# Name : Mukesh Kumar

CIN: FIT/FEB25/CS583

# Incident Response Report

## spond to cyber threats in a timely manne1. Executive Summary

This report provides an in-depth analysis of a simulated cybersecurity incident that involved unauthorized access to a corporate system. The incident was investigated using Splunk, Kibana, and Wireshark to identify the attack vectors, compromised assets, and potential impact. The analysis revealed that the attack originated from a phishing campaign that led to credential compromise, enabling the attacker to gain unauthorized access to critical systems.

The response team conducted a forensic investigation, implemented mitigation steps, and proposed recommendations to prevent future incidents. This document outlines the investigation process, root cause, mitigation strategies, and long-term security recommendations.

## 2. Incident Description

The security team detected unusual login attempts and data transfer activities on the corporate network. A deeper analysis of the logs revealed that an unauthorized entity gained access to an employee account, which was then used to escalate privileges and attempt lateral movement within the network.

The indicators of compromise (IoCs) included:  
- Multiple failed login attempts followed by a successful login from an unrecognized IP address.  
- Unusual data transfer volumes from internal file servers.  
- Command and control (C2) traffic patterns identified in network packets.  
- Newly created user accounts with administrative privileges.  
- Modification of security logs to hide traces of unauthorized activity.

## 3. Investigation Process

The forensic investigation involved log analysis, network traffic monitoring, and event correlation across different security tools. The steps included:  
1. Splunk Analysis : Queries were executed to search for failed and successful login attempts, identifying suspicious patterns of access.  
2. Kibana Dashboard Review : A spike in network traffic from the compromised system was visualized, indicating potential data exfiltration.  
3. Wireshark Packet Analysis : Captured packets revealed outbound connections to an external IP, suggesting potential C2 communications.

The analysis confirmed that the attacker had gained unauthorized access using compromised credentials and attempted to escalate privileges and exfiltrate sensitive information.

## 4. Root Cause Analysis

The root cause of the incident was a successful phishing attack that led to credential compromise. An employee unknowingly clicked on a malicious email link, leading to a fake login page where they entered their credentials. The attacker harvested these credentials and used them to gain access to internal systems. The lack of multi-factor authentication (MFA) allowed the attacker to proceed without additional verification.

## 5. Mitigation Steps

Upon identifying the breach, the following immediate mitigation steps were taken:  
- Revoked access for the compromised account and forced password resets.  
- Enabled multi-factor authentication (MFA) for all employee accounts to prevent similar attacks.  
- Blocked the attacker’s IP addresses at the firewall level to prevent further access.  
- Isolated the affected systems for forensic analysis and cleaned any persistent backdoors.  
- Reviewed security logs and enabled enhanced monitoring to detect further suspicious activity.  
- Conducted a company-wide phishing awareness training to educate employees on email-based threats.

## 6. Recommendations

To strengthen security and prevent future incidents, the following measures are recommended:  
- Enforce strong authentication mechanisms : Implement MFA across all user accounts to prevent credential-based attacks.  
- Improve email security : Deploy advanced email filtering solutions to detect phishing attempts.  
- Continuous monitoring and anomaly detection : Implement AI-driven threat detection to identify unusual activities in real time.  
- Regular security awareness training : Conduct periodic simulations to test employee responses to phishing attacks.  
- Network segmentation : Limit access to critical systems to only those who require it, reducing the attack surface.  
- Incident response drills : Perform regular security drills to ensure rapid response to potential threats.

## 7. Conclusion

This incident highlights the importance of proactive security measures, robust authentication mechanisms, and employee awareness. By implementing the recommended security controls, the organization can significantly reduce its risk exposure and enhance its ability to detect and re r.