🛡️ Day 8 – Lateral Movement Awareness

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

Why would an attacker move laterally instead of attacking directly?

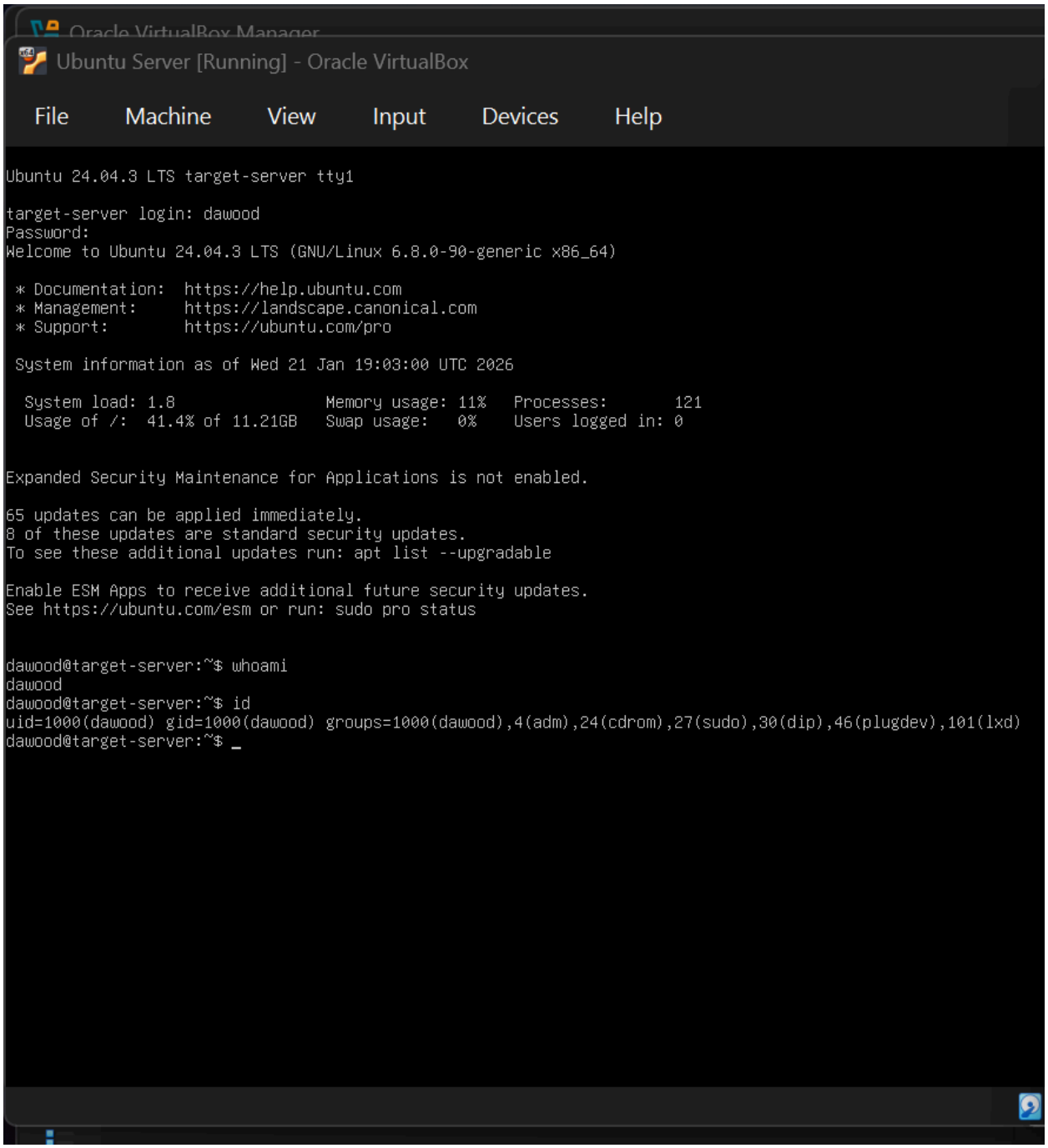
Ans: See first thing first attacker doesn't want to attack simply ,he wants all access to our devices including,my emails,my files,my messages,my funds, my bank details, my files data, attackers are like a fire slowly slowly graduate to take control of all things .they send malicious malware , they overtake 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 ovaid 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

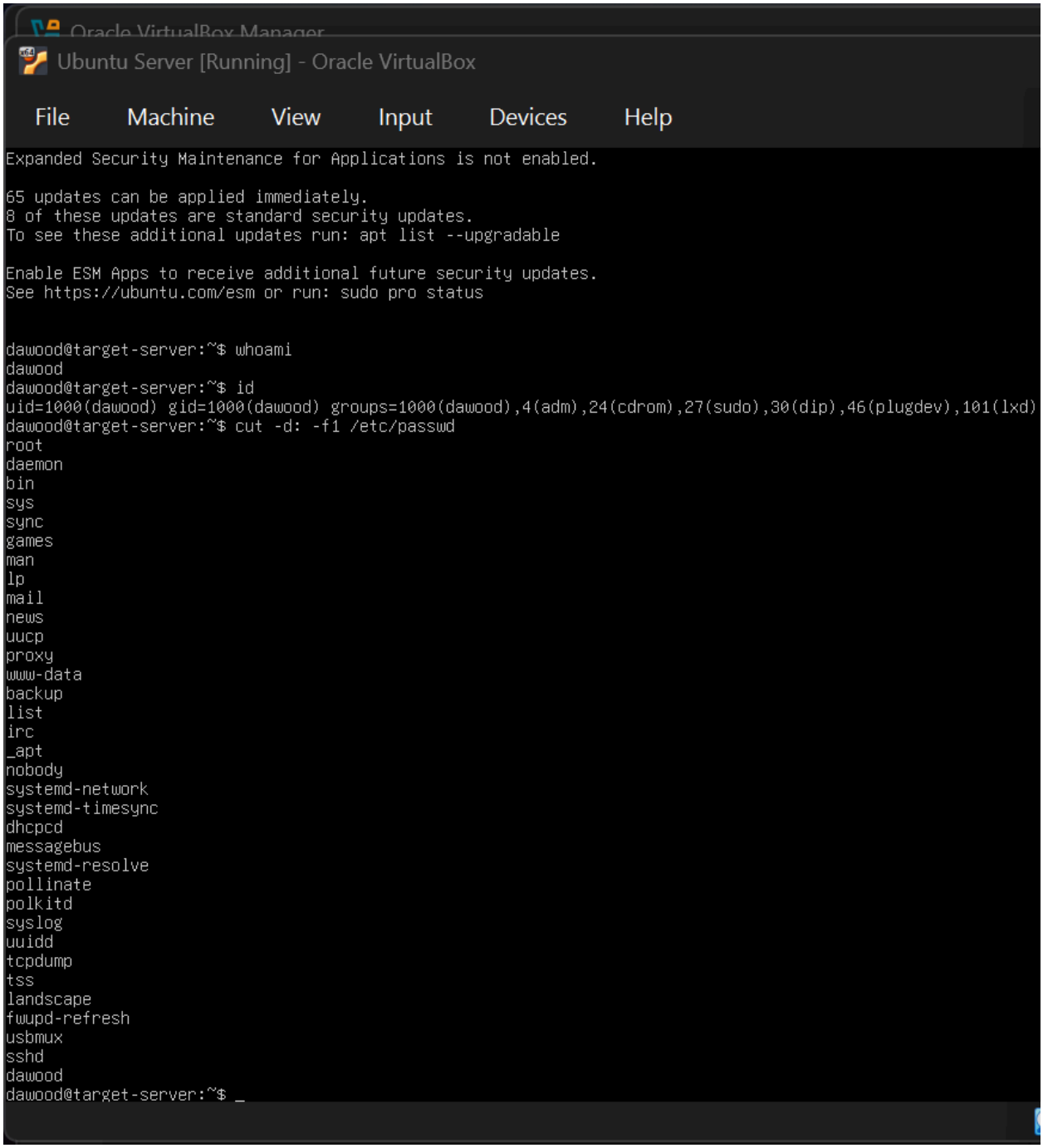


Step 2: List All Users

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

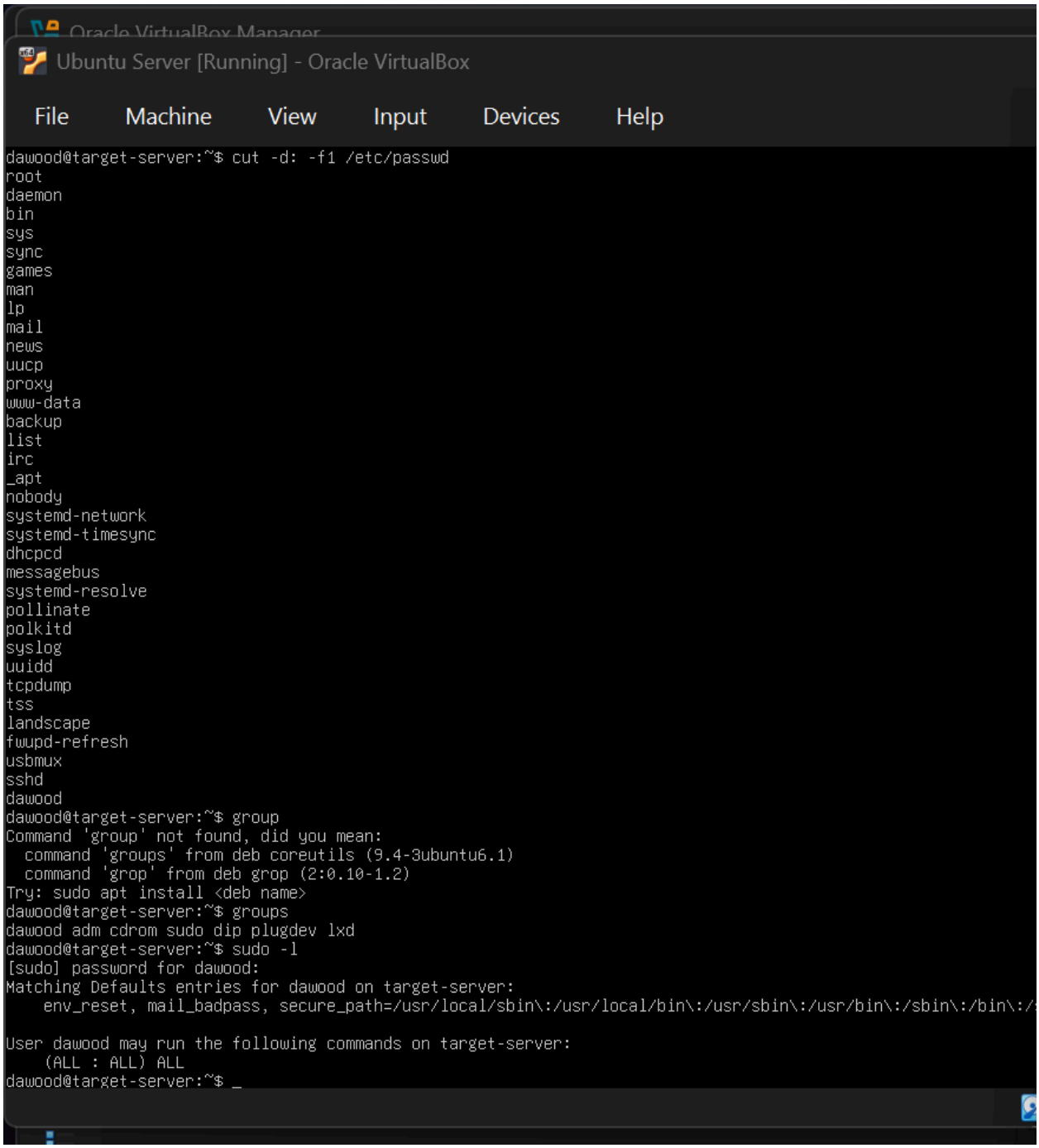
Proof



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



🔹 PHASE 3 – Simulated Lateral Behavior (Safe)

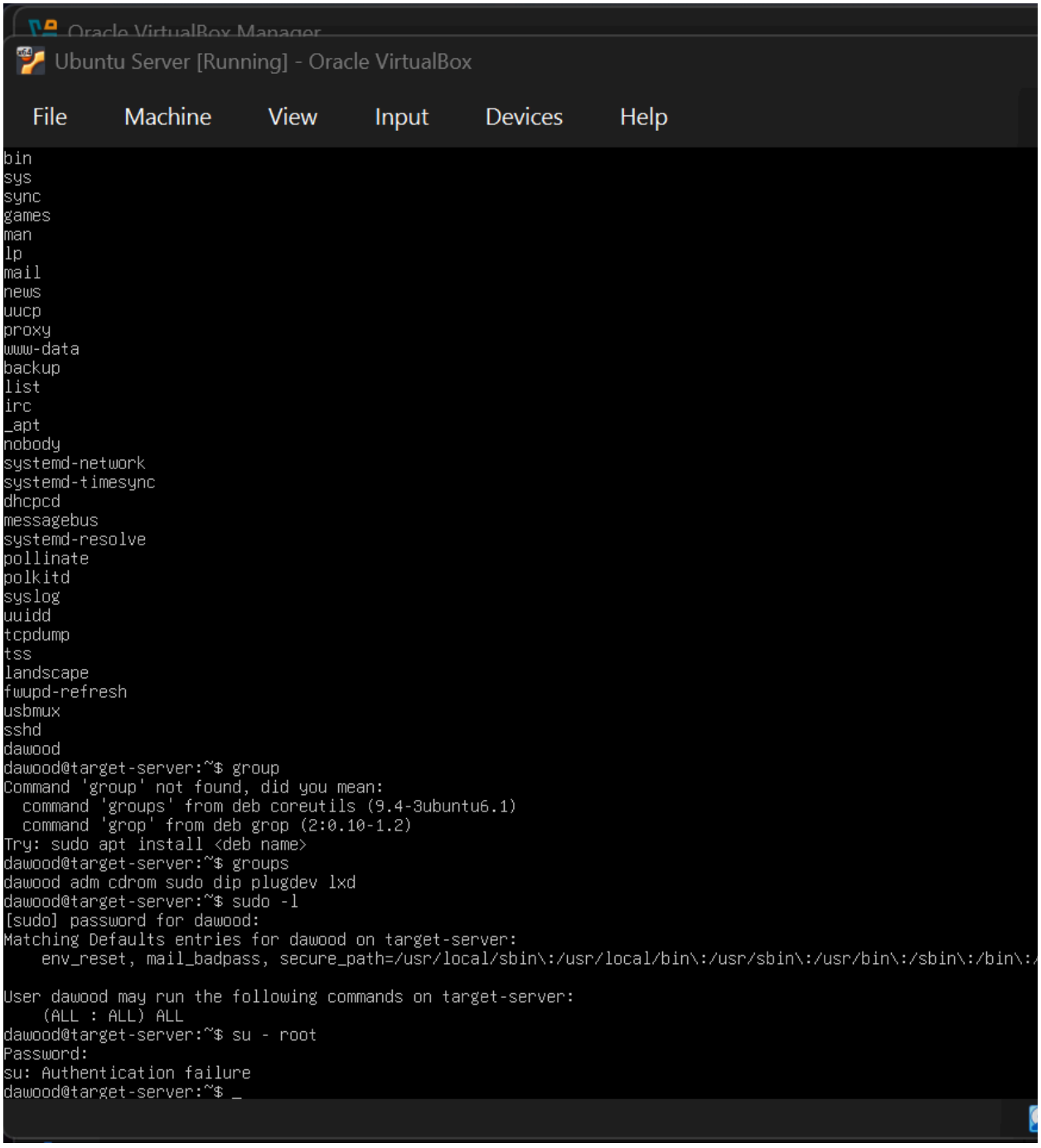
We simulate behavior, not hacking.

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 .

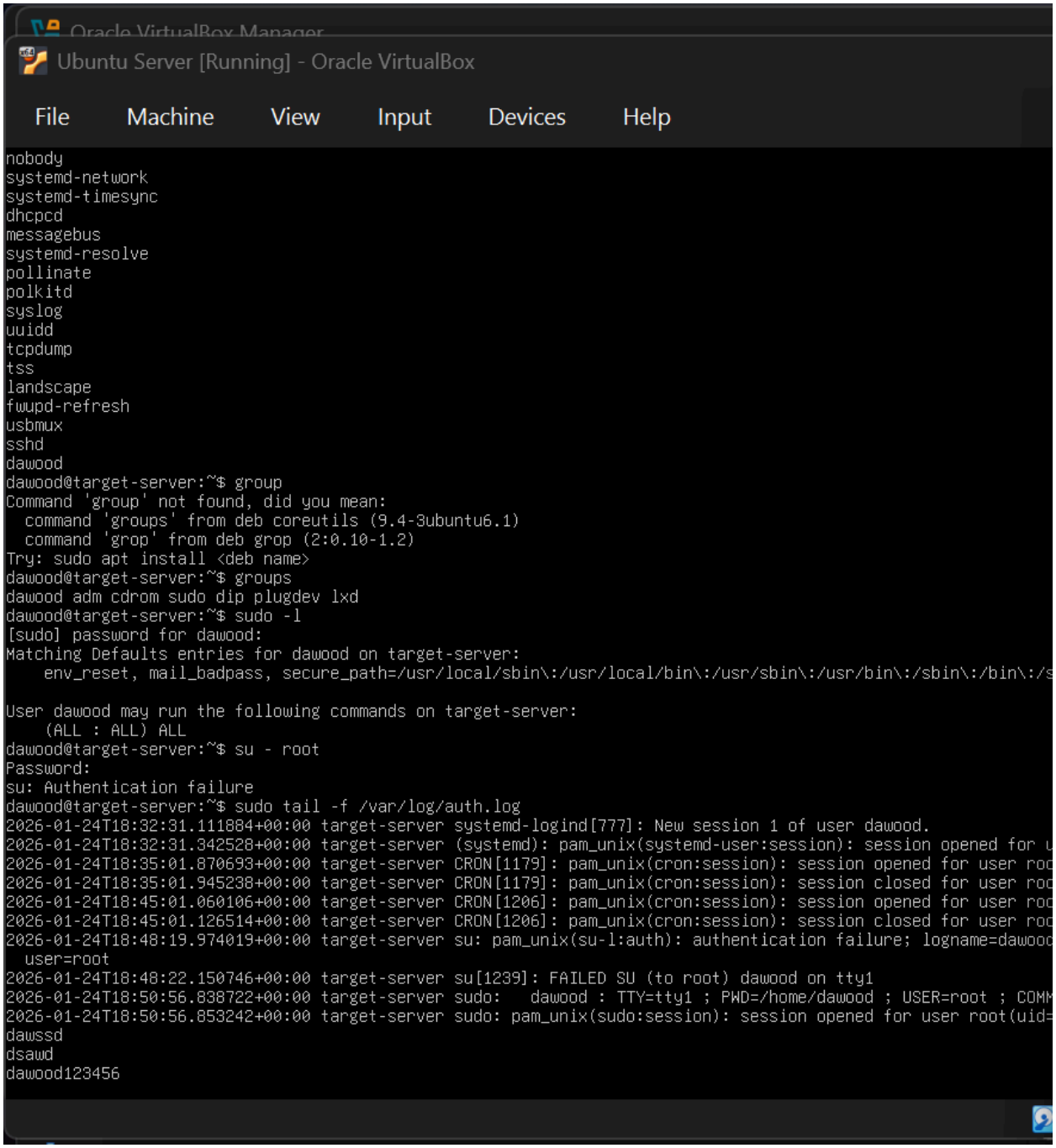
The command we are using in this is (su - username)

Proof



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



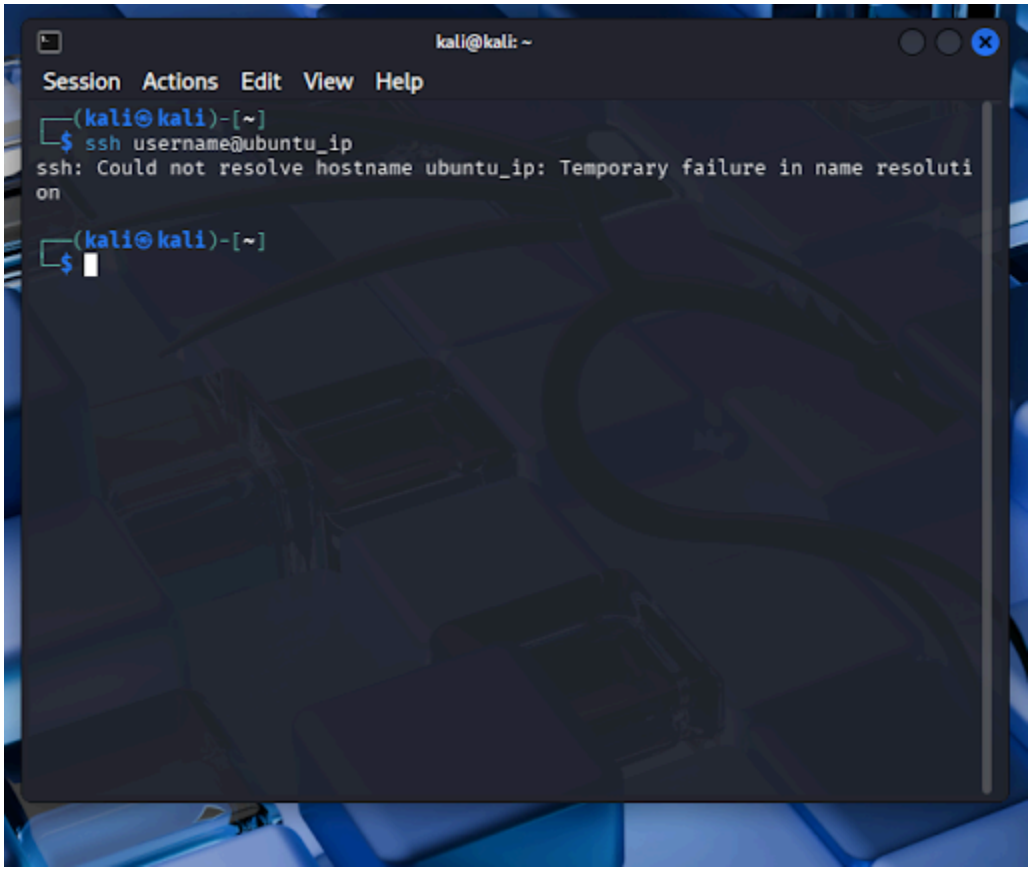
🔹 PHASE 4 – Detection from Defender Side

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



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 auth.log.	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 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.
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.

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.