Brute Force Attack Log Analysis

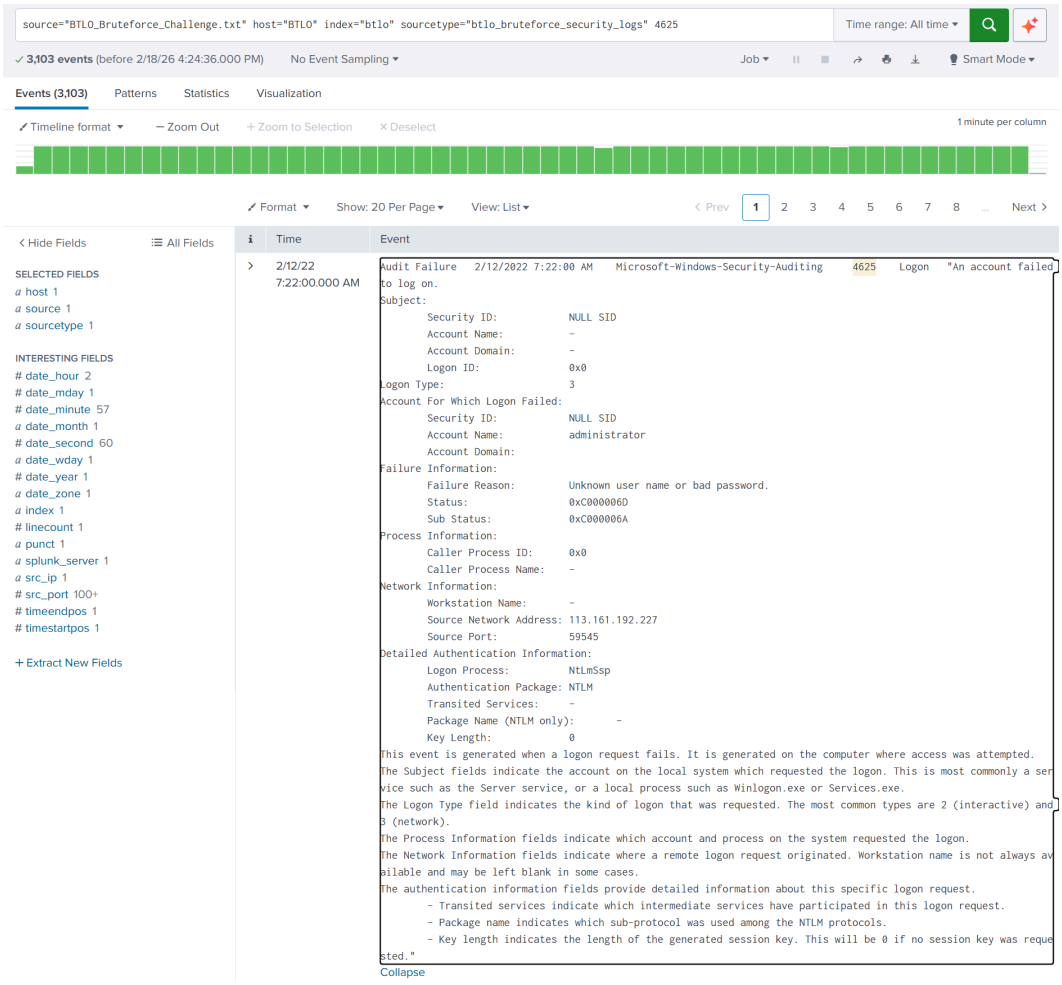
Logs source: Blue Team Labs Online, Challenge: Bruteforce

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".



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})
```

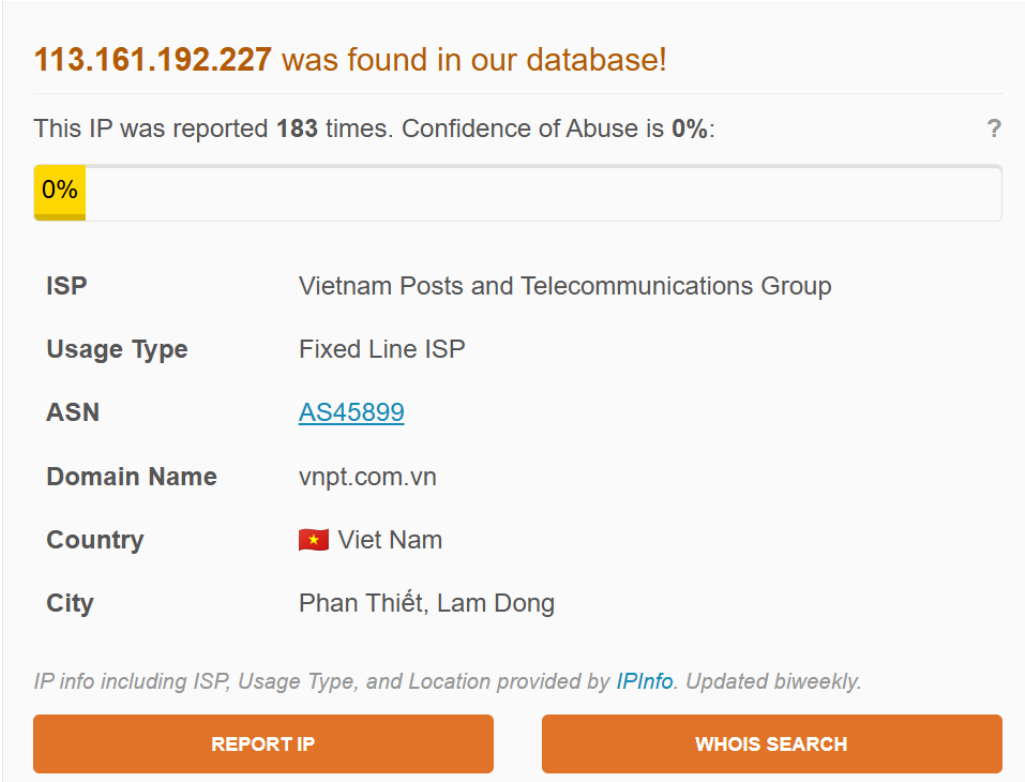
Source Port:

```
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	LowestPort
65534	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.