# Incident Handler’s Journal

## Entry 1

Date: February 15, 2025

Entry ID: 001

### Incident Overview

Incident Type: Unauthorized Access Attempt

Affected System: Remote VPN Gateway

Ticket ID: A-2568

Severity Level: High

Incident Status: Closed

### The 5 W’s of the Incident

Who caused the incident?

A threat actor using a compromised set of employee credentials attempted to access the corporate VPN.

What happened?

A login attempt from an unrecognized IP (45.162.84.21) was flagged by the SIEM system. The login attempt used valid credentials but failed multi-factor authentication (MFA).

When did the incident take place?

February 14, 2025, at 10:45 PM.

Where did the incident occur?

The attack targeted the remote access VPN used by employees.

Why did it happen?

The attacker likely obtained valid credentials through a phishing campaign or dark web credential dumps.

### Investigation Findings

Log analysis confirmed repeated failed login attempts from multiple foreign IPs.

Dark web monitoring indicated leaked credentials from a previous breach.

No successful compromise occurred due to enforced MFA.

### Incident Response Actions Taken

✅ Forced password reset for affected user.

✅ Blocked malicious IP addresses on firewall.

✅ Implemented additional security awareness training.

✅ Enhanced SIEM alerts for repeated login failures.

### Final Assessment & Closure Justification

No unauthorized access was granted.

Security policies prevented a full breach.

Monitoring continues for similar attack attempts.

Status: ✅ Closed

Escalation Required: No

## Entry 2

Date: February 19, 2025

Entry ID: 002

### Incident Overview

Incident Type: Phishing Attempt with Malicious Attachment

Affected System: Employee Workstation on Internal Network

Ticket ID: A-2703

Severity Level: Medium

Incident Status: Closed

### The 5 W’s of the Incident

Who caused the incident?

The phishing email originated from an untrusted source impersonating a job applicant.

What happened?

The email contained a password-protected attachment (bfsvc.exe) designed to install malware.

When did the incident take place?

July 20, 2022, at 09:30 AM.

Where did the incident occur?

The HR department’s email system.

Why did it happen?

The attacker used social engineering tactics to bypass security filters.

### Investigation Findings

Malware analysis confirmed credential theft attempts.

VirusTotal scan flagged the file as malicious.

The sender’s IP (114.114.114.114) was previously associated with phishing attacks.

### Incident Response Actions Taken

✅ Quarantined affected system.

✅ Blocked sender and malicious domain.

✅ Updated firewall rules.

✅ Conducted security awareness training.

Status: ✅ Closed

Escalation Required: No

## Entry 3

Date: February 21, 2025

Entry ID: 003

### Cybersecurity Tool Used: Wireshark

Purpose: Wireshark was used to analyze packet captures during an incident response investigation.

Use Case: Detected anomalous DNS requests communicating with a suspicious domain (xyzmalware.com).

Outcome: Helped identify exfiltration attempts, allowing security teams to block the domain.

## Entry 4

Date: February 22, 2025

Entry ID: 004

### Cybersecurity Tool Used: Splunk

Purpose: Log aggregation and security event correlation.

Use Case: Investigated multiple failed login attempts across multiple geographic locations.

Outcome: Correlated logs identified a brute-force attack attempt, leading to an IP ban.

## Reflections/Notes

Were there any specific activities that were challenging for you? Why or why not?

Yes, investigating packet captures with Wireshark was initially difficult due to the large volume of data. Learning to filter and analyze specific traffic patterns helped simplify the process.

Has your understanding of incident detection and response changed since taking this course?

Yes, I now better understand how to use security tools effectively for incident detection, and I feel more confident in handling security events.

Was there a specific tool or concept that you enjoyed the most? Why?

I enjoyed working with Splunk the most because it allowed for real-time log correlation and simplified large-scale threat analysis.