ETHICAL HACKING PROJECT

Cloud Server Hardening & Secure Access (SSH + Firewall + IAM)

Objective :. The objective of this project is to implement comprehensive Linux server hardening techniques by deploying, configuring, and securing an Ubuntu-based cloud environment. The goal is to minimize attack surfaces by enforcing least-privilege user management, enabling SSH key-based authentication, configuring firewalls using UFW, and implementing real-time intrusion prevention and audit mechanisms with Fail2Ban and Auditd.

Through this project, a secure and monitored system architecture is achieved where different human roles such as administrators, developers, auditors, and guests are assigned role-specific privileges and restrictions, ensuring a balanced combination of security, accessibility, and accountability.

Prerequisites

- Ubuntu Server 20.04 or 22.04 (cloud VM or VMware/VirtualBox)
- SSH client (Linux/macOS Terminal, or Windows PowerShell)
- Local machine to generate SSH keys
- Internet access for package installation

High-level steps :

1. Install and update the server packages
2. Create an administrative user (IAM-like)
3. Harden SSH (disable root login + enable key auth)
4. Configure UFW to allow only SSH and deny other incoming traffic
5. Install and configure Fail2Ban to block brute-force attempts
6. Install and enable auditd to log user logins and sudo commands
7. (Optional) Ship logs to Wazuh/SIEM

Commands used :

Initial update and essentials

```
sudo apt update && sudo apt upgrade -y    # update packages
sudo apt install -y wget curl git vim     # useful utilities
```

Install and start SSH server (if missing)

```
sudo apt install -y openssh-server
sudo systemctl enable --now ssh
hostname -I    # show server IP for SSH
```

Create a new administrative user (example: projectuser01)

Use a username that is unique for your submission.

```
sudo adduser projectuser01
# follow prompts to set a password and optional details
```

Grant sudo privileges using a dedicated sudoers file:

```
# create sudoers entry (run as a sudo-capable user)
echo "projectuser01 ALL=(ALL:ALL) NOPASSWD:ALL" | sudo tee /etc/sudoers.d/projectuser01 > /dev/null
sudo chmod 440 /etc/sudoers.d/projectuser01
```

Verify:

```
sudo cat /etc/sudoers.d/projectuser01
```

Harden SSH — disable root login and disable password auth (key-only)

```
sudo sed -i 's/^#\?PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
sudo sed -i 's/^#\?PasswordAuthentication.*/PasswordAuthentication no/' /etc/ssh/sshd_config
sudo systemctl restart ssh
```

# verify

grep -Ei 'PermitRootLogin|PasswordAuthentication' /etc/ssh/sshd_config

SSH key generation and placement (local → server)

On your **local machine**:

ssh-keygen -t rsa -b 4096 -f ~/.ssh/project_key_$(date +%Y%m%d) -C "project_submission"

Copy the public key to the server (recommended):

ssh-copy-id -i ~/.ssh/project_key_$(date +%Y%m%d).pub projectuser01@<SERVER_IP>

Or copy manually:

# on server (as sudo or projectuser01)

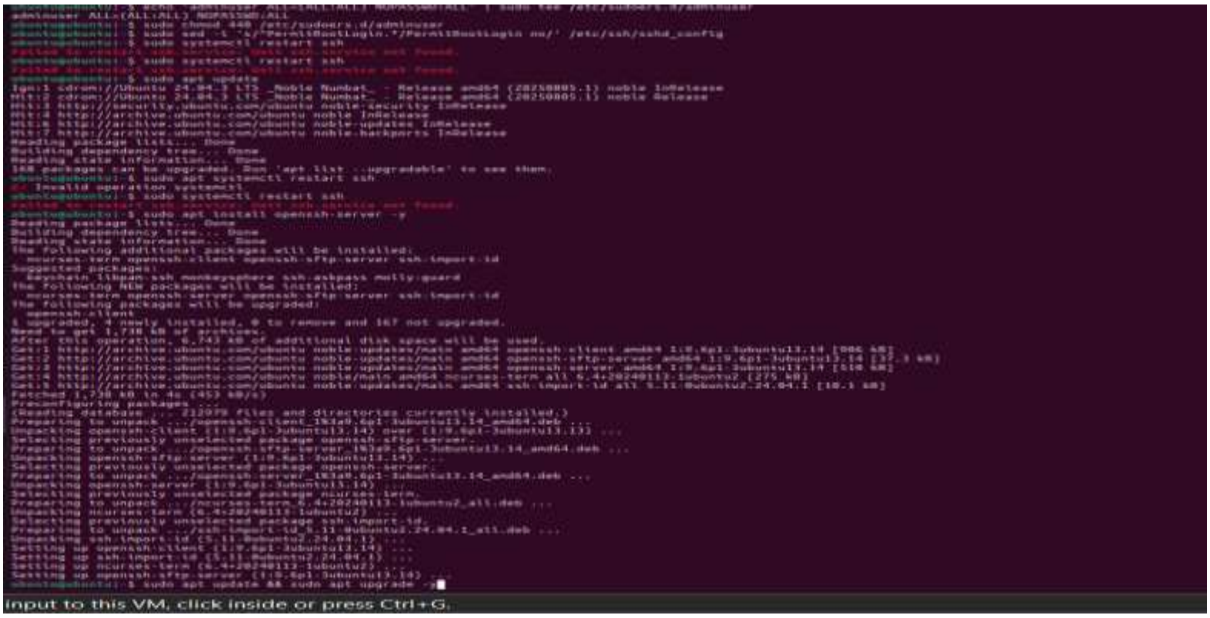
sudo mkdir -p /home/projectuser01/.ssh

sudo nano /home/projectuser01/.ssh/authorized_keys   # paste public key

sudo chown -R projectuser01:projectuser01 /home/projectuser01/.ssh

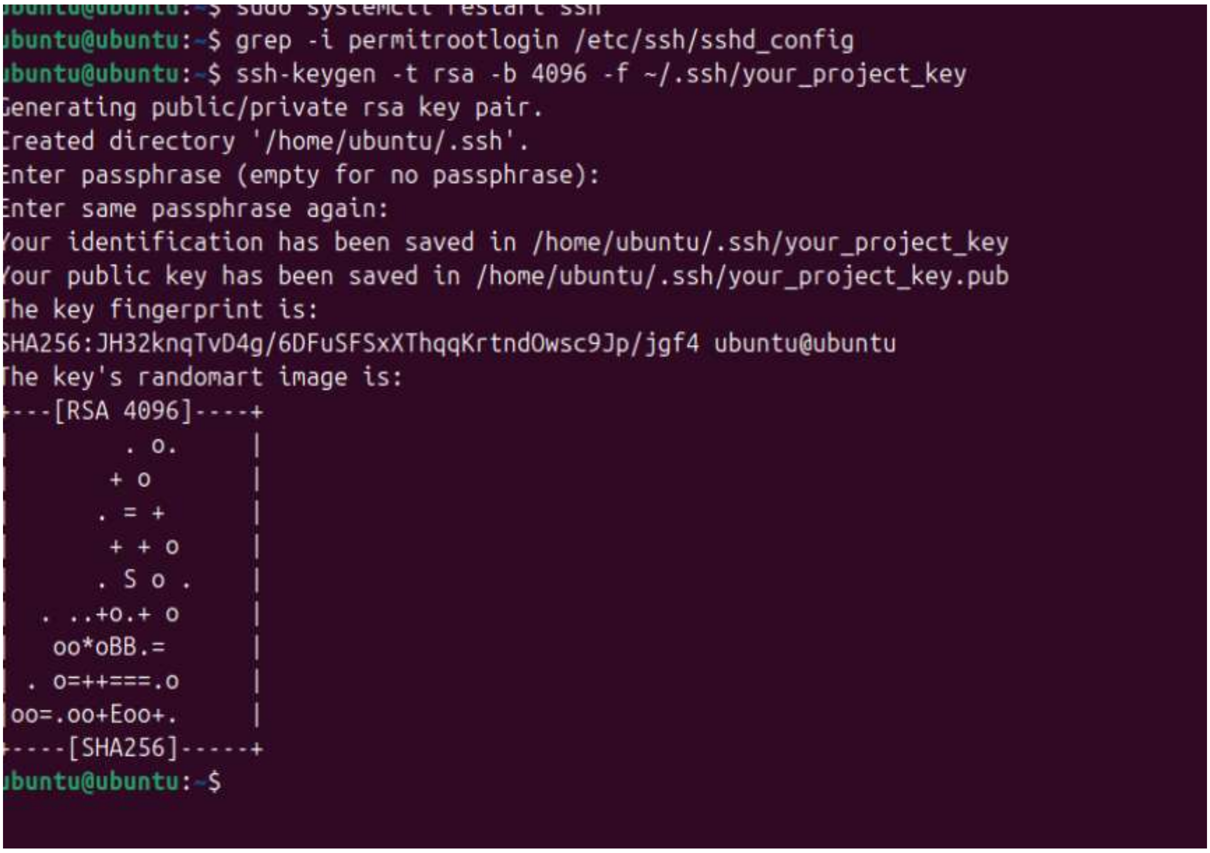
sudo chmod 700 /home/projectuser01/.ssh

sudo chmod 600 /home/projectuser01/.ssh/authorized_keys



```
ubuntu@ubuntu:~$ echo 'adminuser ALL=(ALL:ALL) NOPASSWD:ALL' | sudo tee /etc/sudoers.d/adminuser
adminuser ALL=(ALL:ALL) NOPASSWD:ALL
ubuntu@ubuntu:~$ sudo chmod 440 /etc/sudoers.d/adminuser
ubuntu@ubuntu:~$ sudo sed -i 's/^PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
ubuntu@ubuntu:~$ sudo systemctl restart ssh
Failed to restart ssh.service: Unit ssh.service not found.
ubuntu@ubuntu:~$ sudo systemctl restart ssh
Failed to restart ssh.service: Unit ssh.service not found.
ubuntu@ubuntu:~$ sudo apt update
Ign:1 cdrom://Ubuntu 24.04.3 LTS _Noble Numbat_ - Release amd64 (20250805.1) noble InRelease
Hit:2 cdrom://Ubuntu 24.04.3 LTS _Noble Numbat_ - Release amd64 (20250805.1) noble Release
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:6 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
168 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ubuntu:~$ sudo apt systemctl restart ssh
E: Invalid operation systemctl
ubuntu@ubuntu:~$ sudo systemctl restart ssh
Failed to restart ssh.service: Unit ssh.service not found.
ubuntu@ubuntu:~$ sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 167 not upgraded.
Need to get 1,738 kB of archives.
After this operation, 6,743 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.14 [906 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ssh-import-id all 5.11-0ubuntu2.24.04.1 [10.1 kB]
Fetched 1,738 kB in 4s (453 kB/s)
Preconfiguring packages ...
(Reading database ... 212979 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a9.6p1-3ubuntu13.14_amd64.deb ...
Unpacking openssh-client (1:9.6p1-3ubuntu13.14) over (1:9.6p1-3ubuntu13.13) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a9.6p1-3ubuntu13.14_amd64.deb ...
Unpacking openssh-sftp-server (1:9.6p1-3ubuntu13.14) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.6p1-3ubuntu13.14_amd64.deb ...
Unpacking openssh-server (1:9.6p1-3ubuntu13.14) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.4+20240113-1ubuntu2_all.deb ...
Unpacking ncurses-term (6.4+20240113-1ubuntu2) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu2.24.04.1_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up openssh-client (1:9.6p1-3ubuntu13.14) ...
Setting up ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up ncurses-term (6.4+20240113-1ubuntu2) ...
Setting up openssh-sftp-server (1:9.6p1-3ubuntu13.14) ...
ubuntu@ubuntu:~$ sudo apt update && sudo apt upgrade -y
```

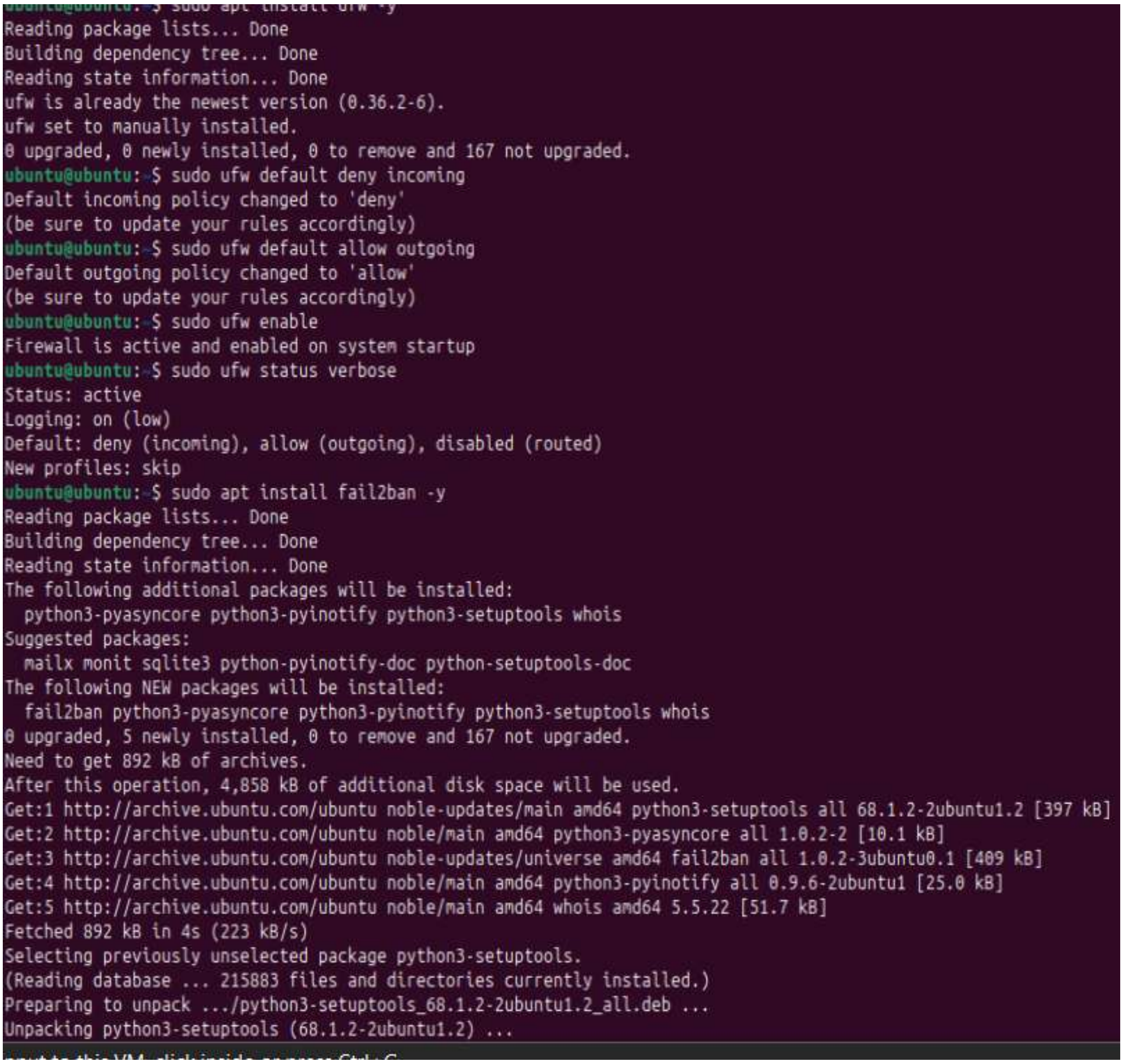
input to this VM, click inside or press Ctrl+G.



```
ubuntu@ubuntu:~$ sudo systemctl restart ssh
ubuntu@ubuntu:~$ grep -i permitrootlogin /etc/ssh/sshd_config
ubuntu@ubuntu:~$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/your_project_key
Generating public/private rsa key pair.
Created directory '/home/ubuntu/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/your_project_key
Your public key has been saved in /home/ubuntu/.ssh/your_project_key.pub
The key fingerprint is:
SHA256:JH32knqTvD4g/6DFuSFSxXThqqKrtndOwsc9Jp/jgf4 ubuntu@ubuntu
The key's randomart image is:
+---[RSA 4096]----+
|        . o.     |
|       + o       |
|      . = +      |
|       + + o     |
|      . S o .    |
|  . ..+o.+ o     |
|   oo*oBB.=      |
|  . o=++===.o    |
|oo=.oo+Eoo+.     |
+----[SHA256]-----+
ubuntu@ubuntu:~$
```

Configure UFW (firewall)

```
sudo apt install -y ufw

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow OpenSSH    # allows ssh (port 22) only

sudo ufw enable

sudo ufw status verbose
```



```
ubuntu@ubuntu:~$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 167 not upgraded.
ubuntu@ubuntu:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
ubuntu@ubuntu:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
ubuntu@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
ubuntu@ubuntu:~$ sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify python3-setuptools whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc python-setuptools-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify python3-setuptools whois
0 upgraded, 5 newly installed, 0 to remove and 167 not upgraded.
Need to get 892 kB of archives.
After this operation, 4,858 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-setuptools all 68.1.2-2ubuntu1.2 [397 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 892 kB in 4s (223 kB/s)
Selecting previously unselected package python3-setuptools.
(Reading database ... 215883 files and directories currently installed.)
Preparing to unpack .../python3-setuptools_68.1.2-2ubuntu1.2_all.deb ...
Unpacking python3-setuptools (68.1.2-2ubuntu1.2) ...
```

Install and configure Fail2Ban :

```
sudo apt install -y fail2ban
```

```
sudo systemctl enable --now fail2ban
```

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

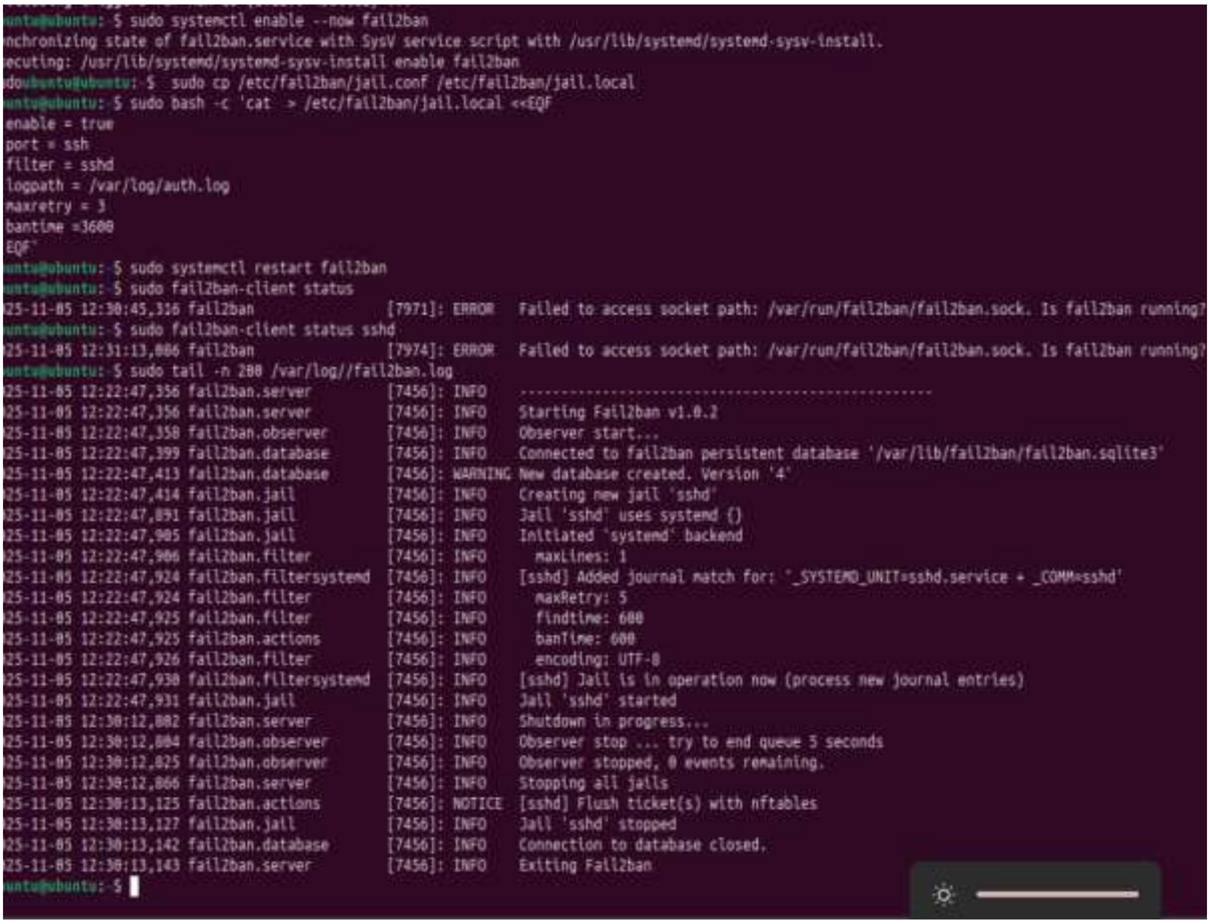
Edit /etc/fail2ban/jail.local and ensure the [sshd] section contains:

```
[sshd]

enabled = true

port    = ssh

filter  = sshd
```

```
logpath = /var/log/auth.log

maxretry = 3

bantime = 3600
```

Then restart:

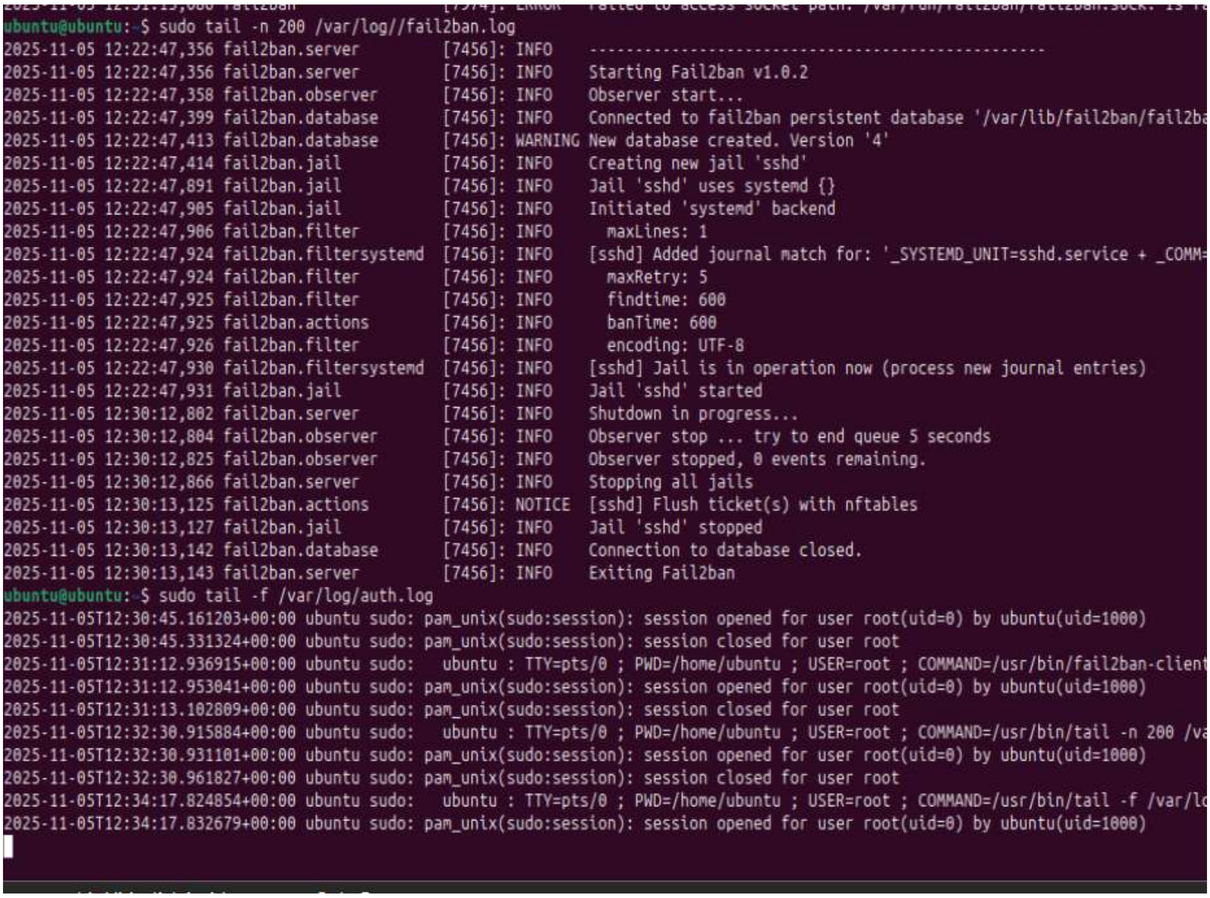
```
sudo systemctl restart fail2ban

sudo fail2ban-client status sshd

sudo tail -n 200 /var/log/fail2ban.log
```



```
untu@ubuntu:~$ sudo systemctl enable --now fail2ban
nchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
ecuting: /usr/lib/systemd/systemd-sysv-install enable fail2ban
doubuntu@ubuntu:~$  sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
untu@ubuntu:~$ sudo bash -c 'cat  > /etc/fail2ban/jail.local <<EOF
enable = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime =3600
EOF'
untu@ubuntu:~$ sudo systemctl restart fail2ban
untu@ubuntu:~$ sudo fail2ban-client status
25-11-05 12:30:45,316 fail2ban                [7971]: ERROR   Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?
untu@ubuntu:~$ sudo fail2ban-client status sshd
25-11-05 12:31:13,006 fail2ban                [7974]: ERROR   Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?
untu@ubuntu:~$ sudo tail -n 200 /var/log//fail2ban.log
25-11-05 12:22:47,356 fail2ban.server         [7456]: INFO    --------------------------------------------------
25-11-05 12:22:47,356 fail2ban.server         [7456]: INFO    Starting Fail2ban v1.0.2
25-11-05 12:22:47,358 fail2ban.observer       [7456]: INFO    Observer start...
25-11-05 12:22:47,399 fail2ban.database       [7456]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
25-11-05 12:22:47,413 fail2ban.database       [7456]: WARNING New database created. Version '4'
25-11-05 12:22:47,414 fail2ban.jail           [7456]: INFO    Creating new jail 'sshd'
25-11-05 12:22:47,891 fail2ban.jail           [7456]: INFO    Jail 'sshd' uses systemd {}
25-11-05 12:22:47,905 fail2ban.jail           [7456]: INFO    Initiated 'systemd' backend
25-11-05 12:22:47,906 fail2ban.filter         [7456]: INFO      maxLines: 1
25-11-05 12:22:47,924 fail2ban.filtersystemd  [7456]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
25-11-05 12:22:47,924 fail2ban.filter         [7456]: INFO      maxRetry: 5
25-11-05 12:22:47,925 fail2ban.filter         [7456]: INFO      findtime: 600
25-11-05 12:22:47,925 fail2ban.actions        [7456]: INFO      banTime: 600
25-11-05 12:22:47,926 fail2ban.filter         [7456]: INFO      encoding: UTF-8
25-11-05 12:22:47,930 fail2ban.filtersystemd  [7456]: INFO    [sshd] Jail is in operation now (process new journal entries)
25-11-05 12:22:47,931 fail2ban.jail           [7456]: INFO    Jail 'sshd' started
25-11-05 12:30:12,802 fail2ban.server         [7456]: INFO    Shutdown in progress...
25-11-05 12:30:12,804 fail2ban.observer       [7456]: INFO    Observer stop ... try to end queue 5 seconds
25-11-05 12:30:12,825 fail2ban.observer       [7456]: INFO    Observer stopped, 0 events remaining.
25-11-05 12:30:12,866 fail2ban.server         [7456]: INFO    Stopping all jails
25-11-05 12:30:13,125 fail2ban.actions        [7456]: NOTICE  [sshd] Flush ticket(s) with nftables
25-11-05 12:30:13,127 fail2ban.jail           [7456]: INFO    Jail 'sshd' stopped
25-11-05 12:30:13,142 fail2ban.database       [7456]: INFO    Connection to database closed.
25-11-05 12:30:13,143 fail2ban.server         [7456]: INFO    Exiting Fail2ban
untu@ubuntu:~$
```

Simulate a ban (from another machine or change IP) by attempting several bad SSH logins and then check ` fail2ban-client status sshd` .

```
sudo tail -f /var/log/auth.log
```



```
ubuntu@ubuntu:~$ sudo tail -n 200 /var/log//fail2ban.log
2025-11-05 12:22:47,356 fail2ban.server        [7456]: INFO    -----------------------------------------------
2025-11-05 12:22:47,356 fail2ban.server        [7456]: INFO    Starting Fail2ban v1.0.2
2025-11-05 12:22:47,358 fail2ban.observer      [7456]: INFO    Observer start...
2025-11-05 12:22:47,399 fail2ban.database      [7456]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ba
2025-11-05 12:22:47,413 fail2ban.database      [7456]: WARNING New database created. Version '4'
2025-11-05 12:22:47,414 fail2ban.jail          [7456]: INFO    Creating new jail 'sshd'
2025-11-05 12:22:47,891 fail2ban.jail          [7456]: INFO    Jail 'sshd' uses systemd {}
2025-11-05 12:22:47,905 fail2ban.jail          [7456]: INFO    Initiated 'systemd' backend
2025-11-05 12:22:47,906 fail2ban.filter        [7456]: INFO      maxLines: 1
2025-11-05 12:22:47,924 fail2ban.filtersystemd [7456]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=
2025-11-05 12:22:47,924 fail2ban.filter        [7456]: INFO      maxRetry: 5
2025-11-05 12:22:47,925 fail2ban.filter        [7456]: INFO      findtime: 600
2025-11-05 12:22:47,925 fail2ban.actions       [7456]: INFO      banTime: 600
2025-11-05 12:22:47,926 fail2ban.filter        [7456]: INFO      encoding: UTF-8
2025-11-05 12:22:47,930 fail2ban.filtersystemd [7456]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-11-05 12:22:47,931 fail2ban.jail          [7456]: INFO    Jail 'sshd' started
2025-11-05 12:30:12,802 fail2ban.server        [7456]: INFO    Shutdown in progress...
2025-11-05 12:30:12,804 fail2ban.observer      [7456]: INFO    Observer stop ... try to end queue 5 seconds
2025-11-05 12:30:12,825 fail2ban.observer      [7456]: INFO    Observer stopped, 0 events remaining.
2025-11-05 12:30:12,866 fail2ban.server        [7456]: INFO    Stopping all jails
2025-11-05 12:30:13,125 fail2ban.actions       [7456]: NOTICE  [sshd] Flush ticket(s) with nftables
2025-11-05 12:30:13,127 fail2ban.jail          [7456]: INFO    Jail 'sshd' stopped
2025-11-05 12:30:13,142 fail2ban.database      [7456]: INFO    Connection to database closed.
2025-11-05 12:30:13,143 fail2ban.server        [7456]: INFO    Exiting Fail2ban
ubuntu@ubuntu:~$ sudo tail -f /var/log/auth.log
2025-11-05T12:30:45.161203+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-11-05T12:30:45.331324+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root
2025-11-05T12:31:12.936915+00:00 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/fail2ban-client
2025-11-05T12:31:12.953041+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-11-05T12:31:13.102809+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root
2025-11-05T12:32:30.915884+00:00 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -n 200 /va
2025-11-05T12:32:30.931101+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2025-11-05T12:32:30.961827+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root
2025-11-05T12:34:17.824854+00:00 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -f /var/lo
2025-11-05T12:34:17.832679+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
```

Install and enable auditd (logging & auditing)

sudo apt install -y auditd audispd-plugins

sudo systemctl enable --now auditd

Add focused audit rules:

# watch sudo binary execs

sudo auditctl -w /usr/bin/sudo -p x -k sudo_exec

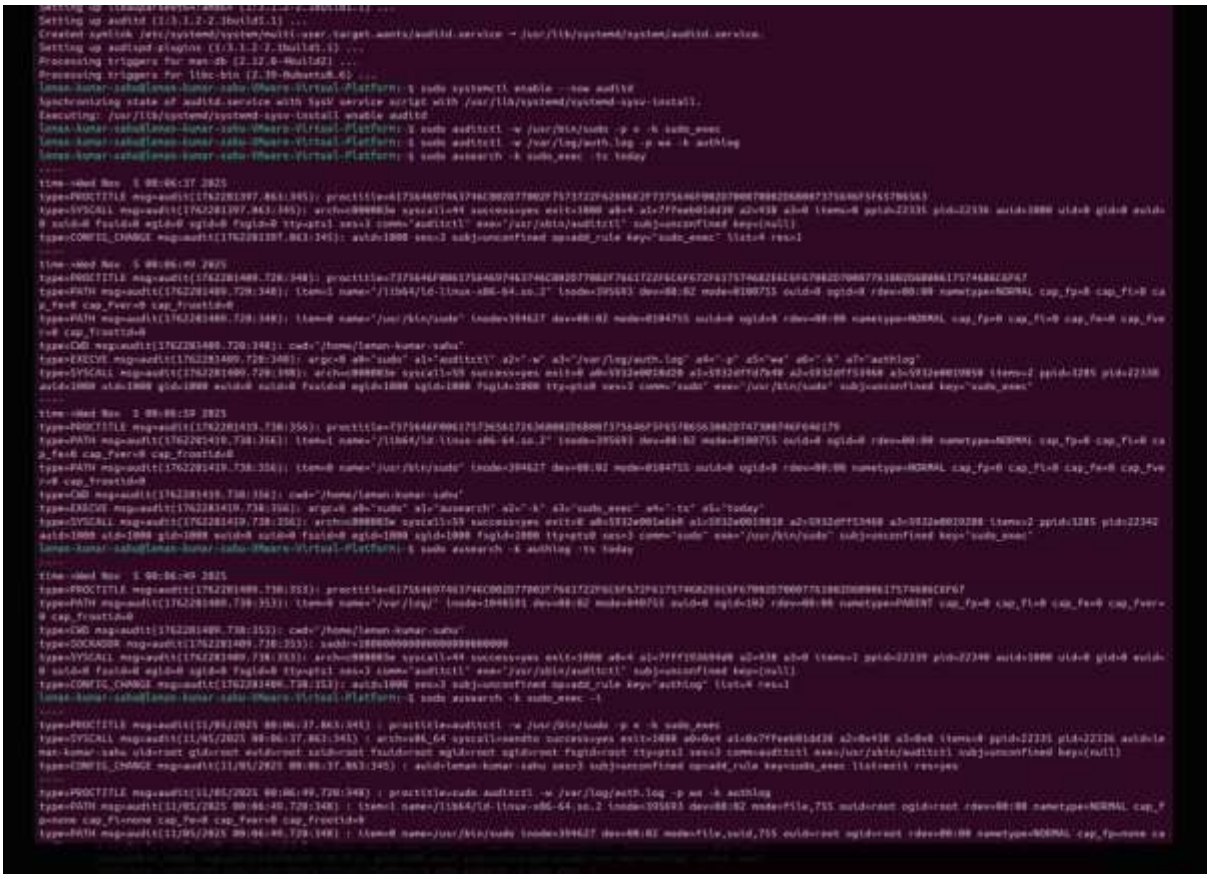
# watch authentication log changes

sudo auditctl -w /var/log/auth.log -p wa -k authlog

Query today's records:

sudo ausearch -k sudo_exec -ts today

sudo ausearch -k authlog -ts today



```
Setting up auditd (1:3.1.2-2.1build1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /usr/lib/systemd/system/auditd.service.
Setting up audispd-plugins (1:3.1.2-2.1build1.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo systemctl enable --now auditd
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo auditctl -w /usr/bin/sudo -p x -k sudo_exec
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo auditctl -w /var/log/auth.log -p wa -k authlog
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo ausearch -k sudo_exec -ts today
----
time->Wed Nov  5 00:06:37 2025
type=PROCTITLE msg=audit(1762281397.863:345): proctitle=[illegible]
type=SYSCALL msg=audit(1762281397.863:345): arch=c000003e syscall=44 success=yes exit=1080 a0=4 a1=[illegible] a2=438 a3=0 items=0 ppid=22335 pid=22336 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1762281397.863:345): auid=1000 ses=3 subj=unconfined op=add_rule key="sudo_exec" list=4 res=1
----
time->Wed Nov  5 00:06:49 2025
type=PROCTITLE msg=audit(1762281409.720:348): proctitle=[illegible]
type=PATH msg=audit(1762281409.720:348): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=395693 dev=08:02 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1762281409.720:348): item=0 name="/usr/bin/sudo" inode=394627 dev=08:02 mode=0104755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1762281409.720:348): cwd="/home/leman-kumar-sahu"
type=EXECVE msg=audit(1762281409.720:348): argc=8 a0="sudo" a1="auditctl" a2="-w" a3="/var/log/auth.log" a4="-p" a5="wa" a6="-k" a7="authlog"
type=SYSCALL msg=audit(1762281409.720:348): arch=c000003e syscall=59 success=yes exit=0 a0=[illegible] a1=[illegible] a2=[illegible] a3=[illegible] items=2 ppid=3285 pid=22338 auid=1000 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" subj=unconfined key="sudo_exec"
----
time->Wed Nov  5 00:06:59 2025
type=PROCTITLE msg=audit(1762281419.738:356): proctitle=[illegible]
type=PATH msg=audit(1762281419.738:356): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=395693 dev=08:02 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1762281419.738:356): item=0 name="/usr/bin/sudo" inode=394627 dev=08:02 mode=0104755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1762281419.738:356): cwd="/home/leman-kumar-sahu"
type=EXECVE msg=audit(1762281419.738:356): argc=6 a0="sudo" a1="ausearch" a2="-k" a3="sudo_exec" a4="-ts" a5="today"
type=SYSCALL msg=audit(1762281419.738:356): arch=c000003e syscall=59 success=yes exit=0 a0=[illegible] a1=[illegible] a2=[illegible] a3=[illegible] items=2 ppid=3285 pid=22342 auid=1000 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="sudo" exe="/usr/bin/sudo" subj=unconfined key="sudo_exec"
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo ausearch -k authlog -ts today
----
time->Wed Nov  5 00:06:49 2025
type=PROCTITLE msg=audit(1762281409.738:353): proctitle=[illegible]
type=PATH msg=audit(1762281409.738:353): item=0 name="/var/log/" inode=1048581 dev=08:02 mode=040755 ouid=0 ogid=102 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1762281409.738:353): cwd="/home/leman-kumar-sahu"
type=SOCKADDR msg=audit(1762281409.738:353): saddr=100000000000000000000000
type=SYSCALL msg=audit(1762281409.738:353): arch=c000003e syscall=44 success=yes exit=1080 a0=4 a1=[illegible] a2=438 a3=0 items=1 ppid=22339 pid=22340 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1762281409.738:353): auid=1000 ses=3 subj=unconfined op=add_rule key="authlog" list=4 res=1
leman-kumar-sahu@leman-kumar-sahu-VMware-Virtual-Platform:~$ sudo ausearch -k sudo_exec -i
----
type=PROCTITLE msg=audit(11/05/2025 00:06:37.863:345) : proctitle=auditctl -w /usr/bin/sudo -p x -k sudo_exec
type=SYSCALL msg=audit(11/05/2025 00:06:37.863:345) : arch=x86_64 syscall=sendto success=yes exit=1080 a0=0x4 a1=[illegible] a2=0x438 a3=0x0 items=0 ppid=22335 pid=22336 auid=leman-kumar-sahu uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts1 ses=3 comm=auditctl exe=/usr/sbin/auditctl subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(11/05/2025 00:06:37.863:345) : auid=leman-kumar-sahu ses=3 subj=unconfined op=add_rule key=sudo_exec list=exit res=yes
----
type=PROCTITLE msg=audit(11/05/2025 00:06:49.720:348) : proctitle=sudo auditctl -w /var/log/auth.log -p wa -k authlog
type=PATH msg=audit(11/05/2025 00:06:49.720:348) : item=1 name=/lib64/ld-linux-x86-64.so.2 inode=395693 dev=08:02 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(11/05/2025 00:06:49.720:348) : item=0 name=/usr/bin/sudo inode=394627 dev=08:02 mode=file,suid,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none ca
```

Conclusion :

In this project, we secured an Ubuntu server by applying key **system hardening techniques**. We created a separate admin user, disabled root SSH login, and enabled **key-based authentication** for safe access. Using **UFW**, we allowed only SSH traffic and blocked all other connections. **Fail2Ban** was configured to prevent brute-force attacks, and **auditd** was enabled to log user and sudo activities.

Overall, the project enhanced understanding of **Linux security, SSH protection, and auditing**, forming a strong foundation for real-world **server hardening** practices.

Key Learnings :

- Learned how to create and manage admin users with proper sudo privileges.
- Understood how to disable root SSH login and enable key-based authentication for secure access.

- Gained hands-on experience in configuring UFW firewall to allow only required network traffic.
- Learned to install and configure Fail2Ban to protect the server from brute-force attacks.
- Practiced using auditd to log and monitor user login and sudo activities.
- Understood the importance of server hardening and system auditing in real-world security setups.
- Improved overall knowledge of Linux system security and administration best practices.