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

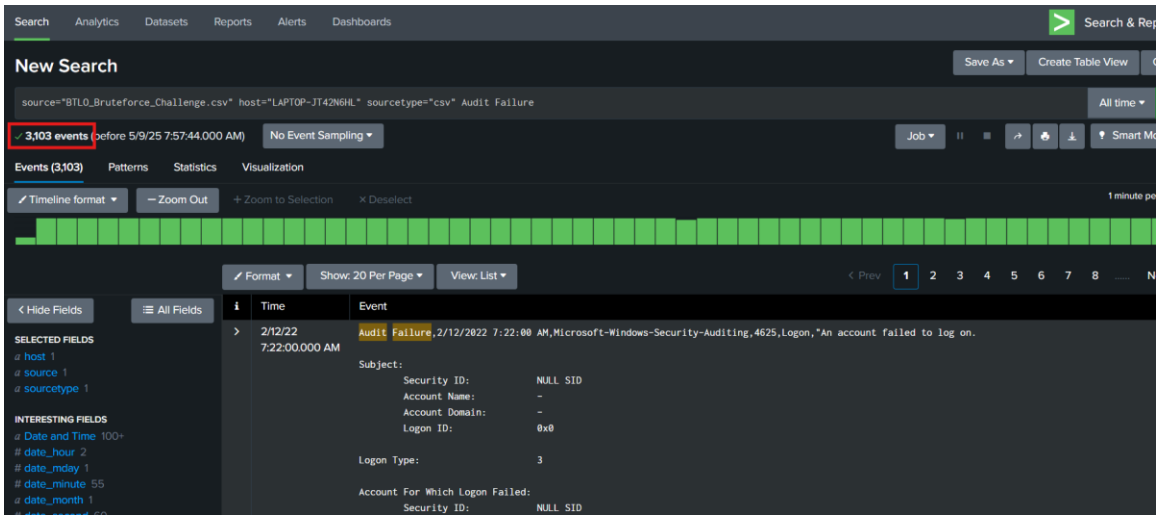
Lab Requirements

- Packet Capture File

- Password: btlo
(inner ZIP: infected)

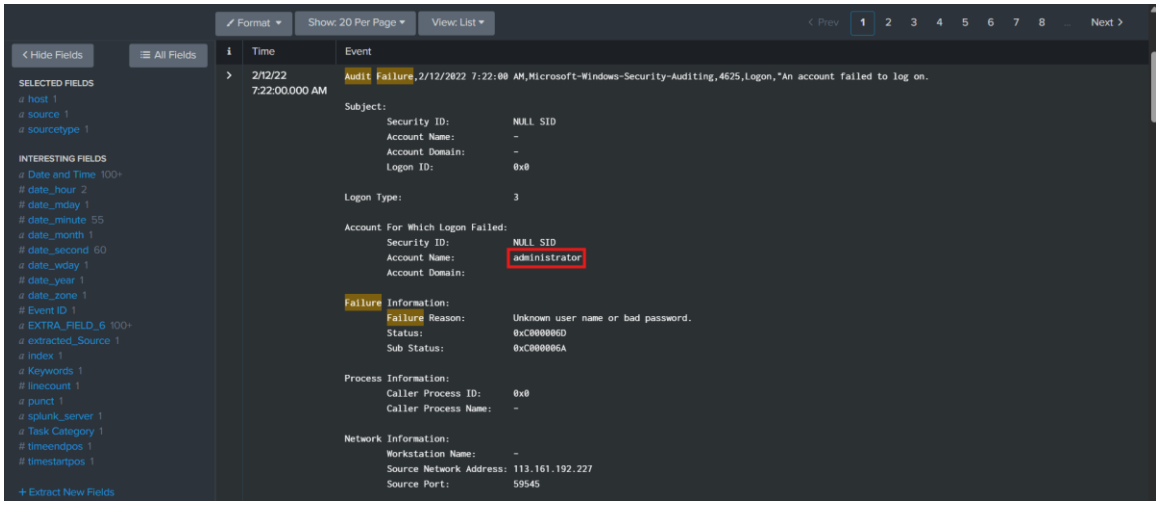
Question 1: How many Audit Failure events are there?

Answer: 3103



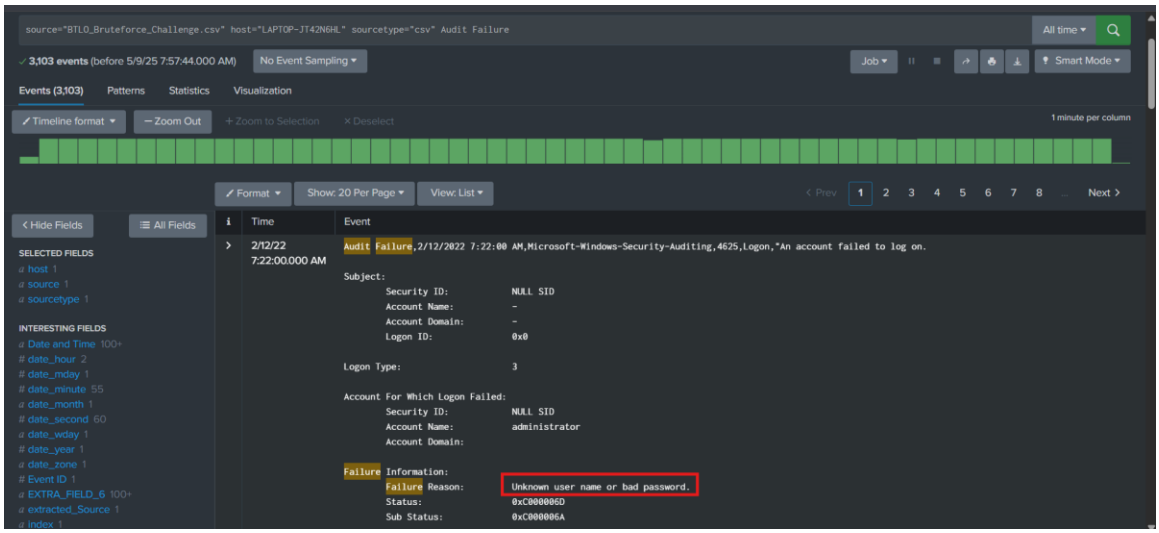
Question 2: What is the username of the local account that is being targeted?

Answer: administrator



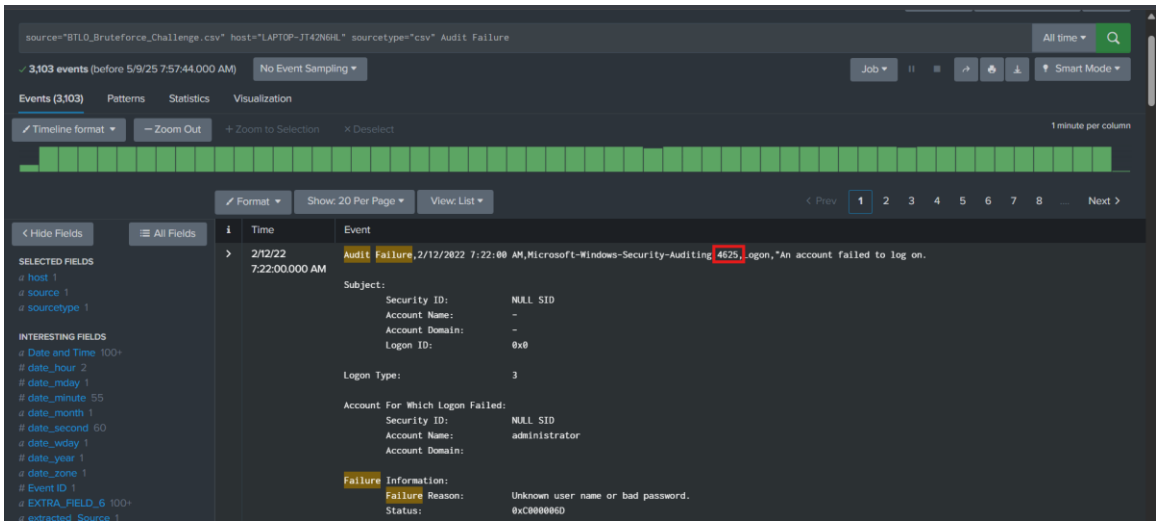
Question 3: What is the failure reason related to the Audit Failure logs?

Answer: Unknown user name or bad password



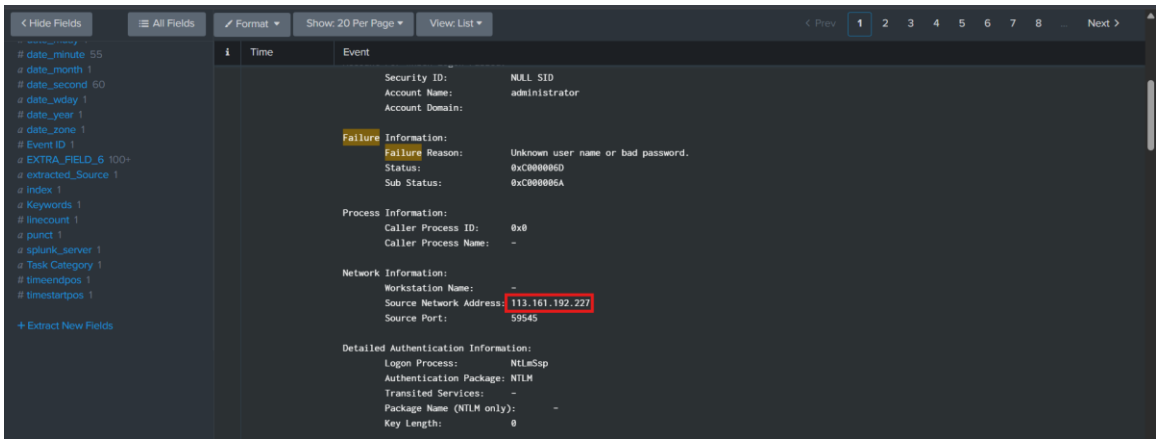
Question 4: What is the Windows Event ID associated with these logon failures?

Answer: 4625



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

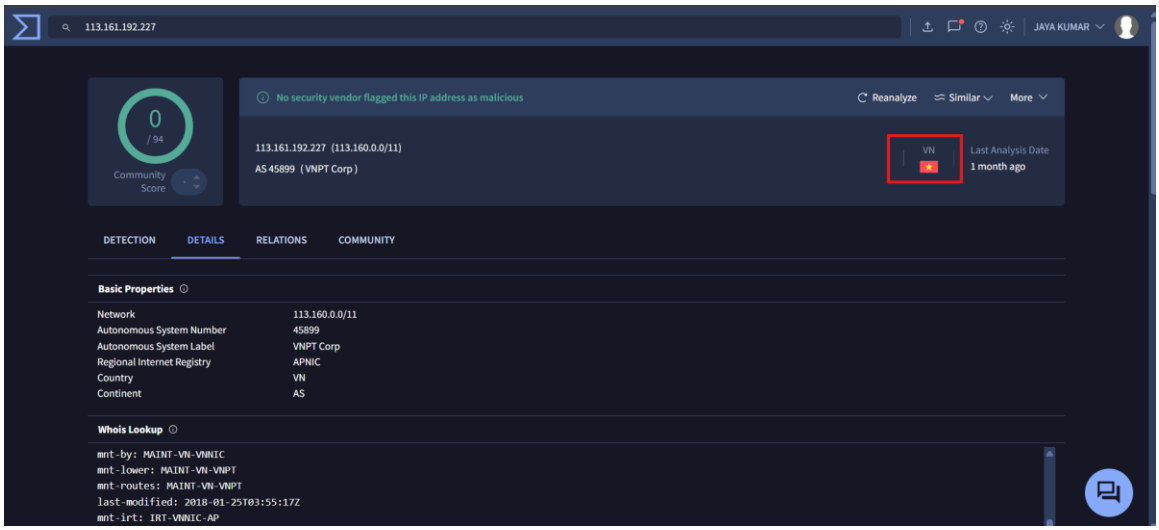
Answer: 113.161.192.227



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

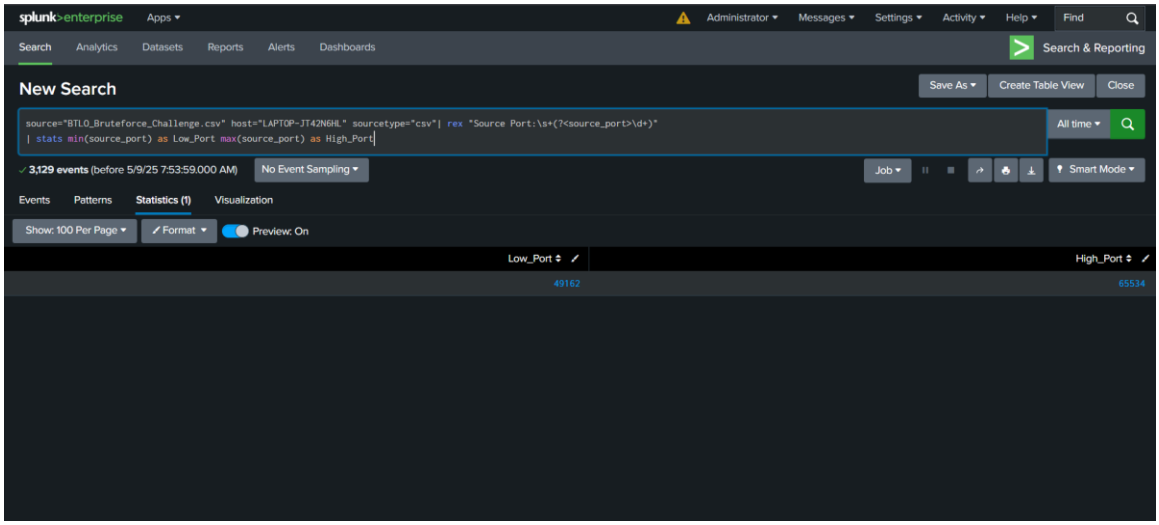
Answer: Vietnam

Check the help_recover_instructions.txt file



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



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.