Case Report: Brute Force Attack

Case ID: INC-2025-0821-002

Date/Time: 21 August 2025, 6:23 PM

Reported By: SOC Analyst (L1) – Kabir Bagalkot

Summary:

A brute force attack was detected on the victim machine **192.168.79.130** (Metasploitable 3) originating from attacker machine **192.168.79.129** (Kali Linux). The attacker used **Hydra** with the **rockyou.txt** wordlist to attempt **SSH login as the root user**. The activity involved hundreds of logins attempts within minutes, and eventually, a successful login was achieved. The behavior clearly indicates automated brute force activity.

Detection Details:

- **Detection Type:** SSH Brute Force Attack.
- **Source IP (Attacker):** 192.168.79.129 using Hydra in Kali Linux.
- **Destination IP:** 192.168.79.130 (Metasploitable3 – SSH service.
- **Targeted Account:** Root.
- **Service Targeted:** SSH (Port 22).
- **Total Attempts:** 500 + attempts within 5 minutes.
- **Log Source:** Syslog/Auth.log
- **Network Capture:** Wireshark (PCAP evidence)

Splunk Detection Query:

```
index=* "Failed password" OR "Accepted password"
| rex "Failed password for (?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| rex "Accepted password for (?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count by src_ip user
| sort - count
```

Query Explanation:

index=* “Failed password” OR “Accepted password”

- It searches all the indexes for logs that contains either
- **“Failed password”** = failed SSH login attempts
- **“Accepted password”** = successful SSH logins

| rex "Failed password for (?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"

- It checks if the logs contain the **“Failed password”** then it extracts **user** and **src_ip** (attackers ip address)

Example log:

Failed password for root from 192.168.79.128 port 56124 ssh2

Then it extracts

1. User – root
2. Src_ip – 192.168.79.128

| rex "Accepted password for (?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"

- It checks if the logs contain the **“Accepted password”** then it extracts **user** and **src_ip** (attackers ip address)
- We have confirmed that no users have successfully logged in.

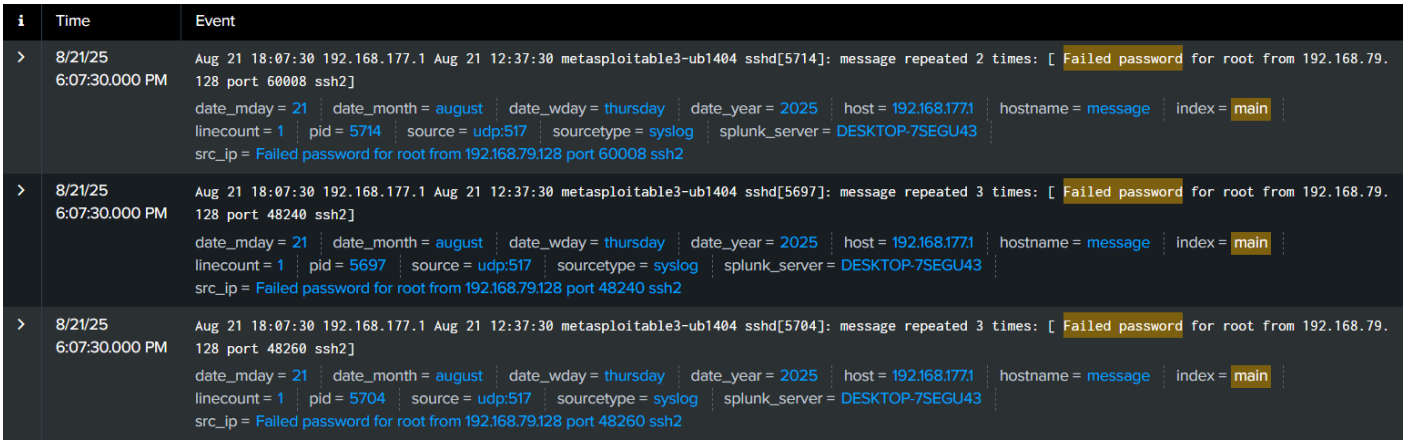
| stats count by src_ip user

- Groups the logs by **IP address (src_ip)** and **username (user).**
- It counts how many times each IP address tried that username.

| sort – count

- It sorts the table in descending order of **count**.
- The **IP** pair with the **highest number of attempts** appears on the top.

Evidence from Logs (Splunk Extract):



Escalation:

Yes, this incident must be escalated to SOC Level 2 (Incident Response) Team.
Reason for Escalation:

- Automated brute force behaviour confirmed (Hydra tool).
- Successful compromise of root account observed.
- Requires containment, forensic analysis, and impact assessment.

Proposed Actions:

Forensic Analysis:

- Someone tried to hack into the system using a tool called Hydra.
- The attacker's IP was 192.168.79.128.
- They tried 1168 times to log in as root.
- Good news: All attempts failed nobody broke in.

Hardening & Security Recommendations:

- Stop root login directly.
- Block repeated failed logins.
- only allow from trusted IPs, or use a VPN.
- Monitor and alert if someone tries too many logins again.
- Block attacker IP at the firewall.

Status:
Incident has been escalated to SOC L2 team. Awaiting forensic investigation results and remediation confirmation.