Day 5: Log Analysis Basics – Linux Auth Log

Objective

Simulate an SSH brute-force attack against an Ubuntu Desktop machine and demonstrate how to detect and analyze it using Linux authentication logs. Learn to extract evidence (failed/successful login attempts), identify attack patterns.

Environment

- Attacker: Kali Linux (hydra)
- Target/Victim: **Ubuntu Desktop** (OpenSSH installed)

Tools

- `hydra` (attacker)
- `openssh-server` (installed on the Ubuntu Desktop to allow SSH)

The Hydra command runs an automated password-guessing attack against the SSH service on the target machine, as shown in the screenshot below.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P password.txt ssh://192.168.18.150
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-05 07:49:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:1/p:20), ~2 tries per task
[DATA] attacking ssh://192.168.18.150:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-05 07:50:07
```

From the screenshot below, the `tail -f /var/log/auth.log` pipeline watches the authentication log in real time and, when piped to `grep "Failed password"`, shows only SSH failed-password attempts as they occur.

```
ubuntu@ubuntu:/var/log$ sudo tail -f /var/log/auth.log | grep --line-buffered "Failed password"
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
2025-11-05T13:50:05.613173+01:00 ubuntu sshd[4674]: Failed password for root from 192.168.18.143 port 50074 ssh2
2025-11-05T13:50:05.623935+01:00 ubuntu sshd[4676]: Failed password for root from 192.168.18.143 port 50088 ssh2
2025-11-05T13:50:05.625417+01:00 ubuntu sshd[4678]: Failed password for root from 192.168.18.143 port 50104 ssh2
2025-11-05T13:50:05.626895+01:00 ubuntu sshd[4675]: Failed password for root from 192.168.18.143 port 50076 ssh2
2025-11-05T13:50:05.633436+01:00 ubuntu sshd[4677]: Failed password for root from 192.168.18.143 port 50094 ssh2
2025-11-05T13:50:05.644567+01:00 ubuntu sshd[4679]: Failed password for root from 192.168.18.143 port 50114 ssh2
```

In conclusion

I set up an Ubuntu target with OpenSSH, launched an SSH brute-force attack from my Kali attacker using Hydra, and monitored `/var/log/auth.log` on the victim to detect and analyze the attack. By filtering for `Failed password` entries, I identified a pattern of rapid failed logins originating from the Kali Linux IP address. This exercise taught me how SSH authentication events are logged and how to extract and interpret evidence of brute-force activity.