SOC PROJECT 2

VPN BRUTE FORCE DETECTION AND INVESTIGATION USING SPLUNK

BY:

MOSHOOD MARIAM OMOSHALEWA (RILEWA)

DATE: 2ND FEBRUARY, 2026

Section 1: Project Documentation

Project Objective

The purpose of this project is to simulate a real Security Operations Center (SOC) investigation using Splunk. The goal is to detect, investigate, and validate a VPN brute force authentication attack and document the findings as a security incident.

This project focuses on identifying authentication abuse that may lead to account compromise by analyzing VPN authentication activity and detecting suspicious login behavior.

Data Source

The data used for this project was obtained from a TryHackMe room. The room provided downloadable VPN authentication logs, which were used directly for this investigation without modification.

- Log type: VPN authentication logs
- Format: JSON
- Source: TryHackMe

Tools Used

- Splunk (local installation)

Splunk was used for log ingestion, validation, analysis, and investigation.

Investigation Focus

The investigation focuses on:

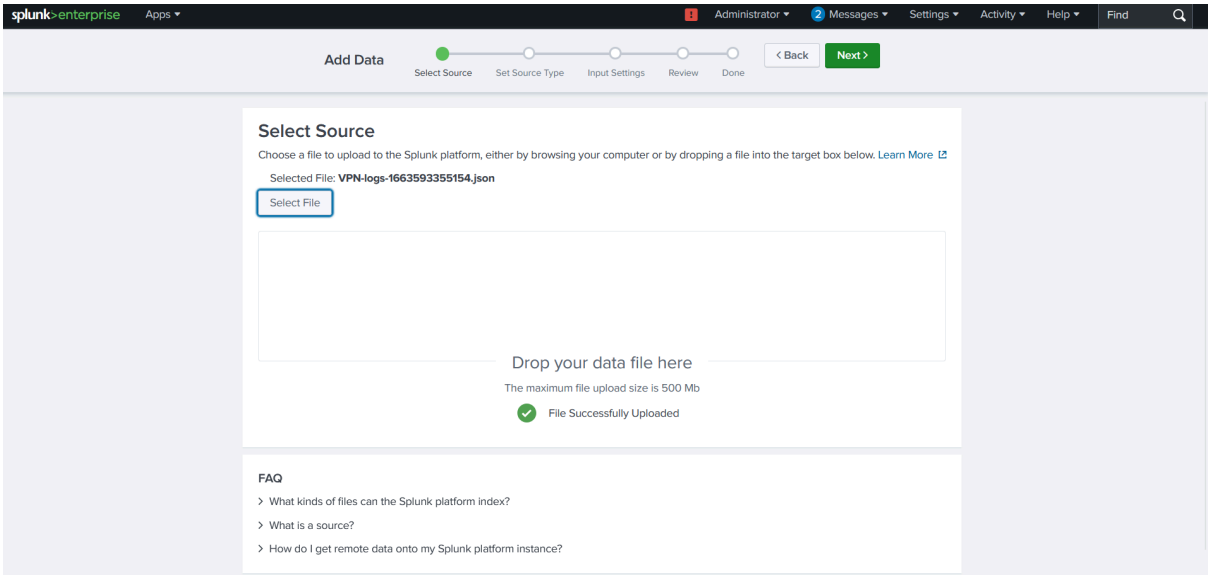
- Authentication abuse
- Potential account compromise
- Repeated failed login attempts
- Identifying suspicious authentication patterns

The objective is to detect failed authentication attempts, analyze their behavior, and determine whether the activity indicates malicious intent.

Stage 1: Log Ingestion and Validation

Log Ingestion

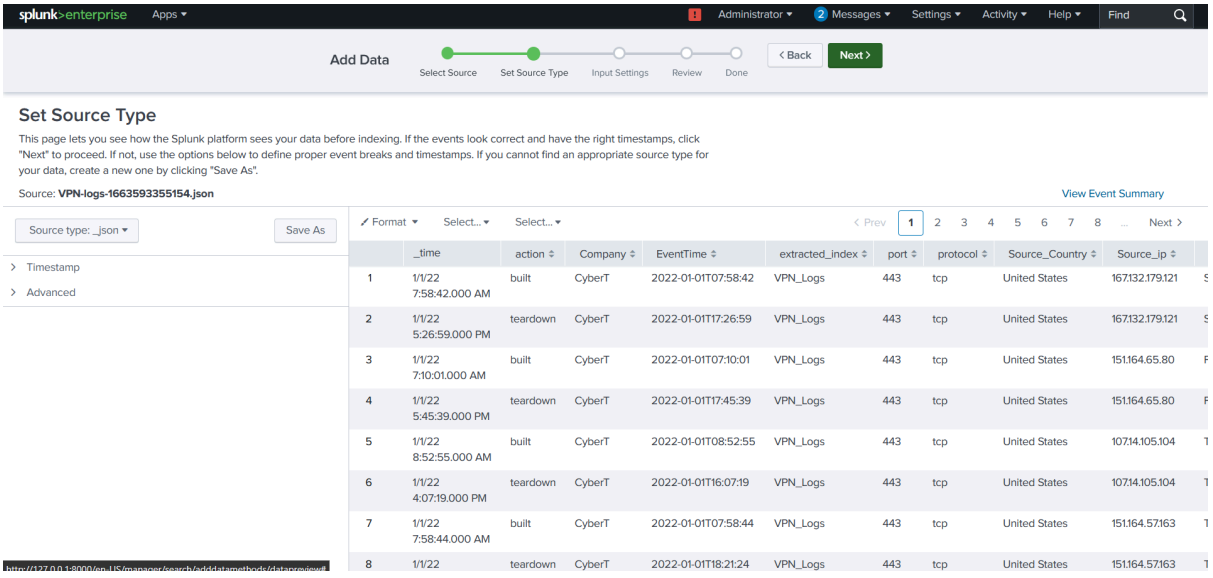
The VPN authentication logs were ingested into Splunk by uploading the downloaded JSON file.



Validation Checks

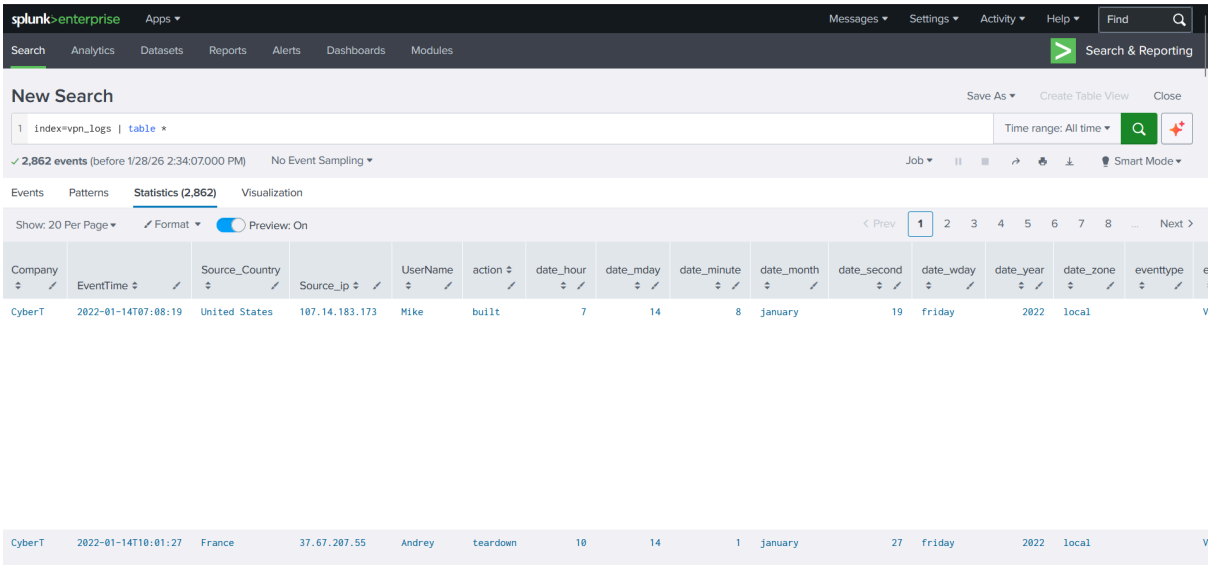
After ingestion, the following validations were performed:

- Confirmed that logs were visible in Splunk
- Confirmed that fields were parsed correctly
- Verified that the source type was JSON
- Queried the logs using the VPN logs index to ensure data accessibility



Initial Log Review

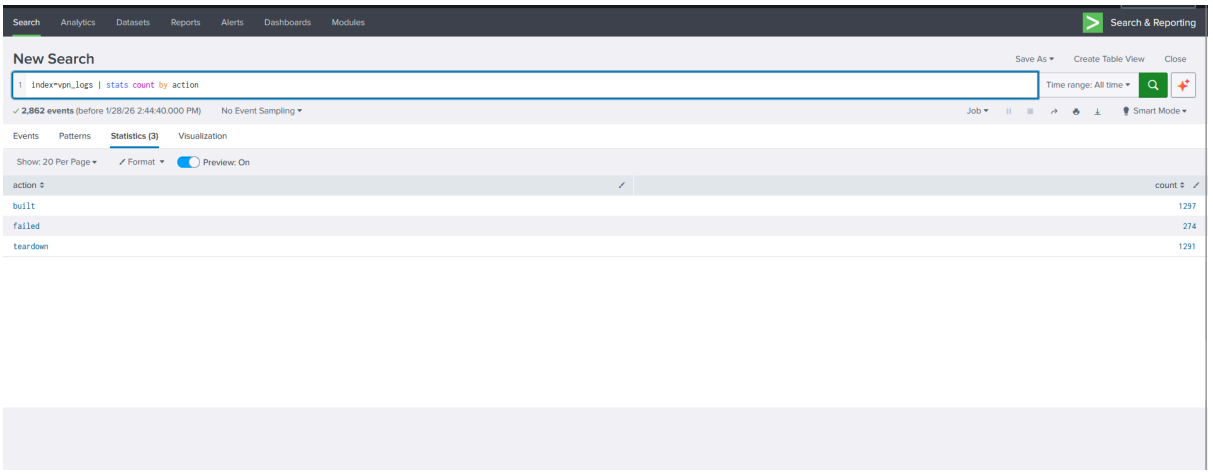
The VPN logs were reviewed in table format to understand the structure and available fields.



Action Analysis

A statistical count of authentication actions was performed using action-based aggregation. The results showed three distinct actions:

- Built: 1,297 events
- Failed: 274 events
- Teardown: 1,291 events



Action meanings:

- Failed indicates authentication or connection failure
- Built indicates a successful VPN connection
- Teardown indicates a VPN session termination

For this investigation, the primary focus is on failed authentication events, as they are most relevant for detecting brute force or unauthorized access attempts.

Stage 2: Suspicious Authentication Analysis

Username Activity Analysis

Statistics were generated to count authentication events by username. This step was performed to identify abnormal or suspicious user behavior.

The analysis showed that the username “Simon” had the highest number of events, with a total count of 278. No other user had a comparable volume of activity.

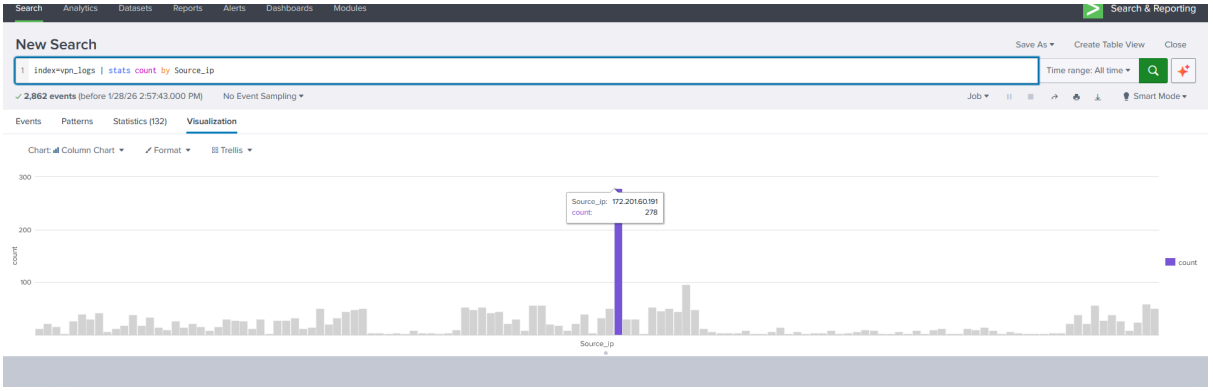
This immediately marked the account as suspicious and required deeper investigation.

Source IP Analysis

Statistics were also generated to count events by source IP address.

The source IP 172.201.60.199 recorded 278 events, matching the total activity count of the user Simon. This confirms that all authentication attempts for Simon originated from a single IP address.

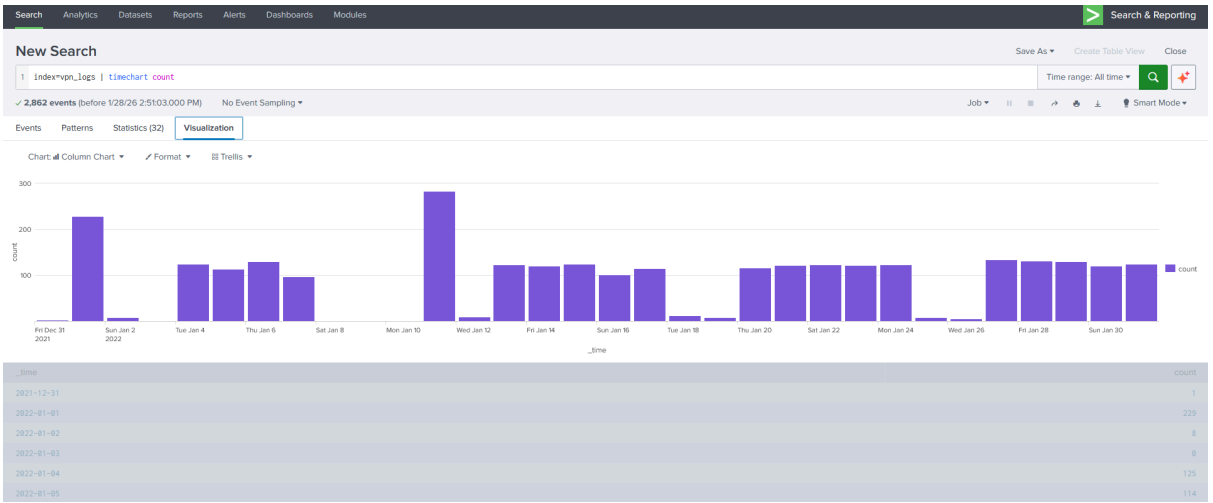
The source IP therefore became directly associated with the suspicious activity.



Time-Based Activity Analysis

A time chart was reviewed to observe authentication activity over time.

The highest concentration of events occurred on Tuesday, January 11th, where authentication activity was significantly higher than on other days. This spike in activity indicated abnormal behavior consistent with automated or repeated login attempts.



Combined Username, IP, and Action Analysis

Further statistics were generated combining:

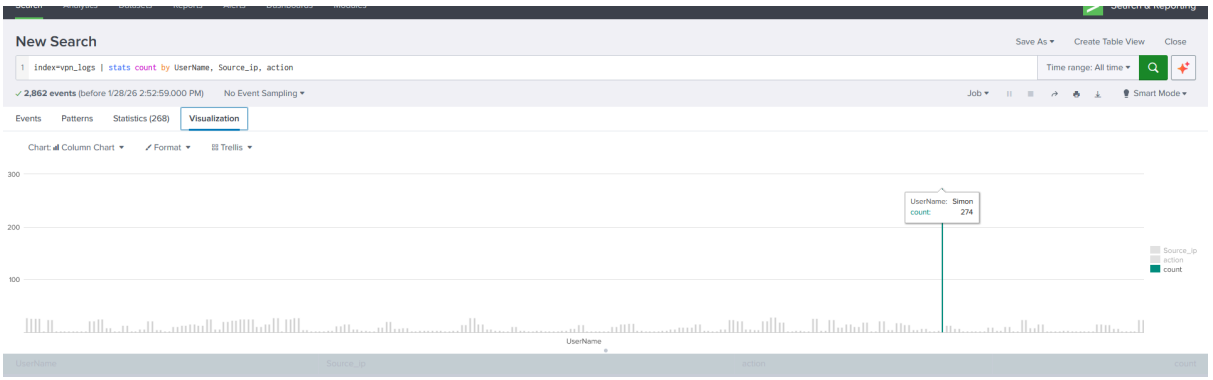
- Username
- Source IP
- Action

This analysis showed:

- Username: Simon
- Source IP: 172.201.60.199
- Action: Failed
- Event count: 274

Out of the total 278 events associated with Simon, 274 were failed authentication attempts.

This confirms a high-volume failed login pattern targeting a single account from a single IP address.

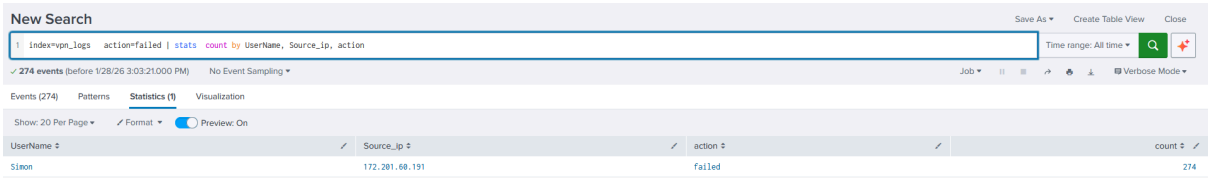


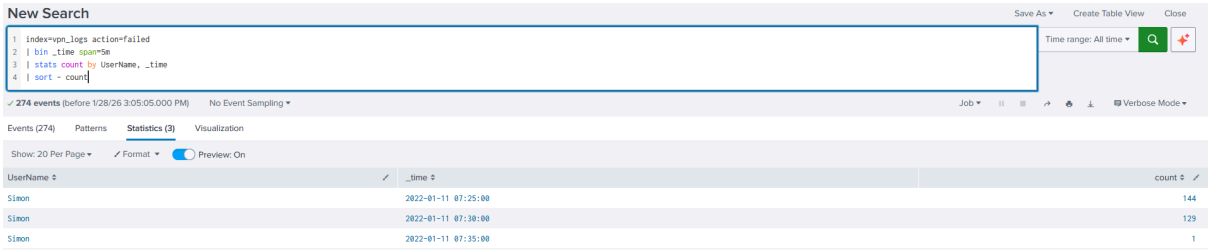
Failed Authentication Burst Analysis

To understand how the failed attempts occurred, failed actions were analyzed over a 5-minute time span.

Results showed:

- Between 07:25 and 07:30 on the same day, there were 144 failed attempts
- At 07:30, an additional 129 failed attempts
- At 07:35, 1 failed attempt





This pattern indicates rapid, repeated authentication attempts within short time intervals, consistent with brute force behavior.

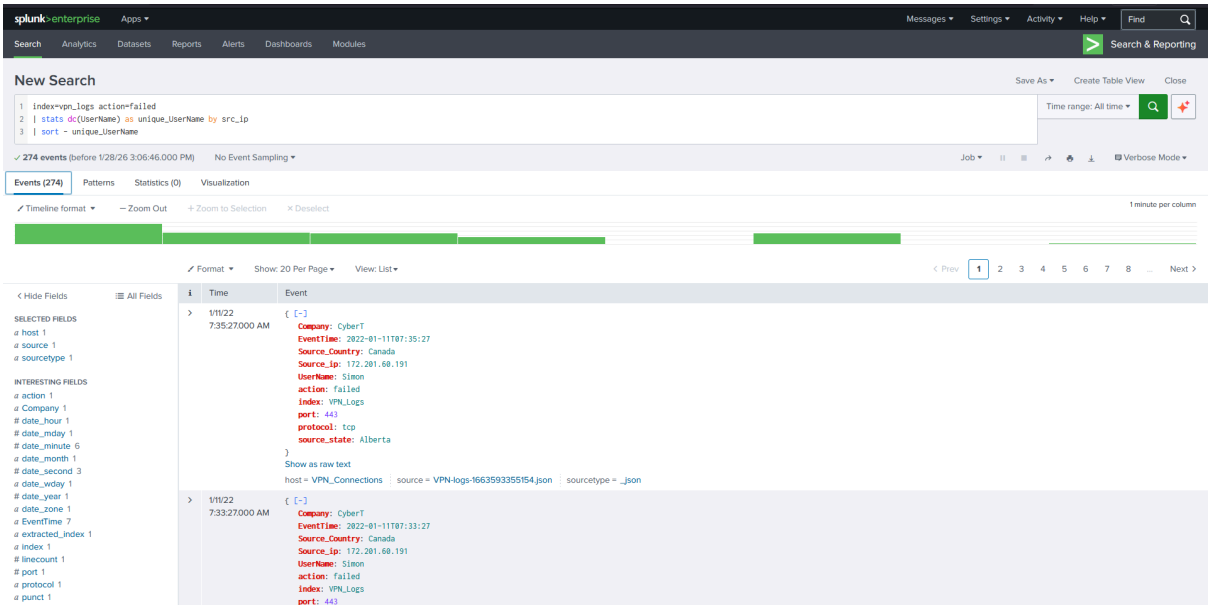
Source Context Review

Additional fields were reviewed to understand the context of the source activity.

The analysis showed:

- Source country: Canada
- Source state: Alberta
- Destination port: 443
- Protocol: TCP
- Username: Simon

This confirmed that the activity originated from a single geographic location and followed a consistent connection pattern.



Successful Authentication Review

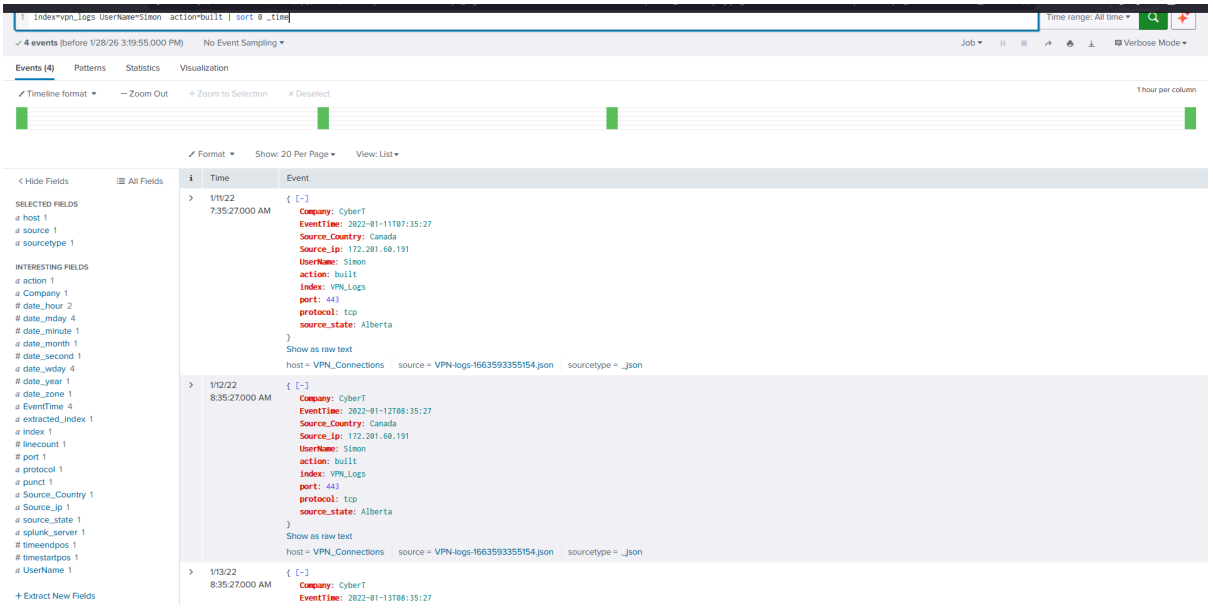
After identifying failed attempts, the investigation checked whether the same user later achieved successful authentication.

The user Simon recorded four successful (built) authentication events after the failed attempts.

These successful connections occurred as follows:

- January 11th at 07:35 AM
- January 12th at 08:35 AM
- January 13th at 08:35 AM
- January 15th at 08:35 AM

This indicates that after repeated failed attempts, authentication was eventually successful.

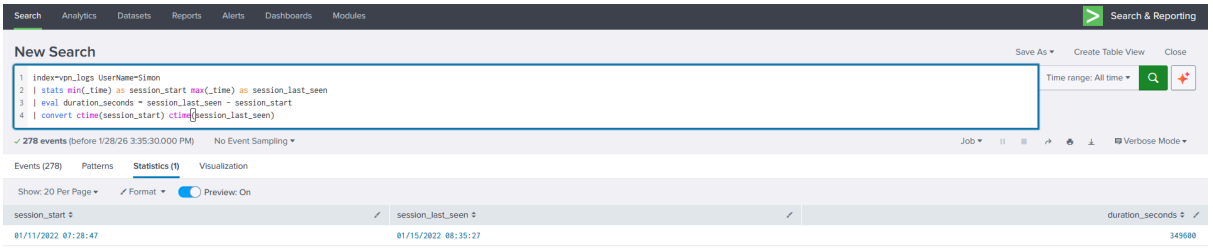


First and Last Activity Analysis

The user's activity timeline was reviewed:

- First observed event: January 11th at 07:28
- Last observed event: January 15th at 08:35

The total observed duration of activity was 349600 seconds (as reported in the logs).



Section 2: Security Incident Report

Incident Name

VPN Brute Force Authentication Attack on User Account

Incident Type

Authentication Abuse
Brute Force Login Attempt
Potential Account Compromise

Affected Account(s)

- Username: Simon

Affected System(s)

- VPN Service
- Remote Access Infrastructure

Detection Method

- Manual log analysis using Splunk
- VPN authentication logs ingested from a TryHackMe lab dataset
- Detection based on abnormal authentication failure patterns and successful login following repeated failures

Data Source

- VPN authentication logs (JSON format)
- Source: TryHackMe lab environment
- Logs ingested and indexed in Splunk (index=vpn_logs)

Incident Summary

A high volume of failed VPN authentication attempts targeting a single user account (Simon) was observed over multiple days. Following these repeated failures, successful VPN authentication events were recorded from the same source IP address. This activity is consistent with a brute force authentication attack that resulted in a potential account compromise.

Incident Timeline

- **January 11**
    - Initial failed VPN authentication attempts observed for user Simon
    - Rapid spike in failed login attempts within short time windows
    - High concentration of failures between approximately 07:25 and 07:35

- **January 11**
    - First successful VPN authentication (“action=build”) recorded after repeated failures
- **January 12**
    - Multiple additional successful VPN authentication events recorded at similar times
- **January 13**
    - Another successful VPN session observed for the same user
- **January 15**
    - Last recorded activity for user Simon
    - Indicates continued access or testing after initial compromise

Observed Indicators

Authentication Activity

- Total events for user Simon: 278
- Failed authentication attempts: 274
- Successful authentication attempts: 4

Source IP

- IP Address: 172.201.60.199
- Source Country: Canada
- Source State: Alberta
- Protocol: TCP
- Destination Port: 443

Analysis Findings

- The volume and frequency of failed authentication attempts indicate automated or scripted activity rather than normal user behavior
- All failed attempts and subsequent successful authentications originated from the same source IP
- Successful authentication events occurred after sustained brute force activity
- Timing patterns suggest persistence rather than accidental login failures

- Activity spanning multiple days increases confidence in malicious intent

Risk Assessment

- **Likelihood of Account Compromise:** High

- **Impact:**

    - Unauthorized VPN access
    - Potential access to internal network resources
    - Increased risk of lateral movement if access was not revoked

Incident Severity: Medium to High

Rationale:

- Single user targeted
- High failure volume
- Confirmed successful authentication after brute force behavior

Recommended Response Actions

- Force password reset for affected user account
- Terminate all active VPN sessions associated with the account
- Block or closely monitor the identified source IP address
- Enforce multi-factor authentication (MFA) for VPN access
- Review VPN and internal logs for signs of post-authentication activity
- Implement alerting for excessive failed authentication attempts

Incident Status

- Investigation completed
- Incident validated
- Remediation actions recommended