Incident Report – FTP Brute Force Attempt

Incident ID: IR-2025-0915-FTPBF
Date/Time Detected: September 15, 2025, 19:45 – 20:00 EDT
Reported By: Splunk SIEM (Home Lab Deployment)
Analyst: Shayaan Rashedin

1. Executive Summary

On September 15, 2025, a brute force attack was simulated against the FTP service running on a Metasploitable2 host (192.168.56.101). A Kali Linux attacker host executed Hydra with the rockyou.txt password list, generating repeated authentication failures. These events were ingested into Splunk via syslog forwarding and the Universal Forwarder. A custom Splunk detection rule identified >10 failed login attempts within a 5-minute window. An automated alert titled “FTP Brute Force Detection” was created to trigger when suspicious activity is observed. This demonstrates end-to-end SIEM functionality, including log ingestion, correlation, detection, and alerting.

2. Environment

- Attacker: Kali Linux VM (192.168.56.101)
- Target: Metasploitable2 VM (192.168.56.101, FTP service active)
- SIEM Platform: Splunk Enterprise (Ubuntu VM, receiving logs on UDP/514 and TCP/9997)
- Data Sources:
  - Syslog from Metasploitable2 (/etc/syslog.conf forwarding to Splunk)
  - Splunk Forwarder from Kali Linux (monitoring /var/log/auth.log, /var/log/syslog)

3. Attack Simulation

The brute force attack was carried out using Hydra with the following command:

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.56.101
-t 4 -V
```

- Hydra attempted thousands of username/password combinations.
- Syslog recorded repeated failures as:
  - pam_unix(ftp:auth): authentication failure
  - last message repeated N times

4. Detection

4.1 Raw Log Evidence

- Authentication failure events were successfully ingested into Splunk (sourcetype=syslog).
- Splunk search confirmed the presence of collapsed repeat messages (last message repeated 70 times, etc.).

4.2 Detection SPL

```
index=main sourcetype=syslog host=192.168.56.101
```

```
("pam_unix(ftp:auth): authentication failure" OR "last message repeated")
| eval base_fail=if(match(_raw,"pam_unix\(ftp:auth\): authentication
failure"),1,0)
| rex field=_raw "last message repeated (?\d+) times"
| eval fail_events=coalesce(rep, base_fail)
| bin _time span=5m
| stats sum(fail_events) as failures by host _time
| where failures > 10
```

Result: Between 19:45 and 20:00 EDT, Splunk detected 200–330 failures per 5-minute window.

5. Alerting

An automated alert was created in Splunk:
- Title: FTP Brute Force Detection
- Schedule: Real-time / per-result (demo)
- Trigger Condition: Number of Results > 0
- Action: Log to Triggered Alerts, optional email notification

6. Impact Assessment

- System Impacted: Metasploitable2 (FTP service)
- Scope: Brute force authentication attempts only; no successful login was achieved in this test.
- Severity: Medium (attack simulation in controlled lab environment)

7. Recommendations

1. Preventive Controls
   - Disable FTP or replace with secure alternatives (SFTP/SSH).
   - Implement strong password policies to reduce brute force success.
   - Deploy intrusion prevention mechanisms such as Fail2Ban.

2. Detection Improvements
   - Expand detection rules to include SSH brute force.
   - Create dashboards visualizing failed logins by host, source IP, and time.

3. Response Playbook
   - Validate alerts, confirm attacking source, block malicious IPs.
   - Escalate incidents if brute force attempts succeed.

8. Conclusion

This lab exercise demonstrates practical SIEM experience:
- Ingesting logs from multiple hosts
- Developing custom SPL correlation searches
- Handling syslog repeat suppression
- Configuring automated alerts
- Documenting incidents with evidence and recommendations

The project successfully simulates how a SOC team detects and responds to brute force authentication attempts in real-world environments.