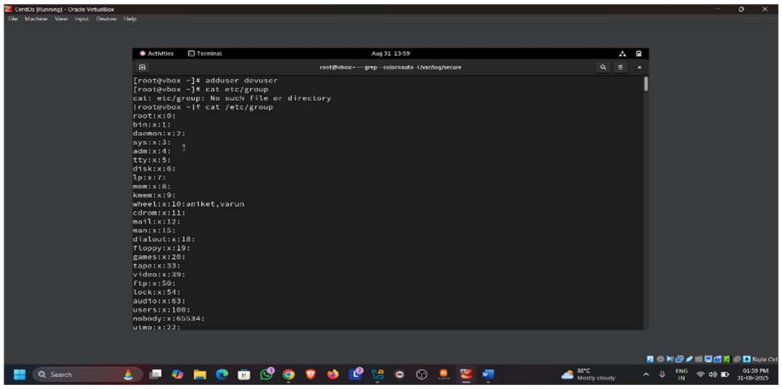
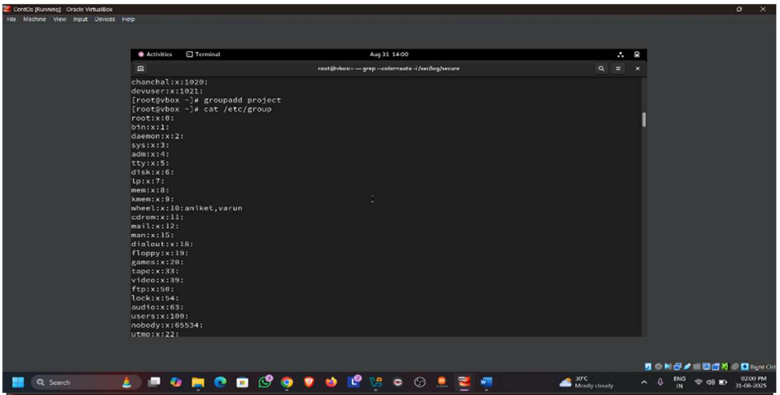
Project 5: Linux Server Hardening & Automation

Description: Configured a secure Linux server with user management, firewall security, automated backups, and system monitoring.
Technologies Used: Linux (Ubuntu/CentOS), Bash, SSH, Fail2Ban, UFW, Auditd, Cron Jobs.
Step 1. User Management & SSH Security
# Create a new user
adduser devuser

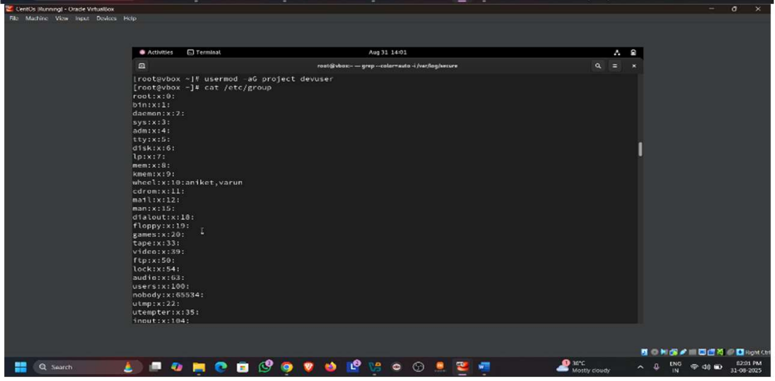


```
[root@vbox ~]# adduser devuser
[root@vbox ~]# cat etc/group
cat: etc/group: No such file or directory
[root@vbox ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:aniket,varun
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
utmp:x:22:
```

# Add user to project group
usermod -aG project devuser



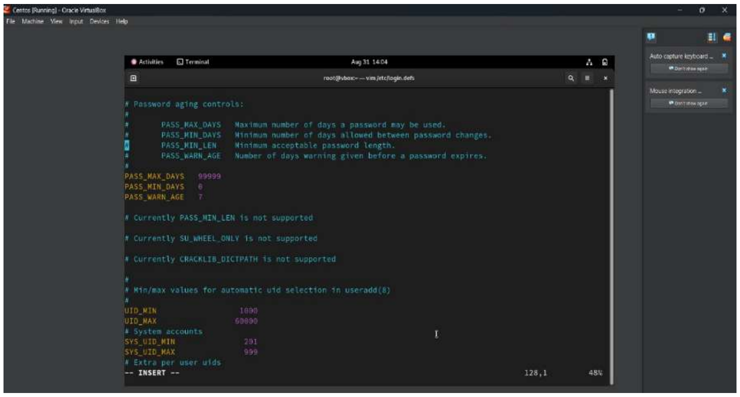
```
chanchal:x:1020:
devuser:x:1021:
[root@vbox ~]# groupadd project
[root@vbox ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:aniket,varun
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
utmp:x:22:
```



```
[root@vbox ~]# usermod -aG project devuser
[root@vbox ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:aniket,varun
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
utmp:x:22:
utempter:x:35:
input:x:104:
```

# Force strong password policy (vim /etc/login.defs or /etc/security/pwquality.conf)

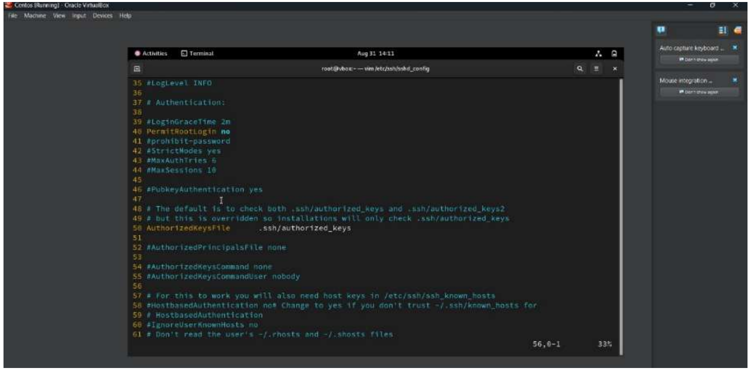
```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
```


Centos [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:04
root@vbox:~ — vim /etc/login.defs
Auto capture keyboard ...
Mouse integration ...

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

# Currently PASS_MIN_LEN is not supported

# Currently SU_WHEEL_ONLY is not supported

# Currently CRACKLIB_DICTPATH is not supported

#
# Min/max values for automatic uid selection in useradd(8)
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
SYS_UID_MIN               201
SYS_UID_MAX               999
# Extra per user uids
-- INSERT --                                                    128,1         48%
```

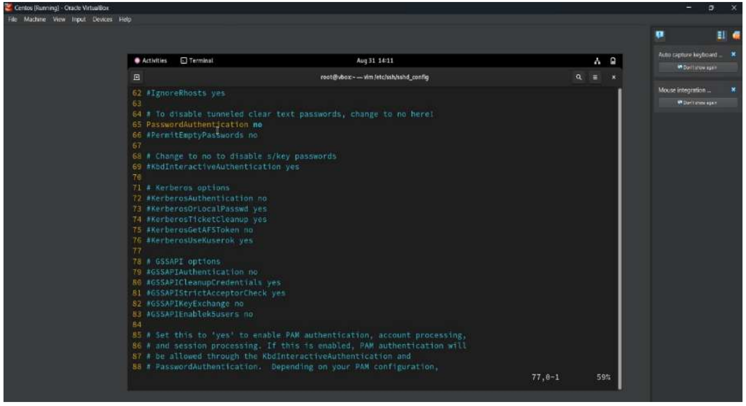
# Disable root login & password authentication (vim /etc/ssh/sshd_config)

PermitRootLogin no **(line 40)**


Centos [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:11
root@vbox:~ — vim /etc/ssh/sshd_config
Auto capture keyboard ...
Mouse integration ...

```
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40 PermitRootLogin no
41 #prohibit-password
42 #StrictModes yes
43 #MaxAuthTries 6
44 #MaxSessions 10
45
46 #PubkeyAuthentication yes
47
48 # The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
49 # but this is overridden so installations will only check .ssh/authorized_keys
50 AuthorizedKeysFile      .ssh/authorized_keys
51
52 #AuthorizedPrincipalsFile none
53
54 #AuthorizedKeysCommand none
55 #AuthorizedKeysCommandUser nobody
56
57 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
58 #HostbasedAuthentication no# Change to yes if you don't trust ~/.ssh/known_hosts for
59 # HostbasedAuthentication
60 #IgnoreUserKnownHosts no
61 # Don't read the user's ~/.rhosts and ~/.shosts files
                                                                56,0-1        33%
```

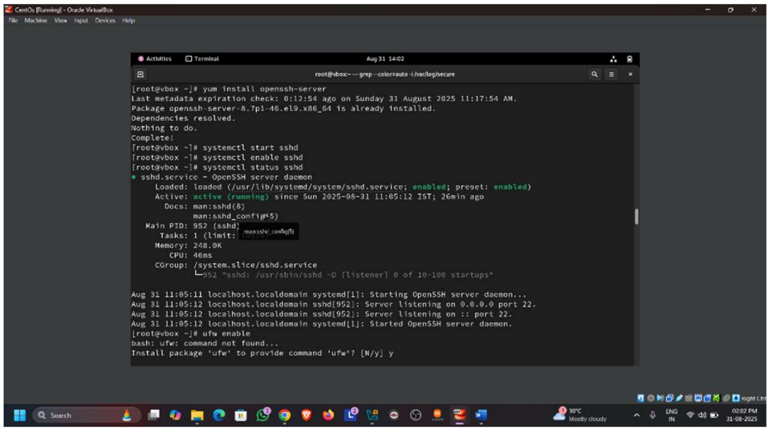
PasswordAuthentication no **(line 66)**


Centos [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:11
root@vbox:~ — vim /etc/ssh/sshd_config
Auto capture keyboard ...
Mouse integration ...

```
62 #IgnoreRhosts yes
63
64 # To disable tunneled clear text passwords, change to no here!
65 PasswordAuthentication no
66 #PermitEmptyPasswords no
67
68 # Change to no to disable s/key passwords
69 #KbdInteractiveAuthentication yes
70
71 # Kerberos options
72 #KerberosAuthentication no
73 #KerberosOrLocalPasswd yes
74 #KerberosTicketCleanup yes
75 #KerberosGetAFSToken no
76 #KerberosUseKuserok yes
77
78 # GSSAPI options
79 #GSSAPIAuthentication no
80 #GSSAPICleanupCredentials yes
81 #GSSAPIStrictAcceptorCheck yes
82 #GSSAPIKeyExchange no
83 #GSSAPIEnablek5users no
84
85 # Set this to 'yes' to enable PAM authentication, account processing,
86 # and session processing. If this is enabled, PAM authentication will
87 # be allowed through the KbdInteractiveAuthentication and
88 # PasswordAuthentication.  Depending on your PAM configuration,
                                                                77,0-1        59%
```

# Restart SSH service

systemctl restart ssh
yum install openssh-server
systemctl start sshd
systemctl enable sshd
systemctl enable sshd



CentOs [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:02
root@vbox:~ — grep --color=auto -i /var/log/secure
man:sshd_config(5)
Search
30°C
Mostly cloudy
ENG
IN
02:02 PM
31-08-2025

```
[root@vbox ~]# yum install openssh-server
Last metadata expiration check: 0:12:54 ago on Sunday 31 August 2025 11:17:54 AM.
Package openssh-server-8.7p1-46.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# systemctl start sshd
[root@vbox ~]# systemctl enable sshd
[root@vbox ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-08-31 11:05:12 IST; 26min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 952 (sshd)
      Tasks: 1 (limit:
     Memory: 248.0K
        CPU: 46ms
     CGroup: /system.slice/sshd.service
             └─952 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 31 11:05:11 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 31 11:05:12 localhost.localdomain sshd[952]: Server listening on 0.0.0.0 port 22.
Aug 31 11:05:12 localhost.localdomain sshd[952]: Server listening on :: port 22.
Aug 31 11:05:12 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[root@vbox ~]# ufw enable
bash: ufw: command not found...
Install package 'ufw' to provide command 'ufw'? [N/y] y
```

Step 2. Firewall Configuration (Uncomplicated Firewall)

# Enable UFW

ufw enable (command)

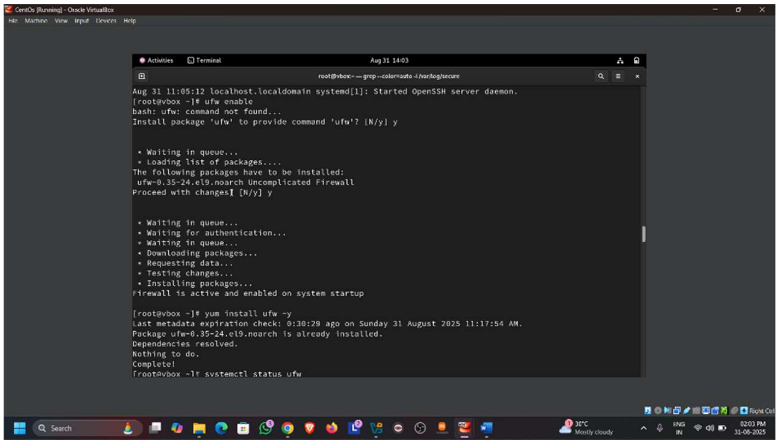
yum install ufw -y

msg: install package ’ufw’ to provide command ‘ufw; ? [N/y] y

msg: proceed with changes? [N/y] y

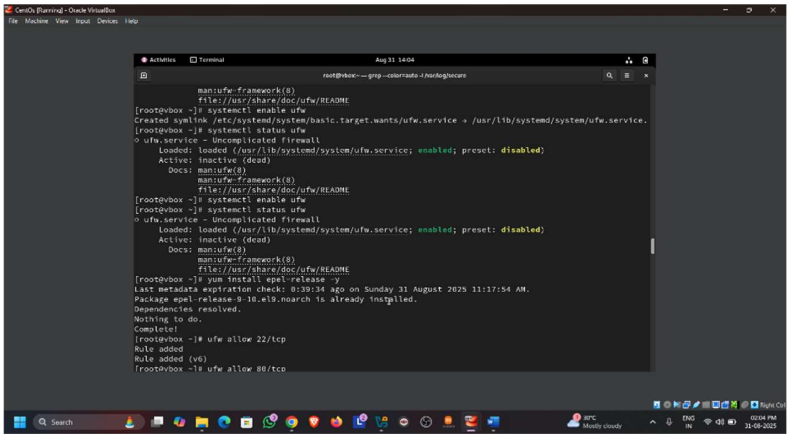
msg: Firewall is active & enabled on system startup

systemctl enable ufw



CentOs [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:03
root@vbox:~ — grep --color=auto -i /var/log/secure
Search
30°C
Mostly cloudy
ENG
IN
02:03 PM
31-08-2025

```
Aug 31 11:05:12 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[root@vbox ~]# ufw enable
bash: ufw: command not found...
Install package 'ufw' to provide command 'ufw'? [N/y] y


 • Waiting in queue...
 • Loading list of packages....
The following packages have to be installed:
 ufw-0.35-24.el9.noarch Uncomplicated Firewall
Proceed with changes? [N/y] y


 • Waiting in queue...
 • Waiting for authentication...
 • Waiting in queue...
 • Downloading packages...
 • Requesting data...
 • Testing changes...
 • Installing packages...
Firewall is active and enabled on system startup

[root@vbox ~]# yum install ufw -y
Last metadata expiration check: 0:30:29 ago on Sunday 31 August 2025 11:17:54 AM.
Package ufw-0.35-24.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# systemctl status ufw
```



CentOs [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 14:04
root@vbox:~ — grep --color=auto -i /var/log/secure
Search
30°C
Mostly cloudy
ENG
IN
02:04 PM
31-08-2025

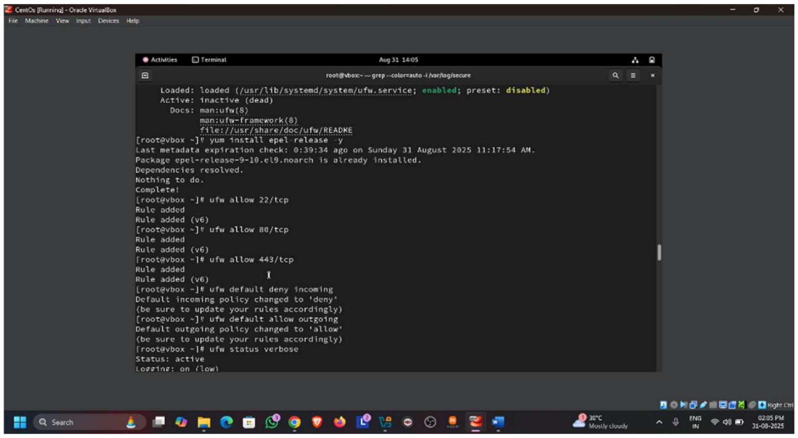
```
             man:ufw-framework(8)
             file://usr/share/doc/ufw/README
[root@vbox ~]# systemctl enable ufw
Created symlink /etc/systemd/system/basic.target.wants/ufw.service → /usr/lib/systemd/system/ufw.service.
[root@vbox ~]# systemctl status ufw
○ ufw.service - Uncomplicated firewall
     Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:ufw(8)
             man:ufw-framework(8)
             file://usr/share/doc/ufw/README
[root@vbox ~]# systemctl enable ufw
[root@vbox ~]# systemctl status ufw
○ ufw.service - Uncomplicated firewall
     Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:ufw(8)
             man:ufw-framework(8)
             file://usr/share/doc/ufw/README
[root@vbox ~]# yum install epel-release -y
Last metadata expiration check: 0:39:34 ago on Sunday 31 August 2025 11:17:54 AM.
Package epel-release-9-10.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# ufw allow 22/tcp
Rule added
Rule added (v6)
[root@vbox ~]# ufw allow 80/tcp
```

# Allow only required ports

ufw allow 22/tcp   # SSH

ufw allow 80/tcp   # HTTP

ufw allow 443/tcp   # HTTPS



```
    Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: disabled)
    Active: inactive (dead)
      Docs: man:ufw(8)
            man:ufw-framework(8)
            file://usr/share/doc/ufw/README
[root@vbox ~]# yum install epel-release -y
Last metadata expiration check: 0:39:34 ago on Sunday 31 August 2025 11:17:54 AM.
Package epel-release-9-10.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# ufw allow 22/tcp
Rule added
Rule added (v6)
[root@vbox ~]# ufw allow 80/tcp
Rule added
Rule added (v6)
[root@vbox ~]# ufw allow 443/tcp
Rule added
Rule added (v6)
[root@vbox ~]# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
[root@vbox ~]# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
[root@vbox ~]# ufw status verbose
Status: active
Logging: on (low)
```

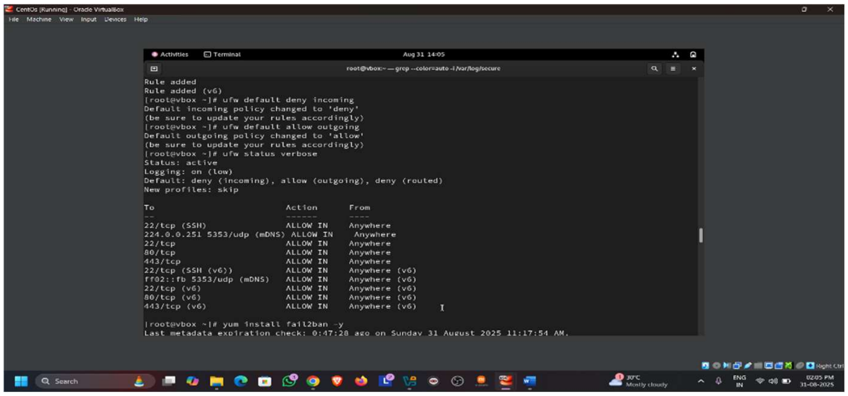
# Deny everything else

ufw default deny incoming

ufw default allow outgoing

# Check status

ufw status verbose

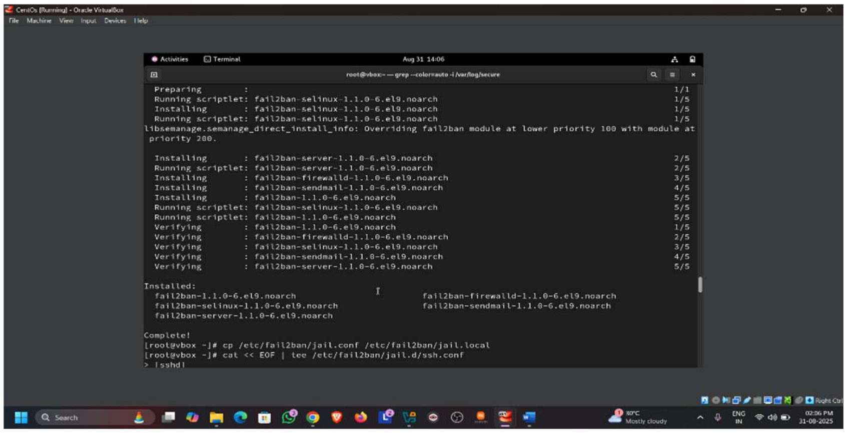


```
Rule added
Rule added (v6)
[root@vbox ~]# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
[root@vbox ~]# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
[root@vbox ~]# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                           Action      From
--                           ------      ----
22/tcp (SSH)                 ALLOW IN    Anywhere
224.0.0.251 5353/udp (mDNS) ALLOW IN    Anywhere
22/tcp                       ALLOW IN    Anywhere
80/tcp                       ALLOW IN    Anywhere
443/tcp                      ALLOW IN    Anywhere
22/tcp (SSH (v6))            ALLOW IN    Anywhere (v6)
ff02::fb 5353/udp (mDNS)     ALLOW IN    Anywhere (v6)
22/tcp (v6)                  ALLOW IN    Anywhere (v6)
80/tcp (v6)                  ALLOW IN    Anywhere (v6)
443/tcp (v6)                 ALLOW IN    Anywhere (v6)

[root@vbox ~]# yum install fail2ban -y
Last metadata expiration check: 0:47:28 ago on Sunday 31 August 2025 11:17:54 AM.
```

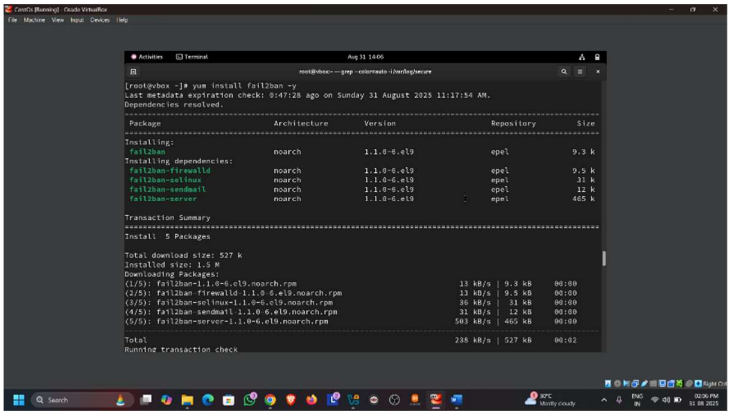
Step 3. Intrusion Prevention with Fail2Ban

# Install Fail2Ban

yum install fail2ban -y



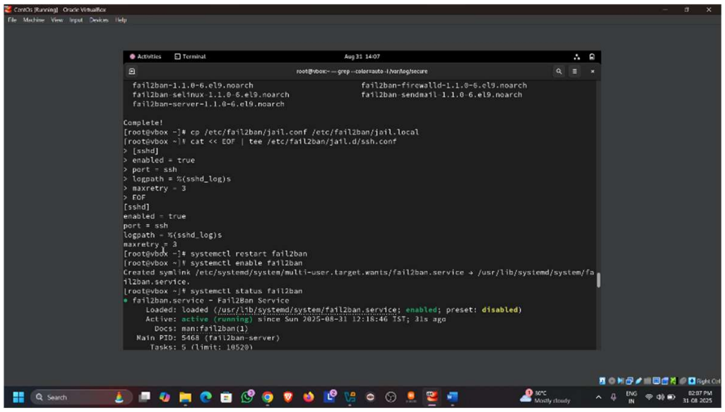
```
  Preparing        :                                                         1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                     1/5
  Installing       : fail2ban-selinux-1.1.0-6.el9.noarch                     1/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                     1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower priority 100 with module at
 priority 200.

  Installing       : fail2ban-server-1.1.0-6.el9.noarch                      2/5
  Running scriptlet: fail2ban-server-1.1.0-6.el9.noarch                      2/5
  Installing       : fail2ban-firewalld-1.1.0-6.el9.noarch                   3/5
  Installing       : fail2ban-sendmail-1.1.0-6.el9.noarch                    4/5
  Installing       : fail2ban-1.1.0-6.el9.noarch                             5/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                     5/5
  Running scriptlet: fail2ban-1.1.0-6.el9.noarch                             5/5
  Verifying        : fail2ban-1.1.0-6.el9.noarch                             1/5
  Verifying        : fail2ban-firewalld-1.1.0-6.el9.noarch                   2/5
  Verifying        : fail2ban-selinux-1.1.0-6.el9.noarch                     3/5
  Verifying        : fail2ban-sendmail-1.1.0-6.el9.noarch                    4/5
  Verifying        : fail2ban-server-1.1.0-6.el9.noarch                      5/5

Installed:
  fail2ban-1.1.0-6.el9.noarch                       fail2ban-firewalld-1.1.0-6.el9.noarch
  fail2ban-selinux-1.1.0-6.el9.noarch               fail2ban-sendmail-1.1.0-6.el9.noarch
  fail2ban-server-1.1.0-6.el9.noarch

Complete!
[root@vbox ~]# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
[root@vbox ~]# cat << EOF | tee /etc/fail2ban/jail.d/ssh.conf
> [sshd]
```



```
[root@vbox ~]# yum install fail2ban -y
Last metadata expiration check: 0:47:28 ago on Sunday 31 August 2025 11:17:54 AM.
Dependencies resolved.
================================================================================
 Package                Architecture     Version               Repository   Size
================================================================================
Installing:
 fail2ban               noarch           1.1.0-6.el9           epel        9.3 k
Installing dependencies:
 fail2ban-firewalld     noarch           1.1.0-6.el9           epel        9.5 k
 fail2ban-selinux       noarch           1.1.0-6.el9           epel         31 k
 fail2ban-sendmail      noarch           1.1.0-6.el9           epel         12 k
 fail2ban-server        noarch           1.1.0-6.el9           epel        465 k

Transaction Summary
================================================================================
Install  5 Packages

Total download size: 527 k
Installed size: 1.5 M
Downloading Packages:
(1/5): fail2ban-1.1.0-6.el9.noarch.rpm                 13 kB/s | 9.3 kB     00:00
(2/5): fail2ban-firewalld-1.1.0-6.el9.noarch.rpm       13 kB/s | 9.5 kB     00:00
(3/5): fail2ban-selinux-1.1.0-6.el9.noarch.rpm         36 kB/s |  31 kB     00:00
(4/5): fail2ban-sendmail-1.1.0-6.el9.noarch.rpm        31 kB/s |  12 kB     00:00
(5/5): fail2ban-server-1.1.0-6.el9.noarch.rpm         503 kB/s | 465 kB     00:00
--------------------------------------------------------------------------------
Total                                                 238 kB/s | 527 kB     00:02
Running transaction check
```

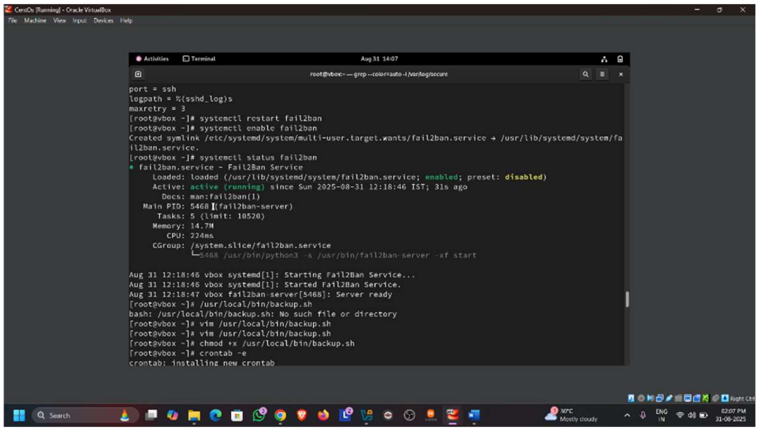
# Copy default config
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

# Example SSH protection config
cat <<EOF | tee /etc/fail2ban/jail.d/ssh.conf
[sshd]
enabled = true
port   = ssh
logpath = %(sshd_log)s
maxretry = 3
EOF



```
  fail2ban-1.1.0-6.el9.noarch                        fail2ban-firewalld-1.1.0-6.el9.noarch
  fail2ban-selinux-1.1.0-6.el9.noarch                fail2ban-sendmail-1.1.0-6.el9.noarch
  fail2ban-server-1.1.0-6.el9.noarch

Complete!
[root@vbox ~]# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
[root@vbox ~]# cat << EOF | tee /etc/fail2ban/jail.d/ssh.conf
> [sshd]
> enabled = true
> port = ssh
> logpath = %(sshd_log)s
> maxretry = 3
> EOF
[sshd]
enabled = true
port = ssh
logpath = %(sshd_log)s
maxretry = 3
[root@vbox ~]# systemctl restart fail2ban
[root@vbox ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fa
il2ban.service.
[root@vbox ~]# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-08-31 12:18:46 IST; 31s ago
       Docs: man:fail2ban(1)
   Main PID: 5468 (fail2ban-server)
      Tasks: 5 (limit: 10520)
```

# Restart Fail2Ban
systemctl restart fail2ban
systemctl enable fail2ban



```
port = ssh
logpath = %(sshd_log)s
maxretry = 3
[root@vbox ~]# systemctl restart fail2ban
[root@vbox ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fa
il2ban.service.
[root@vbox ~]# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-08-31 12:18:46 IST; 31s ago
       Docs: man:fail2ban(1)
   Main PID: 5468 (fail2ban-server)
      Tasks: 5 (limit: 10520)
     Memory: 14.7M
        CPU: 224ms
     CGroup: /system.slice/fail2ban.service
             └─5468 /usr/bin/python3 -s /usr/bin/fail2ban-server -xf start

Aug 31 12:18:46 vbox systemd[1]: Starting Fail2Ban Service...
Aug 31 12:18:46 vbox systemd[1]: Started Fail2Ban Service.
Aug 31 12:18:47 vbox fail2ban-server[5468]: Server ready
[root@vbox ~]# /usr/local/bin/backup.sh
bash: /usr/local/bin/backup.sh: No such file or directory
[root@vbox ~]# vim /usr/local/bin/backup.sh
[root@vbox ~]# vim /usr/local/bin/backup.sh
[root@vbox ~]# chmod +x /usr/local/bin/backup.sh
[root@vbox ~]# crontab -e
crontab: installing new crontab
```

4. Automated Backups (Bash + Cron)
Backup Script (/usr/local/bin/backup.sh)

#!/bin/bash
# Backup important directories to /backup with timestamp

BACKUP_DIR="/backup/$(date +'%Y-%m-%d')"
SOURCE_DIRS="/etc /home /var/www"

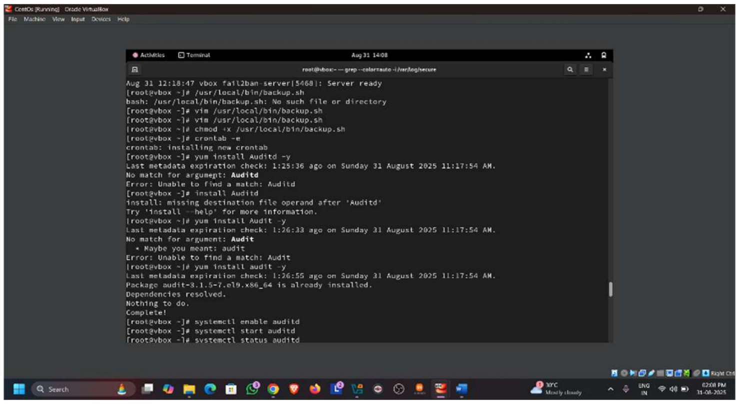
mkdir -p "$BACKUP_DIR"

rsync -a $SOURCE_DIRS "$BACKUP_DIR"

# Keep only last 7 backups
find /backup/* -type d -mtime +7 -exec rm -rf {} \;

Make it executable:
chmod +x /usr/local/bin/backup.sh

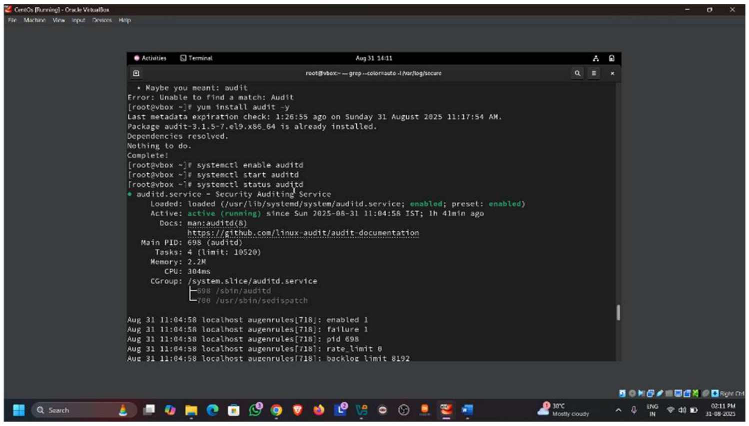
Add to cron (daily backup at 2 AM):
crontab -e
(updated 30 13 * * * /usr/local/bin/backup.sh >> /var/log/backup.log 2>&1
0 2 * * * /usr/local/bin/backup.sh >> /var/log/backup.log 2>&1



```
Aug 31 12:18:47 vbox fail2ban-server[5468]: Server ready
[root@vbox ~]# /usr/local/bin/backup.sh
bash: /usr/local/bin/backup.sh: No such file or directory
[root@vbox ~]# vim /usr/local/bin/backup.sh
[root@vbox ~]# vim /usr/local/bin/backup.sh
[root@vbox ~]# chmod +x /usr/local/bin/backup.sh
[root@vbox ~]# crontab -e
crontab: installing new crontab
[root@vbox ~]# yum install Auditd -y
Last metadata expiration check: 1:25:36 ago on Sunday 31 August 2025 11:17:54 AM.
No match for argument: Auditd
Error: Unable to find a match: Auditd
[root@vbox ~]# install Auditd
install: missing destination file operand after 'Auditd'
Try 'install --help' for more information.
[root@vbox ~]# yum install Audit -y
Last metadata expiration check: 1:26:33 ago on Sunday 31 August 2025 11:17:54 AM.
No match for argument: Audit
  * Maybe you meant: audit
Error: Unable to find a match: Audit
[root@vbox ~]# yum install audit -y
Last metadata expiration check: 1:26:55 ago on Sunday 31 August 2025 11:17:54 AM.
Package audit-3.1.5-7.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# systemctl enable auditd
[root@vbox ~]# systemctl start auditd
[root@vbox ~]# systemctl status auditd
```

Step 5. System Monitoring & Auditing
Install Auditd (yum install audit -y)
sudo apt install auditd -y
systemctl enable auditd

systemctl start auditd



```
  • Maybe you meant: audit
Error: Unable to find a match: Audit
[root@vbox ~]# yum install audit -y
Last metadata expiration check: 1:26:55 ago on Sunday 31 August 2025 11:17:54 AM.
Package audit-3.1.5-7.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@vbox ~]# systemctl enable auditd
[root@vbox ~]# systemctl start auditd
[root@vbox ~]# systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-08-31 11:04:58 IST; 1h 41min ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 698 (auditd)
      Tasks: 4 (limit: 10520)
     Memory: 2.2M
        CPU: 304ms
     CGroup: /system.slice/auditd.service
             ├─698 /sbin/auditd
             └─700 /usr/sbin/sedispatch

Aug 31 11:04:58 localhost augenrules[718]: enabled 1
Aug 31 11:04:58 localhost augenrules[718]: failure 1
Aug 31 11:04:58 localhost augenrules[718]: pid 698
Aug 31 11:04:58 localhost augenrules[718]: rate_limit 0
Aug 31 11:04:58 localhost augenrules[718]: backlog_limit 8192
```

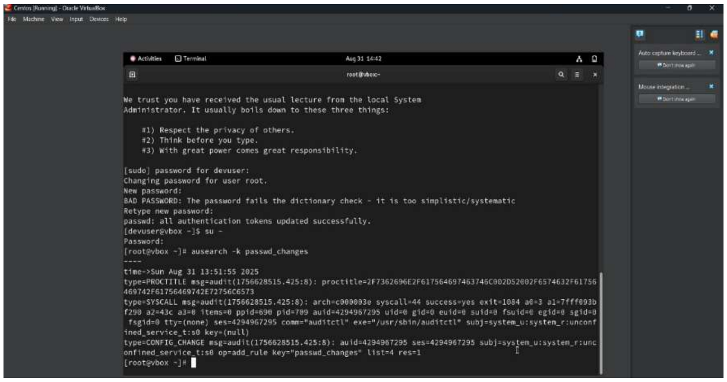
Add monitoring rules (/etc/audit/rules.d/audit.rules):

```
# Track modifications to /etc/passwd
-w /etc/passwd -p wa -k passwd_changes

# Track sudo usage
-w /var/log/sudo.log -p wa -k sudo_activity
```

Restart Auditd:

sudo systemctl restart auditd

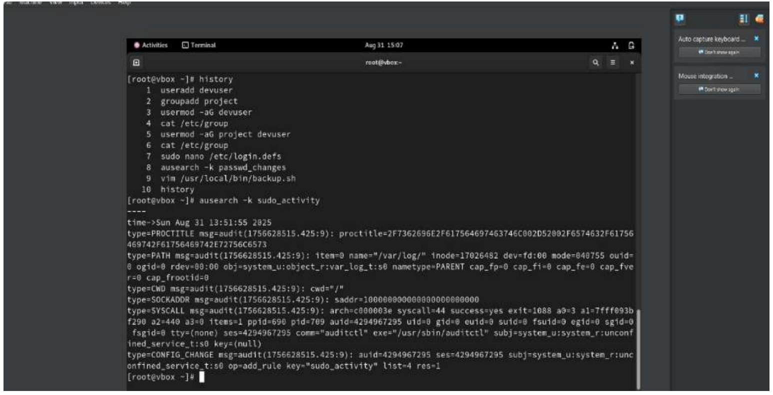
Check logs:



```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for devuser:
Changing password for user root.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[devuser@vbox ~]$ su -
Password:
[root@vbox ~]# ausearch -k passwd_changes
----
time->Sun Aug 31 13:51:55 2025
type=PROCTITLE msg=audit(1756628515.425:8): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756
469742F61756469742E72756C6573
type=SYSCALL msg=audit(1756628515.425:8): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7fff093b
f290 a2=43c a3=0 items=0 ppid=690 pid=709 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconf
ined_service_t:s0 key=(null)
type=CONFIG_CHANGE msg=audit(1756628515.425:8): auid=4294967295 ses=4294967295 subj=system_u:system_r:unc
onfined_service_t:s0 op=add_rule key="passwd_changes" list=4 res=1
[root@vbox ~]#
```

ausearch -k passwd_changes

ausearch -k sudo_activity



```
[root@vbox ~]# history
    1  useradd devuser
    2  groupadd project
    3  usermod -aG devuser
    4  cat /etc/group
    5  usermod -aG project devuser
    6  cat /etc/group
    7  sudo nano /etc/login.defs
    8  ausearch -k passwd_changes
    9  vim /usr/local/bin/backup.sh
   10  history
[root@vbox ~]# ausearch -k sudo_activity
----
time->Sun Aug 31 13:51:55 2025
type=PROCTITLE msg=audit(1756628515.425:9): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756
469742F61756469742E72756C6573
type=PATH msg=audit(1756628515.425:9): item=0 name="/var/log/" inode=17026482 dev=fd:00 mode=040755 ouid=
0 ogid=0 rdev=00:00 obj=system_u:object_r:var_log_t:s0 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fve
r=0 cap_frootid=0
type=CWD msg=audit(1756628515.425:9): cwd="/"
type=SOCKADDR msg=audit(1756628515.425:9): saddr=100000000000000000000000
type=SYSCALL msg=audit(1756628515.425:9): arch=c000003e syscall=44 success=yes exit=1088 a0=3 a1=7fff093b
f290 a2=440 a3=0 items=1 ppid=690 pid=709 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconf
ined_service_t:s0 key=(null)
type=CONFIG_CHANGE msg=audit(1756628515.425:9): auid=4294967295 ses=4294967295 subj=system_u:system_r:unc
onfined_service_t:s0 op=add_rule key="sudo_activity" list=4 res=1
[root@vbox ~]#
```

Group Members

Mr. Umesh Chimankar

Mr. Jay Soni

Miss. Vidya Patil

Miss. Kaveri Kanawade

Miss. Nikita Binnar
Miss. Bhagyashri Bagul