PROJECT- REPORT

ON

SOC MONITORING & LOG ANALYSIS USING SPLUNK

Project Title

SOC Monitoring and Analysis using Splunk

Introduction

This project demonstrates monitoring and analysis of authentication, access, network, and firewall logs using Splunk. The primary goal is to identify suspicious IPs, targeted ports, and attack types to enhance security monitoring and incident detection.

Tools Used

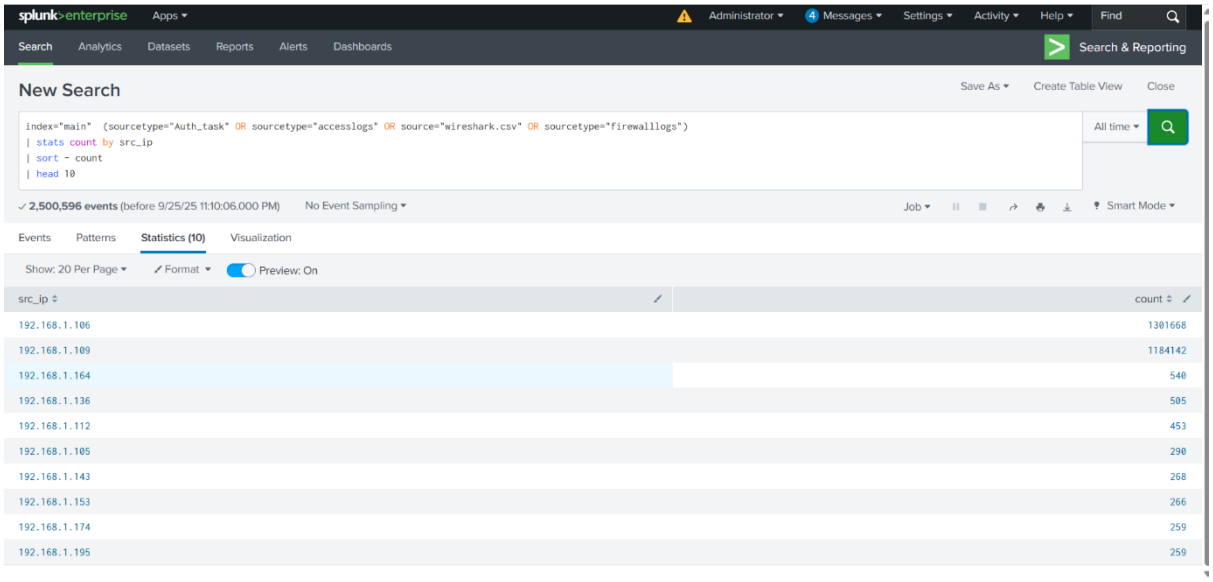
- Splunk Enterprise / Splunk Cloud
- Log Files:

    1.Authentication logs (Auth_task)
    2.Access logs (accesslogs)
    3.Network traffic capture (wireshark.csv)
    4.Firewall logs (firewalllogs)

SPL Queries Used

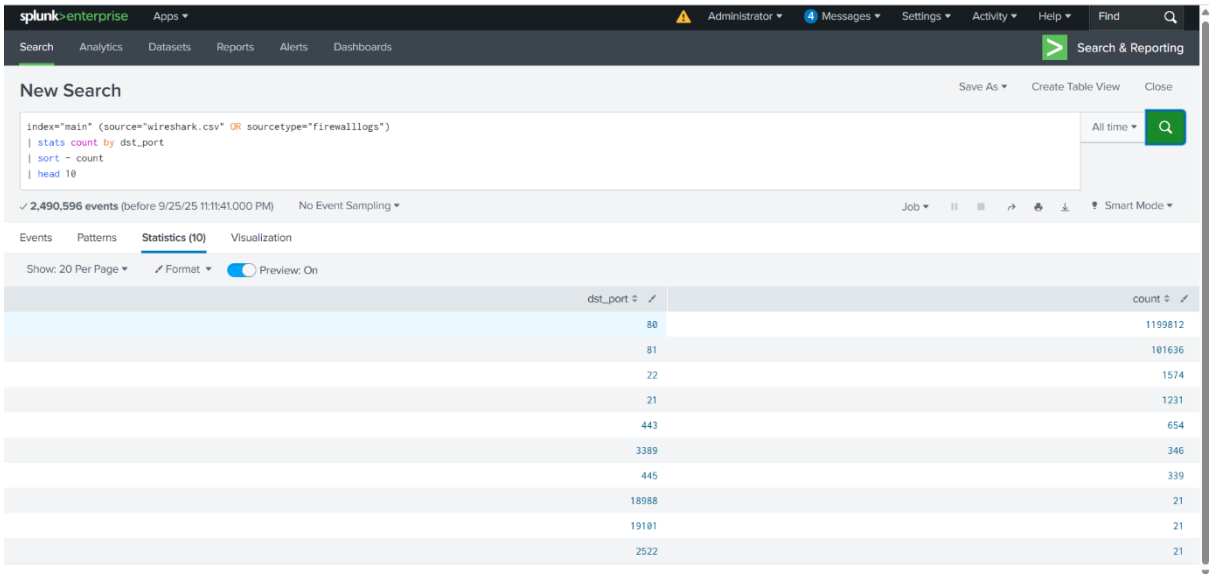
1.Top Suspicious IPs

```
Index=”main”(sourcetype="Auth_task" OR sourcetype="accesslogs" OR source="wireshark.csv" OR sourcetype="firewalllogs")
| stats count by src_ip
| sort - count
| head 10
```



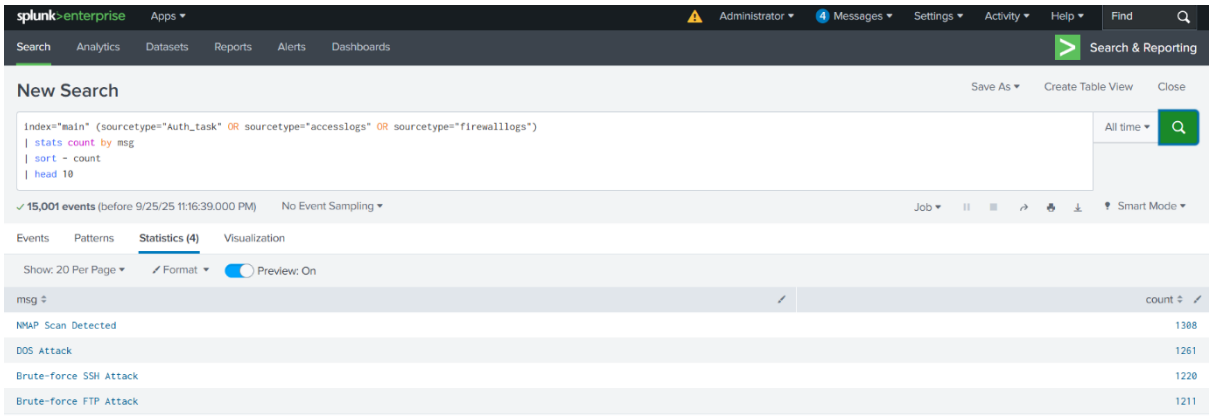
2.Most Targeted Ports/Services

Index=”main”(source="wireshark.csv" OR sourcetype="firewalllogs")
| stats count by dst_port
| sort - count
| head 10



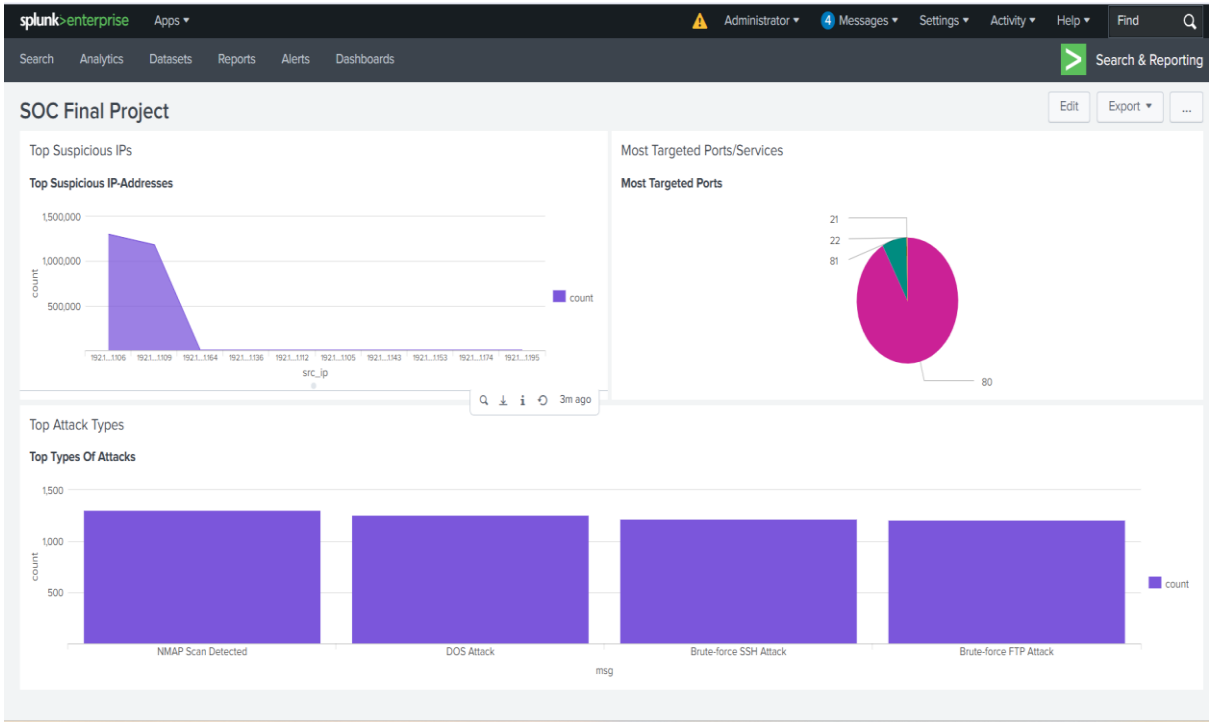
3. Top Attack Types

Index=”main”(sourcetype="Auth_task" OR sourcetype="accesslogs" OR sourcetype="firewalllogs")
| stats count by msg
| sort - count
| head 10



Final SOC Dashboard

Name: SOC Final Project Dashboard
Purpose: Combines all logs to detect top suspicious IPs, most targeted ports, and common attack types.



Findings / Analysis

- Top Suspicious IPs: Identified IPs that appeared most frequently across all logs, indicating potential malicious activity.
- Most Targeted Ports: Highlighted ports that were attacked the most, e.g., port 80 (HTTP) and 22 (SSH).
- Top Attack Types: Showed most common attack types, including DoS and brute-force attacks.

Conclusion

The SOC Final Dashboard provides a comprehensive view of network and authentication threats. It helps identify suspicious IPs, targeted ports, and attack types, supporting proactive security monitoring and mitigation.

Recommendations

- Block or monitor suspicious IPs at the firewall.
- Apply stricter authentication policies for frequently targeted services.
- Regularly monitor top targeted ports to prevent unauthorized access.