Corporate Email Breach Investigation

Digital Forensics Project Report

Prepared by: Dundubhi K
MCA Cybersecurity Student | Amrita Vishwa Vidyapeetham (2025–2027)

Date: August 2025

Executive Summary

This project simulates a real-world corporate email breach investigation. The goal was to analyze a suspicious phishing email in raw .mbox format, extract key forensic evidence, and document findings in a professional case study format. The investigation was performed entirely within Kali Linux using command-line forensic tools, without reliance on GUI-based applications such as Thunderbird.

Investigation Steps

```
1. Setup Investigation Workspace:
mkdir ~/Corporate_Email_Breach_Investigation
cd ~/Corporate_Email_Breach_Investigation
mkdir Evidence Reports Screenshots Tools

2. Downloaded Phishing Email Sample (mbox file):
curl -o Evidence/phishing_sample.mbox https://raw.githubusercontent.com/DFIRScience/
dfir-mbox-tools/main/tests/data/test.mbox

3. Searched for Key Indicators:
grep -i "from:" Evidence/phishing_sample.mbox
grep -i "subject:" Evidence/phishing_sample.mbox
grep -i "http" Evidence/phishing_sample.mbox

4. Extracted URLs for Analysis:
grep -Eo 'http[s]?://[^ >]+' Evidence/phishing_sample.mbox > Evidence/urls.txt

5. Calculated Hash for Evidence Integrity:
sha256sum Evidence/phishing_sample.mbox > Evidence/mbox_hash.txt

6. Collected Metadata (file size, timestamps):
stat Evidence/phishing_sample.mbox > Evidence/mbox_metadata.txt
```

Findings

- The email originated from a suspicious/unverified domain. - Embedded URLs did not match the sender domain (classic phishing indicator). - The subject line attempted to create urgency (potential social engineering tactic). - No legitimate digital signatures (DKIM/SPF/DMARC) were found in headers. - Integrity of the evidence was preserved using SHA-256 hashing.

Conclusion & Learning Outcomes

This investigation demonstrated how phishing emails can be forensically analyzed in a professional environment. Key skills gained include evidence handling, email header and URL analysis, and maintaining chain-of-custody using hashes. The ability to perform such investigations without relying on GUI tools mirrors real corporate DFIR practices. This project will be added to the cybersecurity portfolio to showcase practical digital forensics capabilities.