SSH Brute-Force Detection Lab

Cybersecurity Portfolio Project
Author: Hadis Pazhand
Date: April 2026
Tools: Kali Linux · Metasploit · Nmap · Splunk · Ubuntu Server

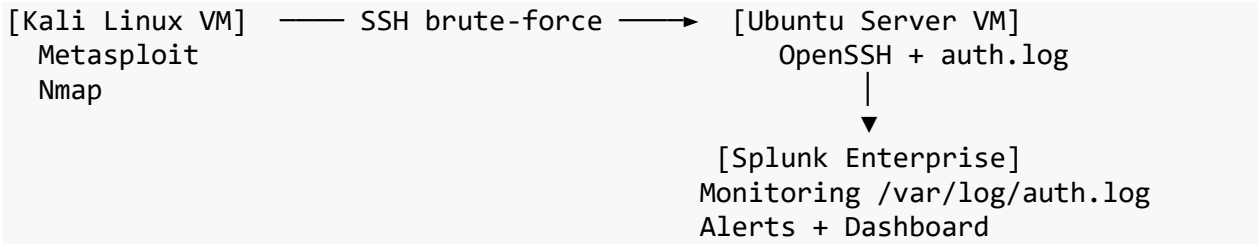
---

Project Overview

This project demonstrates the detection of SSH brute-force attacks using a simulated lab environment. A Kali Linux attacker machine was used to launch credential stuffing attacks against an Ubuntu Server target, while Splunk monitored system logs in real time to detect and alert on suspicious activity.

This is a core skill for any SOC analyst or blue team role — understanding how attackers operate (red team) while building the detection logic to catch them (blue team).

Lab Architecture



Network: Both VMs on an isolated NAT Network (10.0.2.0/24)
Attacker IP: 10.0.2.15 (Kali)
Target IP: 10.0.2.4 (Ubuntu Server)

Phase 1 — Reconnaissance (Nmap)

Before launching the attack, Nmap was used to confirm SSH (port 22) was open and identify the service version on the target.

```
nmap -sV -p 22 10.0.2.4
```

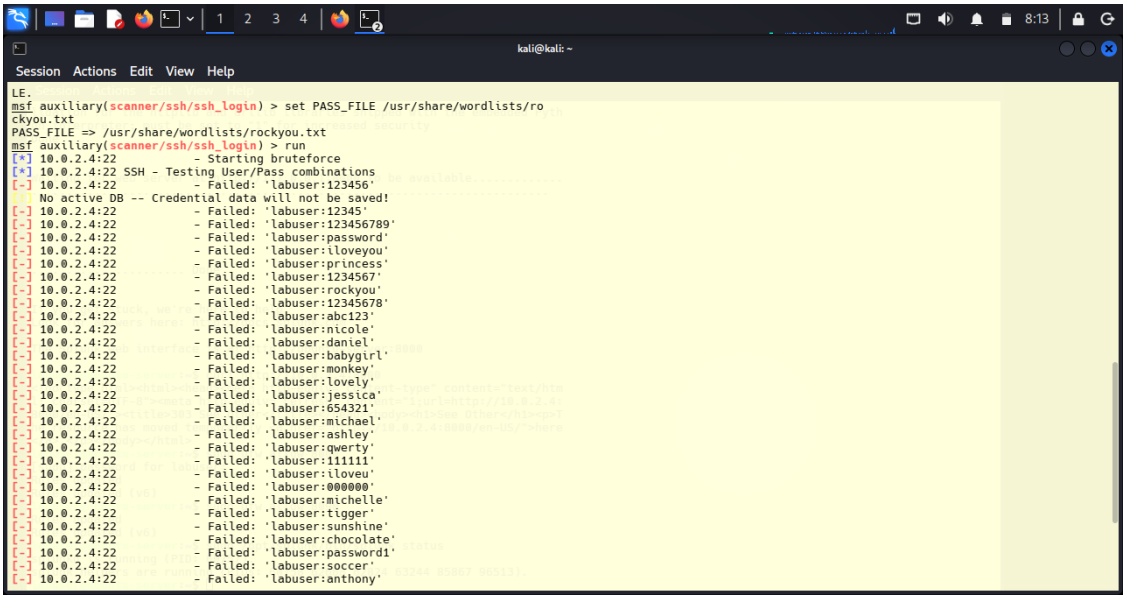
Result: OpenSSH 9.6p1 confirmed running on port 22.

Phase 2 — SSH Brute-Force Attack (Metasploit)

Metasploit's `ssh_login` auxiliary module was configured to perform a dictionary attack against the target using the rockyou.txt wordlist — one of the most common real-world password lists.

```
use auxiliary/scanner/ssh/ssh_login
set RHOSTS 10.0.2.4
set USERNAME labuser
set PASS_FILE /usr/share/wordlists/rockyou.txt
set VERBOSE true
run
```

The attack generated dozens of failed login attempts in rapid succession, simulating real credential abuse patterns.



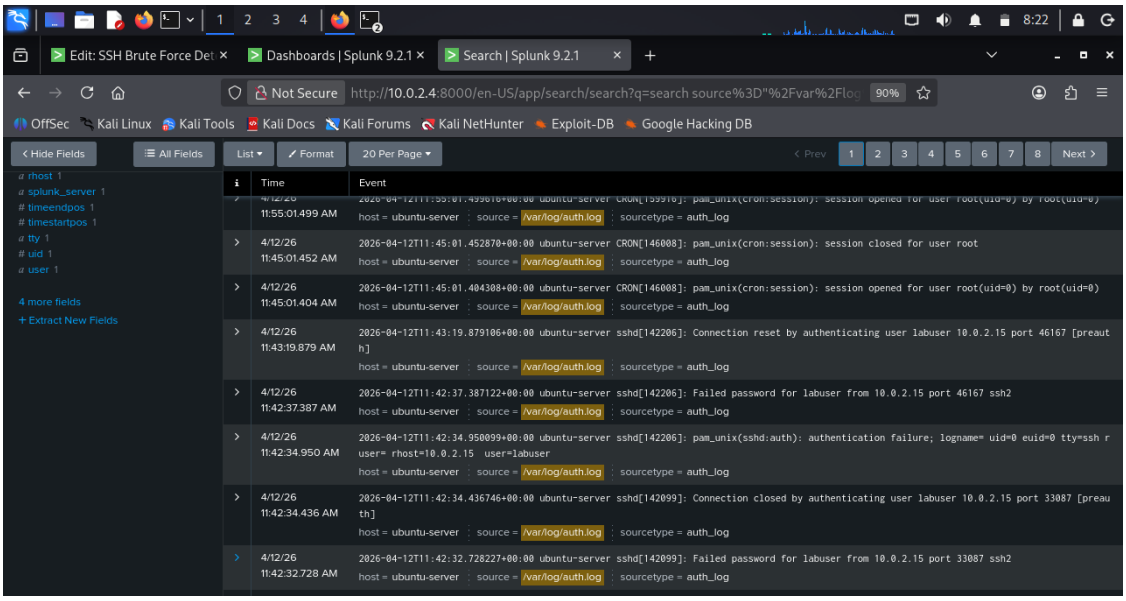
Metasploit brute-force attack in progress

Each [-] line represents a failed login attempt. The attack tested common passwords including 123456, password, iloveyou, princess, and hundreds more from the rockyou wordlist.

Phase 3 — Log Ingestion in Splunk

Splunk Enterprise was installed on the Ubuntu Server and configured to monitor `/var/log/auth.log` — the Linux file that records all authentication events including SSH login attempts.

Every failed login attempt generated by the attack was captured in real time.



Raw auth.log events in Splunk showing Failed password entries

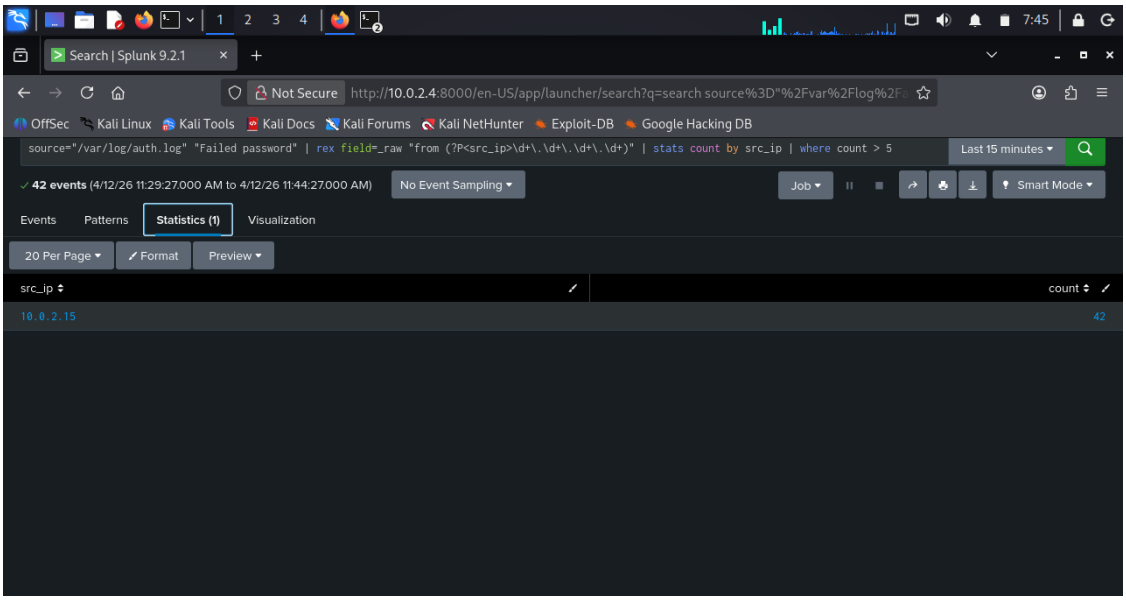
Each event shows the timestamp, source IP (10.0.2.15), target username (labuser), and port number — giving full visibility into the attack.

Phase 4 — Detection Query (SPL)

A Splunk Processing Language (SPL) query was written to extract the source IP from failed login events and count attempts per IP. A threshold filter of greater than 5 failures flags potential brute-force activity.

```
source="/var/log/auth.log" "Failed password"
| rex field=_raw "from (?P<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count by src_ip
| where count > 5
```

Result: IP 10.0.2.15 detected with 42 failed attempts — well above the threshold.



Splunk SPL query detecting attacker IP with 42 failed attempts

The query successfully identified the attacking machine (Kali Linux at 10.0.2.15) as the source of credential abuse.

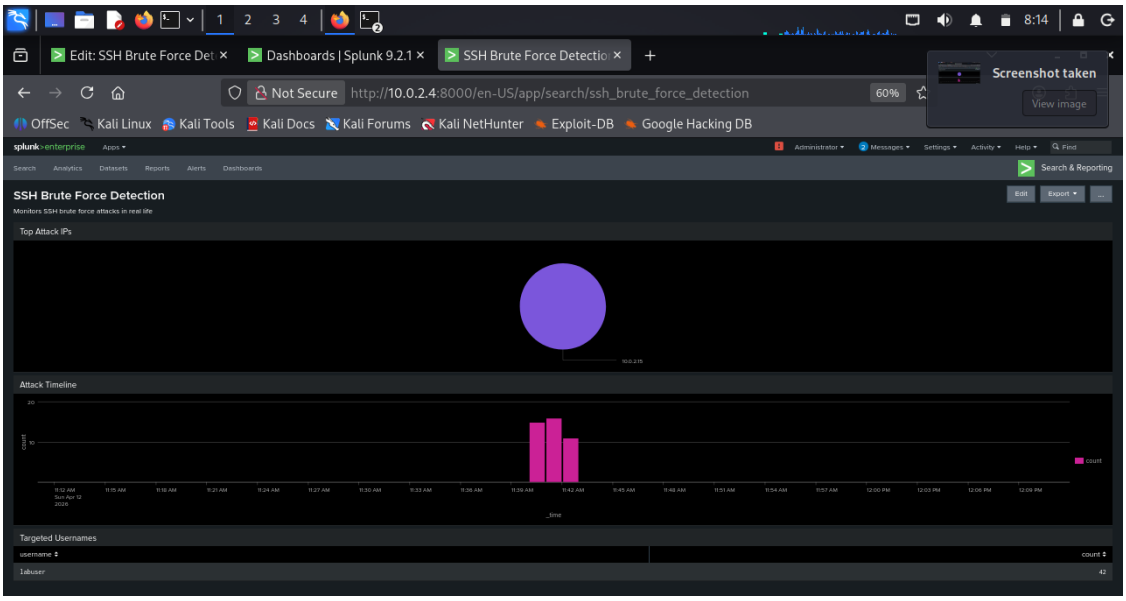
Phase 5 — Splunk Dashboard

A real-time monitoring dashboard was built in Splunk with three panels:

Panel 1 — Top Attacking IPs: Visualises which source IPs are generating the most failed attempts.

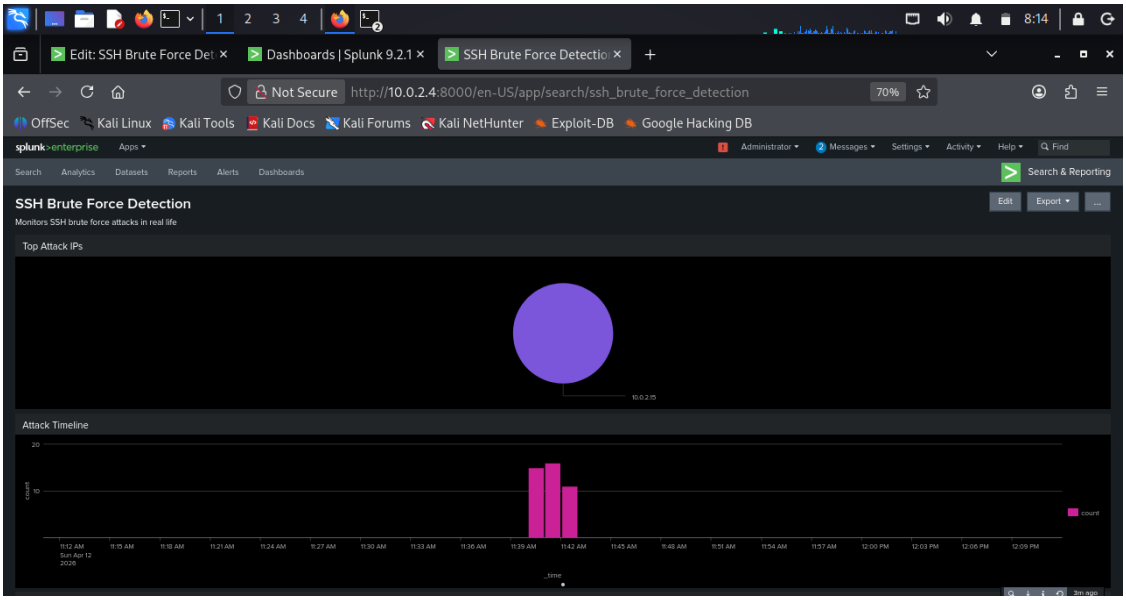
Panel 2 — Attack Timeline: Shows when the attack occurred and how the volume of attempts changed over time.

Panel 3 — Targeted Usernames: Identifies which accounts are being targeted.



SSH Brute Force Detection dashboard showing all 3 panels

The dashboard clearly shows the attack burst between 11:39 AM and 11:42 AM, with 10.0.2.15 as the sole attacking IP targeting the labuser account.



Dashboard view showing attack timeline chart

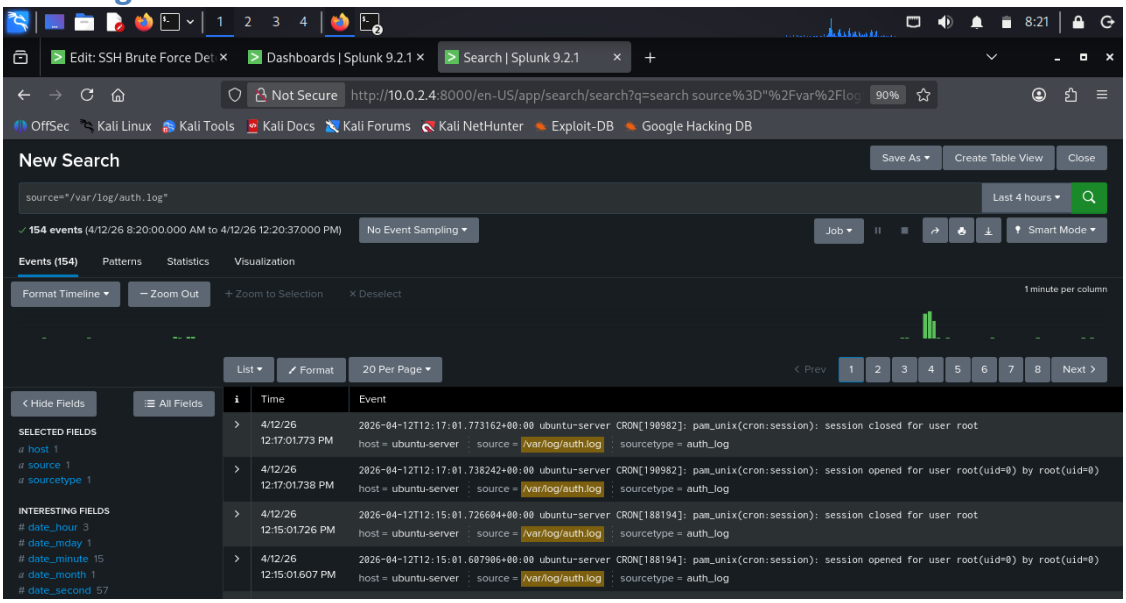
Phase 6 — Automated Alert

A scheduled Splunk alert was configured to automatically trigger when the detection query returns results, enabling proactive notification without manual searching.

Alert Configuration: - **Name:** SSH Brute Force Detected - **Trigger:** When number of results > 0 - **Schedule:** Hourly - **Severity:** High - **Action:** Add to Triggered Alerts

---

Raw Log Evidence



Splunk showing 154 raw auth.log events

154 total authentication events were captured during the lab session, including failed passwords, connection resets, and session events — all ingested and searchable in Splunk.

Key Skills Demonstrated

- **Network reconnaissance** using Nmap to identify open services
- **Offensive security** — simulating real-world SSH brute-force attacks with Metasploit
- **Log analysis** — ingesting and parsing Linux auth.log in Splunk
- **SIEM querying** — writing SPL queries to detect attack patterns
- **Threshold-based alerting** — building automated detection rules
- **Dashboard creation** — visualising security events for SOC monitoring
- **Linux server administration** — SSH, systemctl, file system management
- **Virtual lab setup** — configuring isolated VM environments for safe testing

---

Tools & Technologies

Tool	Purpose
Kali Linux	Attacker machine

Tool	Purpose
Metasploit Framework	SSH brute-force simulation
Nmap	Network reconnaissance
Ubuntu Server 24.04	Target machine
OpenSSH	Attack surface
Splunk Enterprise 9.2	SIEM — log ingestion, detection, dashboards
auth.log	Linux authentication log source
rockyou.txt	Password wordlist for dictionary attack

This project was conducted entirely in an isolated virtual lab environment on personal hardware. No external systems were targeted.