📧 SMTP Log Analysis Using Splunk SIEM

📌 Project Overview

This project demonstrates how a Security Operations Center (SOC) analyst analyzes **SMTP (Simple Mail Transfer Protocol) log files** using **Splunk SIEM** to monitor email activity, detect suspicious behavior, and identify potential security threats such as spam, phishing, brute-force login attempts, and data exfiltration via email.

The project follows a basic SOC workflow:

Log Ingestion → Analysis → Detection → Alerting

🎯 Project Objectives

- Analyze SMTP email traffic using Splunk SIEM
- Identify normal and abnormal email behavior
- Detect suspicious email activity and login attempts
- Create basic detections suitable for a SOC environment

🧰 Tools & Environment

- **SIEM Tool:** Splunk
- **Index:** main
- **Sourcetype:** smtp
- **Log Type:** SMTP email server logs

📥 Step 1: Search for SMTP Events

The first step is to confirm that SMTP logs are successfully ingested into Splunk.

```
index=main sourcetype=smtp
```

This search verifies:

- Email activity is being logged
- Timestamps and SMTP events are visible
- Required fields are available for analysis

🔍 Step 2: Field Identification & Extraction

Key fields identified from SMTP logs:

- sender_ip
- receiver_ip
- user
- action

- status
- attachment_type
- attachment_size
- src_ip

Field extraction can be done using Splunk’s **Field Extractor** or rex commands when required.

📊 Step 3: Analyze Email Traffic Patterns

Top Email Senders

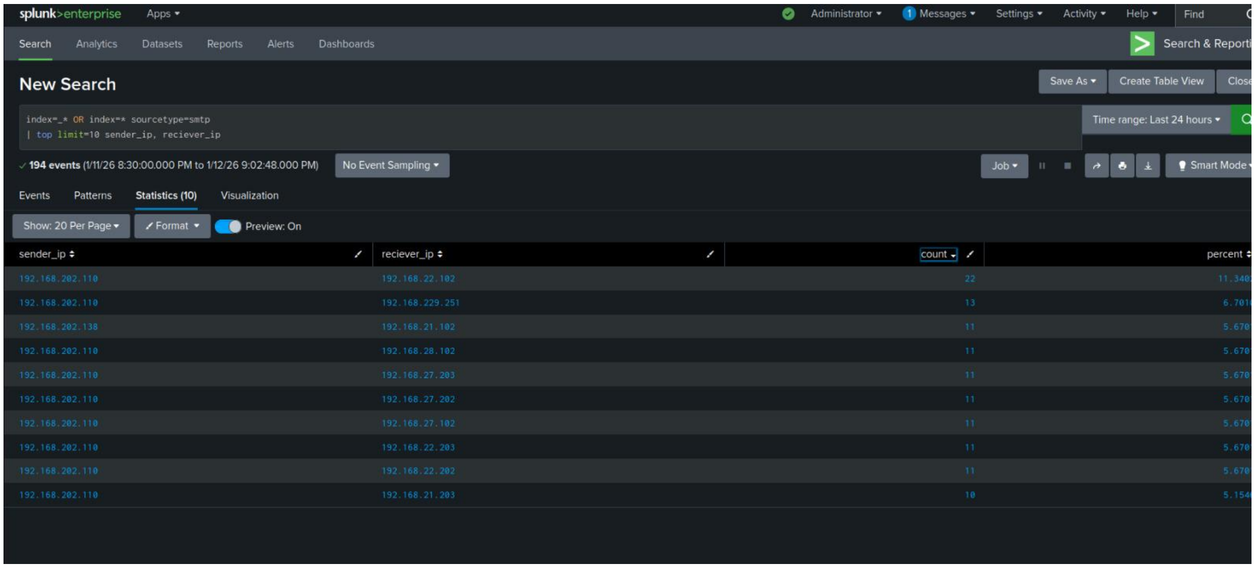
index=main sourcetype=smtp

| top limit=10 sender_ip

Top Email Recipients

index=main sourcetype=smtp

- | top limit=10 receiver_ip



```
index=_* OR index=* sourcetype=smtp
| top limit=10 sender_ip, reciever_ip
```

✓ **194 events** (1/11/26 8:30:00.000 PM to 1/12/26 9:02:48.000 PM)

sender_ip	reciever_ip	count	percent
192.168.202.110	192.168.22.102	22	11.340
192.168.202.110	192.168.229.251	13	6.701
192.168.202.138	192.168.21.102	11	5.670
192.168.202.110	192.168.28.102	11	5.670
192.168.202.110	192.168.27.203	11	5.670
192.168.202.110	192.168.27.202	11	5.670
192.168.202.110	192.168.27.102	11	5.670
192.168.202.110	192.168.22.203	11	5.670
192.168.202.110	192.168.22.202	11	5.670
192.168.202.110	192.168.21.203	10	5.154

These searches help establish a **baseline** of normal email communication.

🚨 Step 4: Detect Anomalies in Email Traffic

Email Volume Over Time

index=main sourcetype=smtp

| timechart span=1h count

Unusual spikes may indicate:

- Spam campaigns
- Compromised email accounts

Suspicious Attachments

```
index=main sourcetype=smtp
| search attachment_type IN ("exe","js","vbs","iso","zip")
```

Used to detect:

- Malware delivery
- Phishing attempts

👤 Step 5: Monitor User Behavior

Email Activity by User

```
index=main sourcetype=smtp
| stats count by user
```

Failed Email Login Attempts

```
index=main sourcetype=smtp
| search action="login" status="failed"
| stats count by user
```

Multiple failed logins may indicate:

- Brute-force attacks
- Account compromise attempts

🔔 Step 6: Detection & Alert Use Cases

Use Case	Description
➢ Spam Detection	• High number of emails from one sender
➢ Phishing Detection	• Suspicious attachment types
➢ Brute Force Detection	• Multiple failed login attempts
➢ Data Exfiltration	• Large email attachments

🧠 MITRE ATT&CK Mapping

Technique ID	Description
• T1071.003	Email Protocol

Technique ID	Description
T1566.001	Phishing Attachment
T1110	Brute Force
T1048	Exfiltration Over Email

📌 Conclusion

This project demonstrates a **basic but effective SMTP log analysis** using Splunk SIEM.
It reflects real-world SOC analyst activities such as monitoring email traffic, identifying anomalies, and detecting suspicious behavior.