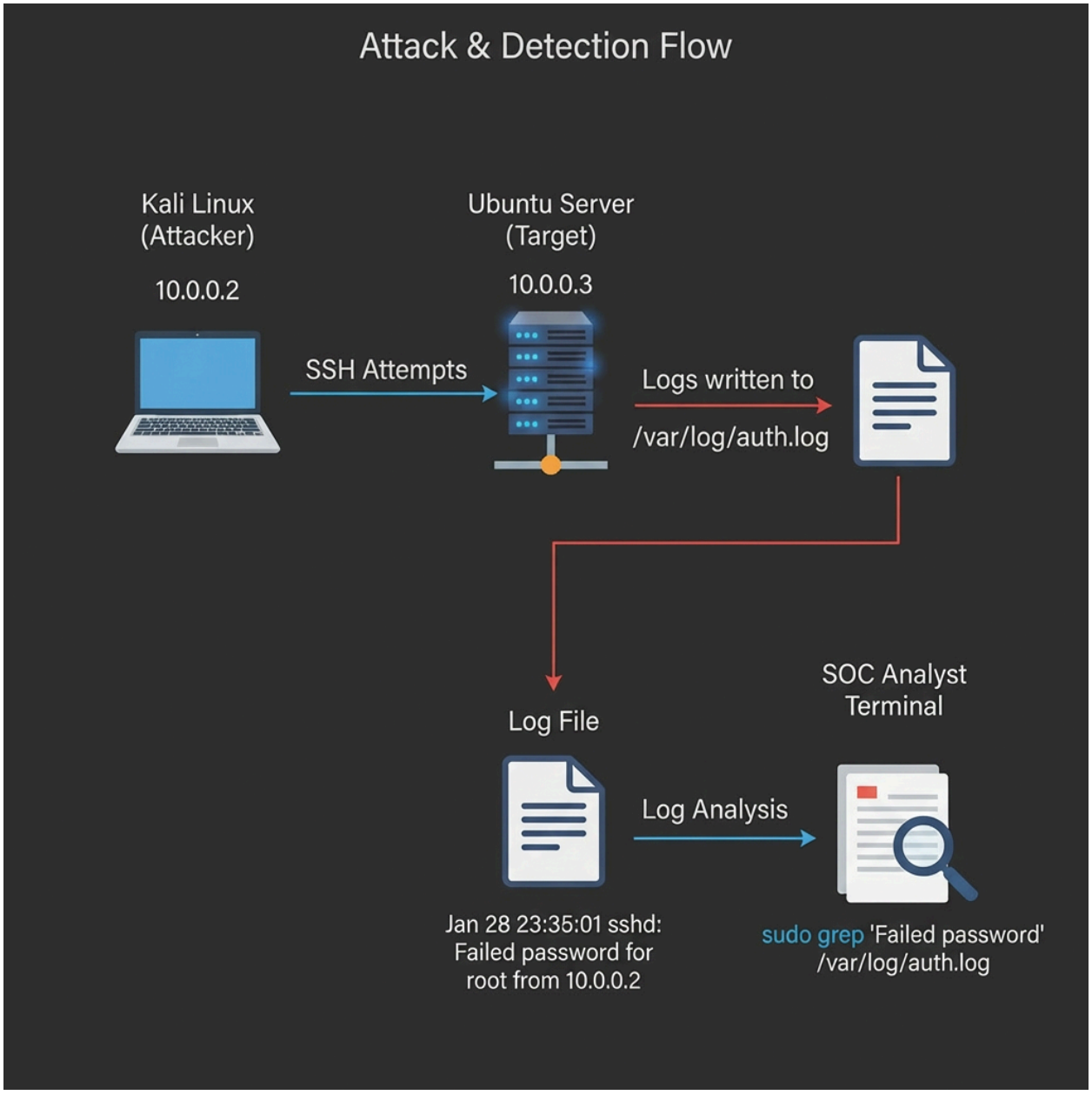


Day 10 – Identity, Authentication & Access Control

Today, we successfully audited the Identity and Access Management (IAM) framework of an Ubuntu Server. Here is the high-level summary of our

accomplishments:

Environment (use what you already have)

- Kali Linux (attacker / auditor)
- Ubuntu Server (target)

Phase 1 – Understand the Identity Model (Ubuntu)

Step 1: List users

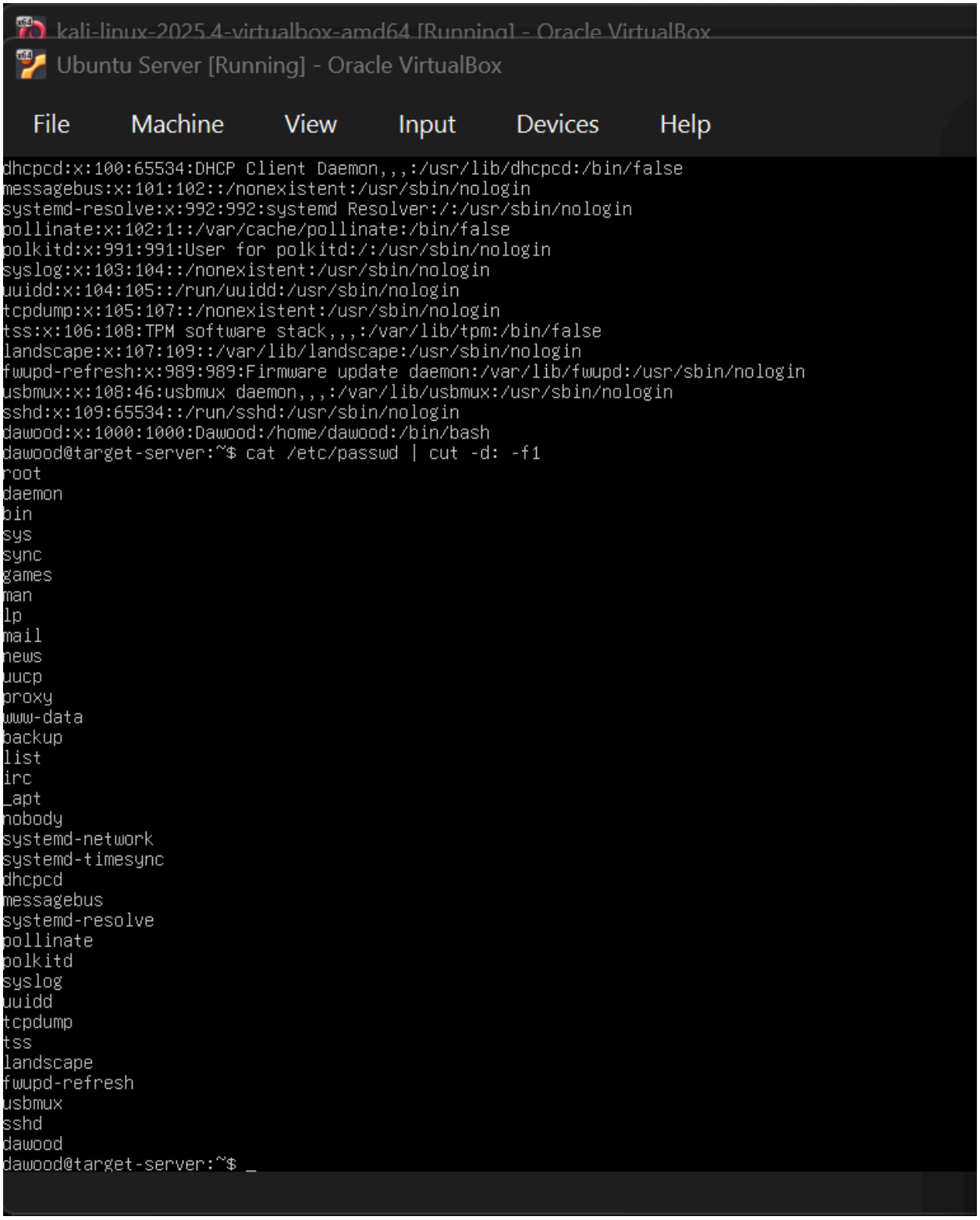
On the Ubuntu terminal step we will look at the Identity Database.
The command we are using is (cat /etc/passwd | cut -d: -f1)

The `|` symbol: This is called a "Pipe." You find it by holding **Shift** and pressing the key above **Enter**.

- **The `-d:` part:** This tells Linux the "divider" is a colon.
- **The `-f1` part:** This tells Linux to show only the "first field" (the name).

WHY?
By listing every user, you created a "Baseline." If you check this again tomorrow and see a new user named hacker1 you know immediately that your system has been compromised. This is the first step in **Identity Inventory**.

Proof



Step 2: Check groups

In this step we will check the groups ,we don't just manage one person at a time; we manage **Groups**. Think of it like a building: instead of giving a key to every single person, you create a "Marketing Team" key and a "Security Team" key.
The command we are using is (cat /etc/group) and after this we will type this command (sudo groups)

Why?
You verified that only authorized users (like `you`) are in the `sudo` group. This proves you are enforcing Access Control,ensuring the "Master Keys" aren't handed out to just anyone.

Proof

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox

Ubuntu Server [Running] - Oracle VirtualBox

File Machine View Input Devices Help

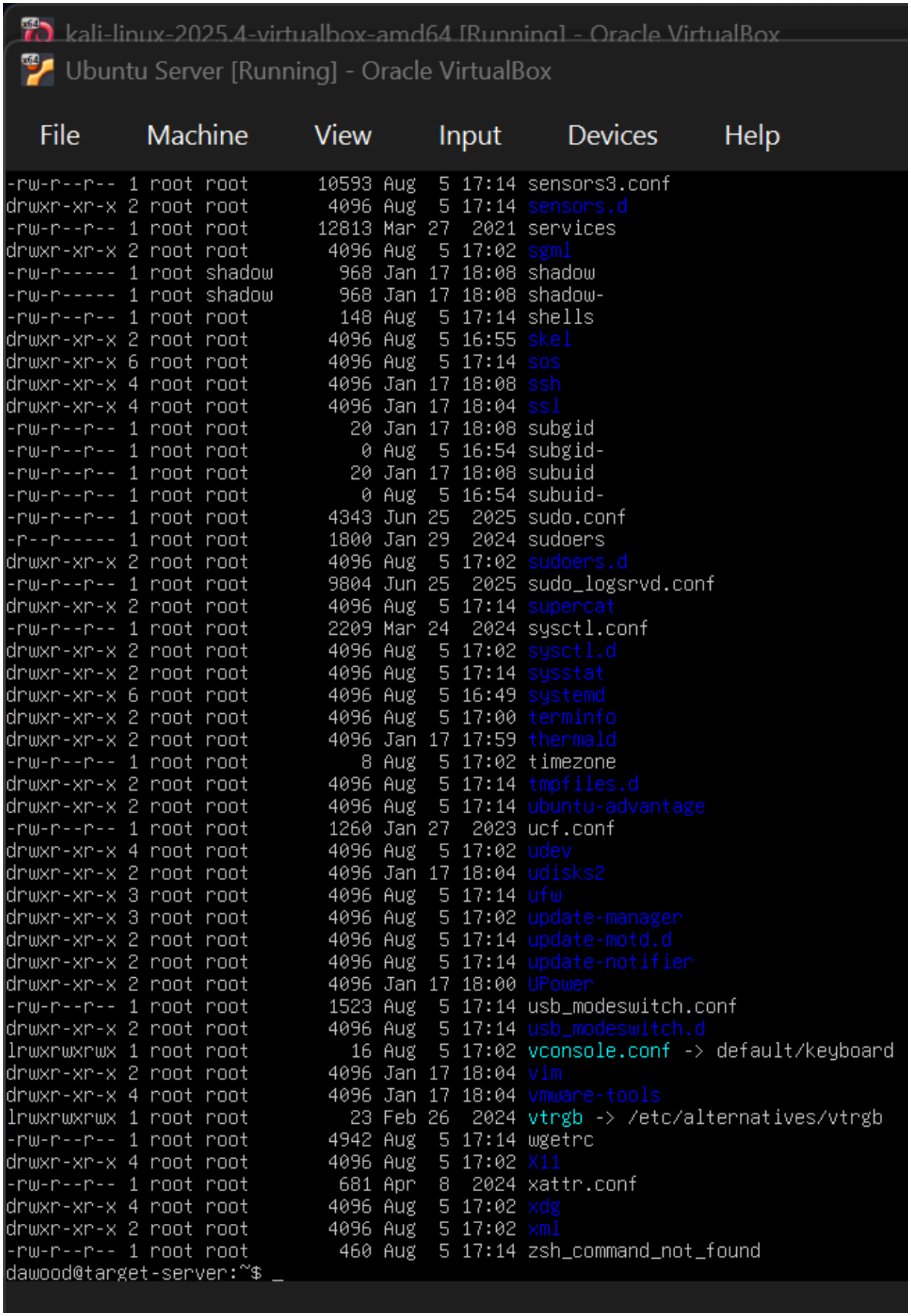
```
floppy:x:25:
tape:x:26:
sudo:x:27:dawood
audio:x:29:
dip:x:30:dawood
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:dawood
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
systemd-timesync:x:997:
input:x:996:
sgx:x:995:
kvm:x:994:
render:x:993:
lxd:x:101:dawood
messagebus:x:102:
systemd-resolve:x:992:
_ssh:x:103:
polkitd:x:991:
crontab:x:990:
syslog:x:104:
uuidd:x:105:
rdma:x:106:
tcpdump:x:107:
tss:x:108:
landscape:x:109:
fwupd-refresh:x:989:
dawood:x:1000:
ssl-cert:x:110:
dawood@target-server:~$ groups
dawood adm cdrom sudo dip plugdev lxd
dawood@target-server:~$ cat /etc/groups
cat: /etc/groups: No such file or directory
dawood@target-server:~$ sudo groups
[sudo] password for dawood:
root
dawood@target-server:~$
```

Phase 2 – Permissions (This is critical)

Step 3: Inspect permissions

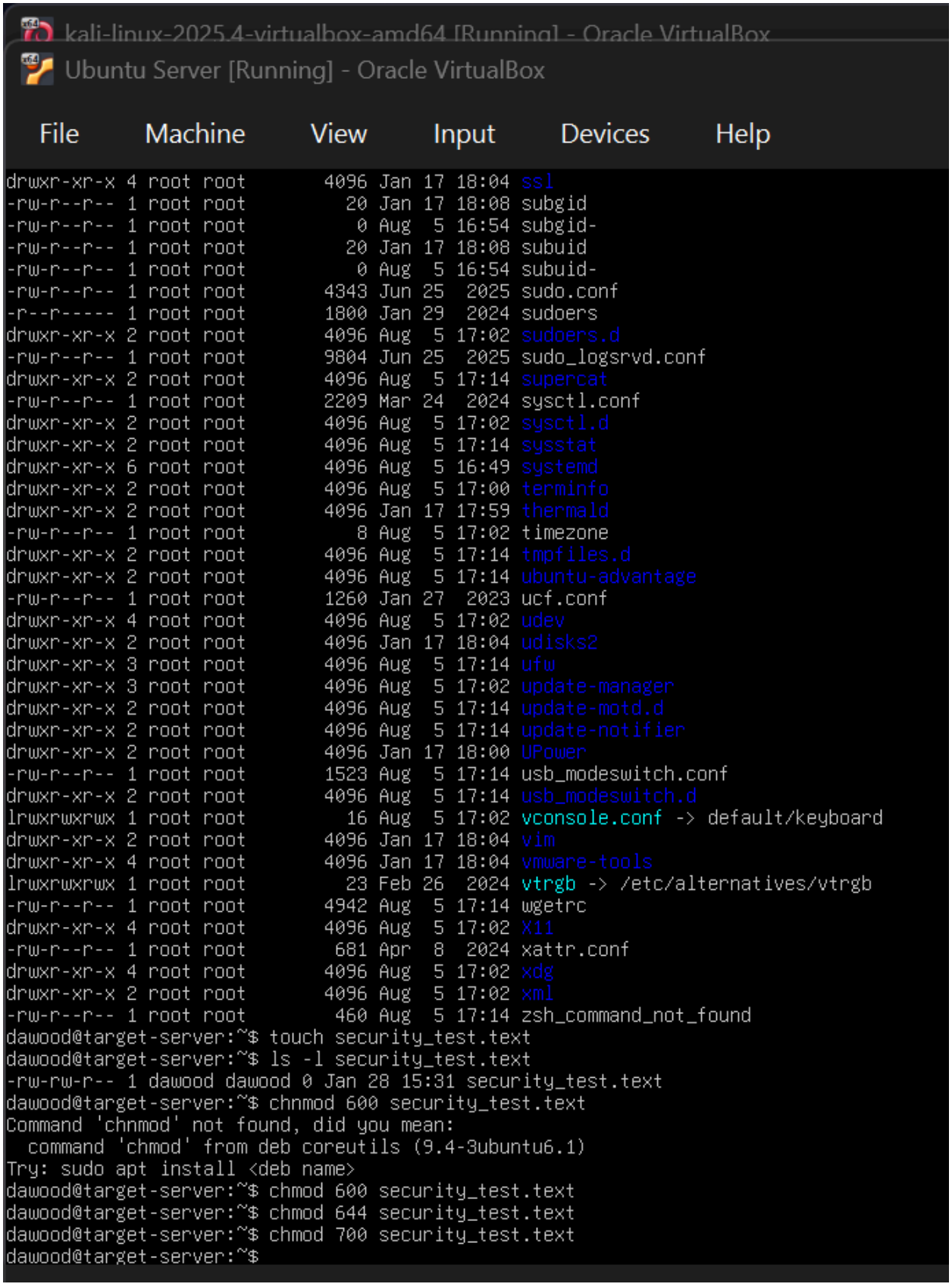
*In this step we will see every file has a set of rules called **Permissions**. These rules decide who can read, who can change, and who can run a file.*
The command we are using in this is (ls -l /etc).

Proof


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
-rw-r--r-- 1 root root 10593 Aug 5 17:14 sensors3.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sensors.d
-rw-r--r-- 1 root root 12813 Mar 27 2021 services
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sgml
-rw-r----- 1 root shadow 968 Jan 17 18:08 shadow
-rw-r----- 1 root shadow 968 Jan 17 18:08 shadow-
-rw-r--r-- 1 root root 148 Aug 5 17:14 shells
drwxr-xr-x 2 root root 4096 Aug 5 16:55 skel
drwxr-xr-x 6 root root 4096 Aug 5 17:14 sos
drwxr-xr-x 4 root root 4096 Jan 17 18:08 ssh
drwxr-xr-x 4 root root 4096 Jan 17 18:04 ssl
-rw-r--r-- 1 root root 20 Jan 17 18:08 subgid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subgid-
-rw-r--r-- 1 root root 20 Jan 17 18:08 subuid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subuid-
-rw-r--r-- 1 root root 4343 Jun 25 2025 sudo.conf
-r--r----- 1 root root 1800 Jan 29 2024 sudoers
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sudoers.d
-rw-r--r-- 1 root root 9804 Jun 25 2025 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 supercat
-rw-r--r-- 1 root root 2209 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sysctl.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysstat
drwxr-xr-x 6 root root 4096 Aug 5 16:49 systemd
drwxr-xr-x 2 root root 4096 Aug 5 17:00 terminfo
drwxr-xr-x 2 root root 4096 Jan 17 17:59 thermald
-rw-r--r-- 1 root root 8 Aug 5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 tmpfiles.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 ubuntu-advantage
-rw-r--r-- 1 root root 1260 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev
drwxr-xr-x 2 root root 4096 Jan 17 18:04 udisks2
drwxr-xr-x 3 root root 4096 Aug 5 17:14 ufw
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-manager
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-motd.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-notifier
drwxr-xr-x 2 root root 4096 Jan 17 18:00 UPower
-rw-r--r-- 1 root root 1523 Aug 5 17:14 usb_modeswitch.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 usb_modeswitch.d
lrwxrwxrwx 1 root root 16 Aug 5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x 2 root root 4096 Jan 17 18:04 vim
drwxr-xr-x 4 root root 4096 Jan 17 18:04 vmware-tools
lrwxrwxrwx 1 root root 23 Feb 26 2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r-- 1 root root 4942 Aug 5 17:14 wgetrc
drwxr-xr-x 4 root root 4096 Aug 5 17:02 X11
-rw-r--r-- 1 root root 681 Apr 8 2024 xattr.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 xdg
drwxr-xr-x 2 root root 4096 Aug 5 17:02 xml
-rw-r--r-- 1 root root 460 Aug 5 17:14 zsh_command_not_found
dawood@target-server:~$ _

Step 4: Change permissions (safe file)

In this step we will create a test file and also change it .
The command we are using is first(touch security_test.txt)then
(ls -l security_test.txt) for now changing the permission we will use is(chmod 600 security_test.txt) (chmod 644 security_test.txt) (chmod 700 security_test.txt)
Proof


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
drwxr-xr-x 4 root root 4096 Jan 17 18:04 ssl
-rw-r--r-- 1 root root 20 Jan 17 18:08 subgid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subgid-
-rw-r--r-- 1 root root 20 Jan 17 18:08 subuid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subuid-
-rw-r--r-- 1 root root 4343 Jun 25 2025 sudo.conf
-r--r----- 1 root root 1800 Jan 29 2024 sudoers
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sudoers.d
-rw-r--r-- 1 root root 9804 Jun 25 2025 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 supercat
-rw-r--r-- 1 root root 2209 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sysctl.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysstat
drwxr-xr-x 6 root root 4096 Aug 5 16:49 systemd
drwxr-xr-x 2 root root 4096 Aug 5 17:00 terminfo
drwxr-xr-x 2 root root 4096 Jan 17 17:59 thermald
-rw-r--r-- 1 root root 8 Aug 5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 tmpfiles.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 ubuntu-advantage
-rw-r--r-- 1 root root 1260 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev
drwxr-xr-x 2 root root 4096 Jan 17 18:04 udisks2
drwxr-xr-x 3 root root 4096 Aug 5 17:14 ufw
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-manager
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-motd.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-notifier
drwxr-xr-x 2 root root 4096 Jan 17 18:00 UPower
-rw-r--r-- 1 root root 1523 Aug 5 17:14 usb_modeswitch.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 usb_modeswitch.d
lrwxrwxrwx 1 root root 16 Aug 5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x 2 root root 4096 Jan 17 18:04 vim
drwxr-xr-x 4 root root 4096 Jan 17 18:04 vmware-tools
lrwxrwxrwx 1 root root 23 Feb 26 2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r-- 1 root root 4942 Aug 5 17:14 wgetrc
drwxr-xr-x 4 root root 4096 Aug 5 17:02 X11
-rw-r--r-- 1 root root 681 Apr 8 2024 xattr.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 xdg
drwxr-xr-x 2 root root 4096 Aug 5 17:02 xml
-rw-r--r-- 1 root root 460 Aug 5 17:14 zsh_command_not_found
dawood@target-server:~$ touch security_test.text
dawood@target-server:~$ ls -l security_test.text
-rw-rw-r-- 1 dawood dawood 0 Jan 28 15:31 security_test.text
dawood@target-server:~$ chnmod 600 security_test.text
Command 'chnmod' not found, did you mean:
command 'chmod' from deb coreutils (9.4-3ubuntu6.1)
Try: sudo apt install <deb name>
dawood@target-server:~$ chmod 600 security_test.text
dawood@target-server:~$ chmod 644 security_test.text
dawood@target-server:~$ chmod 700 security_test.text
dawood@target-server:~$

WHY(3 N 4 STEP)

By changing permissions to `600`, you implemented the Principle of Least Privilege. You proved that even if an attacker gets into the server, they are stopped by a "Locked Door" (the file permission) that prevents them from reading your sensitive data.

Phase 3 – Least Privilege (Admin access)

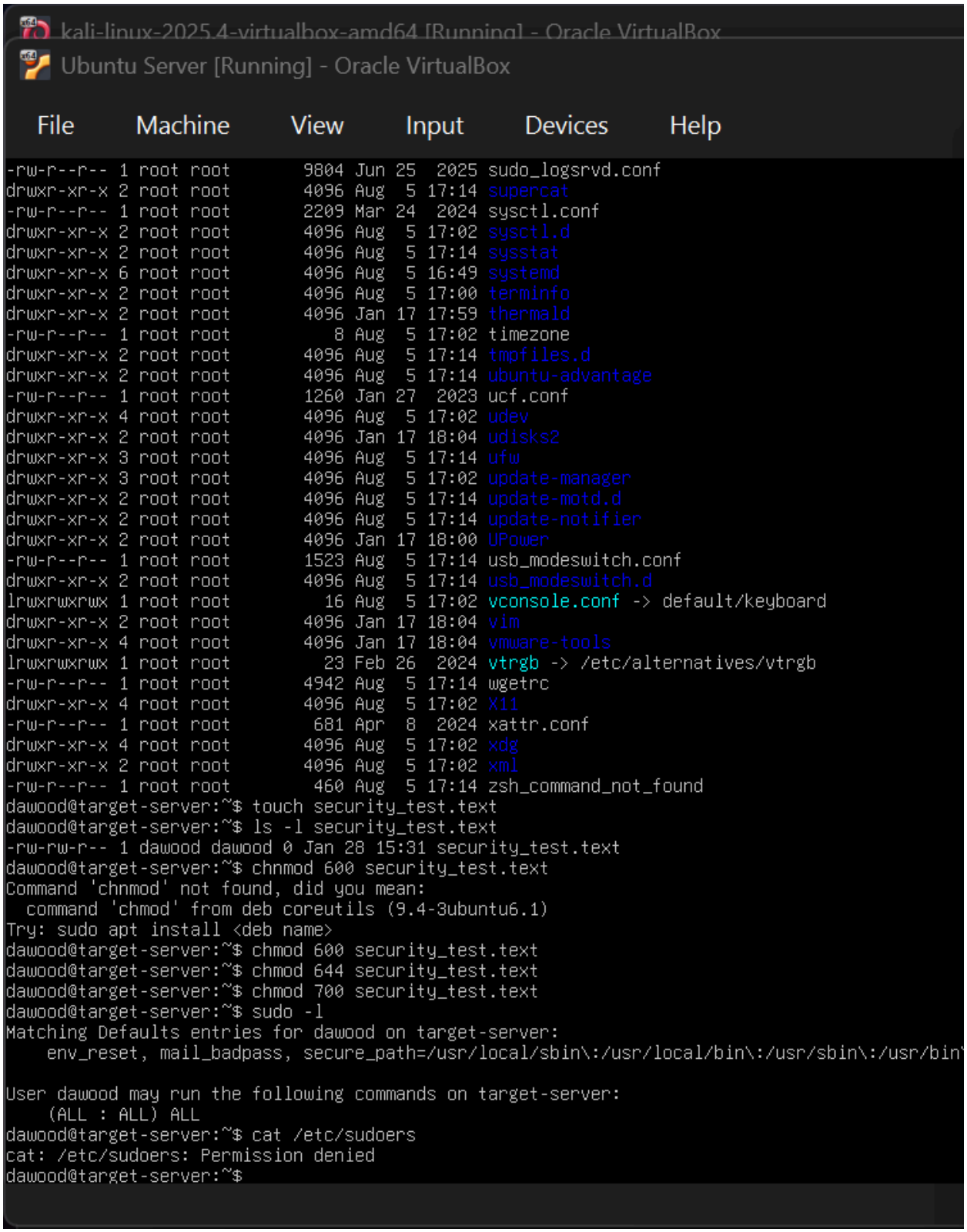
Step 5: Check sudo access

For checking sudo access we will use this command (sudo -l) after this we will use (cat /etc/sudoers)

Why

You inspected the most sensitive configuration file to ensure there were no "backdoor" rules. This ensures **Privilege Integrity**—confirming that nobody can bypass security rules to become Root without your knowledge.

Proof

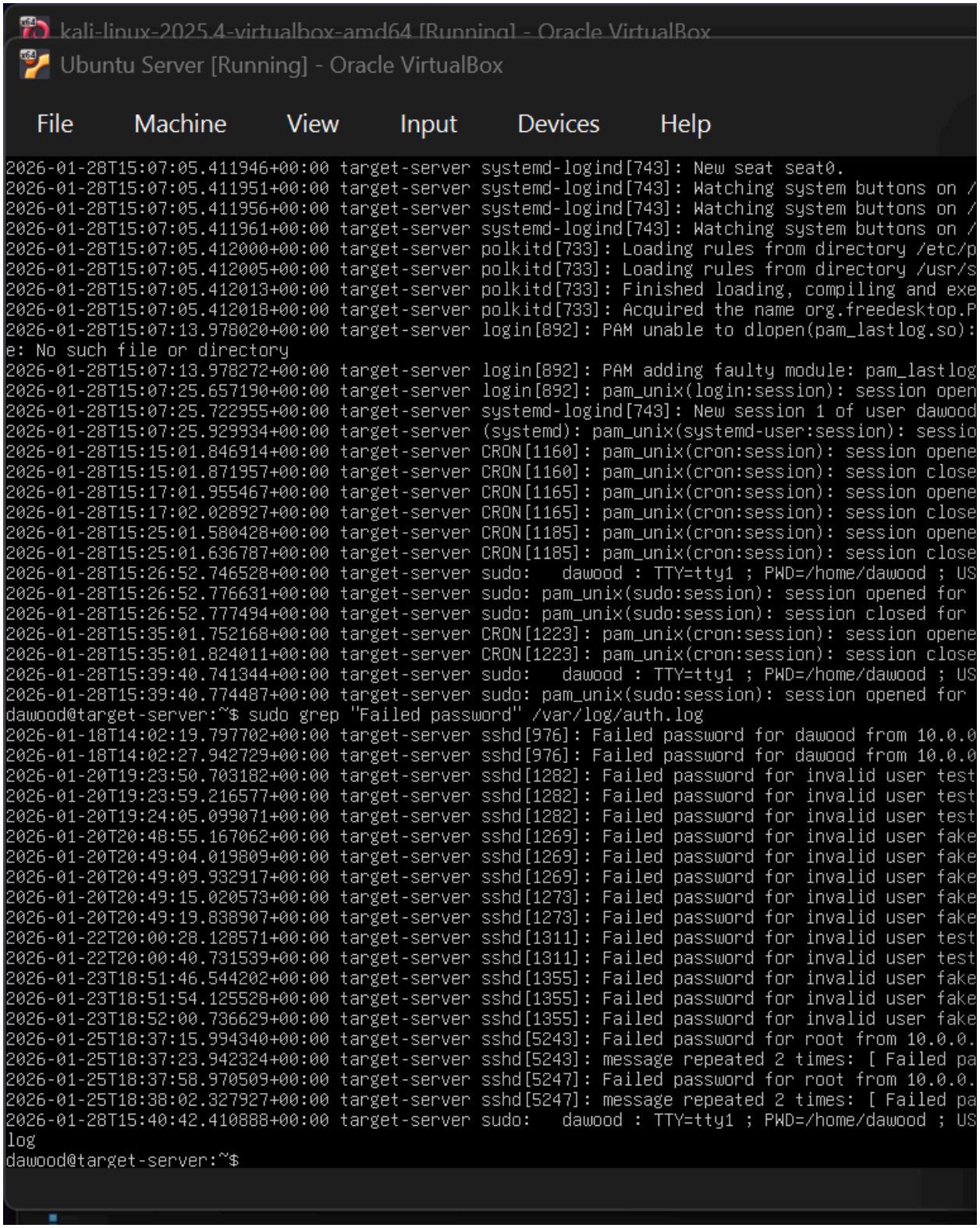

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
-rw-r--r-- 1 root root 9804 Jun 25 2025 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 supercat
-rw-r--r-- 1 root root 2209 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sysctl.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysstat
drwxr-xr-x 6 root root 4096 Aug 5 16:49 systemd
drwxr-xr-x 2 root root 4096 Aug 5 17:00 terminfo
drwxr-xr-x 2 root root 4096 Jan 17 17:59 thermald
-rw-r--r-- 1 root root 8 Aug 5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 tmpfiles.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 ubuntu-advantage
-rw-r--r-- 1 root root 1260 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev
drwxr-xr-x 2 root root 4096 Jan 17 18:04 udisks2
drwxr-xr-x 3 root root 4096 Aug 5 17:14 ufw
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-manager
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-motd.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-notifier
drwxr-xr-x 2 root root 4096 Jan 17 18:00 UPower
-rw-r--r-- 1 root root 1523 Aug 5 17:14 usb_modeswitch.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 usb_modeswitch.d
lrwxrwxrwx 1 root root 16 Aug 5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x 2 root root 4096 Jan 17 18:04 vim
drwxr-xr-x 4 root root 4096 Jan 17 18:04 vmware-tools
lrwxrwxrwx 1 root root 23 Feb 26 2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r-- 1 root root 4942 Aug 5 17:14 wgetrc
drwxr-xr-x 4 root root 4096 Aug 5 17:02 X11
-rw-r--r-- 1 root root 681 Apr 8 2024 xattr.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 xdg
drwxr-xr-x 2 root root 4096 Aug 5 17:02 xml
-rw-r--r-- 1 root root 460 Aug 5 17:14 zsh_command_not_found
dawood@target-server:~$ touch security_test.text
dawood@target-server:~$ ls -l security_test.text
-rw-rw-r-- 1 dawood dawood 0 Jan 28 15:31 security_test.text
dawood@target-server:~$ chnmod 600 security_test.text
Command 'chnmod' not found, did you mean:
command 'chmod' from deb coreutils (9.4-3ubuntu6.1)
Try: sudo apt install <deb name>
dawood@target-server:~$ chmod 600 security_test.text
dawood@target-server:~$ chmod 644 security_test.text
dawood@target-server:~$ chmod 700 security_test.text
dawood@target-server:~$ sudo -l
Matching Defaults entries for dawood on target-server:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
User dawood may run the following commands on target-server:
(ALL : ALL) ALL
dawood@target-server:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
dawood@target-server:~$

Phase 4 – Authentication Logs (This is gold)

Step 6: View login attempts

In this step we will use these command (sudo cat /var/log/auth.log)
After that we will filter and type this (sudo grep "Failed password" /var/log/auth.log)

Proof


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
2026-01-28T15:07:05.411946+00:00 target-server systemd-logind[743]: New seat seat0.
2026-01-28T15:07:05.411951+00:00 target-server systemd-logind[743]: Watching system buttons on /
2026-01-28T15:07:05.411956+00:00 target-server systemd-logind[743]: Watching system buttons on /
2026-01-28T15:07:05.411961+00:00 target-server systemd-logind[743]: Watching system buttons on /
2026-01-28T15:07:05.412000+00:00 target-server polkitd[733]: Loading rules from directory /etc/p
2026-01-28T15:07:05.412005+00:00 target-server polkitd[733]: Loading rules from directory /usr/s
2026-01-28T15:07:05.412013+00:00 target-server polkitd[733]: Finished loading, compiling and exe
2026-01-28T15:07:05.412018+00:00 target-server polkitd[733]: Acquired the name org.freedesktop.P
2026-01-28T15:07:13.978020+00:00 target-server login[892]: PAM unable to dlopen(pam_lastlog.so):
e: No such file or directory
2026-01-28T15:07:13.978272+00:00 target-server login[892]: PAM adding faulty module: pam_lastlog
2026-01-28T15:07:25.657190+00:00 target-server login[892]: pam_unix(login:session): session open
2026-01-28T15:07:25.722955+00:00 target-server systemd-logind[743]: New session 1 of user dawood
2026-01-28T15:07:25.929934+00:00 target-server (systemd): pam_unix(systemd-user:session): sessio
2026-01-28T15:15:01.846914+00:00 target-server CRON[1160]: pam_unix(cron:session): session opene
2026-01-28T15:15:01.871957+00:00 target-server CRON[1160]: pam_unix(cron:session): session close
2026-01-28T15:17:01.955467+00:00 target-server CRON[1165]: pam_unix(cron:session): session opene
2026-01-28T15:17:02.028927+00:00 target-server CRON[1165]: pam_unix(cron:session): session close
2026-01-28T15:25:01.580428+00:00 target-server CRON[1185]: pam_unix(cron:session): session opene
2026-01-28T15:25:01.636787+00:00 target-server CRON[1185]: pam_unix(cron:session): session close
2026-01-28T15:26:52.746528+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; US
2026-01-28T15:26:52.776631+00:00 target-server sudo: pam_unix(sudo:session): session opened for
2026-01-28T15:26:52.777494+00:00 target-server sudo: pam_unix(sudo:session): session closed for
2026-01-28T15:35:01.752168+00:00 target-server CRON[1223]: pam_unix(cron:session): session opene
2026-01-28T15:35:01.824011+00:00 target-server CRON[1223]: pam_unix(cron:session): session close
2026-01-28T15:39:40.741344+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; US
2026-01-28T15:39:40.774487+00:00 target-server sudo: pam_unix(sudo:session): session opened for
dawood@target-server:~$ sudo grep "Failed password" /var/log/auth.log
2026-01-18T14:02:19.797702+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0
2026-01-18T14:02:27.942729+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0
2026-01-20T19:23:50.703182+00:00 target-server sshd[1282]: Failed password for invalid user test
2026-01-20T19:23:59.216577+00:00 target-server sshd[1282]: Failed password for invalid user test
2026-01-20T19:24:05.099071+00:00 target-server sshd[1282]: Failed password for invalid user test
2026-01-20T20:48:55.167062+00:00 target-server sshd[1269]: Failed password for invalid user fake
2026-01-20T20:49:04.019809+00:00 target-server sshd[1269]: Failed password for invalid user fake
2026-01-20T20:49:09.932917+00:00 target-server sshd[1269]: Failed password for invalid user fake
2026-01-20T20:49:15.020573+00:00 target-server sshd[1273]: Failed password for invalid user fake
2026-01-20T20:49:19.838907+00:00 target-server sshd[1273]: Failed password for invalid user fake
2026-01-22T20:00:28.128571+00:00 target-server sshd[1311]: Failed password for invalid user test
2026-01-22T20:00:40.731539+00:00 target-server sshd[1311]: Failed password for invalid user test
2026-01-23T18:51:46.544202+00:00 target-server sshd[1355]: Failed password for invalid user fake
2026-01-23T18:51:54.125528+00:00 target-server sshd[1355]: Failed password for invalid user fake
2026-01-23T18:52:00.736629+00:00 target-server sshd[1355]: Failed password for invalid user fake
2026-01-25T18:37:15.994340+00:00 target-server sshd[5243]: Failed password for root from 10.0.0.
2026-01-25T18:37:23.942324+00:00 target-server sshd[5243]: message repeated 2 times: [Failed pa
2026-01-25T18:37:58.970509+00:00 target-server sshd[5247]: Failed password for root from 10.0.0.
2026-01-25T18:38:02.327927+00:00 target-server sshd[5247]: message repeated 2 times: [Failed pa
2026-01-28T15:40:42.410888+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; US
log
dawood@target-server:~$

Phase 5 – Attacker Mindset (Kali)

From **Kali**, attempt:

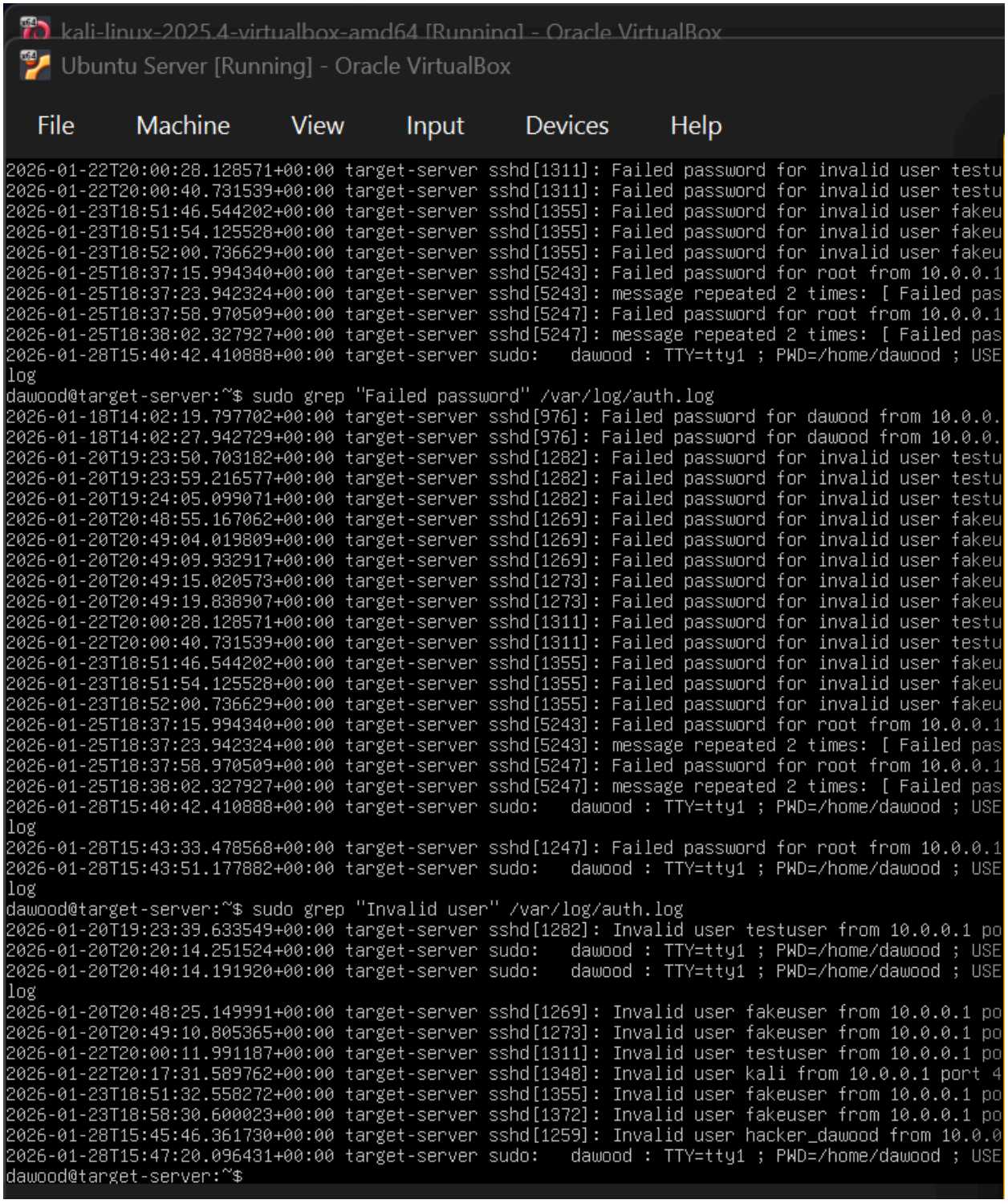
SSH login (wrong password)
Multiple attempts
Then return to Ubuntu logs and **see yourself**.

(Detection + Attribution)

The command we are using in kali is (ssh hacker_dawood@YOUR_UBUNTU_IP) after that this (ssh root@YOUR_UBUNTU_IP) we will attempt wrong password multiple time

Now on the ubuntu we will use this to see attempt (sudo grep "Invalid user" /var/log/auth.log) failed ,we will use this command (sudo grep "root" /var/log/auth.log | grep "Failed")

Why
This was the most important step. You proved you can detect an attack (Brute Force) and perform Attribution (linking the attack to the Kali IP `10.0.0.2`). This is the core job of a SOC Analyst: turning raw data into evidence.
Proof


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
Ubuntu Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
2026-01-22T20:00:28.128571+00:00 target-server sshd[1311]: Failed password for invalid user testu
2026-01-22T20:00:40.731539+00:00 target-server sshd[1311]: Failed password for invalid user testu
2026-01-23T18:51:46.544202+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-23T18:51:54.125528+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-23T18:52:00.736629+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-25T18:37:15.994340+00:00 target-server sshd[5243]: Failed password for root from 10.0.0.1
2026-01-25T18:37:23.942324+00:00 target-server sshd[5243]: message repeated 2 times: [Failed pas
2026-01-25T18:37:58.970509+00:00 target-server sshd[5247]: Failed password for root from 10.0.0.1
2026-01-25T18:38:02.327927+00:00 target-server sshd[5247]: message repeated 2 times: [Failed pas
2026-01-28T15:40:42.410888+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
log
dawood@target-server:~$ sudo grep "Failed password" /var/log/auth.log
2026-01-18T14:02:19.797702+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0.
2026-01-18T14:02:27.942729+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0.
2026-01-20T19:23:50.703182+00:00 target-server sshd[1282]: Failed password for invalid user testu
2026-01-20T19:23:59.216577+00:00 target-server sshd[1282]: Failed password for invalid user testu
2026-01-20T19:24:05.099071+00:00 target-server sshd[1282]: Failed password for invalid user testu
2026-01-20T20:48:55.167062+00:00 target-server sshd[1269]: Failed password for invalid user fakeu
2026-01-20T20:49:04.019809+00:00 target-server sshd[1269]: Failed password for invalid user fakeu
2026-01-20T20:49:09.932917+00:00 target-server sshd[1269]: Failed password for invalid user fakeu
2026-01-20T20:49:15.020573+00:00 target-server sshd[1273]: Failed password for invalid user fakeu
2026-01-20T20:49:19.838907+00:00 target-server sshd[1273]: Failed password for invalid user fakeu
2026-01-22T20:00:28.128571+00:00 target-server sshd[1311]: Failed password for invalid user testu
2026-01-22T20:00:40.731539+00:00 target-server sshd[1311]: Failed password for invalid user testu
2026-01-23T18:51:46.544202+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-23T18:51:54.125528+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-23T18:52:00.736629+00:00 target-server sshd[1355]: Failed password for invalid user fakeu
2026-01-25T18:37:15.994340+00:00 target-server sshd[5243]: Failed password for root from 10.0.0.1
2026-01-25T18:37:23.942324+00:00 target-server sshd[5243]: message repeated 2 times: [Failed pas
2026-01-25T18:37:58.970509+00:00 target-server sshd[5247]: Failed password for root from 10.0.0.1
2026-01-25T18:38:02.327927+00:00 target-server sshd[5247]: message repeated 2 times: [Failed pas
2026-01-28T15:40:42.410888+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
log
2026-01-28T15:43:33.478568+00:00 target-server sshd[1247]: Failed password for root from 10.0.0.1
2026-01-28T15:43:51.177882+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
log
dawood@target-server:~$ sudo grep "Invalid user" /var/log/auth.log
2026-01-20T19:23:39.633549+00:00 target-server sshd[1282]: Invalid user testuser from 10.0.0.1 po
2026-01-20T20:20:14.251524+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
2026-01-20T20:40:14.191920+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
log
2026-01-20T20:48:25.149991+00:00 target-server sshd[1269]: Invalid user fakeuser from 10.0.0.1 po
2026-01-20T20:49:10.805365+00:00 target-server sshd[1273]: Invalid user fakeuser from 10.0.0.1 po
2026-01-22T20:00:11.991187+00:00 target-server sshd[1311]: Invalid user testuser from 10.0.0.1 po
2026-01-22T20:17:31.589762+00:00 target-server sshd[1348]: Invalid user kali from 10.0.0.1 port 4
2026-01-23T18:51:32.558272+00:00 target-server sshd[1355]: Invalid user fakeuser from 10.0.0.1 po
2026-01-23T18:58:30.600023+00:00 target-server sshd[1372]: Invalid user fakeuser from 10.0.0.1 po
2026-01-28T15:45:46.361730+00:00 target-server sshd[1259]: Invalid user hacker_dawood from 10.0.0
2026-01-28T15:47:20.096431+00:00 target-server sudo: dawood : TTY=tty1 ; PWD=/home/dawood ; USE
dawood@target-server:~$

The Command Toolkit

Category	Command	Security Purpose
User Audit	cat /etc/passwd | cut -d: -f1	Inventory all users and spot "Ghost" accounts.
Group Audit	groups & cat /etc/group	Verify who holds administrative (Sudo) power.
Hardening	chmod 600 <filename>	Apply **Least Privilege** by locking files to "Owner Only."
Admin Audit	sudo cat /etc/sudoers	Inspect the master rulebook for backdoor permissions.
Monitoring	grep "Failed password" /var/log/auth.log	**Detection:** Spotting a Brute Force attack in real-time.
Attribution	grep "Invalid user" /var/log/auth.log	**Investigation:** Identifying the attacker's IP and target.