SOC CAPSTONE INVESTIGATION REPORT

Title: Incident Investigation Using Splunk

Tool Used: Splunk Enterprise

Prepared by: Oluwanifemi Felix Oyeniyi

Date: 11/1/2026

1. Introduction

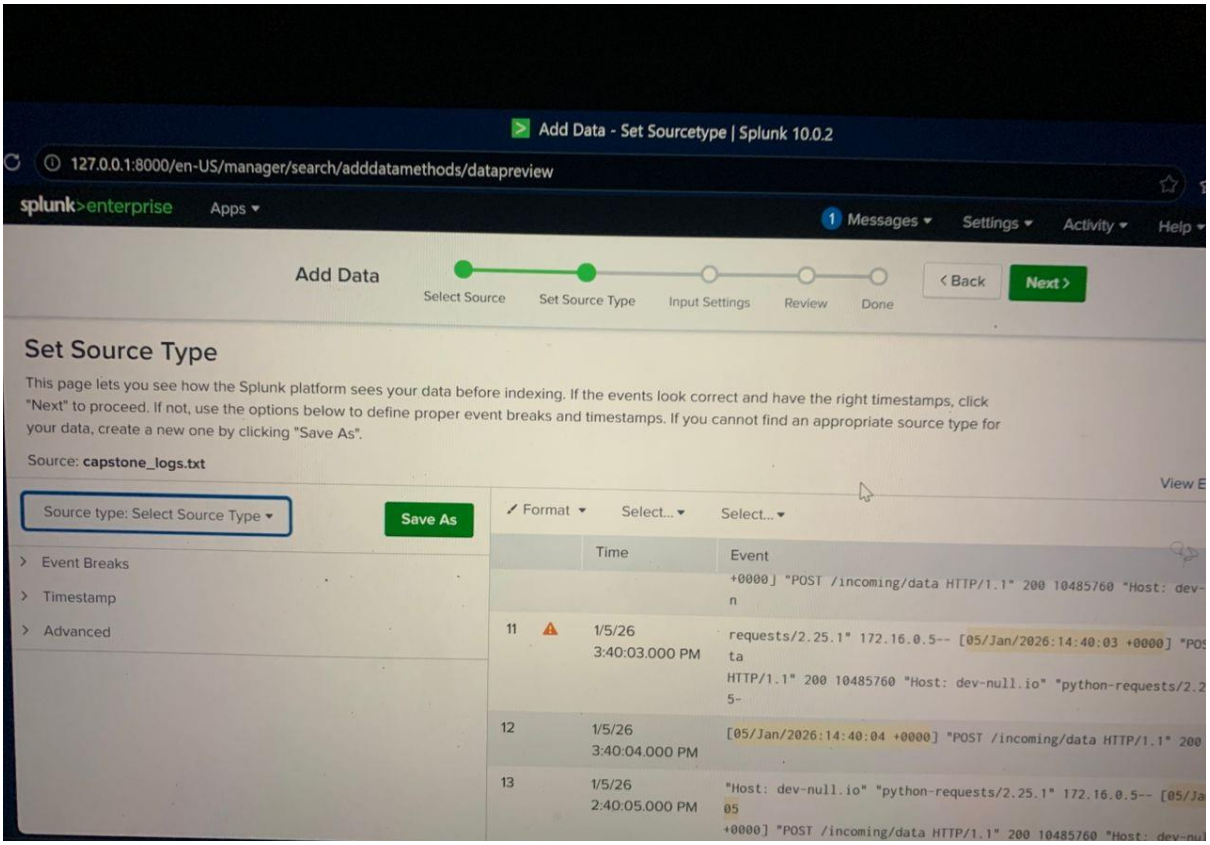
This report documents the investigation of a simulated cyberattack using Splunk as a Security Information and Event Management (SIEM) tool. The objective of the investigation was to analyze provided log data, identify malicious activity, and answer specific questions related to reconnaissance, initial access, persistence, lateral movement, and data exfiltration.

The investigation was conducted by ingesting the provided logs into Splunk and analyzing them using Splunk Search Processing Language (SPL). The findings illustrate how attackers progress through multiple stages of an attack and how such activities can be detected through log analysis.

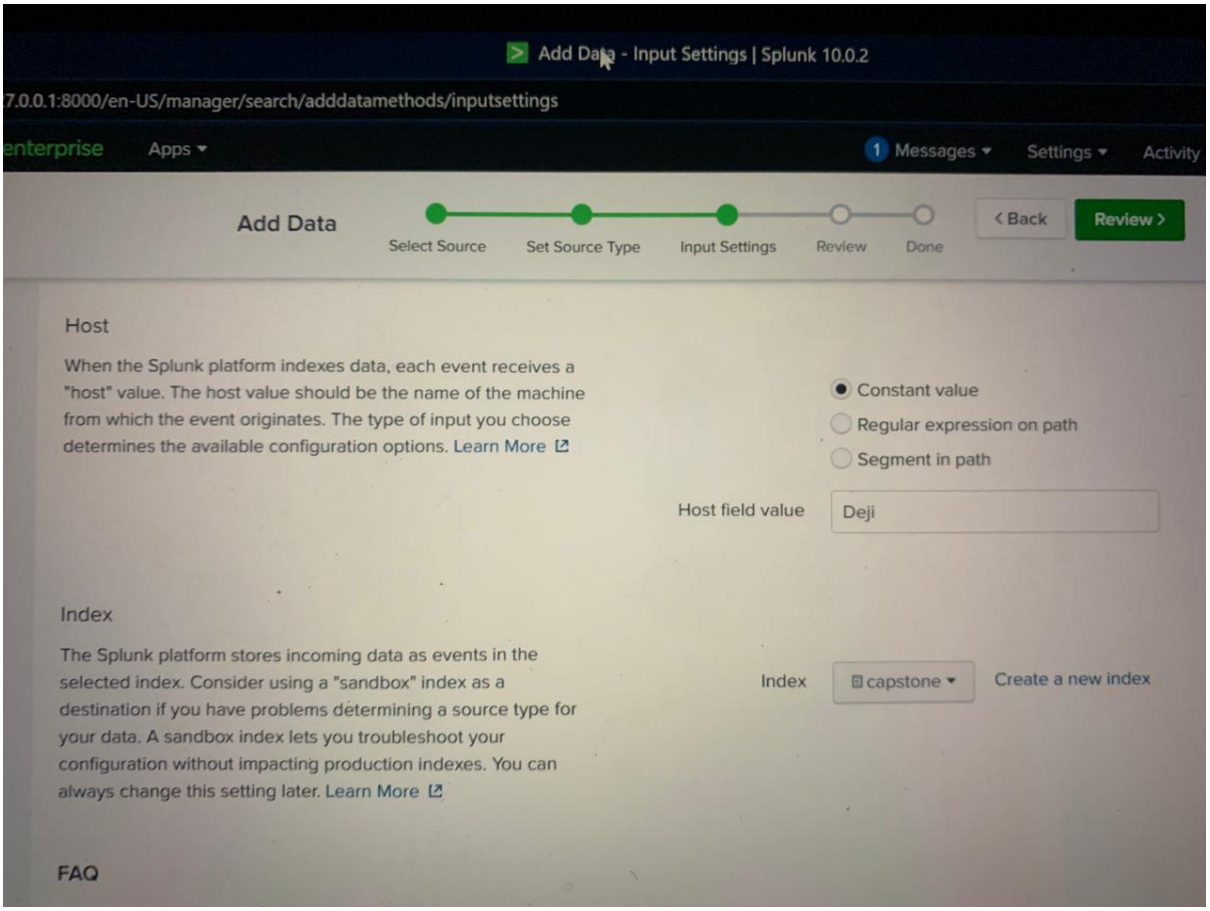
2. Methodology

The investigation followed a structured approach:

The provided logs were converted into a text file and ingested into Splunk.



A custom index named capstone was created to store the data.



Searches were performed using SPL to filter and analyze relevant events.

Suspicious activities were correlated across different log sources to reconstruct the attack timeline.

Indicators of compromise were identified at each stage of the attack.

All searches were performed with the time range set to All Time to ensure complete visibility of events.

3. Findings and Analysis

Question 1: Initial Reconnaissance

Objective

Identify the URL-encoded string used by the attacker, determine the type of attack, and explain the attacker’s objective.

Splunk Query Used

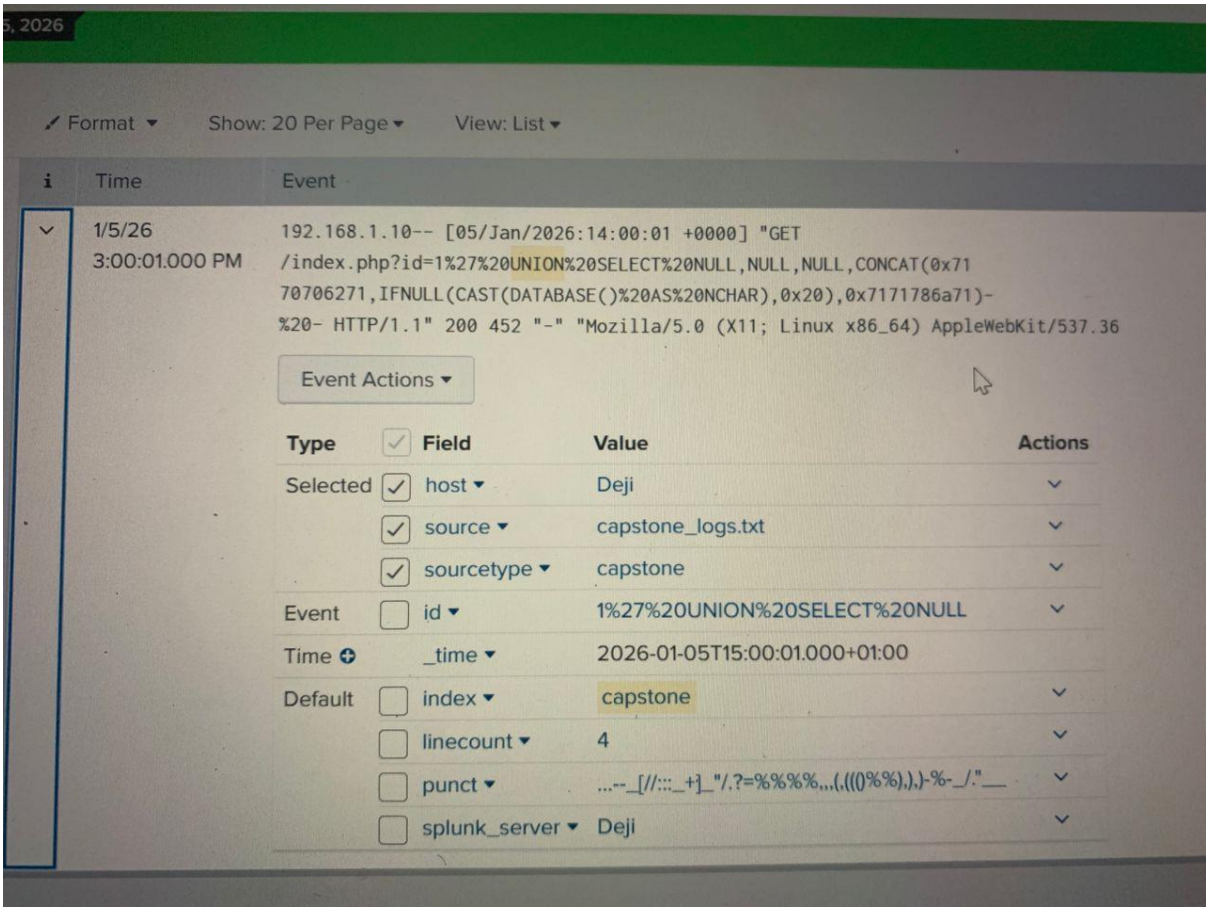
index=capstone "index.php"

Analysis

The logs revealed a suspicious HTTP GET request containing a URL-encoded payload with the keywords UNION SELECT. When decoded, the request was identified as a SQL injection attempt designed to extract information from the backend database.

Findings

URL-encoded string: %27%20UNION%20SELECT



Attack type: Union-based SQL Injection

Attacker's objective: To enumerate the database name using the DATABASE() function

Question 2: The Pivot (Brute Force Attack)

Objective

Identify the external IP address involved in the brute force attack, the exact time of successful login, and the compromised account.

Splunk Query Used

index=capstone "sshd"

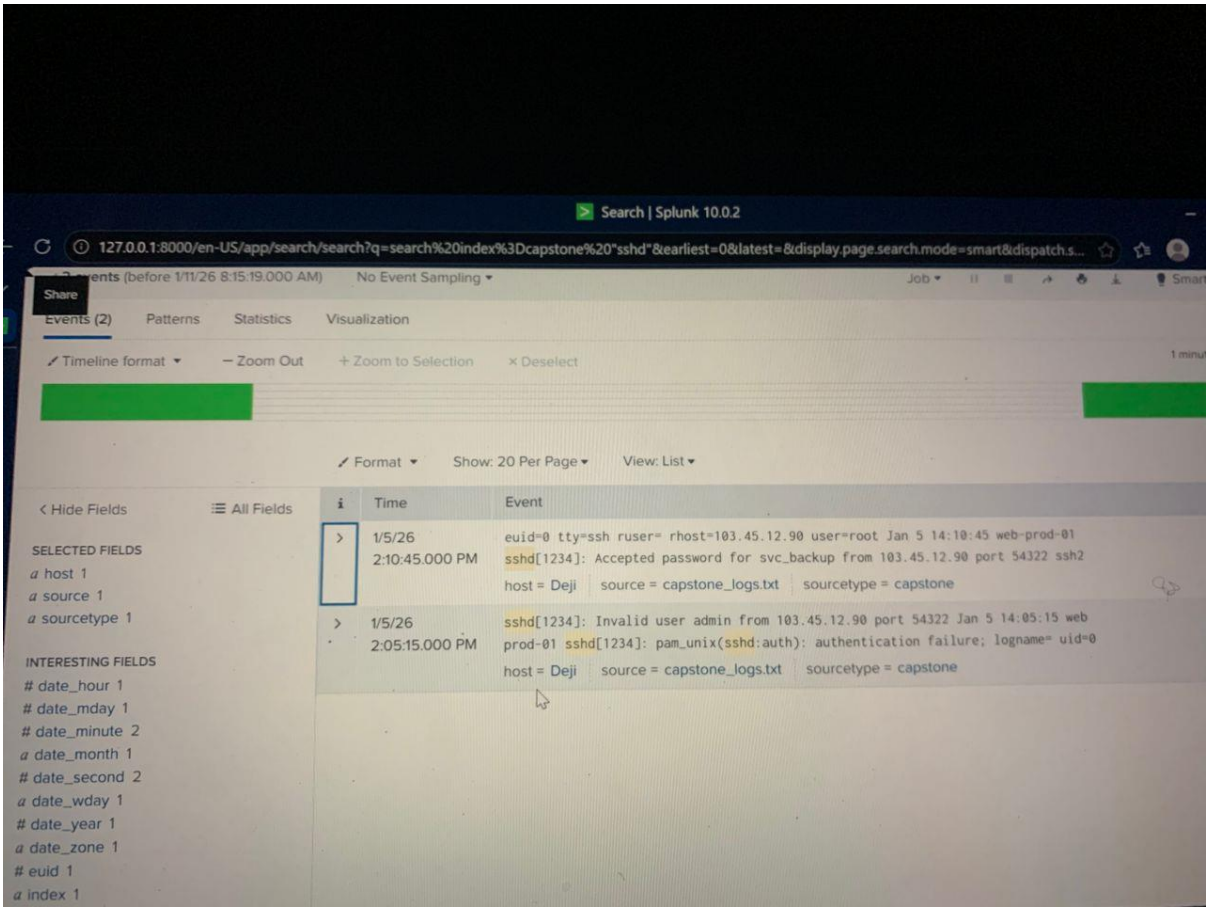
Analysis

Multiple failed SSH login attempts originating from a single external IP address were observed. These attempts were followed by a successful authentication, indicating a successful brute force attack.

Findings

Attacker IP address: 103.45.12.90

Successful login timestamp: 05/Jan/2026 14:10:45



Compromised internal account: svc_backup

Question 3: Hidden Payload (Persistence Mechanism)

Objective

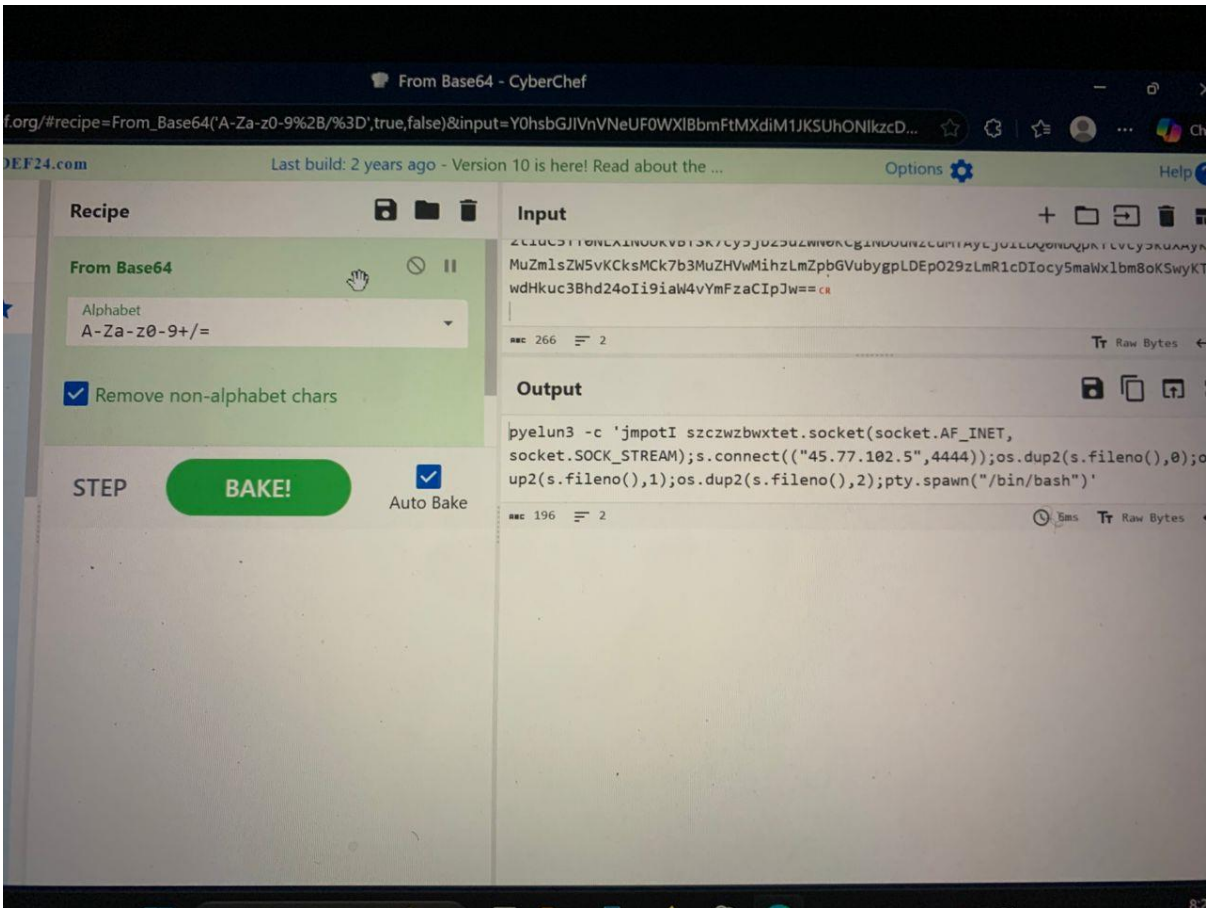
Decode the encoded payload used for persistence, identify the attacker's IP address and port, and determine the scripting language used.

Splunk Query Used

index=capstone "EXECVE"

Analysis

A process execution log contained a long encoded payload associated with a shell command. Further analysis revealed that the payload consisted of a Base64-encoded reverse shell. After decoding the payload using external tools, the script was found to establish a remote connection back to the attacker. I went on to decode the Base64 message using cyberchef



Findings

Attacker IP address: 45.77.102.5

Attacker port: 4444

Script language: Python

Question 4: Lateral Movement

Objective

Identify the scanning technique used, the internal subnet targeted, and the tool installed by the attacker.

Splunk Query Used

index=capstone "nmap"

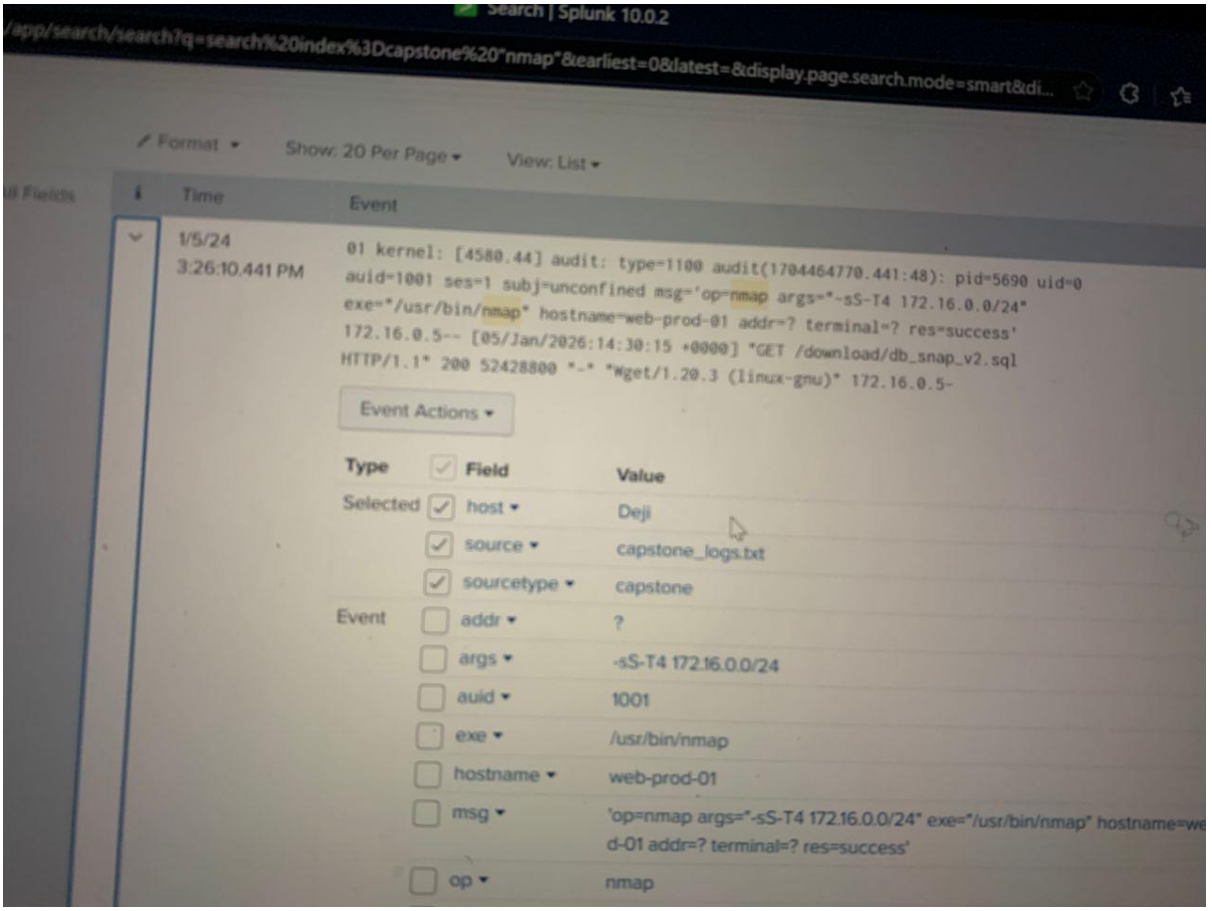
Analysis

Logs showed that the attacker installed and executed the Nmap tool after gaining access to the system. The scan targeted an internal network range using a stealthy scanning technique.

Findings

Scanning technique: TCP SYN scan (-sS)

Target subnet: 172.16.0.0/24



Tool used: Nmap

Question 5: Data Exfiltration (The Grand Theft)

Objective

Identify the stolen file, calculate the total volume of data exfiltrated, and determine the script responsible for the exfiltration.

(a) Stolen File

Splunk Query Used

index=capstone "download"

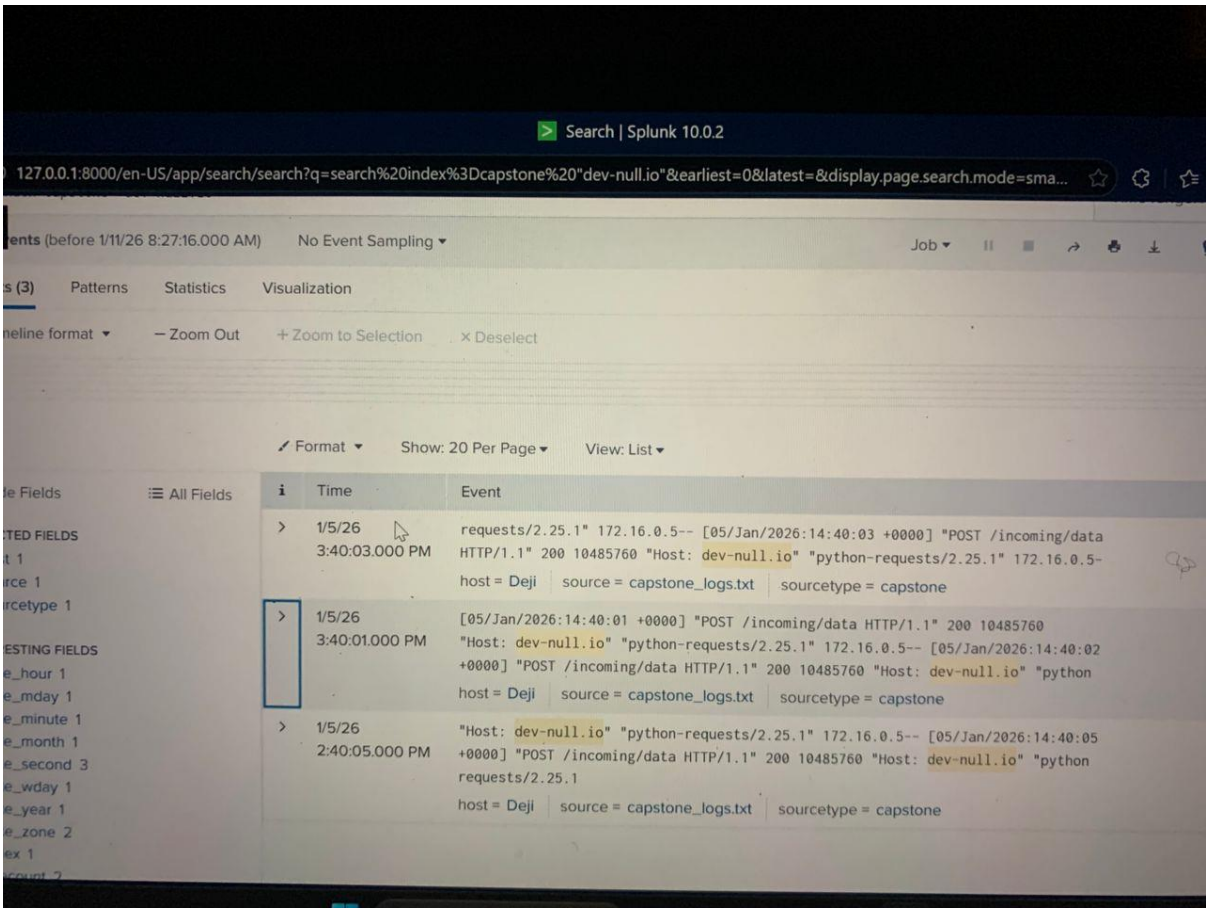
Filename of stolen data: db_snap_v2.sql

(b) Total Volume of Data Sent to dev-null.io

Splunk Query Used

index=capstone "dev-null.io"

| stats sum(bytes)



Analysis of the POST requests sent to the domain dev-null.io showed that the attacker transmitted data in multiple chunks.

Total volume of data exfiltrated: 50 MB

(c) Malicious Script Responsible

The HTTP User-Agent associated with the exfiltration traffic was identified as python-requests, indicating that the attacker used a Python-based script to automate the data exfiltration process.

Malicious script: Python exfiltration script

4. Conclusion

The investigation revealed a complete attack chain beginning with SQL injection reconnaissance, followed by brute force SSH access, persistence through a reverse shell, lateral movement using internal network scanning, and finally large-scale data exfiltration.

This project demonstrates the effectiveness of Splunk as a SIEM tool for detecting and investigating security incidents. Improved monitoring of authentication logs, outbound network traffic, and system command execution could have enabled earlier detection and mitigation of the attack.