Incident Response and Handling Report

Incident Response Plan (IRP)

Framework Used: NIST 800-61

1. Preparation

- Defined IR roles: Incident Analyst, IR Coordinator, IT Support.
- Tools in place: log collection, forensic utilities, segmentation.
- Communication: internal email, Slack. Offline backups enabled.

2. Identification

- Detected multiple failed SSH login attempts from IP 203.0.113.14.
- Sample log:

```
  Mar 26 13:44:12 sshd[4021]: Failed password for invalid user admin from 203.0.113.14 port 49855 ssh2
```

3. Containment

- Blocked IP via iptables, isolated affected host.

4. Eradication

- Removed unused accounts, hardened SSH configuration.

5. Recovery

- Restored SSH with key-only login. Deployed Fail2Ban.

Incident Triage and Categorization

Incident Type	Severity	Business Impact	Action Required
Ransomware Infection	Critical	High	Immediate isolation, restore backups
Phishing Attack	Medium	Moderate	Credential reset, notify users
Port Scanning	Low	Low	Monitor traffic, block IP if needed

Digital Forensics Demonstration

Incident Response and Handling Report

Tool Used: log2timeline (Plaso)

Commands:

```
log2timeline.py incident.plaso /var/log/auth.log
psort.py -o l2tcsv -w timeline.csv incident.plaso
```

Sample output:

```
timestamp: 2025-03-26T13:44:12
source: auth.log
description: Failed SSH login for user 'admin' from 203.0.113.14
```

Evidence Collection and Documentation

Evidence 1 - Log File

- Path: /var/log/auth.log
- SHA256: 18d3c9faec4f721d65df0e1cd042b9cf6a6b5bdf3ef75802ac889872c3f11c99

Evidence 2 - Screenshot

- File: brute_force_evidence.png
- SHA256: b17e4202f3c98a96f7c9189bcade87138fa6ad5cc54e27b7dd9ee3b1b8cdd19a

Chain of Custody:

Timestamp: 2025-03-26 14:00, Handler: Analyst A, Type: Log File, Description: SSH attempts from remote IP, Hash: 18d3c9...

Timestamp: 2025-03-26 14:05, Handler: Analyst A, Type: Screenshot, Description: Terminal output of brute force, Hash: b17e42...

Post-Incident Analysis

Incident Summary:

Brute-force SSH attack from IP 203.0.113.14.

Attack failed, but revealed weak SSH configuration.

Incident Response and Handling Report

Actions Taken:

Hardened SSH, blocked IP, deployed Fail2Ban.

Lessons Learned:

1. SSH configs must enforce key-based login.

2. Real-time alerting is essential to detect brute-force attempts immediately.