🚨 Incident Response and Handling Report

🔒 Executive Summary

This report documents the implementation of a complete Incident Response and Handling process based on a 5-step Incident Response Plan (IRP) framework. It includes practical application of digital forensics tools for data collection, evidence documentation with chain of custody, incident triage with severity categorization, and a post-incident analysis summarizing outcomes and lessons learned. Mock data is used where appropriate to simulate a real-world incident environment.

---

1. 📋 Incident Response Plan (IRP)

The organization follows a structured **5-step Incident Response Framework**:

🔹 Step 1: Preparation

- **Security Policies**: Updated Acceptable Use Policies (AUP) for employees.
- **Tools Ready**: Installed Wireshark, Volatility, and OSSEC for monitoring and forensic analysis.
- **Training Conducted**: Annual cybersecurity awareness training completed by 95% of staff (mock data).

🔹 Step 2: Identification

- **Trigger Event**: OSSEC generated alerts indicating suspicious SSH login attempts from external IP `185.243.12.90`.
- **Initial Detection Timestamp**: `2025-04-26 10:15:47`
- **Alert Sample (Mock from OSSEC Log)**:

log
CopyEdit

```
** Alert 1682533347.1234: - sshd,authentication_failures,
```

```
2025 Apr 26 10:15:47 (parrot) 10.138.16.109->/var/log/auth.log
Rule: 5715 (level 10) -> 'Multiple SSHD authentication failures.'
Src IP: 185.243.12.90
User: root
```

📸 Screenshot attached: OSSEC Dashboard showing triggered alert.

🔹 Step 3: Containment

- **Immediate Action Taken**:

Blocked source IP using `iptables`:
bash
CopyEdit
```
sudo iptables -A INPUT -s 185.243.12.90 -j DROP
```

    -
    - Disabled suspicious accounts temporarily pending further investigation.

🔹 Step 4: Eradication

- **Root Cause Analysis**:
    - Password spraying attack detected.
- **Fixes Applied**:
    - Forced password resets across all user accounts.
    - Implemented SSH key-based authentication and disabled password-based SSH login.

SSH Config (Post-Mitigation):

text
CopyEdit
```
PasswordAuthentication no
PermitRootLogin no
```

🔹 Step 5: Recovery

- **Restoration Measures**:
  - Verified integrity of critical systems via checksum comparison.
  - Monitored for abnormal activities for 72 hours — no further anomalies detected.

✅ Systems declared back to normal operations on `2025-04-29 12:00:00`.

---

2. 🧪 Digital Forensics: Tool Demonstration

Forensic Tool Used: Volatility Framework

Scenario: Memory capture and analysis for possible malware traces.

Steps:

Captured memory image from suspected machine:
bash
CopyEdit

```
sudo dd if=/dev/mem of=/evidence/mem_dump.img bs=1M
```

1.

Analyzed memory with Volatility:
bash
CopyEdit

```
volatility -f /evidence/mem_dump.img --profile=LinuxUbuntu_20_04x64
pslist
```

2.

Sample Output (Mock Data):

text
CopyEdit

```
Offset(V)  Name                PID   PPID  DTB                 Start
Exit
0x1234abcd sshd                1276  1     0x5678abcd
2025-04-26 10:15:00
0x2234abcd netcat              1337  1     0x6678abcd
2025-04-26 10:18:30
```

- Suspicious process `netcat` found — possible reverse shell.

📸 Screenshot: Volatility pslist results.

---

3. 🧾 Evidence Collection and Documentation

📑 Evidence Forms Collected:

- **1. OSSEC Log Files**
- **2. Screenshot of blocked IP in Firewall (`iptables -L` output)**

📋 Chain of Custody Documentation (Mock Example):

Time	Handler	Action	Location
2025-04-26 10:30	John Doe (IR Lead)	Collected OSSEC logs	Secured in `/evidence/incident-0426/`
2025-04-26 10:45	Jane Smith (Forensic Analyst)	Captured Memory Dump	External encrypted drive, sealed evidence bag

✅ Chain of custody form signed digitally using internal case management system.

---

4. 🚦 Incident Triage and Prioritization

Categorized Incidents:

Incident	Severity	Business Impact	Priority
Unauthorized SSH Access Attempt	High	Risk of full system compromise	1
Website Defacement Attempt	Medium	Damage to public image	2
Phishing Email Detected	Low	Risk mitigated by awareness training	3

✅ Each incident triaged based on immediate impact, potential damage, and system criticality.

---

5. 📈 Post-Incident Analysis

Incident Outcome Summary:

- Attack attempt was detected and neutralized before any breach or data loss occurred.
- SSH hardening and user education were reinforced immediately.
- No financial or operational loss reported.

Lessons Learned:

1. **Need for Proactive Monitoring**:
    - Continuous monitoring with alert thresholds improves early detection capabilities.
2. **Strengthening Access Controls**:
    - Default password-based authentication exposed unnecessary risk; moving to SSH key-based authentication significantly reduces attack surface.

🟢 Final Notes:

This Incident Response and Handling exercise demonstrates comprehensive preparation, quick detection and response, detailed evidence handling, logical triage, and practical post-incident reflection based on professional cybersecurity standards.