



Day 8 – Lateral Movement Awareness

- ◆ **PHASE 1 – Concept Lock (Read Before Touching Keyboard)**

Why would an attacker move laterally instead of attacking directly?

Ans: See first thing first attacker doesn't want to attack simply ,he wants all access to our devices including,my emails,my files,my messages,my funds, my bank details, my files data, attackers are like a fire slowly slowly graduate to take control of all things .they send malicious malware , they overtake our social media accounts for accessing our location ,emails,numbers friends ,then they send fishing ,vishing attacks throw emails. To override these things we have to make sure we set authentication passwords, two factor authentications ,and many other things , we also make sure we have secured networks tools to oavid attackers attempts we, can use fail2ban tool, it is like a bouncer or security gerd ,which protect our systems from attacker entering ,and we can use ufw ,which firewall like brick contain our files ,data save.

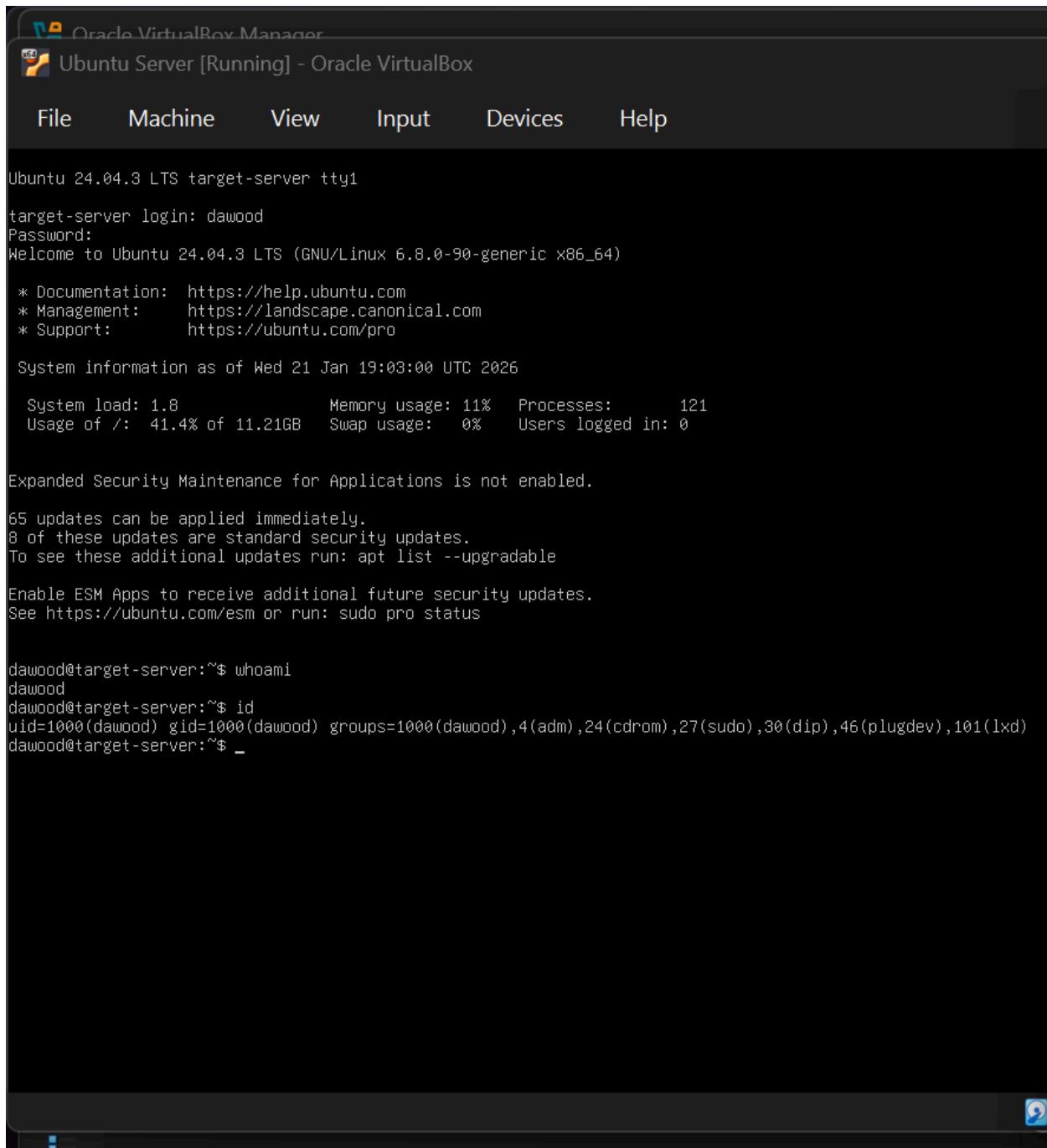
- ◆ **PHASE 2 – User & Privilege Awareness (Ubuntu Target)**

Step 1: Check Current Users

In this step we will check our systems,because attacker moves silently in our systems so have to make sure ,we are aware of User name ,Groups,UID/GID

In this step we will use this(whoami) and this (id) commands to track our system .

Proof



The screenshot shows the Oracle VirtualBox Manager interface with a single virtual machine named "Ubuntu Server [Running]". The machine is running Ubuntu 24.04.3 LTS. The terminal window displays the following system information:

```
Ubuntu 24.04.3 LTS target-server tty1
target-server login: dawood
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed 21 Jan 19:03:00 UTC 2026

 System load: 1.8          Memory usage: 11%   Processes:      121
 Usage of /: 41.4% of 11.21GB Swap usage: 0%     Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

65 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

dawood@target-server:~$ whoami
dawood
dawood@target-server:~$ id
uid=1000(dawood) gid=1000(dawood) groups=1000(dawood),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),101(lxd)
dawood@target-server:~$ _
```

Step 2: List All Users

After checking three thing we also have to make sure to check user list ,and program like ssh ,apache that runs system

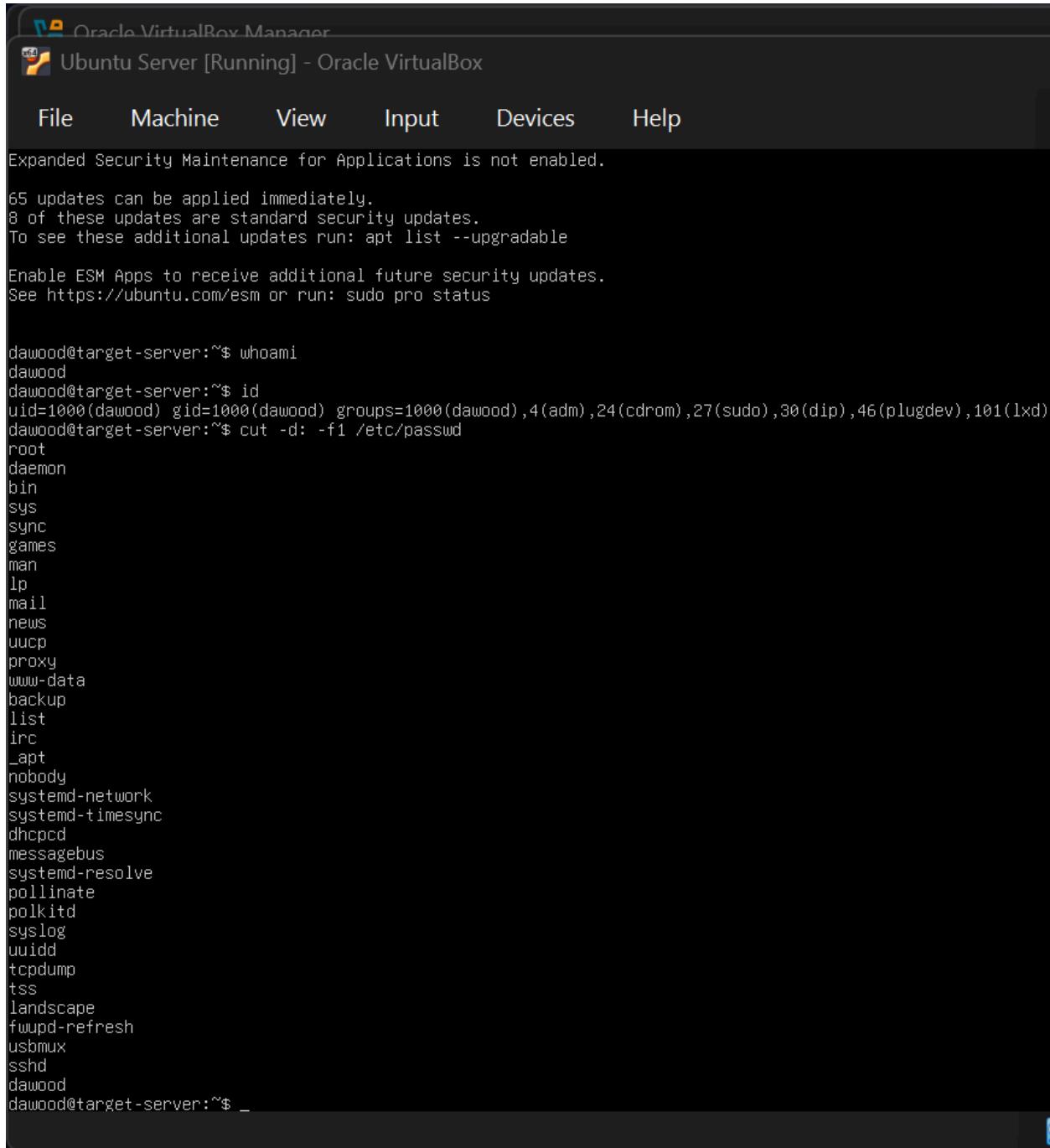
In this step the command we will use is (cut -d: -f1 /etc/passwd).

Normal users like me dawood

Service accounts like bin,ssh,apache,etc

Anything unusual

Proof



The screenshot shows the Oracle VirtualBox Manager interface with a single running VM named "Ubuntu Server [Running]". The VM window displays a terminal session on the Ubuntu server. The terminal output shows the user "dawood" running several commands:

```
Expanded Security Maintenance for Applications is not enabled.  
65 updates can be applied immediately.  
8 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
dawood@target-server:~$ whoami  
dawood  
dawood@target-server:~$ id  
uid=1000(dawood) gid=1000(dawood) groups=1000(dawood),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),101(lxd)  
dawood@target-server:~$ cut -d: -f1 /etc/passwd  
root  
daemon  
bin  
sys  
sync  
games  
man  
lp  
mail  
news  
uucp  
proxy  
www-data  
backup  
list  
irc  
_apt  
nobody  
systemd-network  
systemd-timesync  
dhcpcd  
messagebus  
systemd-resolve  
pollinate  
polkitd  
syslog  
uuid  
tcpdump  
tss  
landscape  
fwupd-refresh  
usbmux  
sshd  
dawood  
dawood@target-server:~$ _
```

Step 3: Check Privileged Access

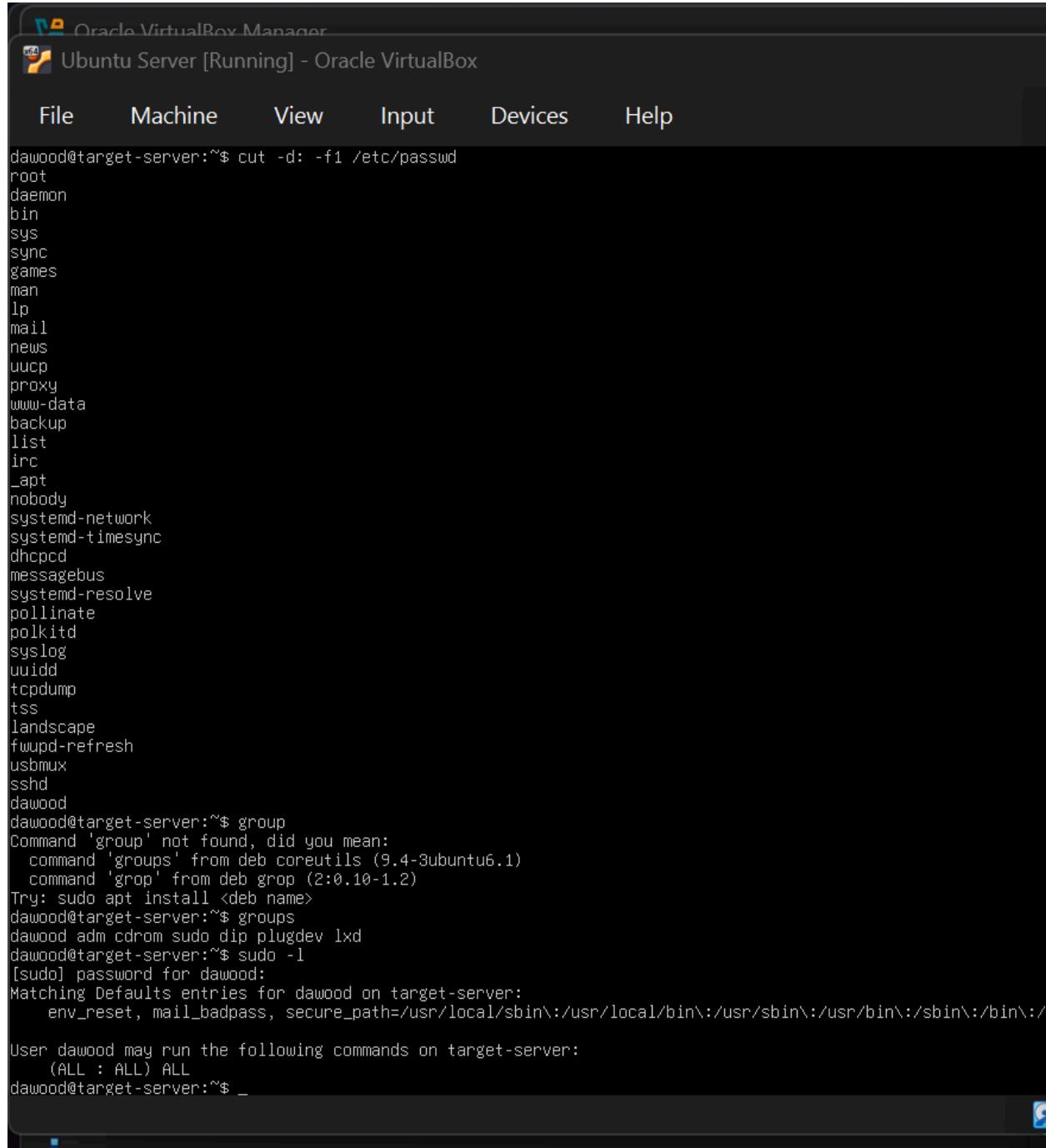
In this step we will privileged access like list of groups ,admins, this access only admin can see

The command we will use in this access is (groups) and after that (sudo -l)

Can this user run sudo? yes

Is password required? Yes

Proof



A screenshot of the Oracle VirtualBox Manager interface. At the top, it shows "Ubuntu Server [Running] - Oracle VirtualBox". Below the title bar is a menu bar with File, Machine, View, Input, Devices, and Help. The main window displays a terminal session for a user named "dawood" on a host named "target-server". The terminal output shows the user running the "cut" command to extract the first field from /etc/passwd, listing various system users. Then, the user runs "group" and receives a command not found error, suggesting they might be root or have sudo privileges. Finally, the user runs "sudo -l" and sees the expected output showing they can run any command.

```
dawood@target-server:~$ cut -d: -f1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
_apt
nobody
systemd-network
systemd-timesync
dhcpcd
messagebus
systemd-resolve
polllinate
polkitd
syslog
uuid
tcpdump
tss
landscape
fwupd-refresh
usbmux
sshd
dawood
dawood@target-server:~$ group
Command 'group' not found, did you mean:
  command 'groups' from deb coreutils (9.4-3ubuntu6.1)
  command 'grop' from deb grep (2:0.10-1.2)
Try: sudo apt install <deb name>
dawood@target-server:~$ groups
dawood adm cdrom sudo dip plugdev lxd
dawood@target-server:~$ sudo -l
[sudo] password for dawood:
Matching Defaults entries for dawood on target-server:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/

User dawood may run the following commands on target-server:
(ALL : ALL) ALL
dawood@target-server:~$ _
```

◆ PHASE 3 – Simulated Lateral Behavior (Safe)

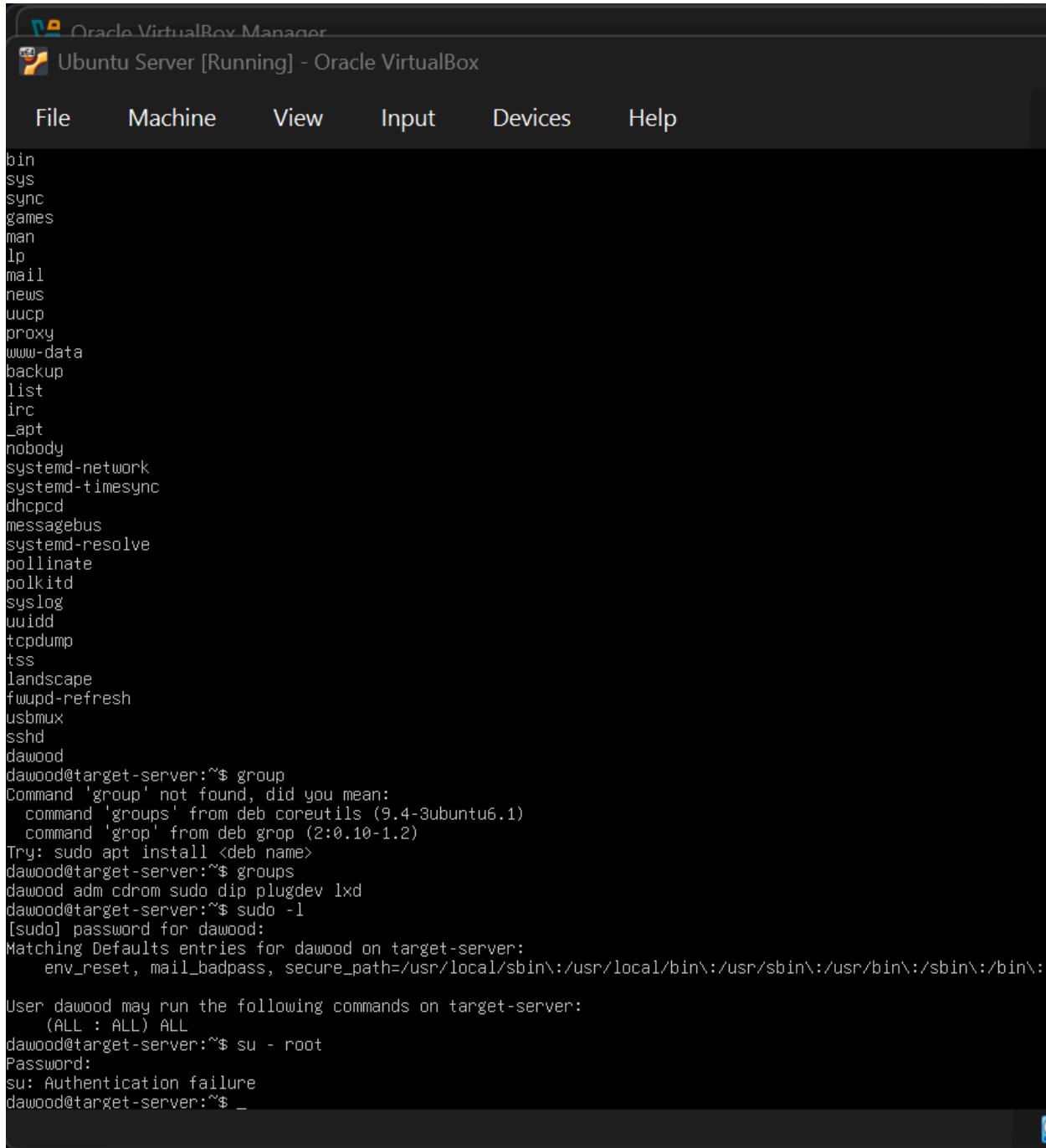
We simulate behavior, not hacking.

Step 4: Switch User (If Possible)

In this step we have to switch to another user ,we will check if we can switch or it will block the movement which is a good sign .

The command we are using in this is (su - username)

Proof



The screenshot shows the Oracle VirtualBox Manager interface. At the top, there's a menu bar with File, Machine, View, Input, Devices, and Help. Below the menu is a list of users and services. The user 'dawood' is currently selected. The terminal window below shows the following session:

```
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
_apt
nobody
systemd-network
systemd-timesync
dhpcd
messagebus
systemd-resolve
pollinate
polkitd
syslog
uuid
tcpdump
tss
landscape
fwupd-refresh
usbmux
sshd
dawood
dawood@target-server:~$ group
Command 'group' not found, did you mean:
  command 'groups' from deb coreutils (9.4-3ubuntu6.1)
  command 'grop' from deb grep (2:0.10-1.2)
Try: sudo apt install <deb name>
dawood@target-server:~$ groups
dawood adm cdrom sudo dip plugdev lxd
dawood@target-server:~$ sudo -l
[sudo] password for dawood:
Matching Defaults entries for dawood on target-server:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
User dawood may run the following commands on target-server:
  (ALL : ALL) ALL
dawood@target-server:~$ su - root
Password:
su: Authentication failure
dawood@target-server:~$ _
```

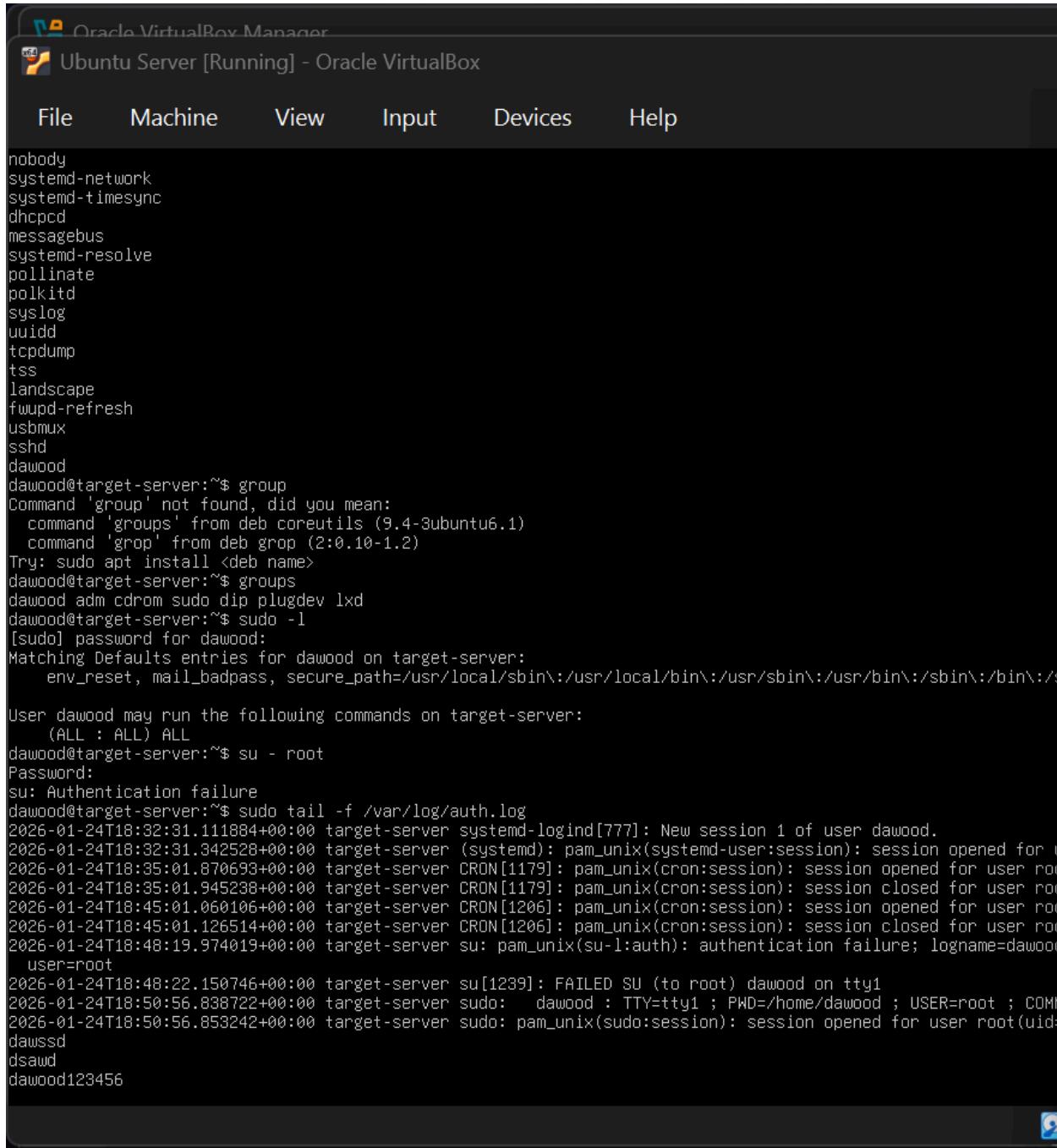
Step 5: Monitor Authentication Logs

In this step we will monitor with the help of auth.log we will see login attempts and many more

The command we are using in this is (sudo tail -f /var/log/auth.log)

The **-f** stands for "follow." It keeps the file open and shows you new logs the exact second they happen

Proof



The screenshot shows the Oracle VirtualBox Manager interface with a single VM named "Ubuntu Server [Running]". The VM window displays a terminal session for the user "dawood" on the target server. The terminal output shows various system logs and command attempts, including a failed password attempt and a failed su command.

```
nobody
systemd-network
systemd-timesync
dhpcd
messagebus
systemd-resolve
pollinate
polkitd
syslog
uuid
tcpdump
tss
landscape
fwupd-refresh
usbmux
sshd
dawood
dawood@target-server:~$ group
Command 'group' not found, did you mean:
  command 'groups' from deb coreutils (9.4-3ubuntu6.1)
  command 'grop' from deb grop (2:0.10-1.2)
Try: sudo apt install <deb name>
dawood@target-server:~$ groups
dawood adm cdrom sudo dip plugdev lxd
dawood@target-server:~$ sudo -l
[sudo] password for dawood:
Matching Defaults entries for dawood on target-server:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/s
User dawood may run the following commands on target-server:
  (ALL : ALL) ALL
dawood@target-server:~$ su - root
Password:
su: Authentication failure
dawood@target-server:~$ sudo tail -f /var/log/auth.log
2026-01-24T18:32:31.111884+00:00 target-server systemd-logind[777]: New session 1 of user dawood.
2026-01-24T18:32:31.342528+00:00 target-server (systemd): pam_unix(systemd-user:session): session opened for user dawood
2026-01-24T18:35:01.870693+00:00 target-server CRON[1179]: pam_unix(cron:session): session opened for user root
2026-01-24T18:35:01.945238+00:00 target-server CRON[1179]: pam_unix(cron:session): session closed for user root
2026-01-24T18:45:01.060106+00:00 target-server CRON[1206]: pam_unix(cron:session): session opened for user root
2026-01-24T18:45:01.126514+00:00 target-server CRON[1206]: pam_unix(cron:session): session closed for user root
2026-01-24T18:48:19.974019+00:00 target-server su: pam_unix(su-1:auth): authentication failure; logname=dawood
  user=root
2026-01-24T18:48:22.150746+00:00 target-server su[1239]: FAILED SU (to root) dawood on tty1
2026-01-24T18:50:56.838722+00:00 target-server sudo:  dawood : TTY=tty1 ; PWD=/home/dawood ; USER=root ; COMM=ls
2026-01-24T18:50:56.853242+00:00 target-server sudo: pam_unix(sudo:session): session opened for user root(uid=dawood)
dawood
dawood123456
```

◆ PHASE 4 – Detection from Defender Side

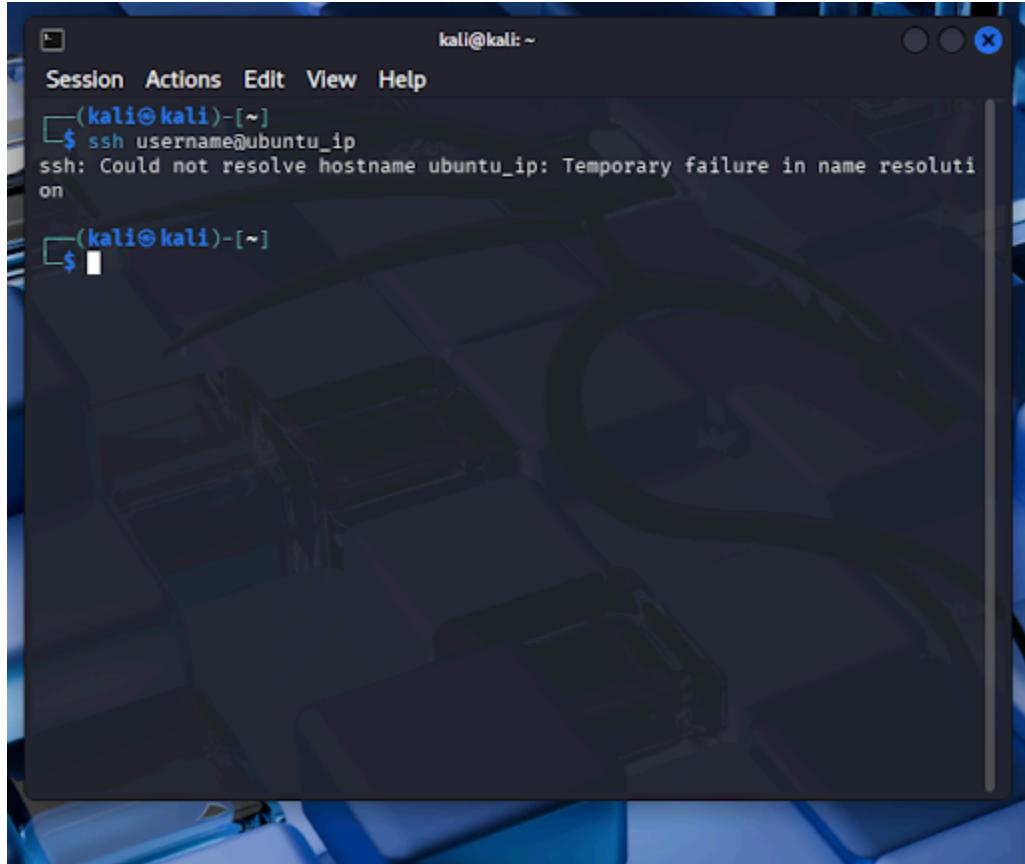
Step 6: From Kali, Attempt SSH Access

In this step we will make detection by using ssh tools , to monitor

ubuntu side but the main important thing after command is to fail to login which is the best and positive sign .

In this the command we are using is (ssh username@ubuntu_ip)
If it fails ,there is more scalability.

Proof



A screenshot of a terminal window titled "kali@kali: ~". The window shows the following text:

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ssh username@ubuntu_ip
ssh: Could not resolve hostname ubuntu_ip: Temporary failure in name resolution
(kali㉿kali)-[~]
$
```

Step 7: Correlate Logs

Auth.log: authentication log tool is monitoring log attempts and any other unusual activity on our system

Fail2Ban: The fail2ban tool is like the security guard of our office. If any drunken men attempt to enter, guards will kick them out and ban them in society.

Who attempted access?

Attacker will attempt the access

From where?

From ssh apache and attacking with malware multiple attempts

Was it normal

Attacks are normal

1. Command Table (The "How-To")

These are the technical actions you performed today to audit the system.

Command	Action	Why a SOC Analyst uses it
whoami	Identity Check	To confirm exactly which user is executing commands.
id	Privilege Check	To see the UID, GID, and specific group memberships (like sudo).
cut -d: -f1 /etc/passwd	User Discovery	To list all accounts on the system and look for unauthorized users.
sudo -l	Rights Audit	To check what specific admin powers a user has.

sudo cat /etc/shadow	Hash Discovery	To see the encrypted passwords (only possible with high privileges).
su - username	Lateral Movement	To attempt to "hop" from one user account to another.
tail -f /var/log/auth.log	Live Monitoring	To watch security events (logins/sudo failures) in real-time.

. Key Concepts Table (The "Knowledge")

These are the "Keys" or core security principles you learned today.

Key Concept	Definition	Importance in Defense
Lateral Movement	Moving from one account/machine to another.	This is how attackers find sensitive data after getting inside.
Privilege Escalation	Moving from a "Low" user to a "High" user (Root).	This is the attacker's goal to gain full control of the server.

Baseline Identity	The normal state of a user's permissions.	You must know "normal" to detect "unusual" behavior.
Password Hashing	Encrypting passwords so they aren't readable.	Prevents attackers from seeing passwords even if they see the file.
Audit Trail	The record of events in <code>auth.log</code> .	Provides the evidence needed to prove an attack happened.

Walaikum Assalam! Excellent idea. Building these tables is how you turn a lab session into a professional **Standard Operating Procedure (SOP)**.

1. Command Table (The "How-To")

These are the technical actions you performed today to audit the system.

Command	Action	Why a SOC Analyst uses it
whoami	Identity Check	To confirm exactly which user is executing commands.

id	Privilege Check	To see the UID, GID, and specific group memberships (like <code>sudo</code>).
<code>cut -d: -f1 /etc/passwd</code>	User Discovery	To list all accounts on the system and look for unauthorized users.
<code>sudo -l</code>	Rights Audit	To check what specific admin powers a user has.
<code>su - username</code>	Lateral Movement	To attempt to "hop" from one user account to another.
<code>tail -f /var/log/auth.log</code>	Live Monitoring	To watch security events (logins/sudo failures) in real-time.

2. Key Concepts Table (The "Knowledge")

These are the "Keys" or core security principles you learned today.

Key Concept	Definition	Importance in Defense

Lateral Movement	Moving from one account/machine to another.	This is how attackers find sensitive data after getting inside.
Privilege Escalation	Moving from a "Low" user to a "High" user (Root).	This is the attacker's goal to gain full control of the server.
Baseline Identity	The normal state of a user's permissions.	You must know "normal" to detect "unusual" behavior.
Password Hashing	Encrypting passwords so they aren't readable.	Prevents attackers from seeing passwords even if they see the file.
Audit Trail	The record of events in auth.log .	Provides the evidence needed to prove an attack happened.

3. Full Form Table (The "Terminology")

Professional communication requires knowing the correct technical names.

Abbreviation	Full Form	Meaning in this Lab

UID	User Identifier	The unique number assigned to every Linux user.
GID	Group Identifier	The number identifying a user's primary group.
IAM	Identity & Access Management	The framework for ensuring the right people have the right access.
SSH	Secure Shell	The protocol used to log in remotely (which we monitored).
SUDO	Superuser DO	A command that allows users to run programs with security privileges.
SOC	Security Operations Center	The team (you!) that monitors and defends the organization.

