Phishing Incident Documentation

Based on NIST SP 800-61 – Incident Response

Introduction

Phishing is one of the most common and dangerous cyberattacks, relying on **social engineering techniques** to deceive users into revealing sensitive information such as usernames and passwords.
This report documents a **Phishing Attack Simulation** conducted in a controlled lab environment, following the **NIST SP 800-61 Incident Response Framework**.

Incident Overview

- **Incident Type:** Phishing Attack
- **Category:** Social Engineering
- **Environment:** Controlled Lab
- **Severity Level:** Medium to High
- **Purpose:** Educational and Defensive

The simulation demonstrates how phishing attacks are executed and how security teams should respond effectively using standardized incident response procedures.

---

1 Identification

The identification phase focuses on detecting and confirming the phishing incident.

Detection Methods:

- User reported a suspicious link
- SOC monitoring detected unusual activity
- Credentials were submitted to an untrusted website

Indicators of Compromise (IOCs):

- Malicious phishing URL
- Fake login page
- Suspicious IP address
- Unauthorized credential submission

---

2 Analysis

During the analysis phase, the incident is examined to understand its scope and impact.

Analysis Details:

- **Attack Vector:** Phishing link
- **Technique:** Social Engineering
- **Tools Used:**
  - Custom ASPX Phishing Page
  - ZPhisher Tool
  - Social-Engineer Toolkit (SET)

Potential Impact:

- Credential compromise
- Unauthorized account access
- Risk of further exploitation

---

3 Containment

The goal of containment is to limit the damage and stop the attack from spreading.

Short-Term Containment:

- Block the malicious URL
- Isolate the victim machine
- Disable compromised user accounts

Long-Term Containment:

- Reset passwords
- Enable Multi-Factor Authentication (MFA)
- Improve email filtering policies

---

4 Eradication

This phase focuses on completely removing the cause of the incident.

Actions Taken:

- Remove phishing pages
- Clean the affected system

- Clear browser cache and stored credentials
- Eliminate any attacker access

---

5 Recovery

Recovery ensures systems return to normal operation while being closely monitored.

Recovery Steps:

- Re-enable user accounts
- Restore network connectivity
- Monitor login attempts
- Verify system integrity

---

6 Lessons Learned

This phase helps prevent similar incidents in the future.

Root Cause:

- User interaction with a malicious link
- Lack of phishing awareness

Improvements:

- Conduct regular security awareness training
- Perform periodic phishing simulations
- Enhance SOC detection and response capabilities

Conclusion

This phishing incident simulation highlights the importance of applying the **NIST Incident Response Framework** to detect, contain, eradicate, and recover from phishing attacks effectively, while strengthening overall security posture.