

# **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
```

**splunk enterprise** Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As ▾ Create Table View Close

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

✓ 2,500,596 events (before 9/25/25 11:10:06.000 PM) No Event Sampling ▾ Job ▾ || ▮ ↶ ↷ ⬇ ⬆ ⬇ ⬆ Smart Mode ▾

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

src_ip ▴ ▾	count ▴ ▾
192.168.1.106	1301668
192.168.1.109	1184142
192.168.1.164	540
192.168.1.136	505
192.168.1.112	453
192.168.1.105	290
192.168.1.143	268
192.168.1.153	266
192.168.1.174	259
192.168.1.195	259

## 2. Most Targeted Ports/Services

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

**splunk enterprise** Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As ▾ Create Table View Close

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

✓ 2,490,596 events (before 9/25/25 11:11:41.000 PM) No Event Sampling ▾ Job ▾ || ▮ ↶ ↷ ⬇ ⬆ ⬇ ⬆ Smart Mode ▾

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

dst_port ▴ ▾	count ▴ ▾
80	1199812
81	101636
22	1574
21	1231
443	654
3389	346
445	339
18988	21
19101	21
2522	21

## 3. Top Attack Types

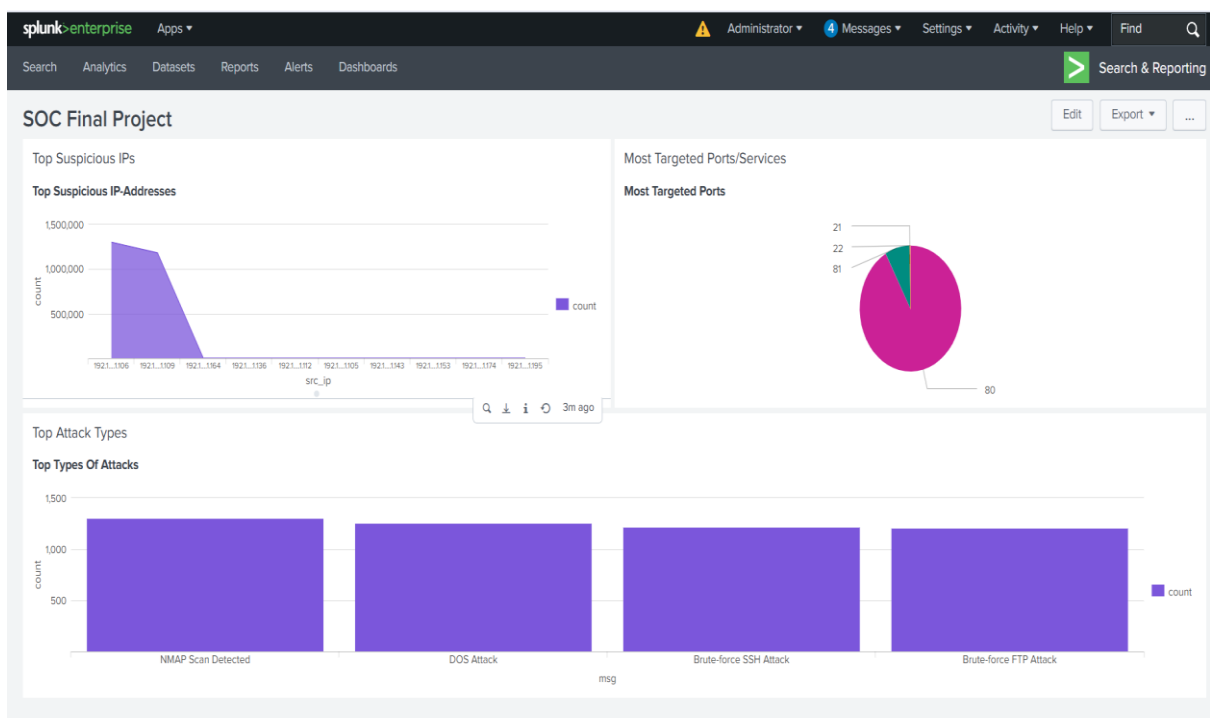
```
Index="main"(sourcetype="Auth_task" OR sourcetype="accesslogs" OR sourcetype="firewalllogs")
| stats count by msg
| sort - count
| head 10
```

New Search	
Index="main" (sourcetype="Auth_task" OR sourcetype="accesslogs" OR sourcetype="firewalllogs")	All time
stats count by msg	
sort - count	
head 10	
✓ 15,001 events (before 9/25/25 11:16:39.000 PM) No Event Sampling	
Events Patterns <b>Statistics (4)</b> Visualization	
Show: 20 Per Page Format Preview: On	
msg	count
NMAP Scan Detected	1308
DOS Attack	1261
Brute-force SSH Attack	1220
Brute-force FTP Attack	1211

## 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.