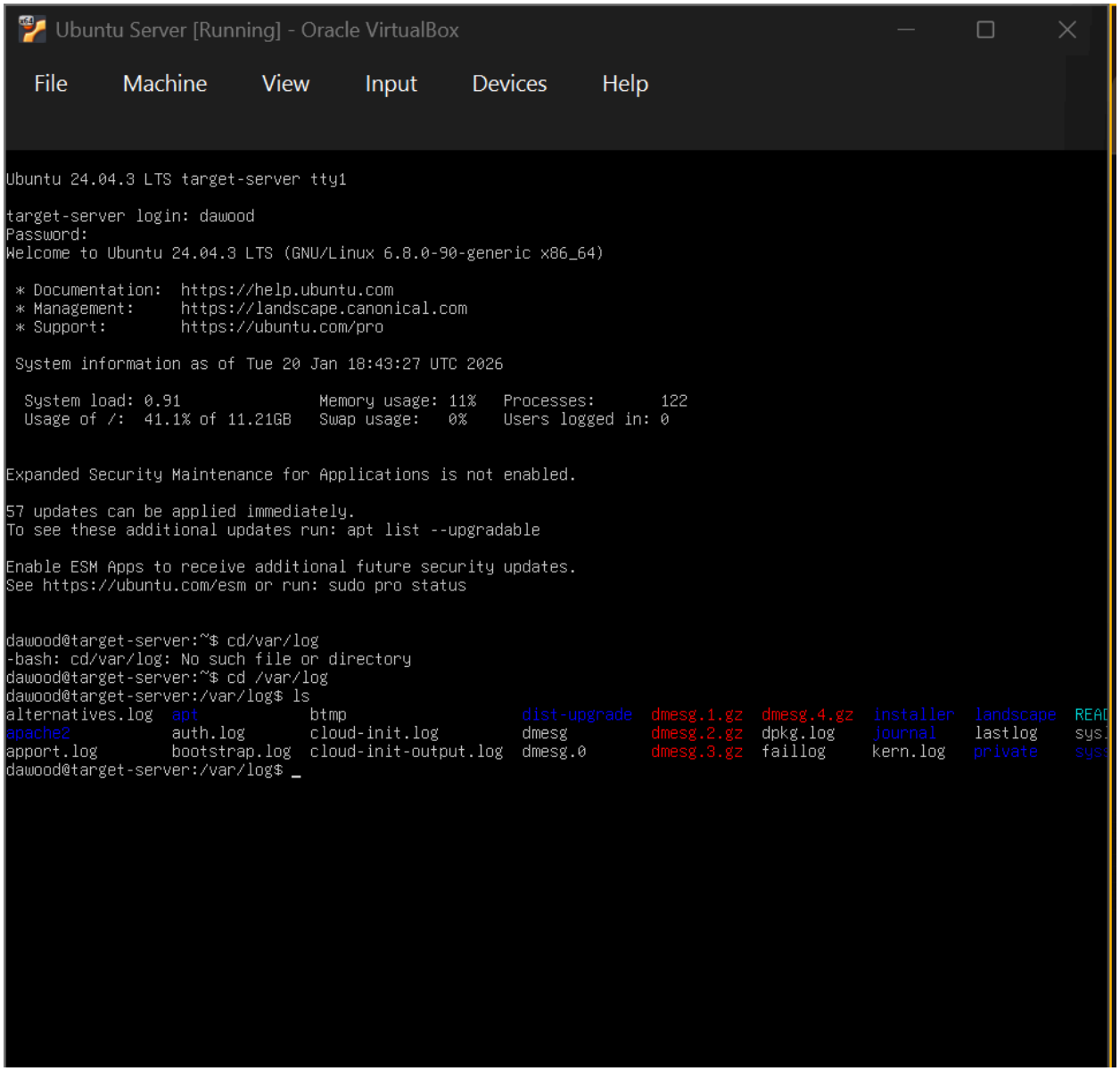
🕵️ DAY 4 — Intrusion Detection & Log Analysis

Role alignment: SOC Analyst → Network Security Engineer
Mindset today: “If someone touched my system, I will know.”

Ubuntu (target)>>kali (attacker):

STEP 1: Know WHERE Linux Stores Security Evidence*:*
In this step we have to think like cc tv camera
The command we are using is (cd /var/log)
If we want to see multiple camera we use this command after that use this command (ls)

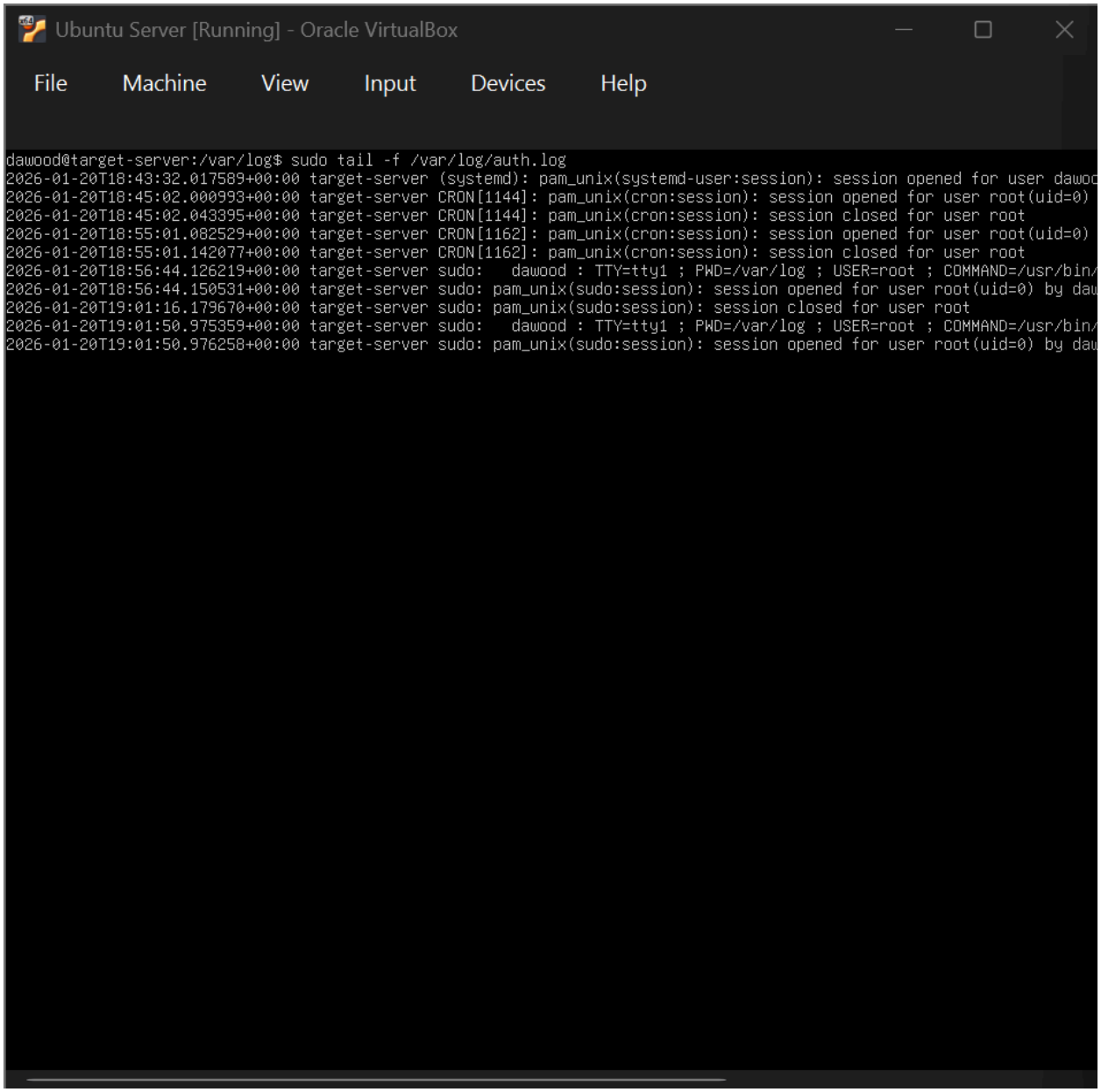


This report confirms that your Ubuntu Server is correctly recording all system and security events.

STEP 2: Monitor Authentication Logs (Defender View)

In this step we will do live monitoring of every steps login attempts.
The command we are using in this is (sudo tail -f /var/log/auth.log)

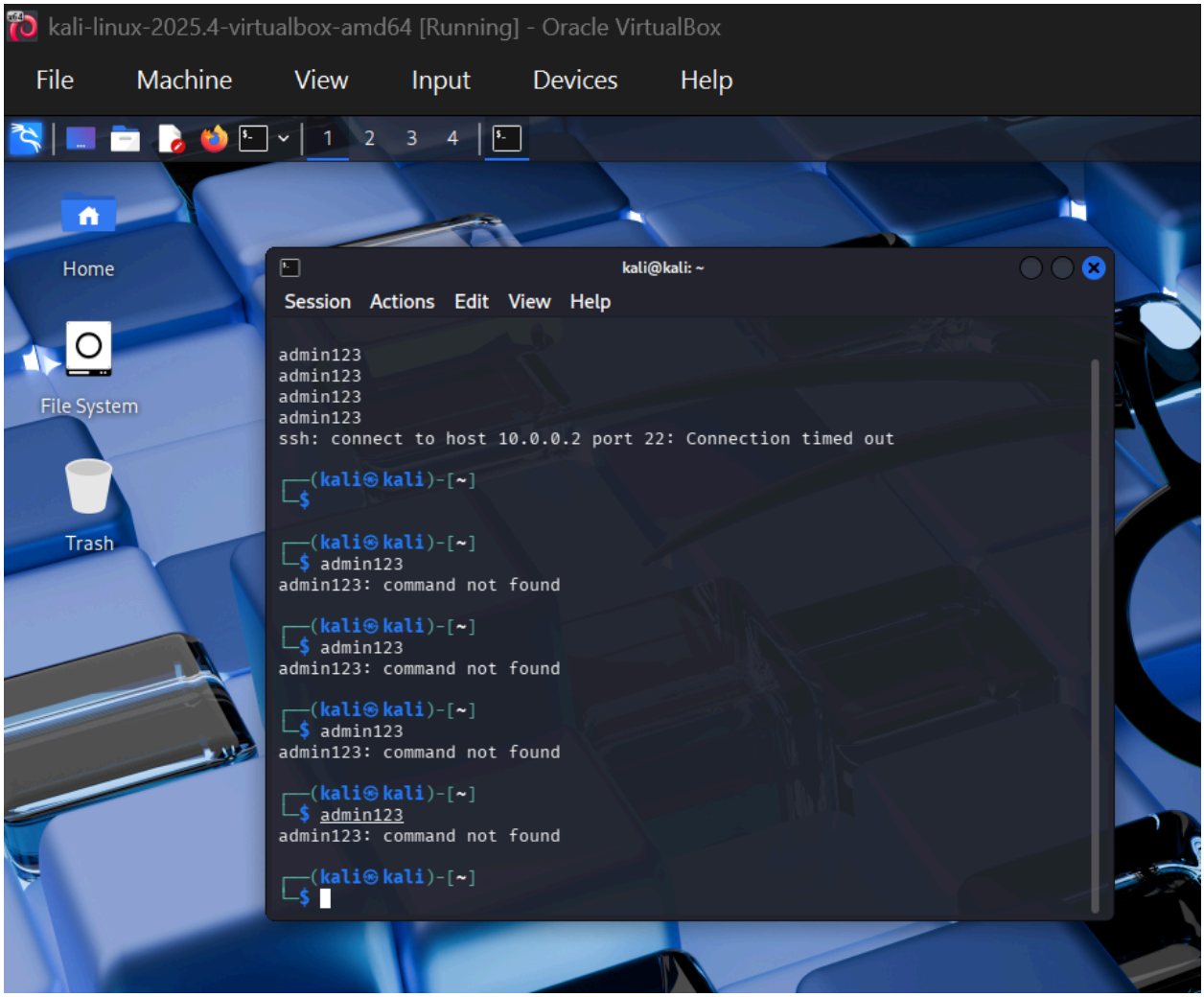
The Tool `tail -f` — The `-f` stands for "follow." It tells Ubuntu to keep the file open and show you every new line the second it is written.



This report confirms that you are now officially monitoring the server's authentication system in real-time

🔹 STEP 3: Simulate an Attack (Attacker View)

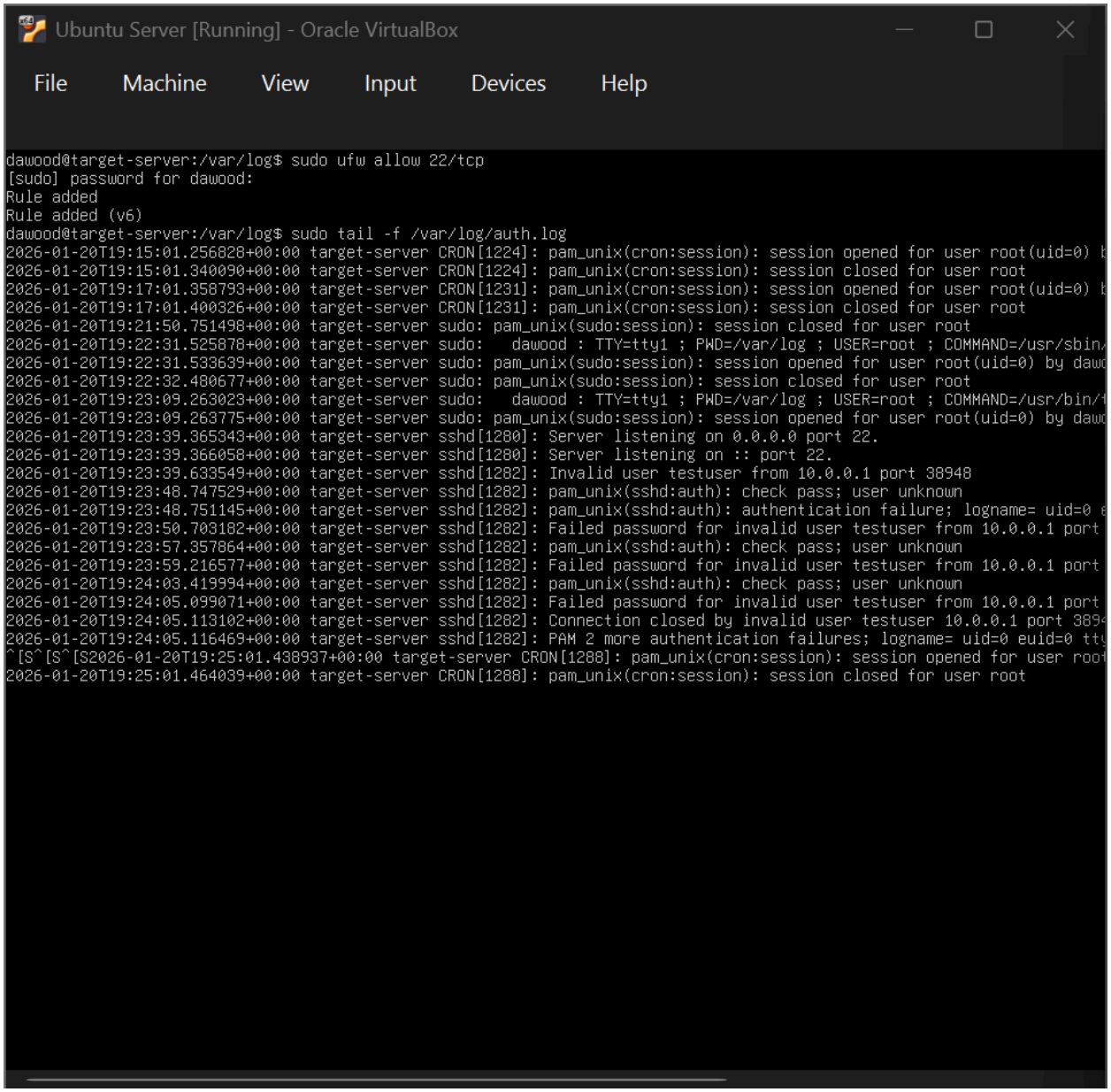
In this step we are using kali linux as a attacker and we are going to attempt some unauthorized to ubuntu(to see live attacks).
The command we are using in this steps is (ssh testuser@10.0.0.2)
After entering command we have to type wrong password attempt atleat 3 to 4 times to see.



This report confirms that your Kali machine has generated the necessary "malicious" traffic to trigger an alert in your logs.

◆ STEP 4: Observe the Evidence (Back to Defender)

In this step we will go back to ubuntu terminal to observe the login failed attempts
As we know on ubuntu server we are doing live monitoring using tail -f
We will see login attempts while live monitoring this is called intrusion detection

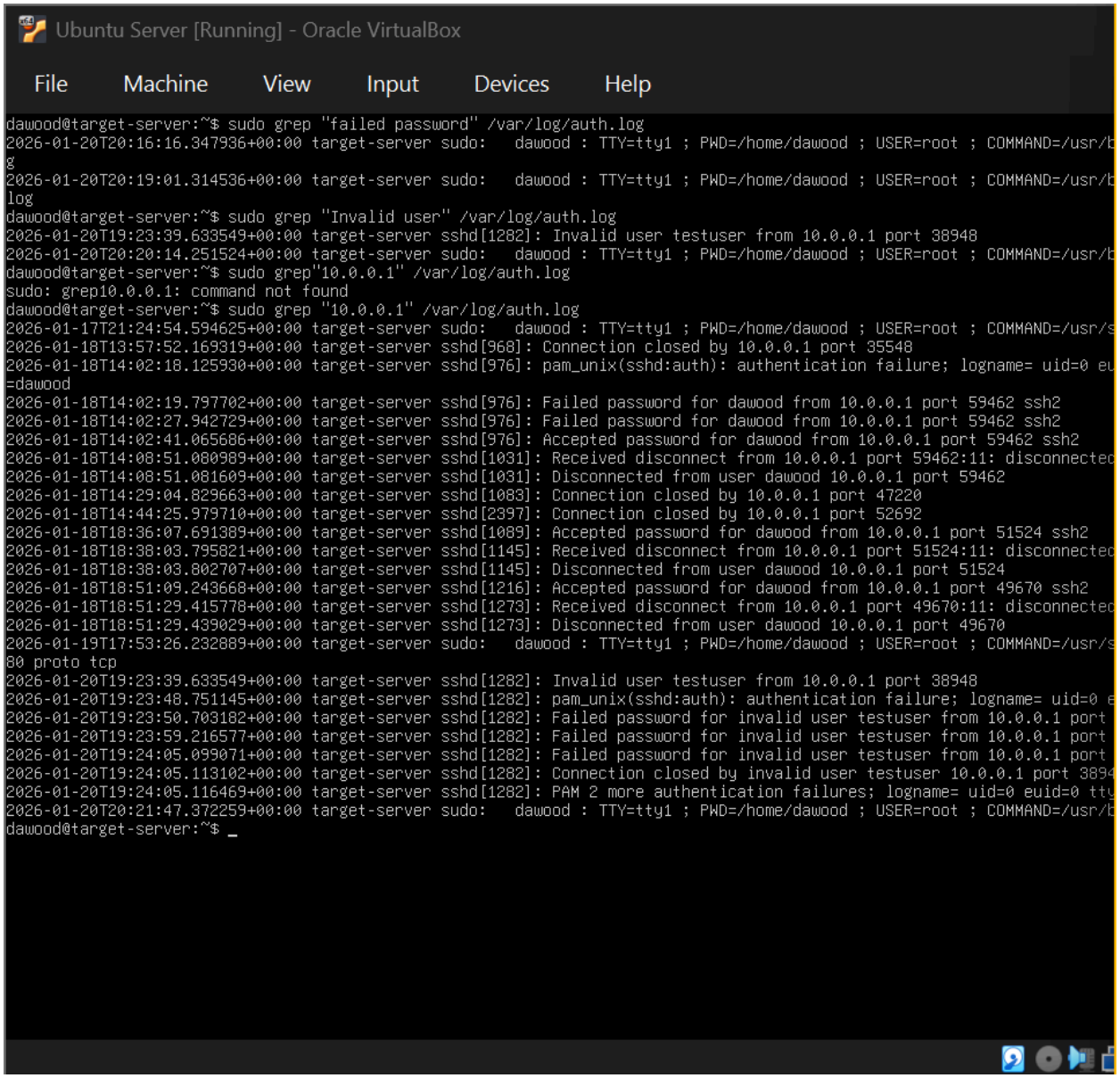


This report confirms that you have successfully captured the digital fingerprints of an unauthorized access attempt.

🔹 STEP 5: Filter Logs Like a SOC Analyst

The Tool `grep` — This is a powerful search tool. It scans through thousands of lines of logs and only pulls out the ones that match your specific keyword.
The command we are using in this is (sudo grep "Failed password" /var/log/auth.log)
(sudo grep "Invalid user" /var/log/auth.log) and (sudo grep "sshd" /var/log/auth.log)
In this Your analysis commands revealed the following malicious activity:

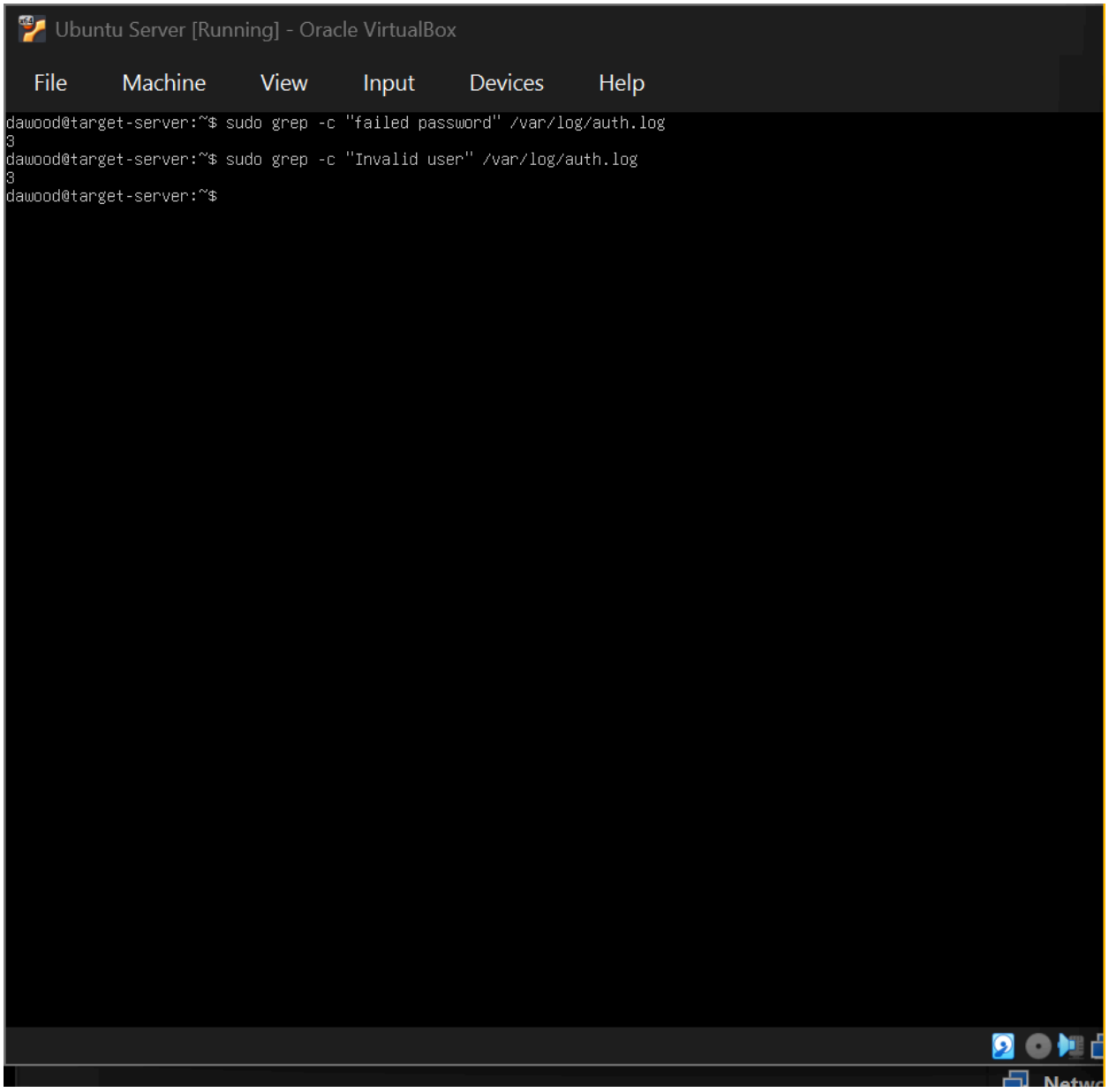
- **Brute Force Detection:** You found multiple "Failed password" attempts. This indicates an attacker trying to guess credentials.
- **Username Enumeration:** You found "Invalid user testuser." This proves the attacker was guessing usernames that do not exist on the system.
- **Connection History:** The search for `10.0.0.1` shows a complete history of the attacker connecting, failing, and being disconnected by the server.



This report summarizes the findings of the "Intrusion Detection" phase. You have successfully moved from seeing "live" events to performing "Forensic Analysis."

🔹 STEP 6: Count Attack Attempts (Professional Touch)

In this step we will f count how many failed attempts has been done
The command we are using in this is (sudo grep -c "Failed password" /var/log/auth.log)
-c stands for count



This report summarizes your successful monitoring, detection, and forensic analysis of a simulated security breach.

🔹 STEP 7: OPTIONAL HARD MODE (Do If Comfortable)

The Goal Instead of typing the command 5 times manually, we will use a **Loop** in Kali to attack the server automatically. This creates a "pattern" that SOC Analysts look for.

The command we are using in this is (for i in {1..5}; do ssh fakeuser@10.0.0.2; done)

What this does: It tells Kali: "Do the SSH command 5 times in a row for the user 'fakeuser'".
Action: Press **Enter**.
Password: It will ask for a password. Just press **Enter** (empty password) or type 123 for each of the 5 attempts until the script finishes.

3. Observe the "Scaling" (Ubuntu)

Switch back to your **Ubuntu** terminal.

- **The Command**:

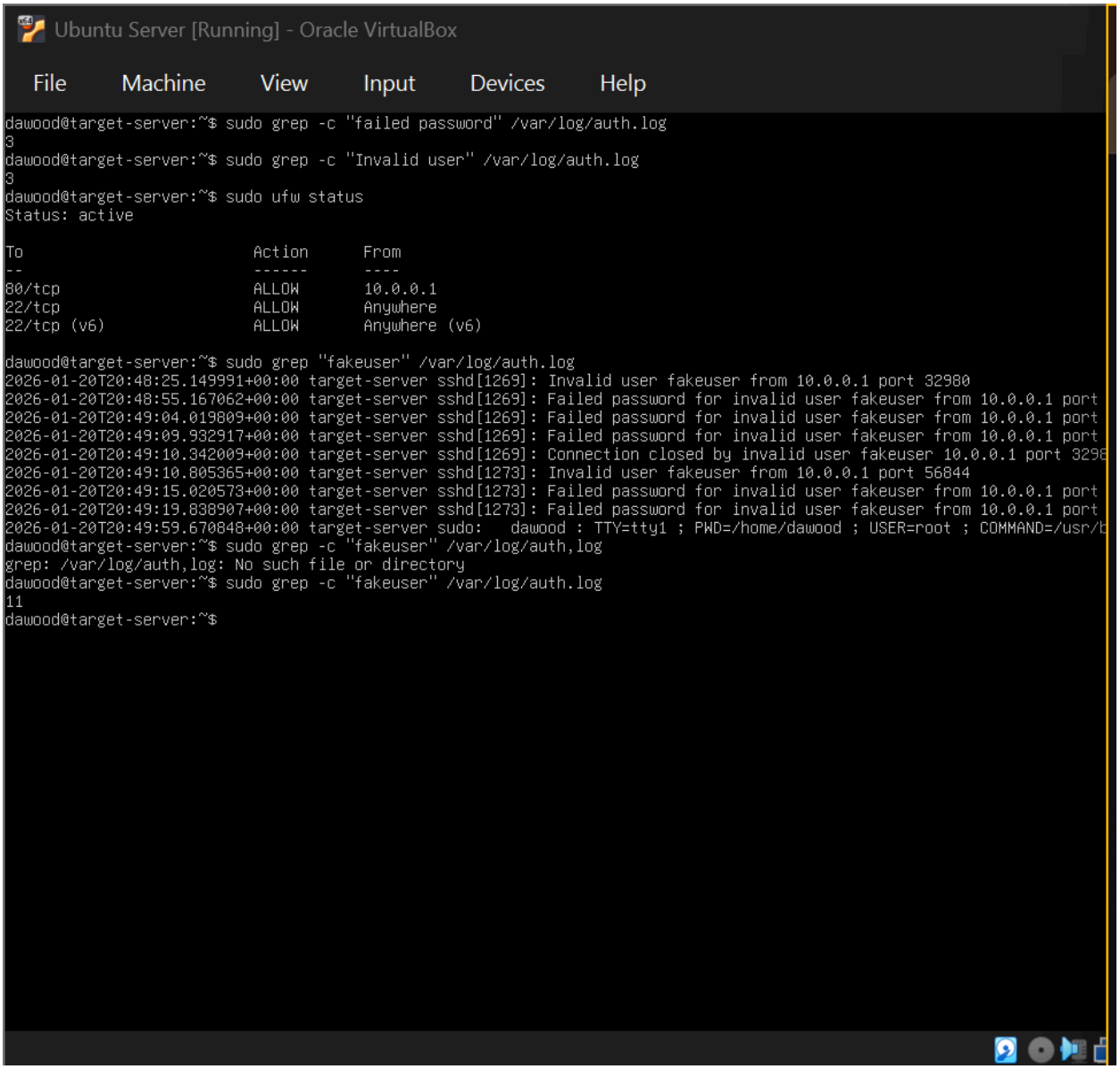
(sudo grep "fakeuser" /var/log/auth.log)

4. Count the "Raid" (Ubuntu)

Use your new favorite tool to see the scale:

- **The Command**:

sudo grep -c "fakeuser" /var/log/auth.log



This report confirms you have successfully simulated and detected a scripted brute-force attack.

Day 4: SOC Analyst Command Master List

Phase	Command	What it does (Purpose)

Monitoring	`tail -f /var/log/auth.log`	Watches the security log live to see "real-time" login attempts.
Filtering	`sudo grep "Failed password" /var/log/auth.log`	Searches for all failed login attempts in the history.
Filtering	`sudo grep "Invalid user" /var/log/auth.log`	Finds attempts where the attacker guessed the wrong username.
Filtering	`sudo grep "10.0.0.1" /var/log/auth.log`	Tracks every single action taken by the Attacker's IP address.
Counting	`sudo grep -c "fakeuser" /var/log/auth.log`	Gives a total number of attacks for a specific name.
Defense	`sudo ufw allow 22/tcp`	Opens the SSH port so we can capture the attacker's fingerprints.
Defense	`sudo ufw status`	Checks the firewall to see which ports are currently open.
Remediation	`sudo ufw delete allow 22/tcp`	**Locks the server** by closing the SSH port after the investigation.
Shutdown	`sudo poweroff`	Safely turns off the server after work is finished.