SECURITY ALERT MONITORING & INCIDENT RESPONSE

REPORT BY:
PRIYA KUMARI

TABLE OF CONTENT

S.NO	TITLE	PAGE NO
1.	Security alert monitoring & incident response	2

LIST OF FIGURES

FIGURE NO.	NAME	PAGE NO.
1.	SSH brute-force attempts	2
2.	Windows failed login attempts	4
3.	Cloud login without MFA (AWS console)	5
4.	Abnormal DNS query behaviour	7

INTRODUCTION AND INFORMATION ABOUT THE REPORT AND THE MACHINE

INTRODUCTION:

During my internship at Future Interns, I was responsible for performing security alert monitoring and incident response.

INFORMATION:

In this hands-on internship task, I performed alert monitoring and responded to incidents using a dataset called botsv3

TOOLS USED:

I've used the following tools for performing alert analysis:

- Splunk Enterprise
- botsv3 dataset

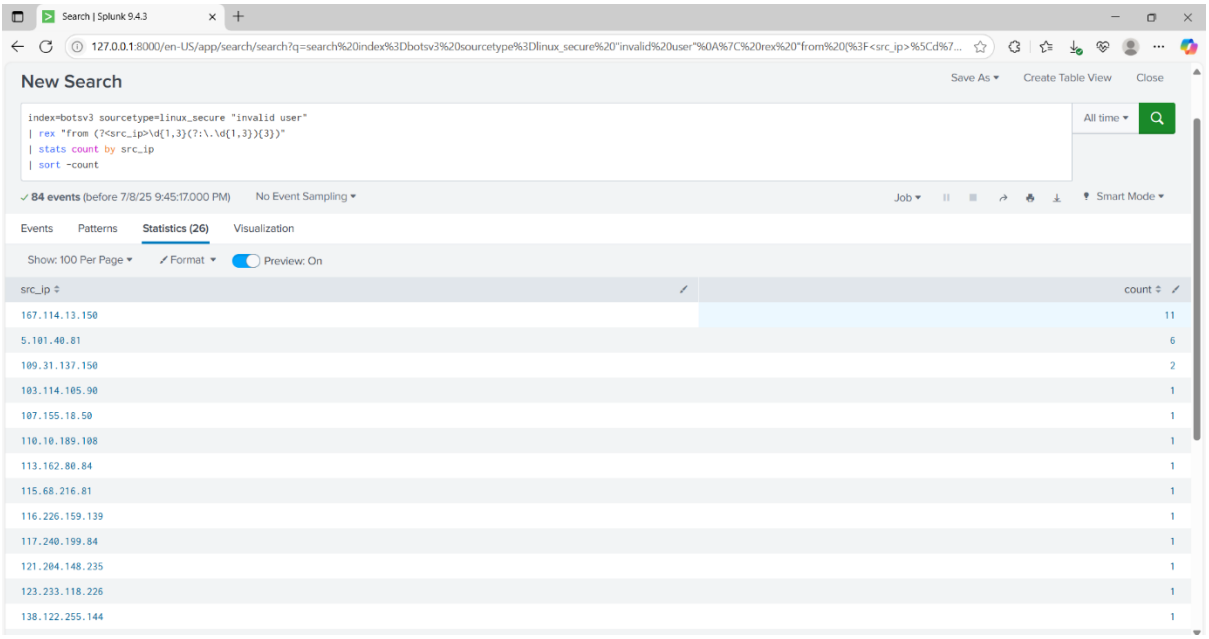
Attack 01: SSH brute-force attempts

Detection Method:

I've used the following in search bar of Splunk Enterprise:

```
index=botsv3 sourcetype=linux_secure "invalid user"
| rex "from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| stats count by src_ip
| sort -count
```

Screenshot:



This above screenshot shows repeated failed SSH login attempts(11 attempts) from the IP address 167.114.13.150 which strongly suggests a brute-force attempt targeting the server. The high number of failures from a single source is a clear red flag for unauthorized access activity.

Impact:

- Indicates repeated unauthorized login attempts via SSH.
- May be an automated script attempting to brute-force valid credentials.
- If left unchecked, can lead to full system compromise.

Recommended mitigations:

- ✓ Enable fail2ban or other SSH intrusion prevention.
- ✓ Configure SSH key-based authentication only
- ✓ Restrict SSH access via firewall to trusted IPs
- ✓ Regularly monitor for login anomalies

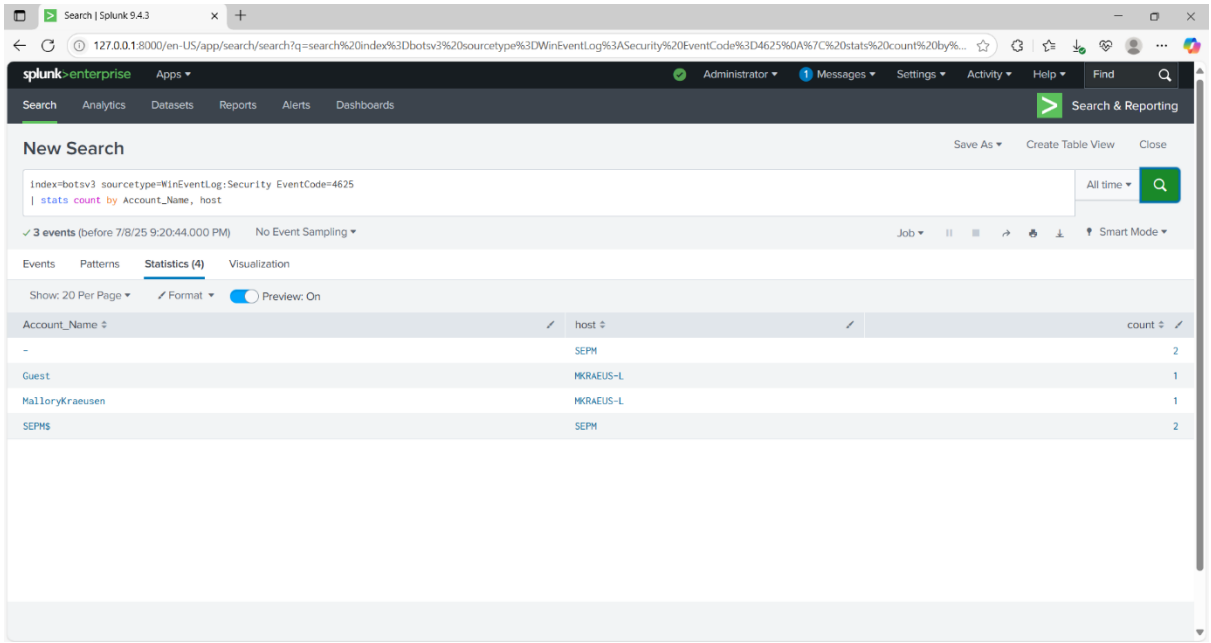
Attack 02: Windows Failed Login Attempts

Detection Method:

I've used the following in search bar of Splunk Enterprise:

```
index=botsv3 sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
```

Screenshot:



Here multiple failed login events across different user accounts on windows systems occurred. Notably, attempts using accounts like guest and (blank) usernames were detected, which are often probed by attackers due to default or weak credential assumptions.

Impact:

- Failed logins suggest brute-force attempts or probing.
- Use of the guest account and (blank) usernames is suspicious
- Targeting of SEPM (possibly a privileged service account) raises concern

Recommended mitigations:

- ✓ Enforce account lockout after repeated login failures.
- ✓ Disable guest account and unused user profiles
- ✓ Implement multi-factor authentication (MFA) for sensitive logins.
- ✓ Audit login attempts periodically and investigate anomalies.

Attack 03: Cloud login without MFA (AWS console)

Detection Method:

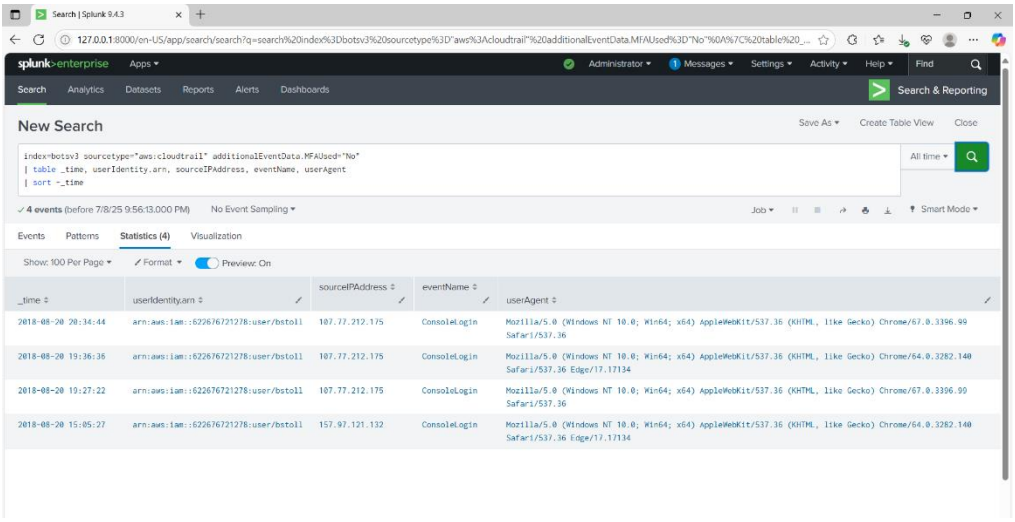
I've used the following in search bar of Splunk Enterprise:

```
index=botsv3 sourcetype="aws:cloudtrail"
additionalEventData.MFAUsed="No"

| table _time, userIdentity.arn, sourceIPAddress, eventName,
userAgent

| sort -_time
```

Screenshot:



This above screenshot reveals IAM user bstoll logging into the AWS management console without multi-factor authentication (MFA)

Lack of MFA for cloud access is a significant security risk, especially when dealing with privileged environments.

Impact:

- Cloud account logins without MFA significantly increase risk
- Any credential leak could lead to unauthorized AWS console access
- Particularly dangerous if permissions include EC2, S3 or IAM policy access.

Recommended mitigations:

- ✓ Enforce MFA for all IAM users, especially those with console access
- ✓ Apply least privilege policy for sensitive users.
- ✓ Monitor login patterns and alert on IP anomalies or geolocation mismatches

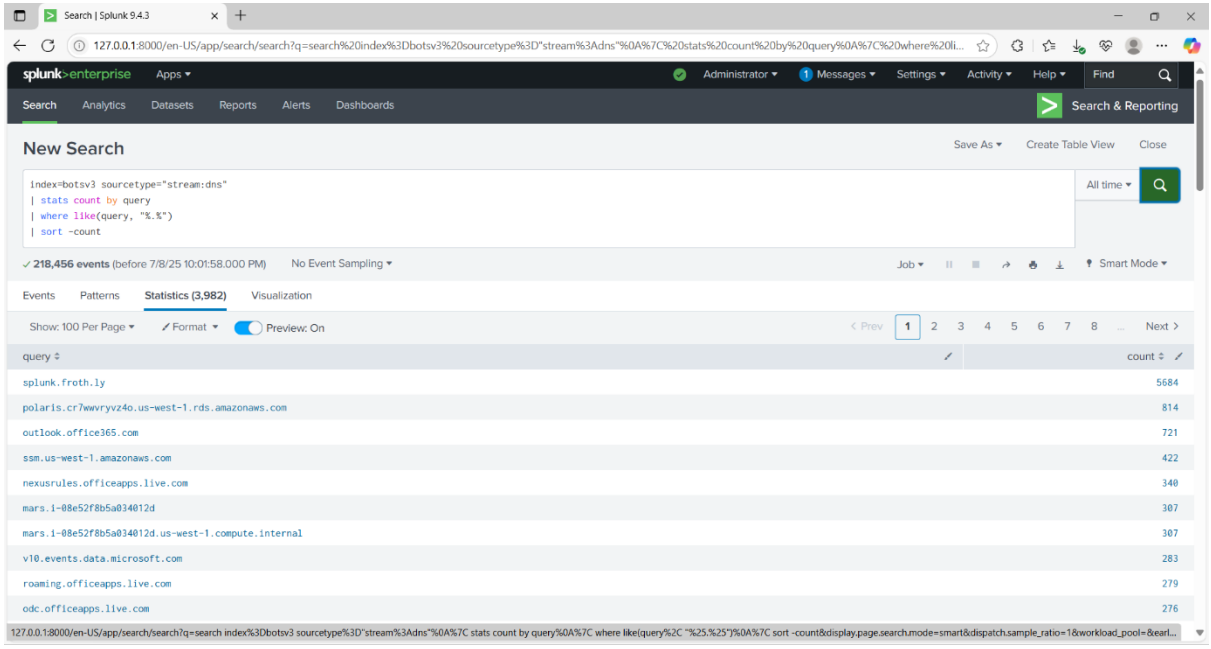
Attack 04: Abnormal DNS query behaviour

Detection Method:

I've used the following in search bar of Splunk Enterprise:

```
index=botsv3 sourcetype="stream:dns"
| stats count by query
| where like(query, "%.%")
| sort -count
```

Screenshot:



In this above screenshot, an unusually high volume of DNS queries to the domain splunk.froth.ly stands out in this screenshot. This repetitive behaviour is often linked to DNS tunneling techniques where attackers hide malicious traffic inside DNS requests to evade detection.

Impact:

- Excessive and repetitive DNS queries to a single domain may suggest DNS tunneling.
- Could be used to exfiltrate data or establish command-and-control (C2) channels

Recommended mitigations:

- ✓ Set thresholds for DNS query frequency
- ✓ Monitor for suspicious domain entropy
- ✓ Block untrusted domains at DNS gateway level

CONCLUSION:

This task gave me practical insight into how real threats surface in log data. By identifying patterns like brute-force attempts, failed logins, risky access behaviour and many more, I learned how to detect, classify and respond to security incidents using Splunk tool.

It strengthened both my technical skills and analytical thinking.