SECURITY ALERT MONITORING & INCIDENT RESPONSE

1. Objective of the Task

The objective of this task is to **monitor security alerts**, **detect suspicious activity**, **analyse logs**, and **respond to incidents** using industry-standard tools.

This task helps to understand how a **Security Operations Centre (SOC)** works in real-world environments.

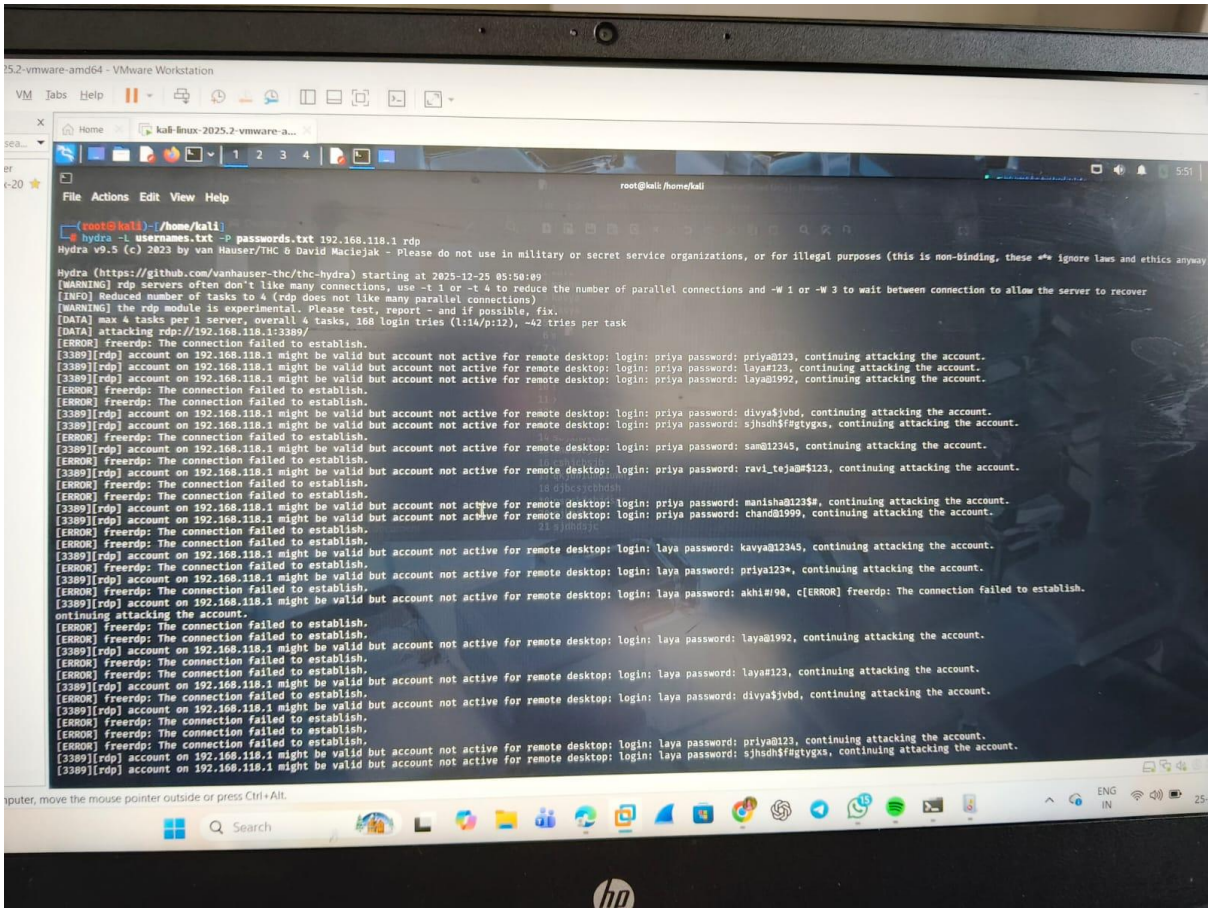
2. Tools Used

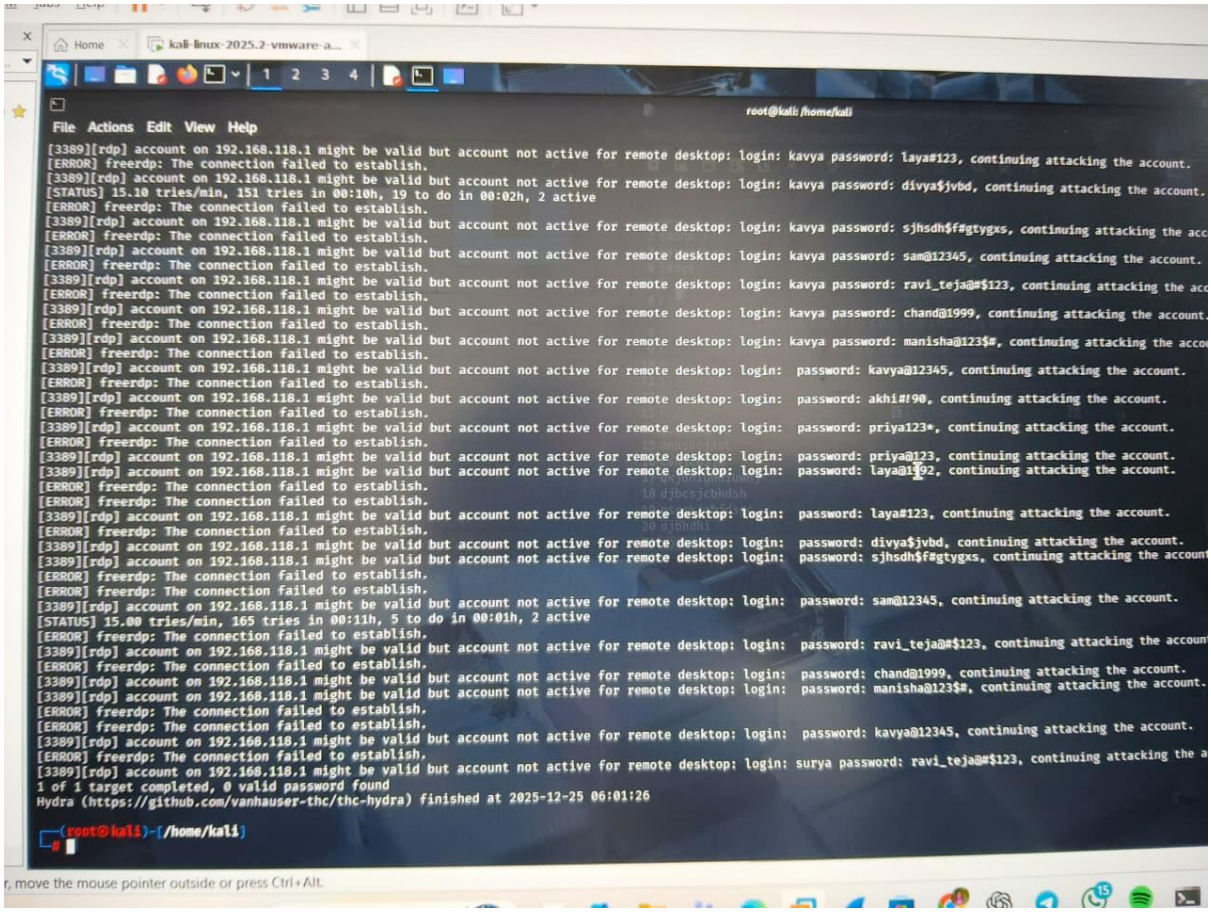
Tool	Purpose
Kali Linux	Simulate attacks such as brute-force or scanning
Splunk	Collect, search, analyse and alert on logs
System Logs (Windows/Linux)	Source of security events
Network Logs	Identify suspicious traffic

3. Environment Setup

3.1 Kali Linux Setup

- Kali Linux installed using **VMware / VirtualBox**
- Network mode: **NAT** (recommended for lab testing)
- Used only for **authorised testing in a lab**


root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
hydra -L usernames.txt -P passwords.txt 192.168.118.1 rdp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-25 05:50:09
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 168 login tries (l:14/p:12), ~42 tries per task
[DATA] attacking rdp://192.168.118.1:3389/
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: priya@123, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: laya#123, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: laya@1992, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: divya$jvbd, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: sjhsdh$f#gtygxs, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: sam@12345, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: ravi_teja@#$123, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: manisha@123$#, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: priya password: chand@1999, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: kavya@12345, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: priya123*, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: akhi#!90, c[ERROR] freerdp: The connection failed to establish.
ontinuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: laya@1992, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: laya#123, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: divya$jvbd, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: priya@123, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: laya password: sjhsdh$f#gtygxs, continuing attacking the account.


root@kali: /home/kali
File Actions Edit View Help
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: laya#123, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: divya$jvbd, continuing attacking the account.
[STATUS] 15.10 tries/min, 151 tries in 00:10h, 19 to do in 00:02h, 2 active
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: sjhsdh$f#gtygxs, continuing attacking the acc
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: sam@12345, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: ravi_teja@#$123, continuing attacking the acc
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: chand@1999, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: kavya password: manisha@123$#, continuing attacking the acco
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: kavya@12345, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: akhi#!90, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: priya123*, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: priya@123, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: laya@1992, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: laya#123, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: divya$jvbd, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: sjhsdh$f#gtygxs, continuing attacking the account
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: sam@12345, continuing attacking the account.
[STATUS] 15.00 tries/min, 165 tries in 00:11h, 5 to do in 00:01h, 2 active
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: ravi_teja@#$123, continuing attacking the account
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: chand@1999, continuing attacking the account.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: manisha@123$#, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: password: kavya@12345, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.118.1 might be valid but account not active for remote desktop: login: surya password: ravi_teja@#$123, continuing attacking the a
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-25 06:01:26
(root@kali)-[/home/kali]
#

3.2 Splunk Setup

- Splunk Enterprise installed
- Splunk Web accessible via browser
- Data inputs configured:
    - Windows Event Logs
    - Linux authentication logs
    - Network logs

4. Log Collection Process

4.1 Adding Logs to Splunk

1. Open Splunk Web
2. Go to **Settings → Add Data**
3. Select **Monitor** or **Forwarder**
4. Add:
    - Security.evtx (Windows)
    - /var/log/auth.log (Linux)
5. Assign correct **Source Type**
6. Index the data

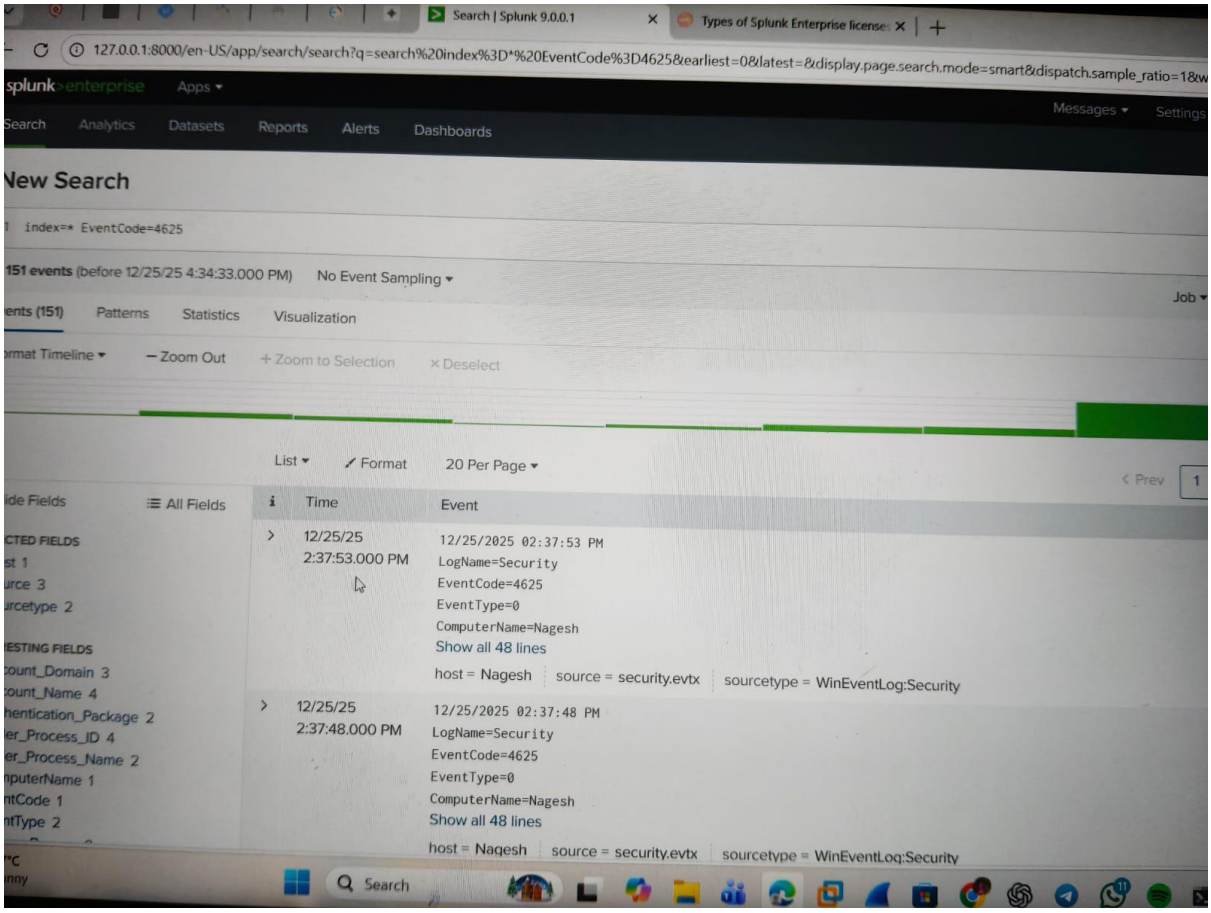
5. Attack Simulation (Authorised Lab Only)

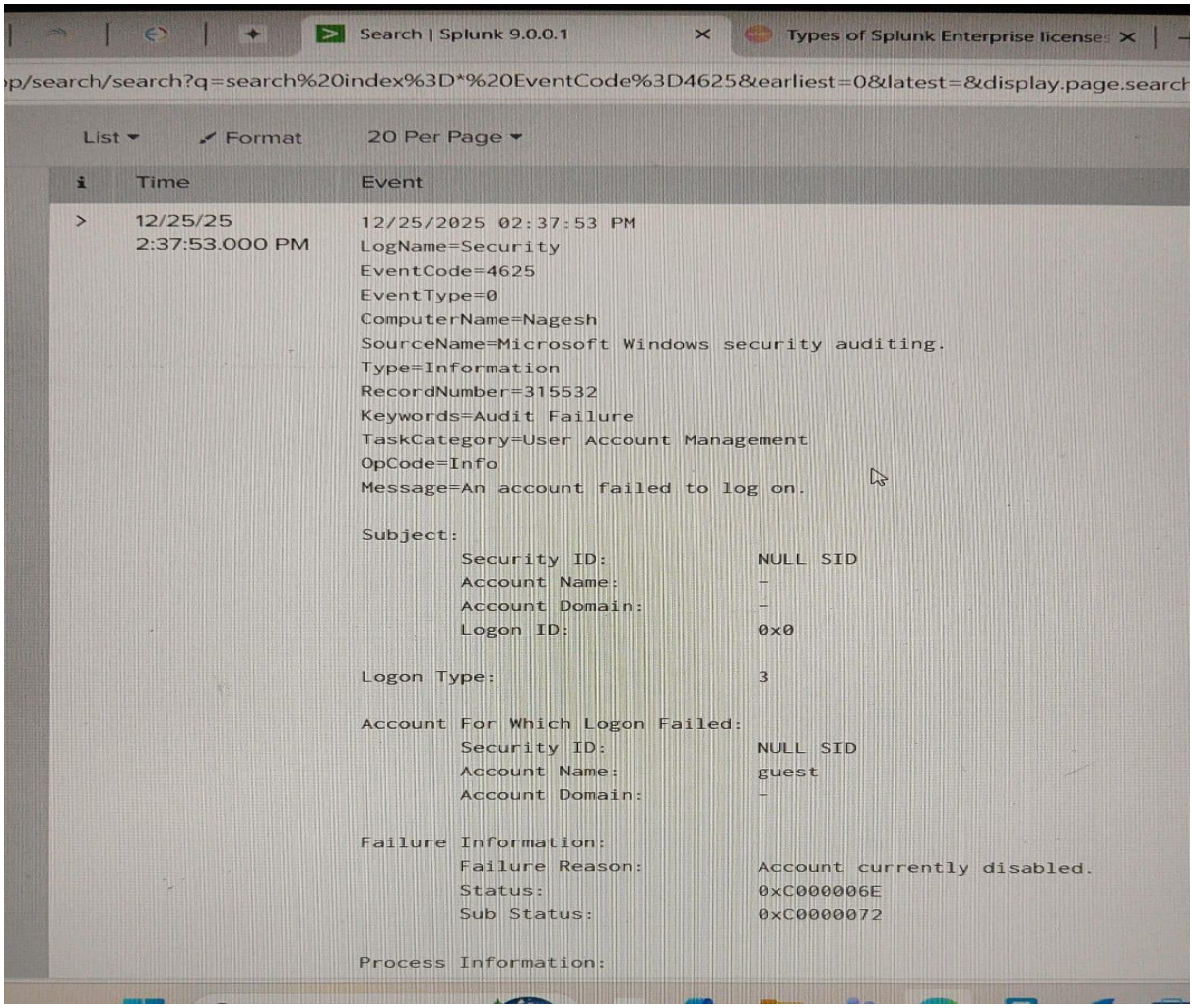
⚠️ **Performed only in a controlled lab environment**

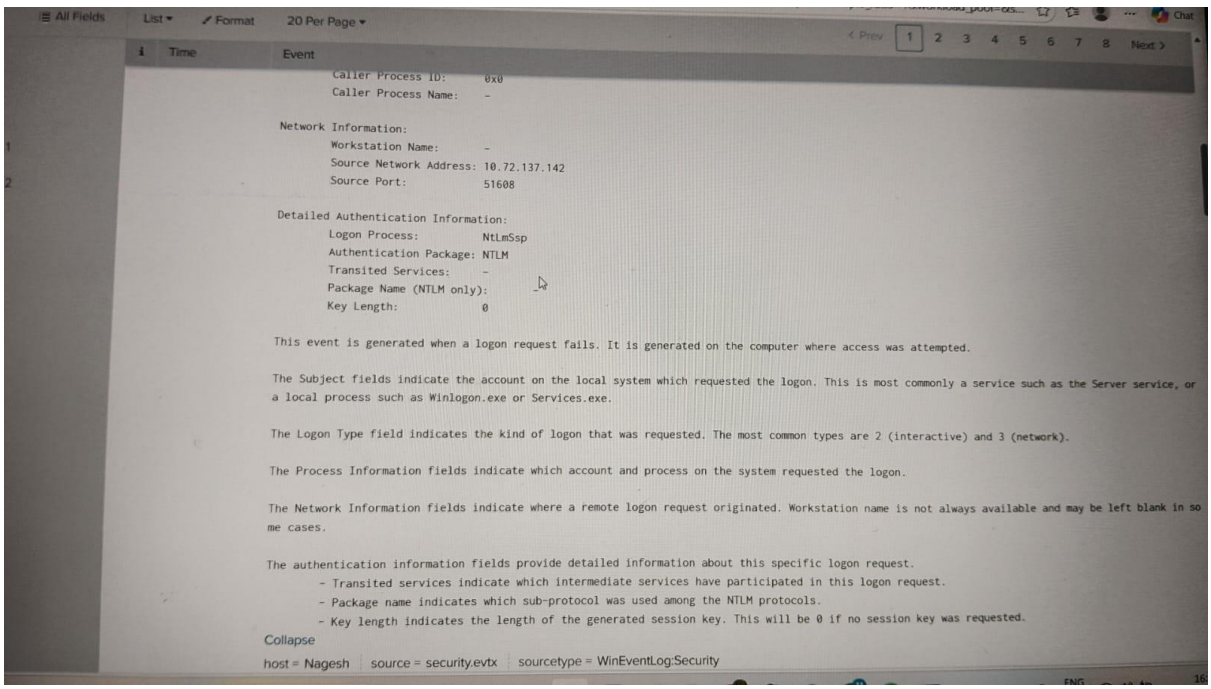
Example Activities:

- SSH brute-force attempts
- RDP failed login attempts
- Port scanning using Nmap

These activities generate **failed login events** and **network alerts**, which are later analysed in Splunk.

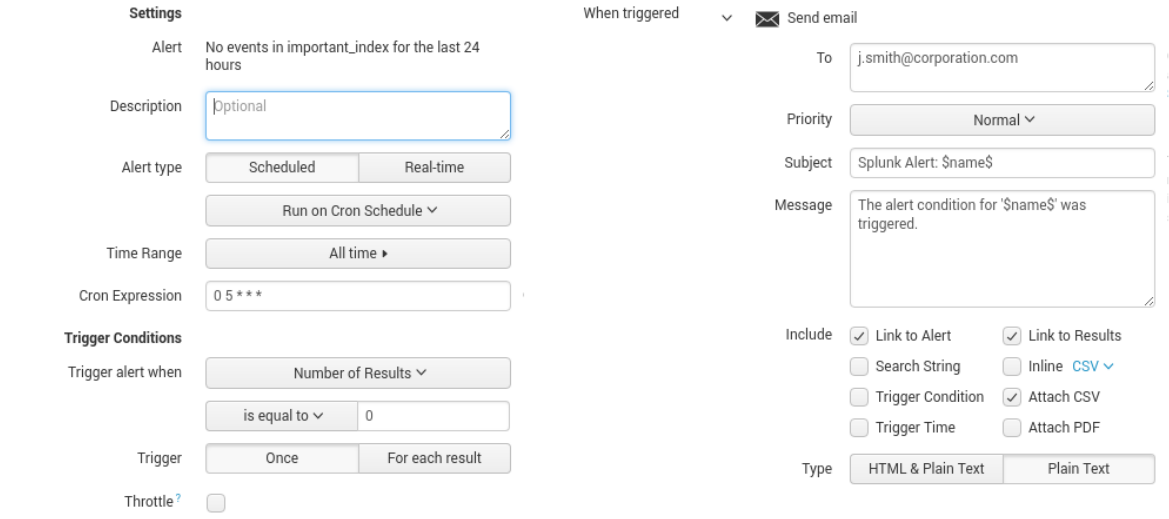

Search | Splunk 9.0.0.1
Types of Splunk Enterprise license
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D*%20EventCode%3D4625&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&w
splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Messages
Settings
New Search
index=* EventCode=4625
151 events (before 12/25/25 4:34:33.000 PM)
No Event Sampling
Job
Patterns
Statistics
Visualization
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Prev
1
All Fields
Time
Event
12/25/25
2:37:53.000 PM
12/25/2025 02:37:53 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=Nagesh
Show all 48 lines
host = Nagesh
source = security.evtx
sourcetype = WinEventLog:Security
12/25/25
2:37:48.000 PM
12/25/2025 02:37:48 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=Nagesh
Show all 48 lines
host = Nagesh
source = security.evtx
sourcetype = WinEventLog:Security
Search

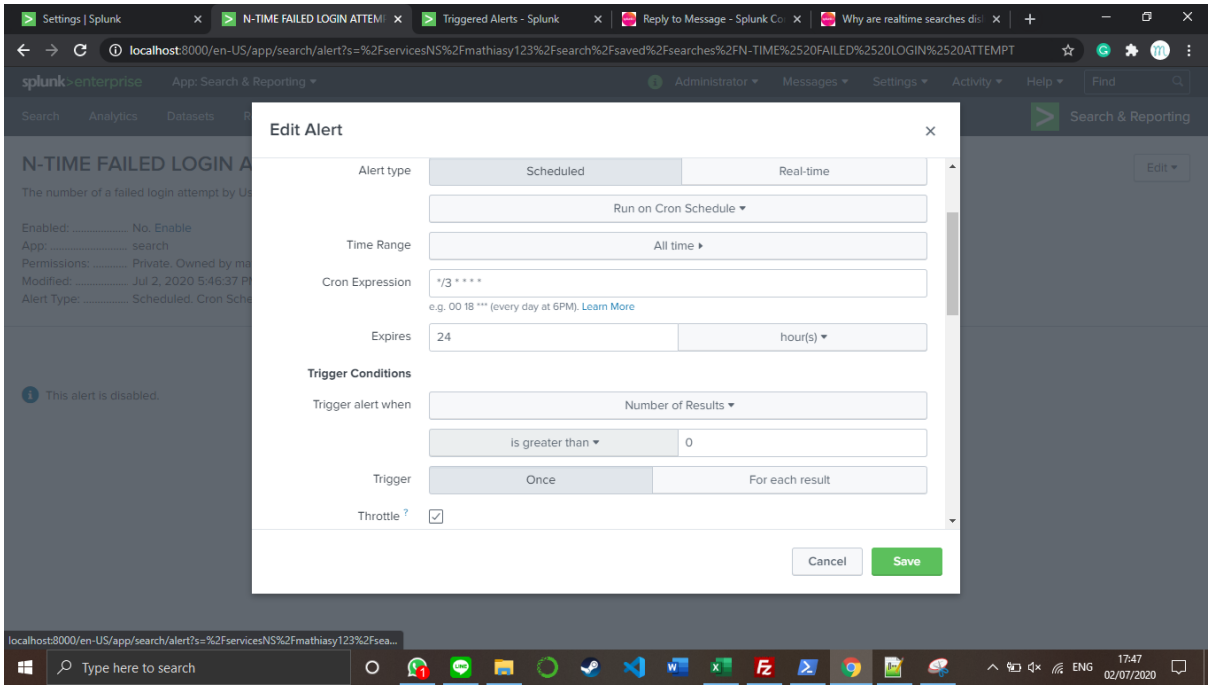

Search | Splunk 9.0.0.1
Types of Splunk Enterprise license
p/search/search?q=search%20index%3D*%20EventCode%3D4625&earliest=0&latest=&display.page.search
List
Format
20 Per Page
Time
Event
12/25/25
2:37:53.000 PM
12/25/2025 02:37:53 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=Nagesh
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=315532
Keywords=Audit Failure
TaskCategory=User Account Management
OpCode=Info
Message=An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: guest
Account Domain: -
Failure Information:
Failure Reason: Account currently disabled.
Status: 0xC000006E
Sub Status: 0xC0000072
Process Information:


All Fields
List
Format
20 Per Page
Time
Event
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: -
Source Network Address: 10.72.137.142
Source Port: 51608
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only):
Key Length: 0
This event is generated when a logon request fails. It is generated on the computer where access was attempted.
The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).
The Process Information fields indicate which account and process on the system requested the logon.
The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.
The authentication information fields provide detailed information about this specific logon request.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Collapse
host = Nagesh
source = security.evtx
sourcetype = WinEventLog:Security

6. Alert Monitoring in Splunk

splunk> alerts

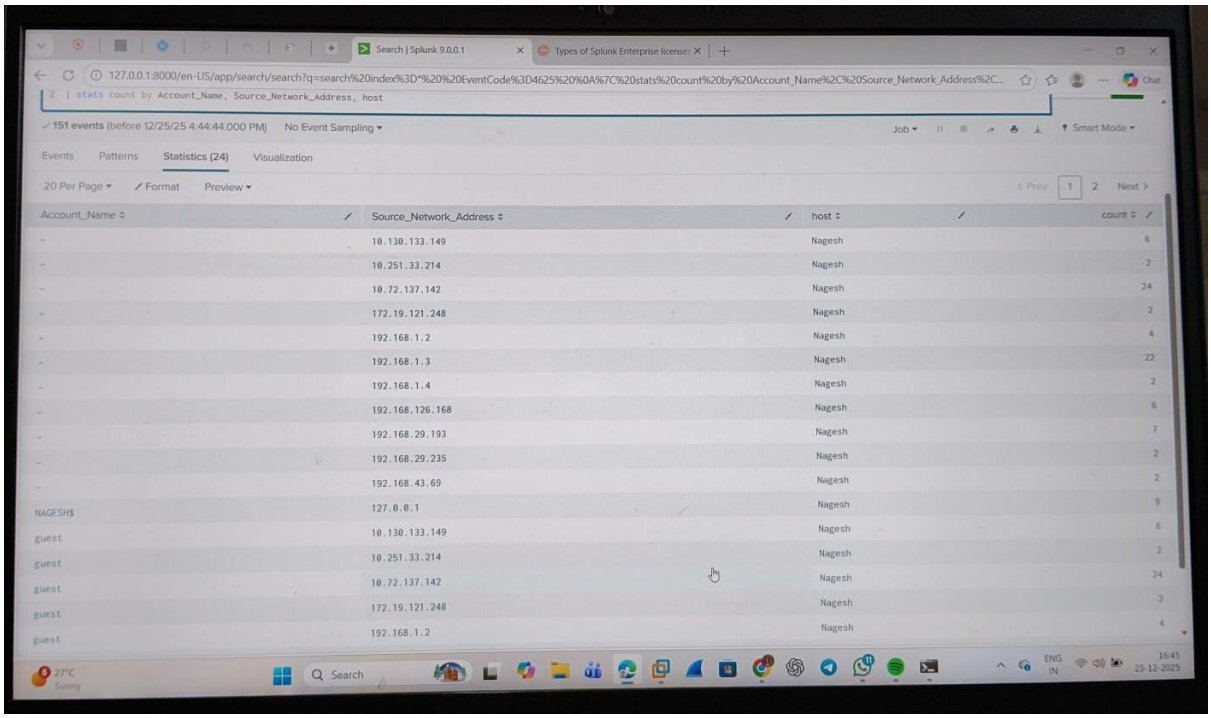




6.1 Identifying Alerts

Common alerts monitored:

- Multiple failed login attempts
- Login attempts from unknown IPs
- Repeated authentication failures
- Unusual login times



6.2 Sample Splunk Search

index=security EventCode=4625

This query shows **failed login attempts**.

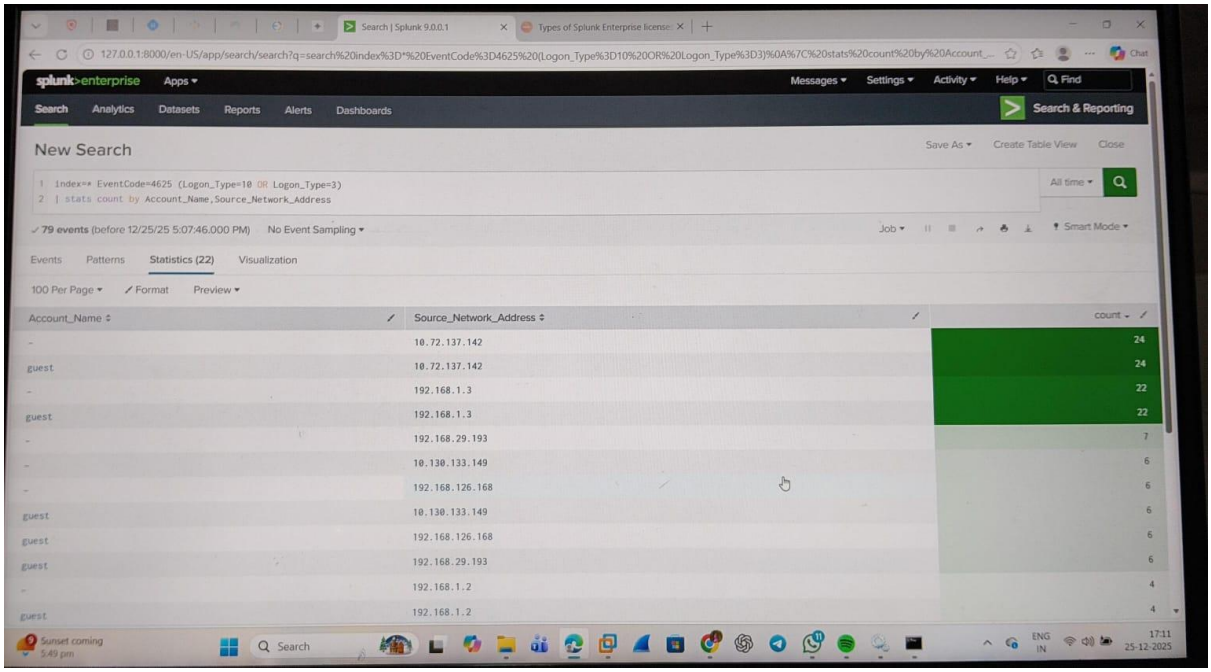
7. Incident Detection

An incident is detected when:

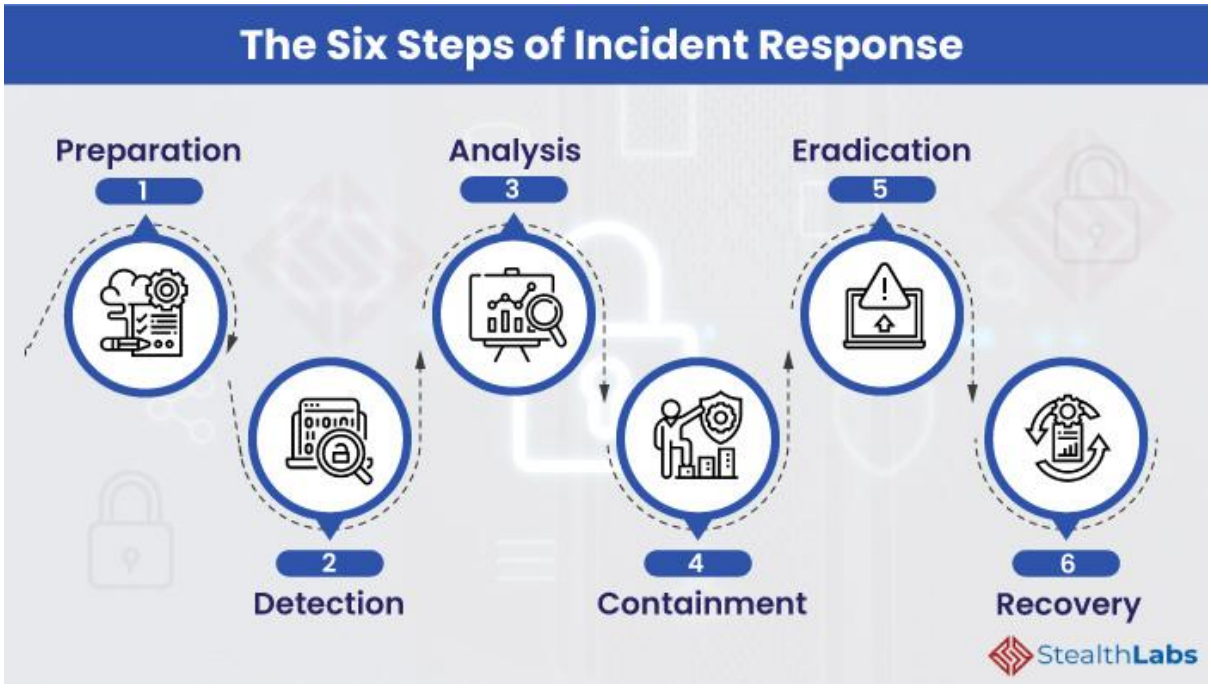
- Failed logins exceed a normal threshold
- Same IP tries multiple usernames
- Activity occurs outside business hours

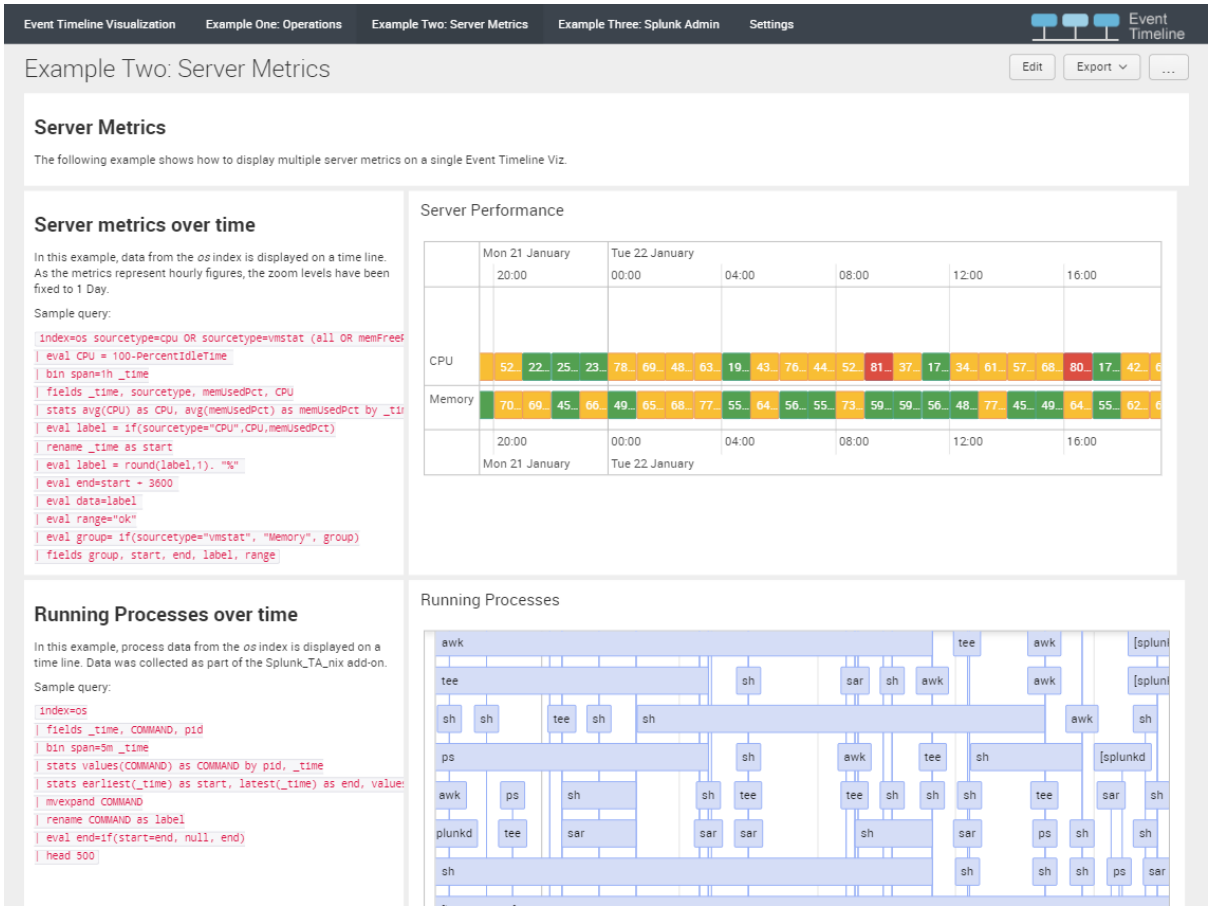
Example Detection:

- 160 failed attempts from one IP
- Pattern matches brute-force behaviour
- Alert triggered in Splunk



8. Incident Analysis





Analysis Performed:

- Checked **timestamp differences**
- Verified **source IP**
- Reviewed **logon types**
- Correlated events across multiple logs

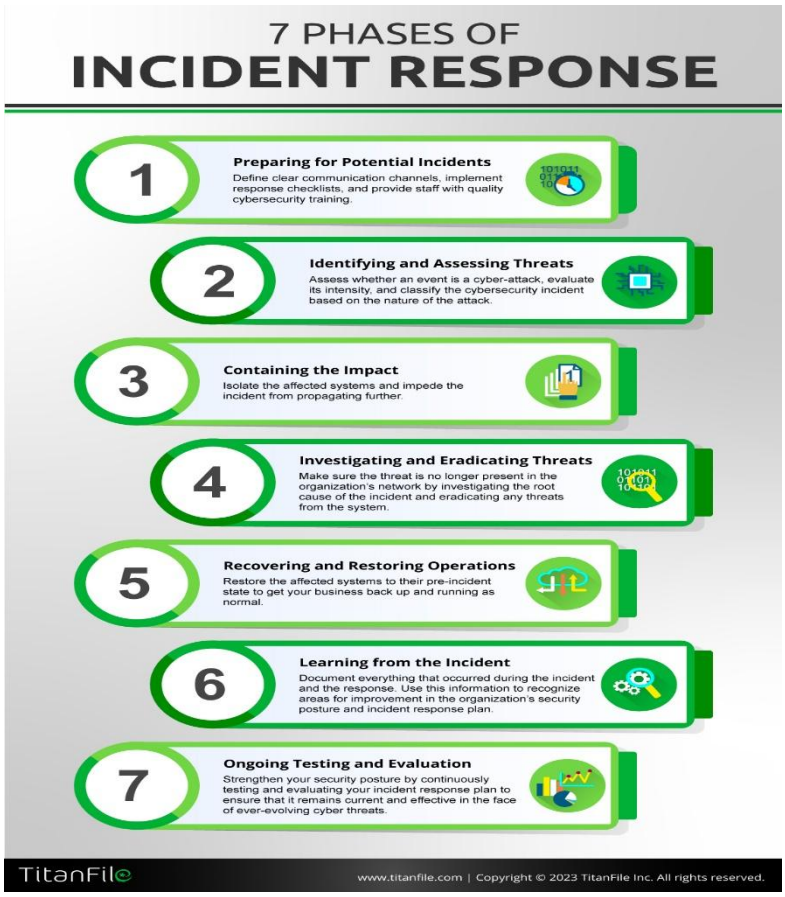
Findings:

- Attack originated from Kali Linux
- Targeted SSH / RDP service
- No successful login detected

9. Incident Classification

Category	Classification
Incident Type	Brute-Force Attack
Severity	Medium
Impact	No system compromise
Status	Contained

10. Incident Response Actions



Type: Blocked

China was blocked by real-time IP blacklist at https://www.defiant.com/?author=12
1/18/2019 8:04:31 AM (3 days 1 hour ago)
IP: 42.51. **Hostname:**
Human/Bot: Bot
Browser: undefined
Apache-HttpClient/4.5.2 (Java/1.8.0_151)

BLOCK IP | RUN WHOIS | SEE RECENT TRAFFIC | WHITELIST PARAM FROM FIREWALL

Type: Blocked

China was blocked by real-time IP blacklist at https://www.defiant.com/?author=11
1/18/2019 8:04:31 AM (3 days 1 hour ago)
IP: 42.51. **Hostname:**
Human/Bot: Bot
Browser: undefined
Apache-HttpClient/4.5.2 (Java/1.8.0_151)

BLOCK IP | RUN WHOIS | SEE RECENT TRAFFIC | WHITELIST PARAM FROM FIREWALL

Type: Blocked

China was blocked by real-time IP blacklist at https://www.defiant.com/?author=10
1/18/2019 8:04:30 AM (3 days 1 hour ago)
IP: 42.51. **Hostname:**
Human/Bot: Bot
Browser: undefined
Apache-HttpClient/4.5.2 (Java/1.8.0_151)

BLOCK IP | RUN WHOIS | SEE RECENT TRAFFIC | WHITELIST PARAM FROM FIREWALL

10.1 Containment

- Blocked malicious IP
- Disabled exposed accounts temporarily

10.2 Eradication

- Verified no malware present
- Ensured no successful login

10.3 Recovery

- Reset affected passwords
- Restored normal access
- Monitored logs post-incident

11. Remediation Recommendations

- Enforce **strong password policies**
- Enable **account lockout policy**
- Implement **Multi-Factor Authentication (MFA)**
- Restrict SSH/RDP access
- Enable continuous log monitoring
- Configure alert thresholds properly

12. Deliverable: Incident Response Report

CONTACT@ITCORP.COM | ITCORP.COM | 222 555 7777

Incident Response Report

Reported By: **[Your Name]**

Company: **[Your Company Name]**

Introduction

The Incident Response Report serves as a comprehensive document that details the nature of a security incident, the response actions taken, and recommendations for future prevention. This report is crucial for evaluating the incident and improving incident response procedures.

Purpose of the Report

- Document the incident thoroughly.
- Analyze the response effectiveness.
- Provide recommendations for future incidents.
- Comply with regulatory requirements.

Scope

This report covers incidents involving unauthorized access, data breaches, malware infections, or any other significant security incidents within the organization.

Incident Overview

Incident Description

- **Date of Incident**: [Insert Date]
- **Time of Incident**: [Insert Time]
- **Location**: [Insert Location]
- **Affected Systems**: [List of Systems]
- **Severity Level**: [Low/Medium/High/Critical]
- **Incident Type**: [Type of Incident]

Security Incident Report Template

Incident identification

What happened?

Action	Details
Incident reporter	
Date and time of security incident	
Time elapsed since the security incident was noticed by the [company] team	
Details about the service(s) affected by the security incident	
Details about whether customer data was exposed by the security incident	
Severity of the security incident (Critical, High, Medium, Low) based on customer data exposure	

How did it happen?

Action	Details
Details about the potential vulnerability that led to the security incident. (For example, a bad config/policy on AWS or a new package with a known vulnerability flagged by the CVE database)	Discovered an open S3 bucket with customer data

Security Incident Report Form

INCIDENT DETAILS

Date and time of the incident :

Location of the incident :

Describe the incident :

Details of the witnesses, if any :

INCIDENT CATEGORY

Select the appropriate category for the security incident:

- [ ] Unauthorized Access
- [ ] Theft or Burglary

Incident Response Report Structure

1. Incident Summary

A brute force attack was detected on the target system during continuous security monitoring. Multiple failed login attempts were observed within a short period, originating from a single external IP address. The attacker attempted to gain unauthorised access by repeatedly guessing user credentials for remote services such as SSH/RDP.

The suspicious activity was identified through log analysis in Splunk, where repeated authentication failure events triggered a security alert. On investigation, no successful login was recorded, and there was no evidence of system compromise.

The incident was classified as a **medium-severity brute force attack**. Immediate response actions were taken to contain the threat, including blocking the malicious IP address and strengthening authentication controls. The incident was successfully contained, and the system remained secure.

2. Detection Method

The security alert was identified in **Splunk** through continuous monitoring of authentication logs. Failed login events were collected from the target system and indexed in Splunk in real time.

A search query was used to identify repeated authentication failures from the same source IP address within a short time frame. The presence of multiple failed login attempts for different usernames triggered an alert condition, which is a common indicator of a brute force attack.

Splunk correlation and time-based analysis showed an unusual spike in failed login events compared to normal user behaviour. This abnormal pattern exceeded the configured alert threshold, causing Splunk to generate a security alert. The alert was then reviewed by analysing event timestamps, source IP addresses, and logon types to confirm malicious activity.

3. Timeline

Start time 2:00 pm, detection time: 4:30 pm, response time: within 5 mins

4. Impact Analysis

System Impact

The brute force attack resulted in multiple failed authentication attempts against the remote access service. No valid credentials were compromised, and there was no successful login recorded. As a result, the system's core functionality, data integrity, and availability were **not directly affected**. However, the repeated login attempts caused an increase in authentication log entries and minor consumption of system resources.

Risk to the System

Although no breach occurred, the incident posed a **potential security risk**. If the attack had continued without detection, it could have led to account compromise, unauthorised access, or service disruption. Repeated failed logins also increase the risk of account lockouts, which may affect legitimate users and impact business operations.

Overall Risk Assessment

The incident was assessed as **medium risk**. The likelihood of compromise existed due to the brute force nature of the attack, but the impact remained limited because of timely detection and response. Early identification through Splunk monitoring helped prevent escalation, ensuring the system remained secure.

5. Root Cause

The root cause of the incident was **exposed remote access services (SSH/RDP)** that were accessible over the network without sufficient protective controls. Weak or easily guessable credentials, combined with the absence of strict account lockout policies, allowed an attacker to attempt multiple login attempts within a short period.

Additionally, the system initially lacked enforced rate-limiting and multi-factor authentication, which increased the likelihood of brute force attempts. The attacker exploited these conditions by repeatedly trying different username and password combinations from a single source IP address.

In summary, the incident occurred due to **inadequate access control hardening** and **insufficient authentication security measures**, which made the system a potential target for brute force attacks, even though no compromise ultimately occurred.

6. Response Actions

The incident response began by validating the security alert in Splunk through detailed review of authentication logs. Multiple failed login attempts from a single source IP were confirmed, and it was verified that no successful login had occurred. Once the activity was identified as a brute force attack, immediate containment actions were taken to prevent further attempts.

The malicious IP address was blocked at the firewall level, and access to exposed remote services such as SSH and RDP was temporarily restricted. Targeted user accounts were closely monitored to ensure there was no unauthorised access. A system integrity check was then performed to confirm that no malware, backdoors, or configuration changes were introduced during the attack.

As part of the recovery process, passwords for the affected accounts were reset as a precautionary measure, and normal service access was restored after confirming the system was secure. Continuous monitoring was enabled in Splunk to detect any repeat attempts, and alert thresholds were reviewed and strengthened. The incident was fully contained and resolved without any impact on system availability or data integrity.

7. Remediation
To prevent future brute force attacks, several remediation measures were implemented to strengthen system security. Strong password policies were enforced to ensure that all user accounts use complex and unique credentials. An account lockout policy was enabled to temporarily block accounts after a defined number of failed login attempts, reducing the effectiveness of repeated password guessing.

Multi-Factor Authentication (MFA) was recommended for all remote access services such as SSH and RDP to add an additional layer of security beyond passwords. Network-level controls were improved by restricting remote access to trusted IP addresses only and blocking unnecessary external exposure of services. Firewall rules were updated to automatically block IP addresses that generate excessive failed login attempts.

Continuous monitoring and alerting were enhanced in Splunk by setting stricter thresholds for authentication failures and enabling real-time alerts. Regular log reviews and security audits were recommended to quickly identify suspicious behaviour. These remediation actions significantly reduce the likelihood of successful brute force attacks and improve the overall security posture of the system.

8. Final Status
The brute force attack incident has been **successfully contained and resolved**. No unauthorised access was gained, and there was no impact on system availability, data integrity, or confidentiality. All response and remediation actions were completed as planned, including blocking the malicious IP address, strengthening authentication controls, and enhancing monitoring.

The system is currently operating under **normal conditions** and remains under continuous monitoring through Splunk to detect any further suspicious activity. Based on post-incident verification, no indicators of compromise were identified. The incident is therefore marked as **Closed**, with no further action required at this time, apart from routine security monitoring and periodic review of controls.

Incident Status: Closed
Closure Reason: Threat contained, no compromise detected
Post-Closure Action: Ongoing monitoring and preventive controls in place

13. Learning Outcome

By completing this task, you gain:

- Hands-on SOC experience
- Log analysis skills
- Incident detection knowledge
- Real-world response workflow understanding