Brute Force Attack Detection Report – Splunk SIEM

Author: Juan Marcos Lázaro Rey
Title: Cybersecurity Professional — SOC & GRC
Location: Miami, FL, USA
Email: juanmarcos.lazaro@gmail.com

Overview

This report presents brute force authentication detection using **Splunk SIEM**. Security logs were analyzed and mapped to **MITRE ATT&CK Technique T1110.001 – Password Guessing**, focusing on repeated unauthorized login attempts targeting user accounts.

The investigation demonstrates how scripted login attempts can bypass basic monitoring unless proper alerting, account lockout, and authentication policies are enforced.

Evidence Summary

Field	**Value**
Source IP	127.0.0.1
Total Failed Attempts	74
Attack Duration	4 minutes 33 seconds

Detection Details

Data Source

- Windows Security Log
- Event ID **4625 (Failed Login)**

Detection Query (Splunk)

Detection Queries (SSH Brute Force – linux_secure)

1. Basic search for SSH authentication events

```
index=main sourcetype=linux_secure ssh*
| head 50
```

2. Search for failed SSH attempts

```
index=main sourcetype=linux_secure "Failed password"
| head 50
```

3. Advanced query to identify brute force patterns

```
index=main sourcetype=linux_secure "Failed password"
| rex field=_raw "Failed password for (?<username>\S+) from (?<src_ip>\S+)"
| stats count by username, src_ip
| where count > 3
| sort -count
```

4. Correlate failed and successful logins

```
index=main sourcetype=linux_secure (("Failed password" OR "Accepted password") AND ssh*)
| rex field=_raw "(?<auth_result>Failed|Accepted) password for (?<username>\S+) from (?<src_ip>\S+)"
| eval auth_status=if(match(_raw, "Failed"), "Failed", "Success")
| table _time, auth_status, username, src_ip
| sort _time
```

5. First failed login (timestamp + user + source IP)

```
index=main sourcetype=linux_secure "Failed password"
| rex field=_raw "Failed password for (?<username>\S+) from (?<src_ip>\S+)"
| head 1
| table _time, username, src_ip
```

6. First successful login after failures

```
index=main sourcetype=linux_secure "Accepted password"

| rex field=_raw "Accepted password for (?<username>\S+) from (?<src_ip>\S+)"

| head 1

| table _time, username, src_ip
```

7. Total attempts by IP and username

```
index=main sourcetype=linux_secure ("Failed password" OR "Accepted password")

| rex field=_raw "(?<auth_result>Failed|Accepted) password for (?<username>\S+) from (?<src_ip>\S+)"

| stats count by src_ip, username

| sort -count
```

8. Primary brute force detection query (deliverable)

```
index=main sourcetype=linux_secure "Failed password"

| rex field=_raw "Failed password for (?<username>\S+) from (?<src_ip>\S+)"

| stats count as failed_attempts by username, src_ip, host

| where failed_attempts >= 3

| sort -failed_attempts
```

Indicators of Compromise

Indicator	**Description**
Repeated login failures	Same username targeted repeatedly
Same originating IP	Consistent source attempting access
Short interval between attempts	Scripted brute-force behavior

MITRE ATT&CK Mapping

MITRE ID	Technique	Description
T1110.001	Brute Force — Password Guessing	High volume failed logins targeting credentials

---

Recommended Mitigations

Type	Recommendation
Technical	Enforce account lockout policies
Technical	Require strong password policies
Monitoring	Create Splunk real-time alerts
Policy	Enforce MFA on privileged accounts

Conclusion

The alert triggered by Splunk demonstrates a **high-frequency brute-force credential attack**. Mapping this activity to **MITRE ATT&CK T1110.001** strengthens classification and supports SOC response workflows.

Enforcing **account lockouts, strong passwords, MFA, and SIEM alerting** significantly reduces unauthorized access attempts and minimizes attack surface in enterprise networks.