

Day 8: BRUTEFORCE ATTACK ANALYSIS USING SPLUNK



Date: May 09, 2025

Author: Gubbala Jaya Kumar

Challenge: 30 Days of Cybersecurity Attacks Monitoring and Detection

Scenario

One of our system administrators identified a large number of Audit Failure events in the Windows Security Event log. There are a number of different ways to approach the analysis of these logs! Consider the suggested tools, but there are many others out there.

A system administrator reported a spike in **Audit Failure** events in the **Windows Security Event Log**, potentially indicating an **RDP brute-force attack**. As part of this challenge, I conducted an investigation using **Splunk** for log analysis and **VirusTotal** for IP reputation checking.

Challenge Submission

- How many Audit Failure events are there? (Format: Count of Events)
- What is the username of the local account that is being targeted? (Format: Username)
- What is the failure reason related to the Audit Failure logs? (Format: String)
- What is the Windows Event ID associated with these logon failures? (Format: ID)
- What is the source IP conducting this attack? (Format: X.X.X.X)
- What country is this IP address associated with? (Format: Country)
- What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)

Tools Used

- Splunk
- Virus Total

Lab Requirements

- **Packet Capture File**
- Password: btlo
(inner ZIP: infected)

💡 Question 1: How many Audit Failure events are there?

Answer: 3103

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="BTLO_BruteForce_Challenge.csv" host="LAPTOP-JT42N9HL" sourcetype="csv" Audit Failure
- Event Count:** 3,103 events (highlighted in red)
- Time Range:** Before 5/9/25 7:57:44.000 AM
- Event Sampling:** No Event Sampling
- Panel Headers:** Events (3,103), Patterns, Statistics, Visualization
- Timeline Format:** Timeline format (selected), Zoom Out, + Zoom to Selection, X Deselect
- Table Headers:** Time, Event
- Event Data:** A single event row is expanded:
 - Time:** 2/12/22 7:22:00.000 AM
 - Event Type:** Audit Failure
 - Subject:**
 - Security ID: NULL SID
 - Account Name: -
 - Account Domain: -
 - Logon ID: 0x0
 - Logon Type:** 3
 - Account For Which Logon Failed:**
 - Security ID: NULL SID
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Date and Time, date_hour, date_minute, date_month, date_second

💡 Question 2: What is the username of the local account that is being targeted?

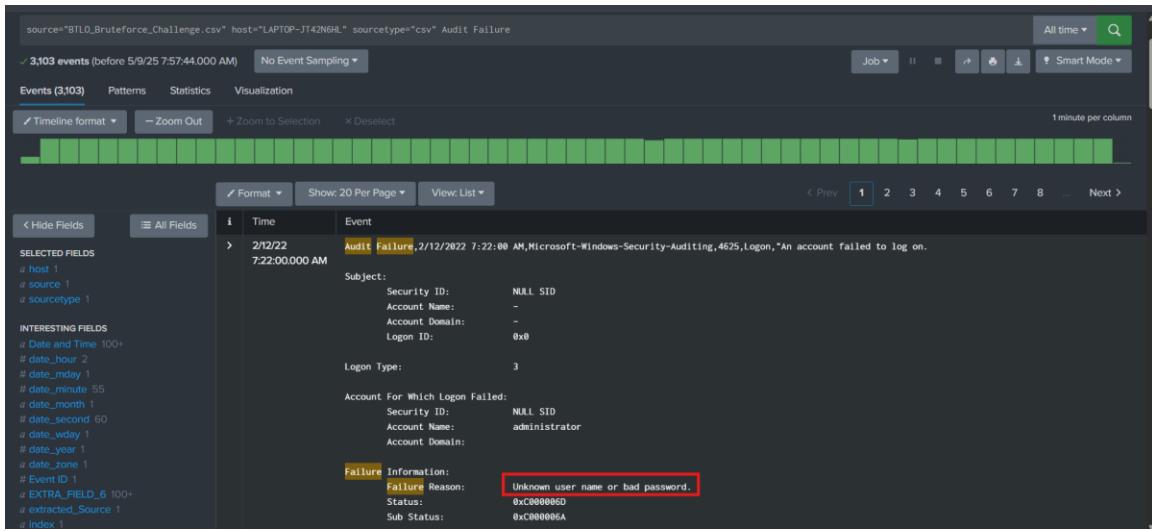
Answer: administrator

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="BTLO_BruteForce_Challenge.csv" host="LAPTOP-JT42N9HL" sourcetype="csv" Audit Failure
- Event Count:** 3,103 events
- Time Range:** Before 5/9/25 7:57:44.000 AM
- Event Sampling:** No Event Sampling
- Panel Headers:** Events (3,103), Patterns, Statistics, Visualization
- Timeline Format:** Timeline format (selected), Zoom Out, + Zoom to Selection, X Deselect
- Table Headers:** Time, Event
- Event Data:** A single event row is expanded:
 - Time:** 2/12/22 7:22:00.000 AM
 - Event Type:** Audit Failure
 - 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 (highlighted in red)
 - Account Domain: -
 - Failure Information:**
 - Failure Reason: Unknown user name or bad password.
 - Status: 0xC00006D
 - Sub Status: 0xC00006A
 - Process Information:**
 - Caller Process ID: 0x0
 - Caller Process Name: -
 - Network Information:**
 - Workstation Name: -
 - Source Network Address: 113.161.192.227
 - Source Port: 59545
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Date and Time, date_hour, date_minute, date_month, date_second, date_wday, date_year, date_zone, Event ID, EXTRA_FIELD_6, extracted_Source, index, Keywords, linecount, punct, splunk_server, Task Category, timestamppos
- Buttons:** + Extract New Fields

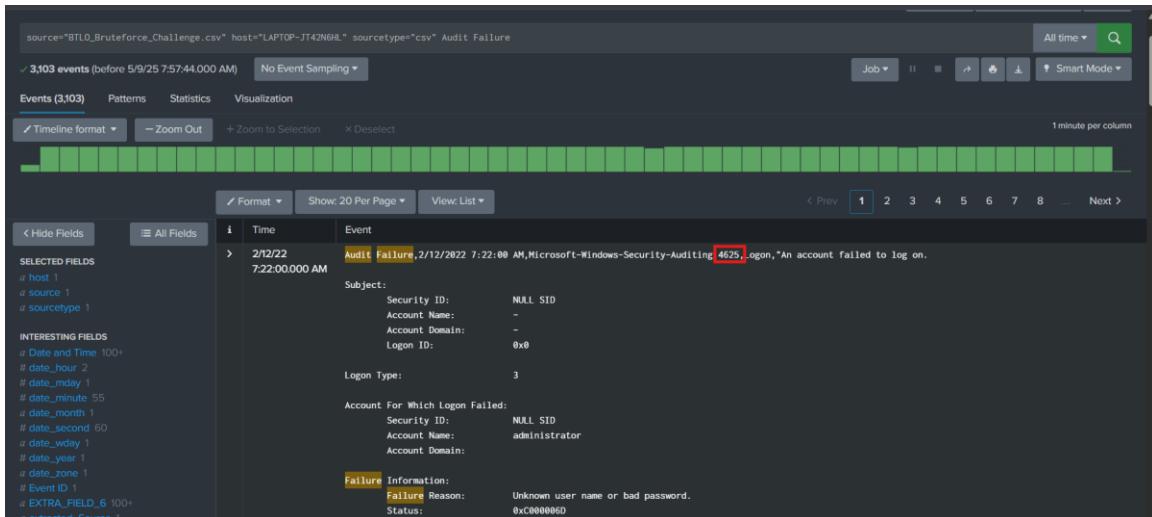
💡 Question 3: What is the failure reason related to the Audit Failure logs?

Answer: Unknown user name or bad password



✿ Question 4: What is the Windows Event ID associated with these logon failures?

Answer: 4625



✿ Question 5: What is the source IP conducting this attack?

Answer: 113.161.192.227

		Time	Event	
# date_minute	55		Security ID:	NULL SID
# date_month	1		Account Name:	administrator
# date_second	60		Account Domain:	
# date_weekday	1		Failure Information:	
# date_year	1		Failure Reason:	Unknown user name or bad password.
# date_zone	1		Status:	0xC000006D
# Event ID	1		Sub Status:	0xC000006A
# EXTRA_FIELD	6 100+		Process Information:	
# extracted_Source	1		Caller Process ID:	0x0
# index	1		Caller Process Name:	-
# Keywords	1		Network Information:	
# Linecount	1		Workstation Name:	-
# punct	1		Source Network Address:	113.161.192.227
# splunk_server	1		Source Port:	59545
# task_Category	1		Detailed Authentication Information:	
# timendipos	1		Logon Process:	NtLmSpn
# timestamppos	1		Authentication Package:	NTLM
+ Extract New Fields			Transited Services:	-
			Package Name (NTLM only):	-
			Key Length:	0

❖ Question 6: What country is this IP address associated with?

Answer: Vietnam

Check the help_recover_instructions.txt file

The screenshot shows a network analysis interface for the IP address 113.161.192.227. Key details displayed include:

- No security vendor flagged this IP address as malicious.
- IP address: 113.161.192.227 (113.160.0.0/11)
- Autonomous System Number: AS45899 (VNPT Corp)
- Country: VN (Vietnam)
- Last Analysis Date: 1 month ago
- Basic Properties table:

Network	113.160.0.0/11
Autonomous System Number	45899
Autonomous System Label	VNPT Corp
Regional Internet Registry	APNIC
Country	VN
Continent	AS
- Whois Lookup table:

mnt-by: MAINT-VN-VNNIC
mnt-lower: MAINT-VN-VNPT
mnt-routes: MAINT-VN-VNPT
Last-modified: 2018-01-25T03:55:17Z
mnt-irt: IRT-VNNIC-AP

❖ Question 7: What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)

Answer: 49162-65534

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following command:

```
source="BTLO_BruteForce_Challenge.csv" host="LAPTOP-JT42N6HE" sourcetype="csv" | rex "Source Port:\s*(?<source_port>\d+)" | stats min(source_port) as Low_Port max(source_port) as High_Port
```

The search results indicate 3,129 events found before 5/9/25 7:53:59.000 AM. The Statistics tab is selected, showing two numerical values: 49162 for Low_Port and 65534 for High_Port.

📋 Conclusion

This analysis demonstrates how attackers systematically attempt to brute-force RDP logins using automated tools. With **Splunk**, we were able to correlate logs efficiently, and **VirusTotal** helped validate the IP's threat level and origin. Continuous monitoring and threat intelligence integration are essential to detect and prevent such attacks in real time.