



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)

```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

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 Tue 20 Jan 18:43:27 UTC 2026

System load: 0.91      Memory usage: 11%    Processes:      122
Usage of /:  41.1% of 11.21GB  Swap usage:  0%    Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
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:~$ cd/var/log
-bash: cd/var/log: No such file or directory
dawood@target-server:~$ cd /var/log
dawood@target-server:/var/log$ ls
alternatives.log  apt          btmap          dist-upgrade  dmesg.1.gz  dmesg.4.gz  installer  landscape  REAL
apache2          auth.log     cloud-init.log dmesg         dmesg.2.gz  dpkg.log    journal    lastlog    sys.
apport.log       bootstrap.log cloud-init-output.log dmesg.0      dmesg.3.gz  faillog     kern.log   private    sys.
dawood@target-server:/var/log$ _
```

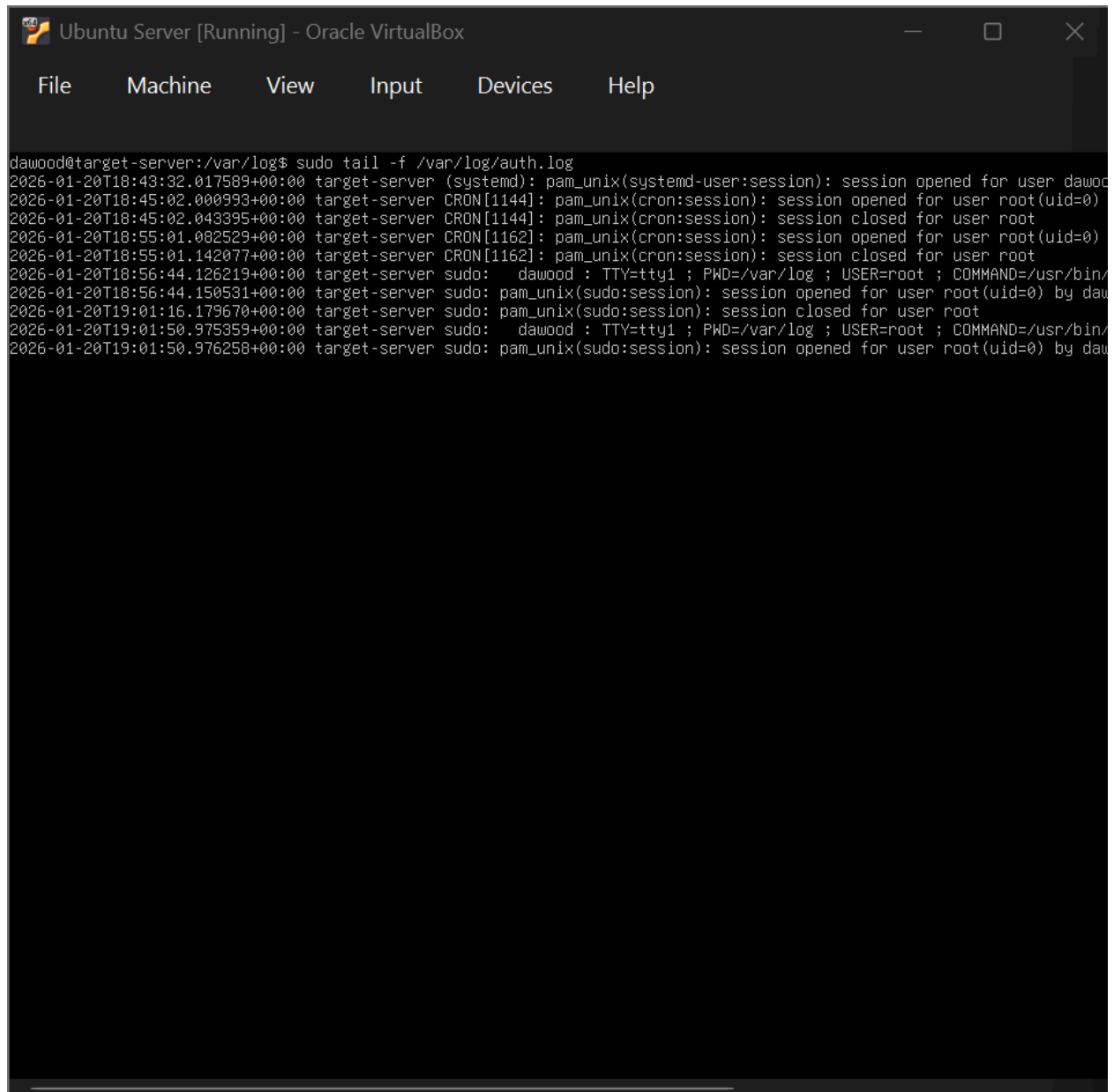
This report confirms that your Ubuntu Server is correctly recording all system and security events.

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.



```
dawood@target-server:/var/log$ sudo tail -f /var/log/auth.log
2026-01-20T18:43:32.017589+00:00 target-server (systemd): pam_unix(systemd-user:session): session opened for user dawood
2026-01-20T18:45:02.000993+00:00 target-server CRON[1144]: pam_unix(cron:session): session opened for user root(uid=0)
2026-01-20T18:45:02.043395+00:00 target-server CRON[1144]: pam_unix(cron:session): session closed for user root
2026-01-20T18:55:01.082529+00:00 target-server CRON[1162]: pam_unix(cron:session): session opened for user root(uid=0)
2026-01-20T18:55:01.142077+00:00 target-server CRON[1162]: pam_unix(cron:session): session closed for user root
2026-01-20T18:56:44.126219+00:00 target-server sudo:    dawood : TTY=ttty1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/sudo
2026-01-20T18:56:44.150531+00:00 target-server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by dawood
2026-01-20T19:01:16.179670+00:00 target-server sudo: pam_unix(sudo:session): session closed for user root
2026-01-20T19:01:50.975359+00:00 target-server sudo:    dawood : TTY=ttty1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/sudo
2026-01-20T19:01:50.976258+00:00 target-server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by dawood
```

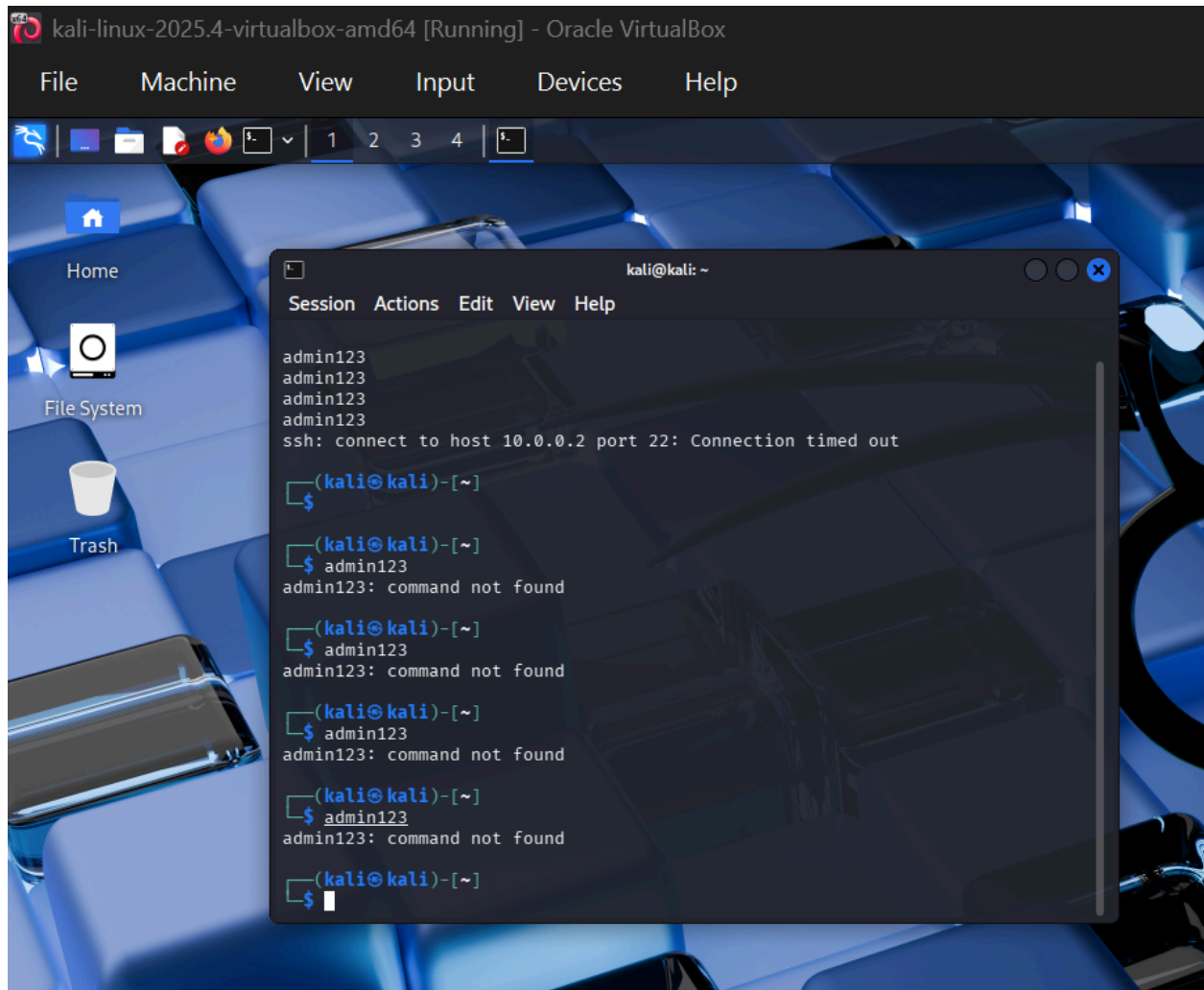
This report confirms that you are now officially monitoring the server's authentication system in real-time

◆ 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 atleast 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

```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

dawood@target-server:/var/log$ sudo ufw allow 22/tcp
[sudo] password for dawood:
Rule added
Rule added (v6)
dawood@target-server:/var/log$ sudo tail -f /var/log/auth.log
2026-01-20T19:15:01.256828+00:00 target-server CRON[1224]: pam_unix(cron:session): session opened for user root(uid=0) by dawood
2026-01-20T19:15:01.340090+00:00 target-server CRON[1224]: pam_unix(cron:session): session closed for user root
2026-01-20T19:17:01.358793+00:00 target-server CRON[1231]: pam_unix(cron:session): session opened for user root(uid=0) by dawood
2026-01-20T19:17:01.400326+00:00 target-server CRON[1231]: pam_unix(cron:session): session closed for user root
2026-01-20T19:21:50.751498+00:00 target-server sudo: pam_unix(sudo:session): session closed for user root
2026-01-20T19:22:31.525878+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/sudoedit -s
2026-01-20T19:22:31.533639+00:00 target-server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by dawood
2026-01-20T19:22:32.480677+00:00 target-server sudo: pam_unix(sudo:session): session closed for user root
2026-01-20T19:23:09.263023+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2026-01-20T19:23:09.263775+00:00 target-server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by dawood
2026-01-20T19:23:39.365343+00:00 target-server sshd[1280]: Server listening on 0.0.0.0 port 22.
2026-01-20T19:23:39.366058+00:00 target-server sshd[1280]: Server listening on :: port 22.
2026-01-20T19:23:39.633549+00:00 target-server sshd[1282]: Invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:23:48.747529+00:00 target-server sshd[1282]: pam_unix(sshd:auth): check pass; user unknown
2026-01-20T19:23:48.751145+00:00 target-server sshd[1282]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty= ssh from=10.0.0.1 port=38948
2026-01-20T19:23:50.703182+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:23:57.357864+00:00 target-server sshd[1282]: pam_unix(sshd:auth): check pass; user unknown
2026-01-20T19:23:59.216577+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:24:03.419994+00:00 target-server sshd[1282]: pam_unix(sshd:auth): check pass; user unknown
2026-01-20T19:24:05.099071+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:24:05.113102+00:00 target-server sshd[1282]: Connection closed by invalid user testuser 10.0.0.1 port 38948
2026-01-20T19:24:05.116469+00:00 target-server sshd[1282]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty= ssh from=10.0.0.1 port=38948
2026-01-20T19:25:01.438937+00:00 target-server CRON[1288]: pam_unix(cron:session): session opened for user root(uid=0) by dawood
2026-01-20T19:25:01.464039+00:00 target-server CRON[1288]: pam_unix(cron:session): session closed for user root
```

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

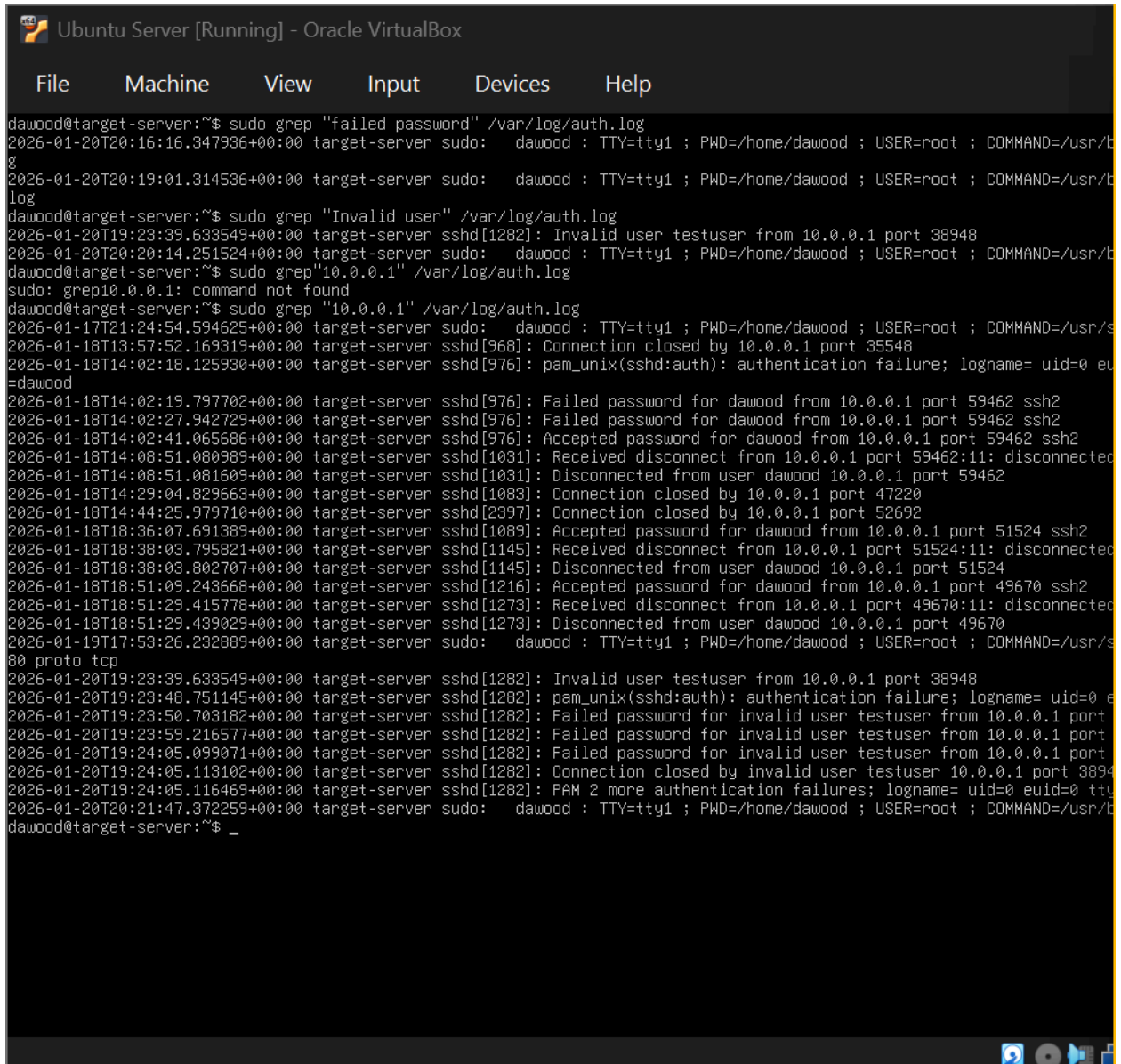
◆ STEP 5: Filter Logs Like a SOC Analyst

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.



```

dawood@target-server:~$ sudo grep "failed password" /var/log/auth.log
2026-01-20T20:16:16.347936+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/grep
2026-01-20T20:19:01.314536+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/grep
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 port 38948
2026-01-20T20:20:14.251524+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/grep
dawood@target-server:~$ sudo grep "10.0.0.1" /var/log/auth.log
sudo: grep10.0.0.1: command not found
dawood@target-server:~$ sudo grep "10.0.0.1" /var/log/auth.log
2026-01-17T21:24:54.594625+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/sudo
2026-01-18T13:57:52.169319+00:00 target-server sshd[968]: Connection closed by 10.0.0.1 port 35548
2026-01-18T14:02:18.125930+00:00 target-server sshd[976]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=
=dawood
2026-01-18T14:02:19.797702+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0.1 port 59462 ssh2
2026-01-18T14:02:27.942729+00:00 target-server sshd[976]: Failed password for dawood from 10.0.0.1 port 59462 ssh2
2026-01-18T14:02:41.065686+00:00 target-server sshd[976]: Accepted password for dawood from 10.0.0.1 port 59462 ssh2
2026-01-18T14:08:51.080989+00:00 target-server sshd[1031]: Received disconnect from 10.0.0.1 port 59462:11: disconnected
2026-01-18T14:08:51.081609+00:00 target-server sshd[1031]: Disconnected from user dawood 10.0.0.1 port 59462
2026-01-18T14:29:04.829663+00:00 target-server sshd[1083]: Connection closed by 10.0.0.1 port 47220
2026-01-18T14:44:25.979710+00:00 target-server sshd[2397]: Connection closed by 10.0.0.1 port 52692
2026-01-18T18:36:07.691389+00:00 target-server sshd[1089]: Accepted password for dawood from 10.0.0.1 port 51524 ssh2
2026-01-18T18:38:03.795821+00:00 target-server sshd[1145]: Received disconnect from 10.0.0.1 port 51524:11: disconnected
2026-01-18T18:38:03.802707+00:00 target-server sshd[1145]: Disconnected from user dawood 10.0.0.1 port 51524
2026-01-18T18:51:09.243668+00:00 target-server sshd[1216]: Accepted password for dawood from 10.0.0.1 port 49670 ssh2
2026-01-18T18:51:29.415778+00:00 target-server sshd[1273]: Received disconnect from 10.0.0.1 port 49670:11: disconnected
2026-01-18T18:51:29.439029+00:00 target-server sshd[1273]: Disconnected from user dawood 10.0.0.1 port 49670
2026-01-19T17:53:26.232889+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/sudo
80 proto tcp
2026-01-20T19:23:39.633549+00:00 target-server sshd[1282]: Invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:23:48.751145+00:00 target-server sshd[1282]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=
2026-01-20T19:23:50.703182+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:23:59.216577+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:24:05.099071+00:00 target-server sshd[1282]: Failed password for invalid user testuser from 10.0.0.1 port 38948
2026-01-20T19:24:05.113102+00:00 target-server sshd[1282]: Connection closed by invalid user testuser 10.0.0.1 port 38948
2026-01-20T19:24:05.116469+00:00 target-server sshd[1282]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=
2026-01-20T20:21:47.372259+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/bin/sudo
dawood@target-server:~$ _

```

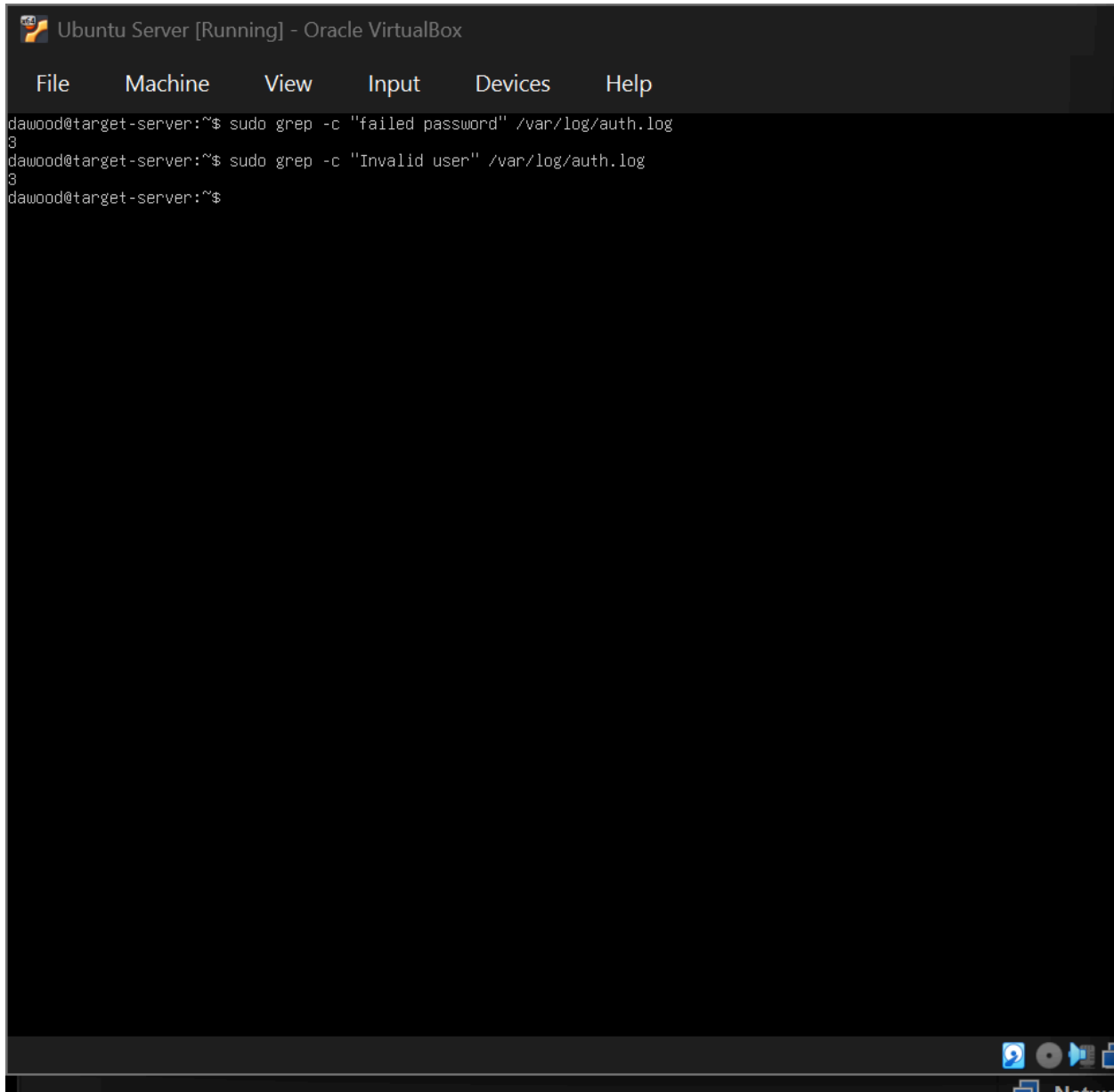
This report summarizes the findings of the "Intrusion Detection" phase. You have successfully moved from seeing "live" events to performing "Forensic Analysis."

◆ STEP 6: Count Attack Attempts (Professional Touch)

In this step we will count how many failed attempts have been done

The command we are using in this is (sudo grep -c "Failed password" /var/log/auth.log)

-c stands for count



```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
dawood@target-server:~$ sudo grep -c "failed password" /var/log/auth.log
3
dawood@target-server:~$ sudo grep -c "Invalid user" /var/log/auth.log
3
dawood@target-server:~$
```

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
```



```

Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
dawood@target-server:~$ sudo grep -c "failed password" /var/log/auth.log
3
dawood@target-server:~$ sudo grep -c "Invalid user" /var/log/auth.log
3
dawood@target-server:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW 10.0.0.1
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

dawood@target-server:~$ sudo grep "fakeuser" /var/log/auth.log
2026-01-20T20:48:25.149991+00:00 target-server sshd[1269]: Invalid user fakeuser from 10.0.0.1 port 32980
2026-01-20T20:48:55.167062+00:00 target-server sshd[1269]: Failed password for invalid user fakeuser from 10.0.0.1 port
2026-01-20T20:49:04.019809+00:00 target-server sshd[1269]: Failed password for invalid user fakeuser from 10.0.0.1 port
2026-01-20T20:49:09.932917+00:00 target-server sshd[1269]: Failed password for invalid user fakeuser from 10.0.0.1 port
2026-01-20T20:49:10.342009+00:00 target-server sshd[1269]: Connection closed by invalid user fakeuser 10.0.0.1 port 3298
2026-01-20T20:49:10.805365+00:00 target-server sshd[1273]: Invalid user fakeuser from 10.0.0.1 port 56844
2026-01-20T20:49:15.020573+00:00 target-server sshd[1273]: Failed password for invalid user fakeuser from 10.0.0.1 port
2026-01-20T20:49:19.838907+00:00 target-server sshd[1273]: Failed password for invalid user fakeuser from 10.0.0.1 port
2026-01-20T20:49:59.670848+00:00 target-server sudo: dawood : TTY=ttty1 ; PWD=/home/dawood ; USER=root ; COMMAND=/usr/b
dawood@target-server:~$ sudo grep -c "fakeuser" /var/log/auth.log
grep: /var/log/auth.log: No such file or directory
dawood@target-server:~$ sudo grep -c "fakeuser" /var/log/auth.log
11
dawood@target-server:~$
```

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