

Brute Force Attack Log Analysis

Logs source: Blue Team Labs Online, Challenge: Bruteforce

Scenario:

One of our system administrators identified a large number of Audit Failure events in the Windows Security Event log. The task is to analyze logs from an attempted RDP brute-force attack, identify the attacker's source IP and source ports, and summarize failed login patterns.

Analysis:

I ingested the raw logs into Splunk for analysis, allowing automatic parsing of the multi-line text file. I noticed, there were many failed attempts to log on, so I focused my investigation on Windows Event ID 4625. There were 3103 failed attempts to log on to the administrator account, all with the reason: "Unknown user name or bad password".

The screenshot shows the Splunk interface with the following details:

- Search bar: source="BTLO_Bruteforce_Challenge.txt" host="BTLO" index="btlo" sourcetype="btlo_bruteforce_security_logs" 4625
- Time range: All time
- Event count: 3,103 events (before 2/18/26 4:24:36.000 PM)
- Event sampling: No Event Sampling
- Job mode: Smart Mode
- Events (3,103) selected, Patterns, Statistics, Visualization tabs available.
- Timeline format: 1 minute per column.
- Event details:
 - Time: 2/12/22 7:22:00.000 AM
 - Event ID: 4625
 - Type: Logon
 - Reason: "An account failed to log on."
 - Subject:
 - Security ID: NULL SID
 - Account Name: -
 - Account Domain: -
 - Logon ID: 0x0
 - Logon Type: 3
 - Account For Which Logon Failed:
 - Security ID: NULL SID
 - Account Name: administrator
 - Account Domain: -
 - Failure Information:
 - Failure Reason: Unknown user name or bad password.
 - Status: 0xC000006D
 - Sub Status: 0xC000006A
 - Process Information:
 - Caller Process ID: 0x0
 - Caller Process Name: -
 - Network Information:
 - Workstation Name: -
 - Source Network Address: 113.161.192.227
 - Source Port: 59545
 - Detailed Authentication Information:
 - Logon Process: NtLmssp
 - Authentication Package: NTLM
 - Transited Services: -
 - Package Name (NTLM only): -
 - Key Length: 0
 - Text explaining the event:

This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.

 - Transited services indicate which intermediate services have participated in this logon request.
 - Package name indicates which sub-protocol was used among the NTLM protocols.
 - Key length indicates the length of the generated session key. This will be 0 if no session key was requested."

Since the logs were multi-line text, the UI field extractor could not be used effectively. I extracted the source IP and source port fields using SPL regex, which requires naming the capture groups:

Source IP:

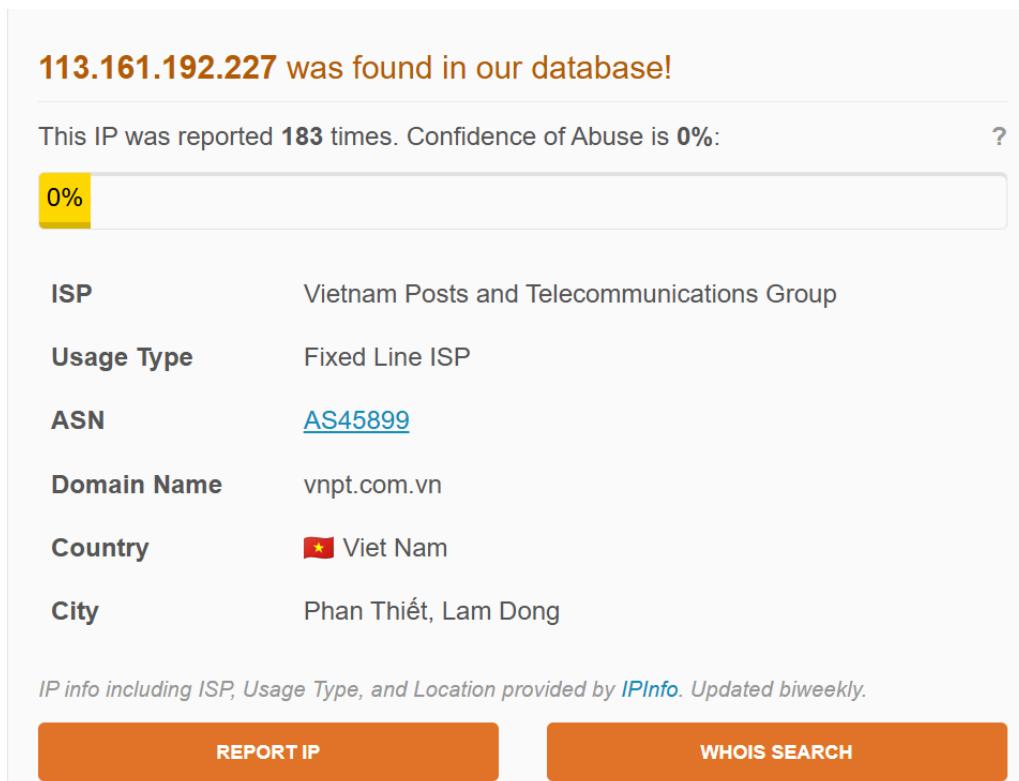
```
Source Network Address:\s+(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

Source Port:

```
Source Port:\s+(?<src_port>\d+)
```

Threat Intelligence:

Using AbuseIPDB, the attacker's IP address (133.161.192.227) was found to be associated with Vietnam, indicating an external malicious actor.



Attacker Behavior:

Analysis of the extracted source ports using Splunk's `stats` command indicate the attacker used ports in the range 49162-65534 in about 55 minutes. This is consistent with automated brute-force attempts.

Port Range:

```
source="BTLO_Bruteforce_Challenge.txt" host="BTLO" index="btlo"
sourcetype="btlo_bruteforce_security_logs"
| stats max(src_port) as HighestPort, min(src_port) as LowestPort
```

HighestPort ↴ ↵

65534

LowestPort ↴ ↵

49162

Time Elapsed:

```
source="BTLO_Bruteforce_Challenge.txt" host="BTLO" index="btlo"
sourcetype="btlo_bruteforce_security_logs"
| stats count min(_time) as first_attempt max(_time) as last_attempt
by src_ip
| eval duration_minutes=(last_attempt-first_attempt)/60
```

count ↴ ↵

first_attempt ↴ ↵

last_attempt ↴ ↵

duration_minutes ↴ ↵

3103

1644676003

1644679320

55.28333333333333

SOC-Relevant Insights/Recommendations:

Implement a firewall or IPS rules to block traffic from the malicious IP.

Create alerts for repeated Windows Event ID 4625 failures to detect future attacks.

Monitor for unusual source ports during login attempts to catch automated attack tools early.

Conclusion:

This analysis demonstrates end-to-end SOC investigation skills: raw log ingestion, regex field extraction for multi-line logs, SPL analysis, and integration with threat intelligence to identify and contextualize malicious activity.