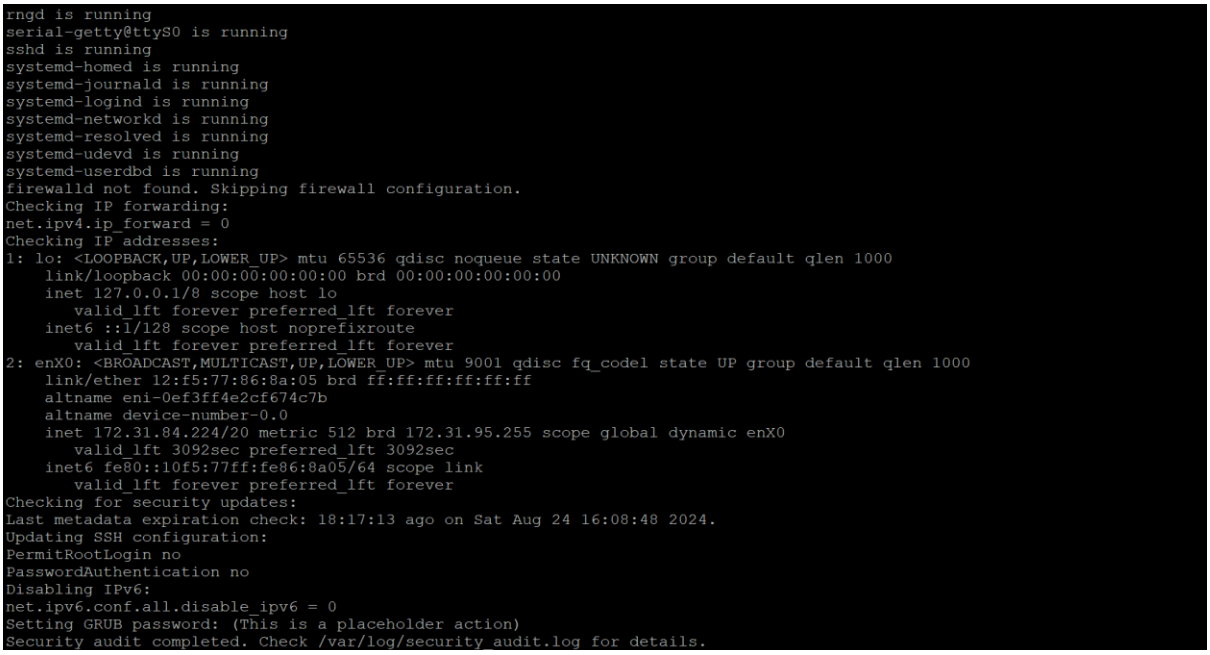
```
lp
mem
kmem
wheel
cdrom
mail
man
dialout
floppy
games
tape
video
ftp
lock
audio
users
nobody
utmp
utempter
dbus
input
kvm
render
sgx
systemd-journal
systemd-network
systemd-oom
systemd-resolve
ssh_keys
sshd
rpc
libstoragemgmt
systemd-coredump
systemd-timesync
chrony
ec2-instance-connect
stapusr
stapsys
stapdev
```



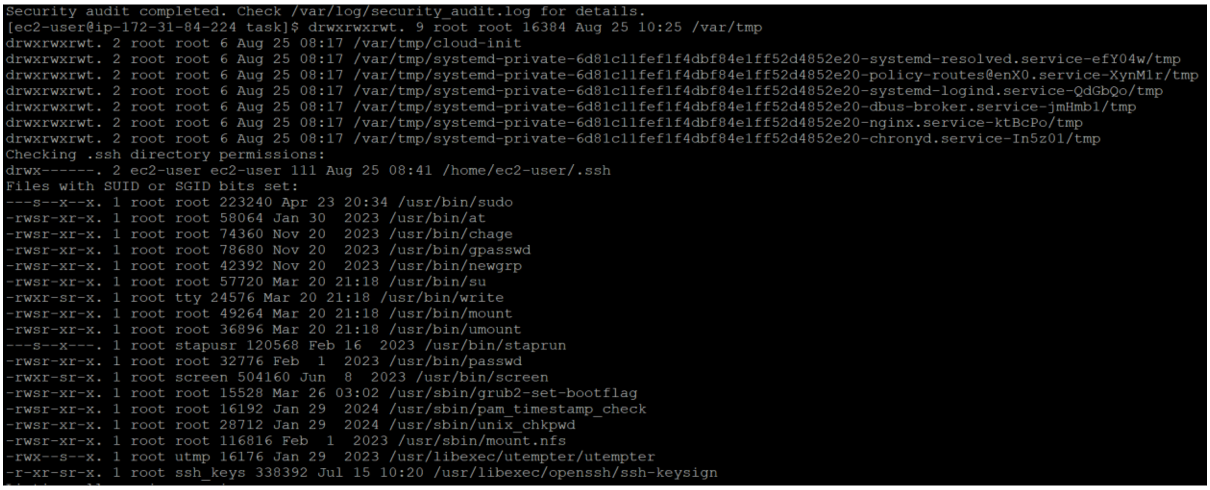
```
screen
ec2-user
nginx
Users with UID 0:
root
Users without passwords:
World-writable files and directories:
drwxrwxrwt. 13 root root 260 Aug 25 10:25 /tmp
drwxrwxrwt. 9 root root 16384 Aug 25 10:25 /var/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/cloud-init
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-resolved.service-efY04w/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-policy-routes@enX0.service-XynM1r/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-logind.service-QdGbQo/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-dbus-broker.service-jmHmb1/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-nginx.service-ktBcPo/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-chronyd.service-In5z01/tmp
Checking .ssh directory permissions:
drwx------. 2 ec2-user ec2-user 111 Aug 25 08:41 /home/ec2-user/.ssh
Files with SUID or SGID bits set:
---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
```



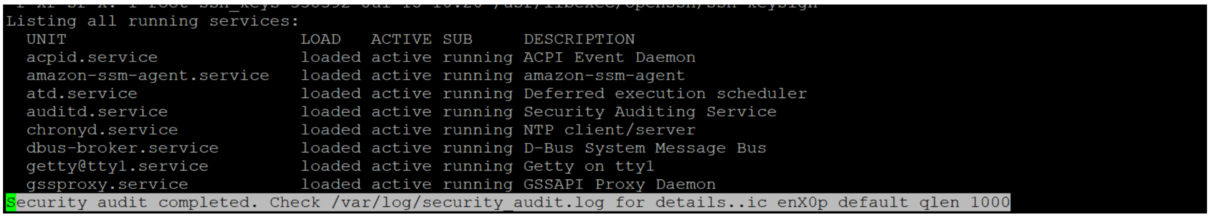
```
Listing all running services:
  UNIT                        LOAD   ACTIVE SUB     DESCRIPTION
  acpid.service               loaded active running ACPI Event Daemon
  amazon-ssm-agent.service    loaded active running amazon-ssm-agent
  atd.service                 loaded active running Deferred execution 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
  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
  nginx.service               loaded active running The nginx HTTP and reverse proxy server
  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.
Ensuring critical services are running:
acpid is running
amazon-ssm-agent is running
atd is running
auditd is running
chronyd is running
dbus-broker is running
getty@tty1 is running
gssproxy is running
libstoragemgmt is running
```



```
rngd is running
serial-getty@ttyS0 is running
sshd is running
systemd-homed is running
systemd-journald is running
systemd-logind is running
systemd-networkd is running
systemd-resolved is running
systemd-udevd is running
systemd-userdbd is running
firewalld not found. Skipping firewall configuration.
Checking IP forwarding:
net.ipv4.ip_forward = 0
Checking IP addresses:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 12:f5:77:86:8a:05 brd ff:ff:ff:ff:ff:ff
    altname eni-0ef3ff4e2cf674c7b
    altname device-number-0.0
    inet 172.31.84.224/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 3092sec preferred_lft 3092sec
    inet6 fe80::10f5:77ff:fe86:8a05/64 scope link
       valid_lft forever preferred_lft forever
Checking for security updates:
Last metadata expiration check: 18:17:13 ago on Sat Aug 24 16:08:48 2024.
Updating SSH configuration:
PermitRootLogin no
PasswordAuthentication no
Disabling IPv6:
net.ipv6.conf.all.disable_ipv6 = 0
Setting GRUB password: (This is a placeholder action)
Security audit completed. Check /var/log/security_audit.log for details.
```



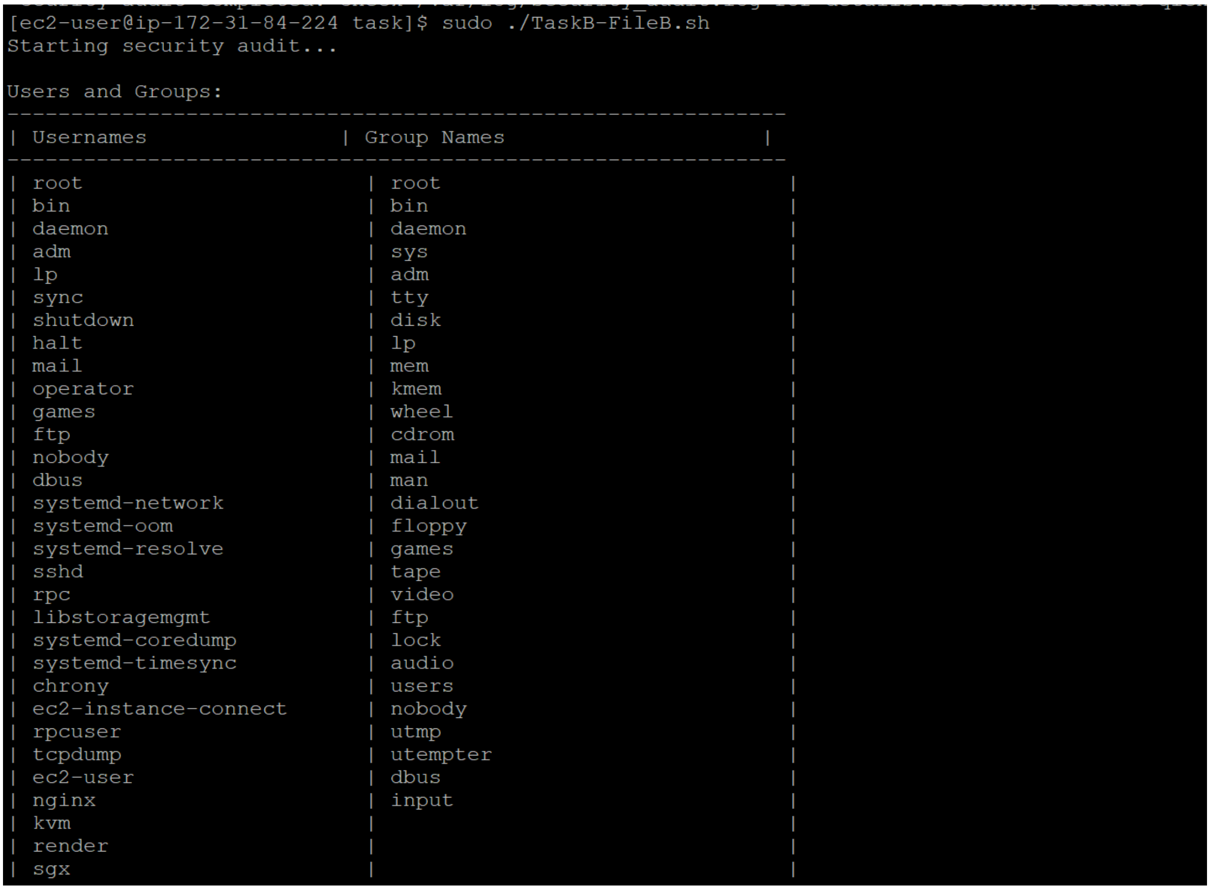
```
Security audit completed. Check /var/log/security_audit.log for details.
[ec2-user@ip-172-31-84-224 task]$ drwxrwxrwt. 9 root root 16384 Aug 25 10:25 /var/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/cloud-init
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-resolved.service-efY04w/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-policy-routes@enX0.service-XynM1r/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-logind.service-QdGbQo/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-dbus-broker.service-jmHmb1/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-nginx.service-ktBcPo/tmp
drwxrwxrwt. 2 root root 6 Aug 25 08:17 /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-chronyd.service-In5z01/tmp
Checking .ssh directory permissions:
drwx------. 2 ec2-user ec2-user 111 Aug 25 08:41 /home/ec2-user/.ssh
Files with SUID or SGID bits set:
---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
```



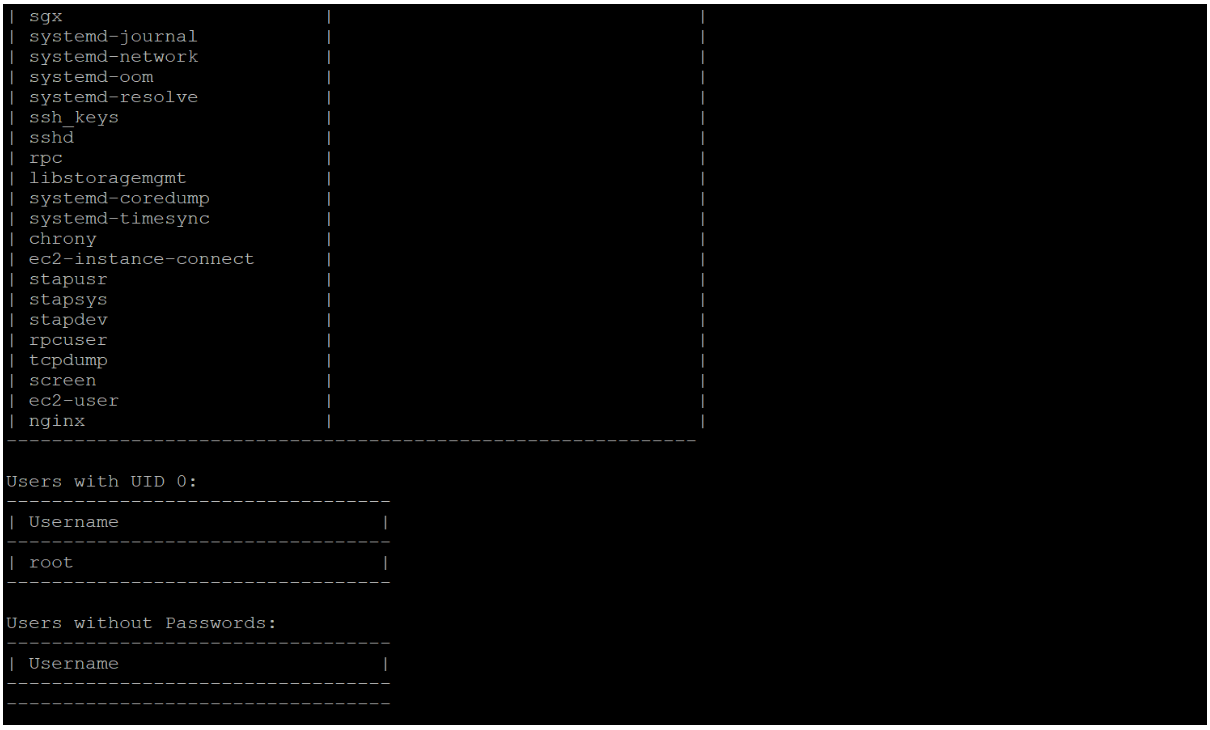
```
-r-xr-sr-x. 1 root ssh_keys 338392 Jul 15 10:20 /usr/libexec/openssh/ssh-keysign
Listing all running services:
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  acpid.service                 loaded active running ACPI Event Daemon
  amazon-ssm-agent.service      loaded active running 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
  getty@tty1.service            loaded active running Getty on tty1
  gssproxy.service              loaded active running GSSAPI Proxy Daemon
Security audit completed. Check /var/log/security_audit.log for details..ic enX0p default qlen 1000
```

Now, here is another script for same, but in customized and well organised manner. Likewise, using table format.

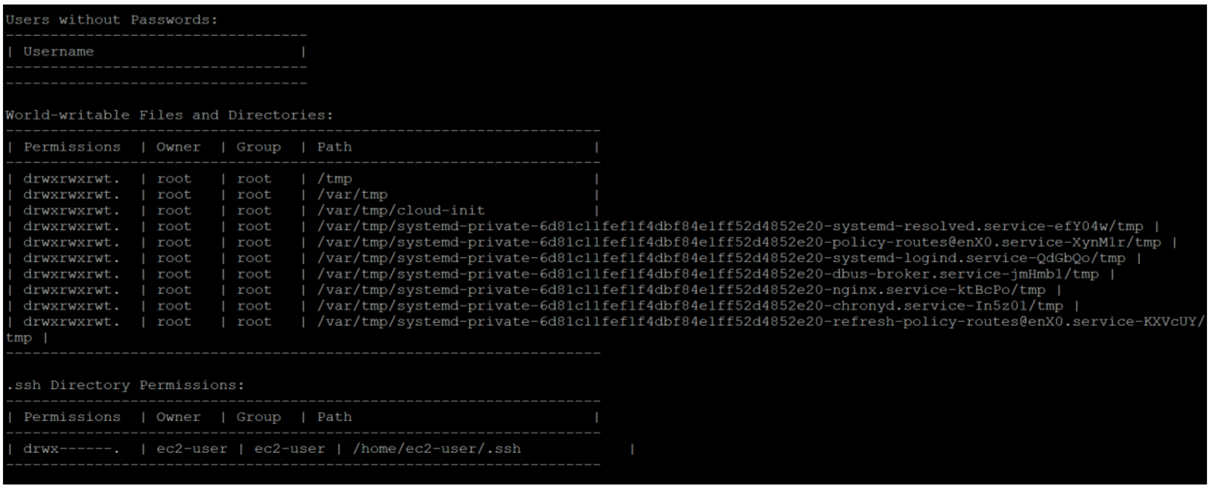
(Refer script TaskB-FileB.sh for the same from GitHub Repository)



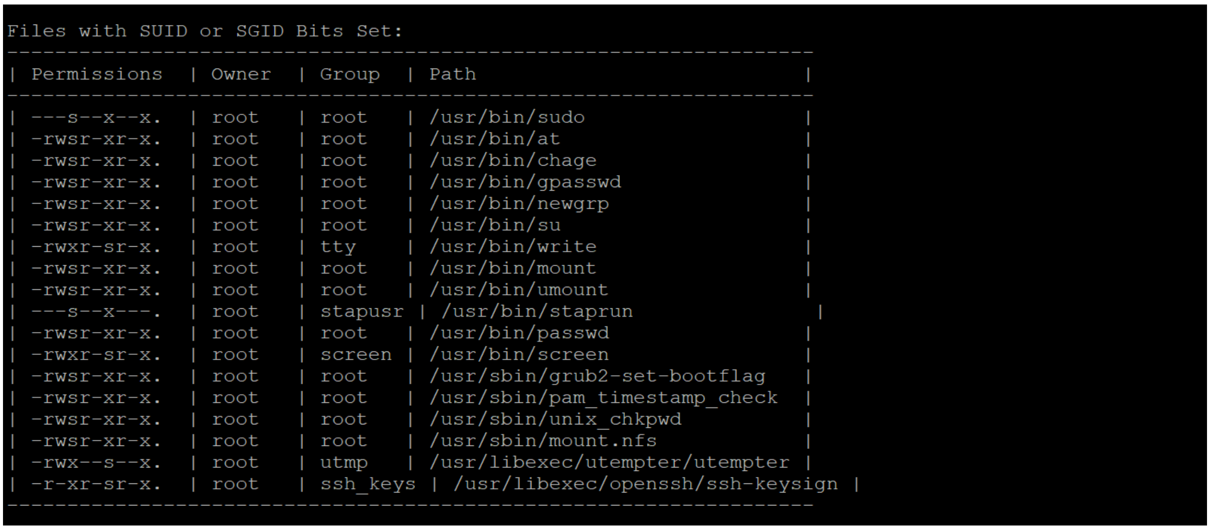
```
[ec2-user@ip-172-31-84-224 task]$ sudo ./TaskB-FileB.sh
Starting security audit...

Users and Groups:
-------------------------------------------------------------
| Usernames                  | Group Names                  |
-------------------------------------------------------------
| root                         | root                          |
| bin                          | bin                           |
| daemon                       | daemon                        |
| adm                          | sys                           |
| lp                           | adm                           |
| sync                         | tty                           |
| shutdown                     | disk                          |
| halt                         | lp                            |
| mail                         | mem                           |
| operator                     | kmem                          |
| games                        | wheel                         |
| ftp                          | cdrom                         |
| nobody                       | mail                          |
| dbus                         | man                           |
| systemd-network              | dialout                       |
| systemd-oom                  | floppy                        |
| systemd-resolve              | games                         |
| sshd                         | tape                          |
| rpc                          | video                         |
| libstoragemgmt               | ftp                           |
| systemd-coredump             | lock                          |
| systemd-timesync             | audio                         |
| chrony                       | users                         |
| ec2-instance-connect         | nobody                        |
| rpcuser                      | utmp                          |
| tcpdump                      | utempter                      |
| ec2-user                     | dbus                          |
| nginx                        | input                         |
| kvm                          |                               |
| render                       |                               |
| sgx                          |                               |
```



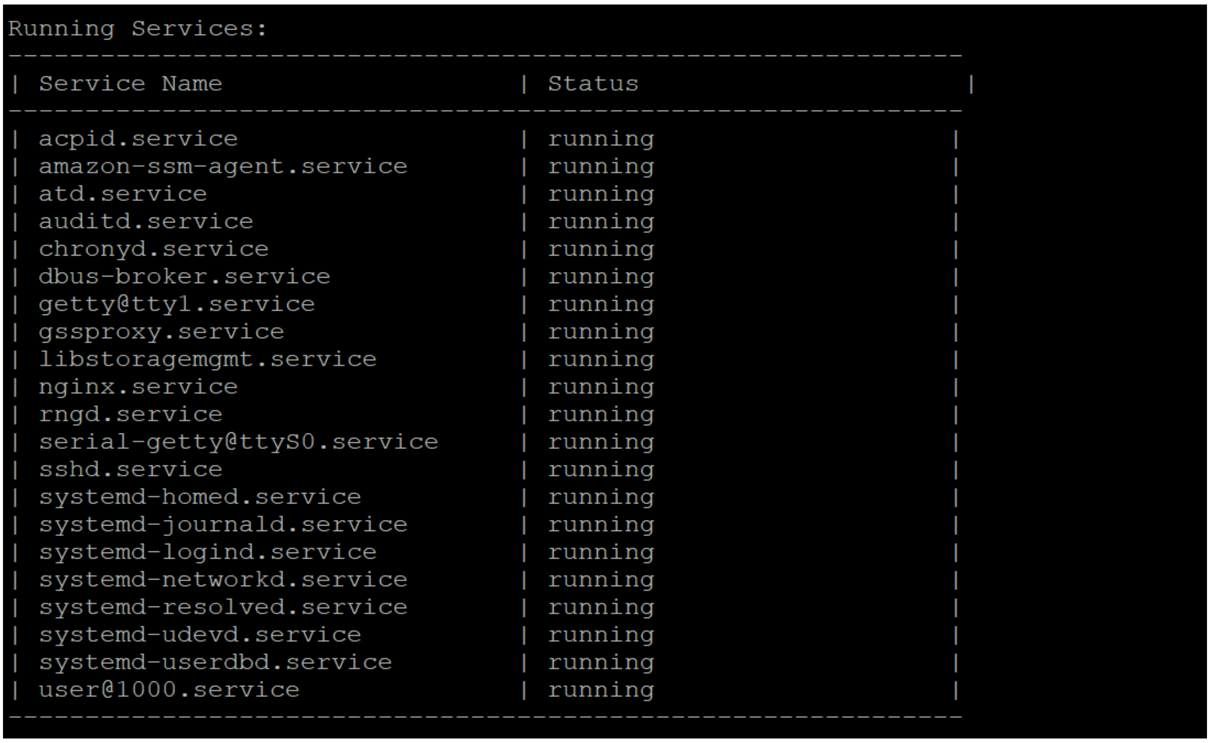
```
| sgx                          |                               |
| systemd-journal              |                               |
| systemd-network              |                               |
| systemd-oom                  |                               |
| systemd-resolve              |                               |
| ssh_keys                     |                               |
| sshd                         |                               |
| rpc                          |                               |
| libstoragemgmt               |                               |
| systemd-coredump             |                               |
| systemd-timesync             |                               |
| chrony                       |                               |
| ec2-instance-connect         |                               |
| stapusr                      |                               |
| stapsys                      |                               |
| stapdev                      |                               |
| rpcuser                      |                               |
| tcpdump                      |                               |
| screen                       |                               |
| ec2-user                     |                               |
| nginx                        |                               |
-------------------------------------------------------------

Users with UID 0:
----------------------------------
| Username                       |
----------------------------------
| root                           |
----------------------------------

Users without Passwords:
----------------------------------
| Username                       |
----------------------------------
----------------------------------
```



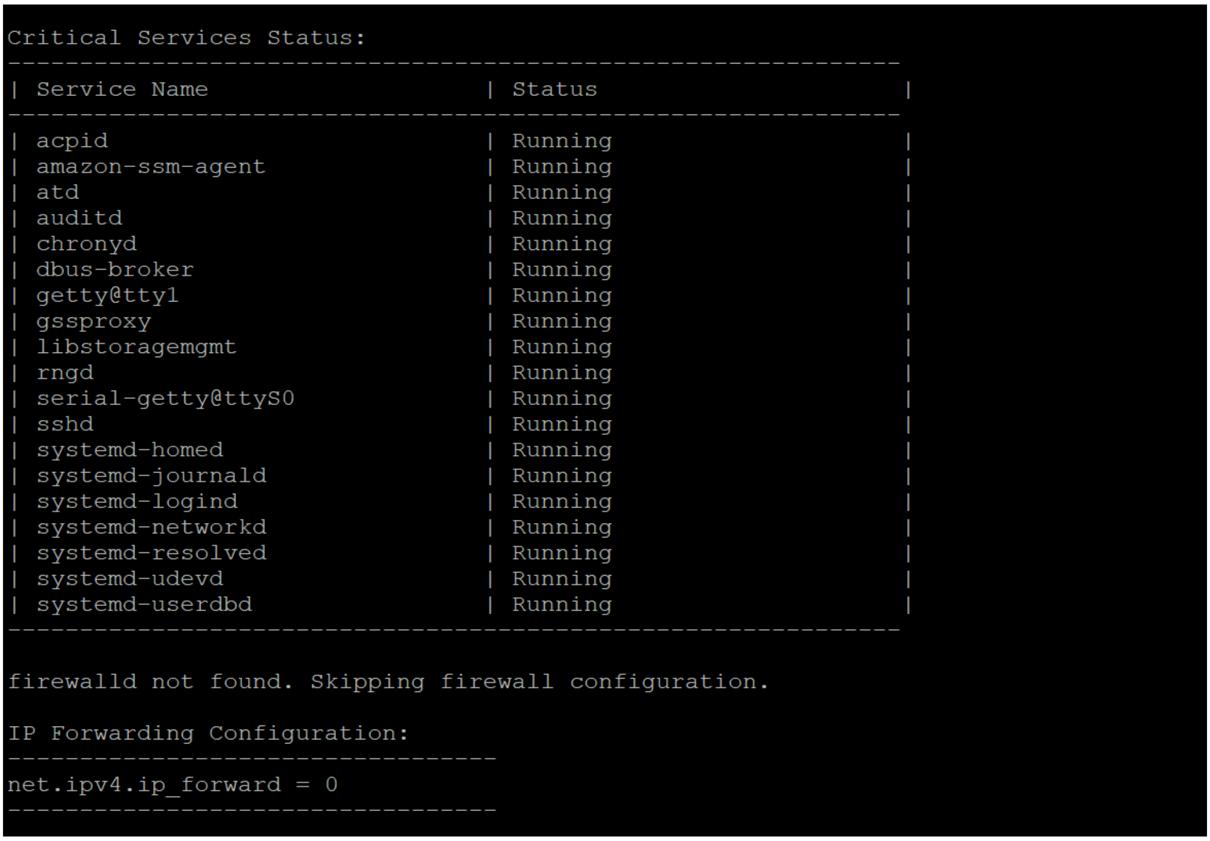
```
Users without Passwords:
----------------------------------
| Username                       |
----------------------------------
----------------------------------

World-writable Files and Directories:
-------------------------------------------------------------------
| Permissions  | Owner  | Group  | Path                           |
-------------------------------------------------------------------
| drwxrwxrwt.  | root   | root   | /tmp                           |
| drwxrwxrwt.  | root   | root   | /var/tmp                       |
| drwxrwxrwt.  | root   | root   | /var/tmp/cloud-init            |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-resolved.service-efY04w/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-policy-routes@enX0.service-XynM1r/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-systemd-logind.service-QdGbQo/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-dbus-broker.service-jmHmb1/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-nginx.service-ktBcPo/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-chronyd.service-In5z01/tmp |
| drwxrwxrwt.  | root   | root   | /var/tmp/systemd-private-6d81c11fef1f4dbf84e1ff52d4852e20-refresh-policy-routes@enX0.service-KXVcUY/
tmp |
-------------------------------------------------------------------

.ssh Directory Permissions:
-------------------------------------------------------------------
| Permissions  | Owner  | Group  | Path                           |
-------------------------------------------------------------------
| drwx------.  | ec2-user | ec2-user | /home/ec2-user/.ssh           |
-------------------------------------------------------------------
```



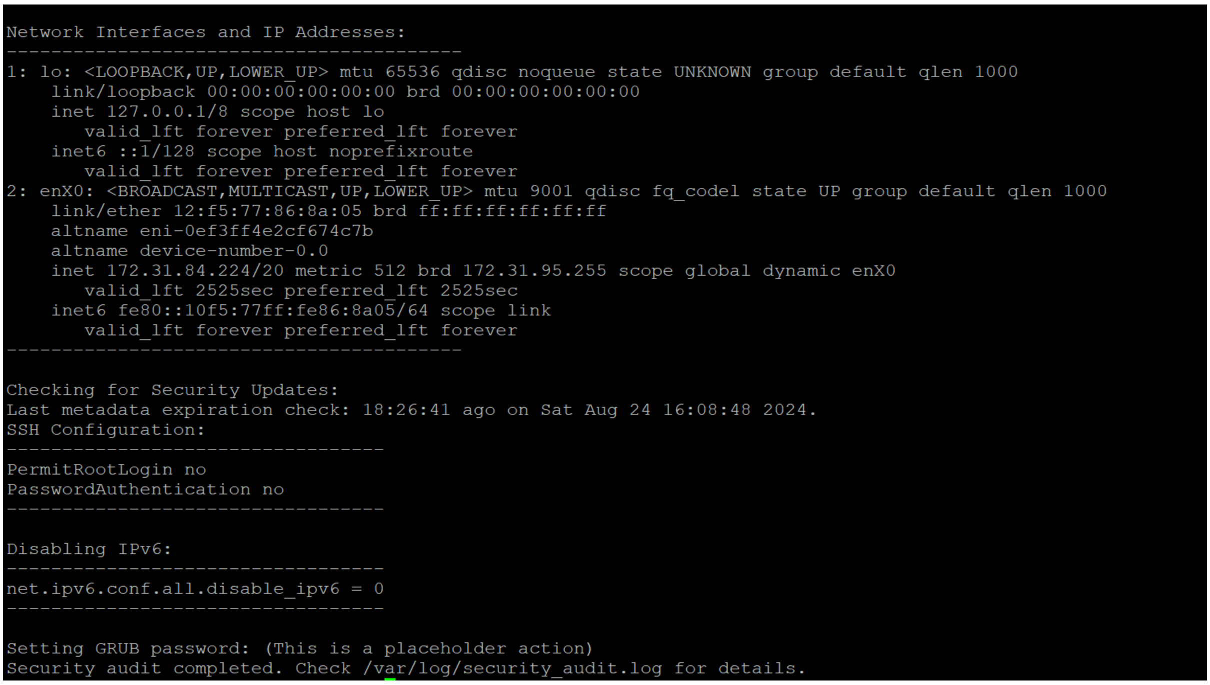
```
Files with SUID or SGID Bits Set:
-------------------------------------------------------------------
| Permissions  | Owner  | Group  | Path                           |
-------------------------------------------------------------------
| ---s--x--x.  | root   | root   | /usr/bin/sudo                  |
| -rwsr-xr-x.  | root   | root   | /usr/bin/at                    |
| -rwsr-xr-x.  | root   | root   | /usr/bin/chage                 |
| -rwsr-xr-x.  | root   | root   | /usr/bin/gpasswd               |
| -rwsr-xr-x.  | root   | root   | /usr/bin/newgrp                |
| -rwsr-xr-x.  | root   | root   | /usr/bin/su                    |
| -rwxr-sr-x.  | root   | tty    | /usr/bin/write                 |
| -rwsr-xr-x.  | root   | root   | /usr/bin/mount                 |
| -rwsr-xr-x.  | root   | root   | /usr/bin/umount                |
| ---s--x---.  | root   | stapusr | /usr/bin/staprun               |
| -rwsr-xr-x.  | root   | root   | /usr/bin/passwd                |
| -rwxr-sr-x.  | root   | screen | /usr/bin/screen                |
| -rwsr-xr-x.  | root   | root   | /usr/sbin/grub2-set-bootflag   |
| -rwsr-xr-x.  | root   | root   | /usr/sbin/pam_timestamp_check  |
| -rwsr-xr-x.  | root   | root   | /usr/sbin/unix_chkpwd          |
| -rwsr-xr-x.  | root   | root   | /usr/sbin/mount.nfs            |
| -rwx--s--x.  | root   | utmp   | /usr/libexec/utempter/utempter |
| -r-xr-sr-x.  | root   | ssh_keys | /usr/libexec/openssh/ssh-keysign |
-------------------------------------------------------------------
```



```
Running Services:
--------------------------------------------------------------
| Service Name                     | Status                    |
--------------------------------------------------------------
| acpid.service                    | running                  |
| amazon-ssm-agent.service         | running                  |
| atd.service                      | running                  |
| auditd.service                   | running                  |
| chronyd.service                  | running                  |
| dbus-broker.service              | running                  |
| getty@tty1.service               | running                  |
| gssproxy.service                 | running                  |
| libstoragemgmt.service           | running                  |
| nginx.service                    | running                  |
| rngd.service                     | running                  |
| serial-getty@ttyS0.service       | running                  |
| sshd.service                     | running                  |
| systemd-homed.service            | running                  |
| systemd-journald.service         | running                  |
| systemd-logind.service           | running                  |
| systemd-networkd.service         | running                  |
| systemd-resolved.service         | running                  |
| systemd-udevd.service            | running                  |
| systemd-userdbd.service          | running                  |
| user@1000.service                | running                  |
--------------------------------------------------------------
```



```
Critical Services Status:
-------------------------------------------------------------
| Service Name                     | Status                   |
-------------------------------------------------------------
| acpid                            | Running                  |
| amazon-ssm-agent                 | Running                  |
| atd                              | Running                  |
| auditd                           | Running                  |
| chronyd                          | Running                  |
| dbus-broker                      | Running                  |
| getty@tty1                       | Running                  |
| gssproxy                         | Running                  |
| libstoragemgmt                   | Running                  |
| rngd                             | Running                  |
| serial-getty@ttyS0               | Running                  |
| sshd                             | Running                  |
| systemd-homed                    | Running                  |
| systemd-journald                 | Running                  |
| systemd-logind                   | Running                  |
| systemd-networkd                 | Running                  |
| systemd-resolved                 | Running                  |
| systemd-udevd                    | Running                  |
| systemd-userdbd                  | Running                  |
-------------------------------------------------------------

firewalld not found. Skipping firewall configuration.

IP Forwarding Configuration:
---------------------------------
net.ipv4.ip_forward = 0
---------------------------------
```



```
Network Interfaces and IP Addresses:
-----------------------------------------
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 12:f5:77:86:8a:05 brd ff:ff:ff:ff:ff:ff
    altname eni-0ef3ff4e2cf674c7b
    altname device-number-0.0
    inet 172.31.84.224/20 metric 512 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 2525sec preferred_lft 2525sec
    inet6 fe80::10f5:77ff:fe86:8a05/64 scope link
       valid_lft forever preferred_lft forever
-----------------------------------------

Checking for Security Updates:
Last metadata expiration check: 18:26:41 ago on Sat Aug 24 16:08:48 2024.
SSH Configuration:
----------------------------------
PermitRootLogin no
PasswordAuthentication no
----------------------------------

Disabling IPv6:
----------------------------------
net.ipv6.conf.all.disable_ipv6 = 0
----------------------------------

Setting GRUB password: (This is a placeholder action)
Security audit completed. Check /var/log/security_audit.log for details.
```

These security audits are also stored on server logs

We can see logs by

⇨ sudo nano/var/log/security_audit.log