Incident Response Documentation & Reporting

1. Introduction

This report details the **Incident Response (IR) documentation and reporting process** executed in **Parrot OS**. The objective is to establish a structured approach to handling security incidents, ensuring prompt detection, containment, eradication, and recovery while maintaining comprehensive documentation.

The project covers:

- **Incident Response Playbook:** Documenting step-by-step response procedures for various security incidents.
- **Tool-Specific Commands:** Utilizing Parrot OS tools for forensic investigation and evidence collection.
- **Incident Tracking System:** Implementing a structured approach to logging security incidents, responses, and timelines.
- **Incident Report:** Documenting a real-world security event following standard reporting formats.
- **Documentation of IR Tools & Procedures:** Maintaining a detailed reference guide for all IR-related tools in Parrot OS.

---

2. Incident Response Playbook

Purpose

The **Incident Response Playbook** is a predefined guide that security analysts follow to efficiently detect, contain, and mitigate cybersecurity threats. It ensures uniformity, reduces response time, and enhances forensic evidence collection.

Types of Incidents Covered

The playbook includes detailed response procedures for:

- **Unauthorized Access** (e.g., brute-force attacks, stolen credentials)
- **Malware Infection** (e.g., ransomware, trojans, worms)
- **Denial-of-Service (DoS) Attacks**

- **Phishing & Social Engineering Attacks**
- **Insider Threats & Data Breaches**

Example: Unauthorized Access Response Procedure

1️⃣ Identification

- Check active user sessions:
  who -a
- Review recent login attempts:
  last -a
- Check authentication logs for failed SSH attempts:
  cat /var/log/auth.log | grep "Failed password"

2️⃣ Containment

- Block the attacker's IP address:
  sudo ufw deny from <attacker-IP>
- Disable a compromised user account:
  sudo usermod -L <username>

3️⃣ Eradication

Identify and terminate suspicious processes:
ps aux | grep <suspicious_process>

- sudo kill -9 <PID>
- Perform a malware scan:
  sudo clamtk

4️⃣ Recovery

- Restore affected system files from a secure backup.
- Apply patches and enforce multi-factor authentication (MFA).

5️⃣ Documentation & Lessons Learned

- Log all actions taken.
- Conduct a post-incident analysis to enhance security measures.

✅ **This structured playbook ensures rapid and effective incident handling.**

---

3. Incident Tracking System

Purpose

An **Incident Tracking System** records and organizes details of security incidents to maintain logs, analyze attack patterns, and track response effectiveness.

Implementation

A CSV-based tracking system was created in **Parrot OS** for structured data entry.

Incident ID, Date & Time, Type, Description, Actions Taken, Timeline, Status
IR001, 2025-03-03 14:30, Unauthorized Access, SSH brute-force attack detected, Blocked attacker IP, disabled account, 14:35 Blocked, Closed

Example Entry Format

Incident ID	Date & Time	Type	Description	Actions Taken	Timeline	Status
IR001	2025-03-03 14:30	Unauthorized Access	SSH brute-force attack detected	Blocked attacker IP, disabled account	14:35 Blocked, 14:40 Disabled account	Closed

✅ **This tracking system allows easy documentation and future reference.**

---

4. Incident Report

Purpose

A well-documented **Incident Report** provides a **formal record** of security incidents, assisting with legal compliance, forensic investigation, and future incident prevention.

Example Incident Report

🚨 **INCIDENT REPORT: Unauthorized Access** 🚨

- **Incident ID:** IR001
- **Date:** March 3, 2025
- **Time:** 14:30 EST
- **Affected System:** Parrot OS (192.168.1.5)
- **Description:** A brute-force attack targeted SSH login. The attacker made repeated login attempts using multiple username-password combinations.

- **Indicators:**
  - Multiple failed login attempts in `/var/log/auth.log`
  - Suspicious IP (203.0.113.15) attempting SSH connections
- **Containment Actions:**
  - Blocked attacker IP using `ufw`
  - Disabled the compromised user account
- **Eradication & Recovery:**
  - No malware detected
  - Updated SSH security settings (disabling root login, enforcing key-based authentication)
- **Conclusion & Lessons Learned:**
  - Implemented 2FA for SSH
  - Enhanced network monitoring using IDS/IPS solutions

✅ **This report documents all incident-handling steps.**

---

5. Documentation of IR Tools & Procedures

Purpose

A comprehensive documentation of **IR tools** ensures a clear understanding of available resources, helping forensic analysts apply the right tool for each situation.

Tools & Their Functions in Parrot OS

Tool	Purpose	Command Example
who	Check logged-in users	`who -a`
netstat	View active network connections	`netstat -antp`
ufw	Manage firewall rules	`sudo ufw deny from <IP>`
Volatility	Memory forensics analysis	`volatility -f memory_dump.raw imageinfo`
dd	Disk imaging for forensic analysis	`sudo dd if=/dev/sdX of=disk_image.dd bs=4M status=progress`
log2timeline	Timeline creation for event correlation	`log2timeline.py timeline.plaso /var/logs/`

Example Commands Used in the IR Process

1️⃣ Live Data Collection

```
who -a > live_data.txt
netstat -antp >> live_data.txt
ps aux >> live_data.txt
```

2️⃣ Memory Analysis with Volatility

```
volatility -f memory_dump.raw imageinfo > imageinfo.txt
profile=$(grep "Suggested Profile(s)" imageinfo.txt | awk -F ':' '{print $2}' | awk '{print $1}')
volatility -f memory_dump.raw --profile=$profile pslist > processes.txt
```

3️⃣ Disk Imaging & Verification

```
sudo dd if=/dev/sdX of=/mnt/usb/disk_image.dd bs=4M status=progress
md5sum /mnt/usb/disk_image.dd
```

✅ **This documentation serves as a detailed reference for security analysts.**

---

6. Conclusion

This report successfully implemented a **structured Incident Response Documentation & Reporting system in Parrot OS**, ensuring:

- ✅ A well-defined **Incident Response Playbook**.
- ✅ A structured **Incident Tracking System**.
- ✅ A **formal Incident Report** with forensic details.
- ✅ Comprehensive **IR Tools Documentation**.

This standardized approach enhances cybersecurity readiness and forensic response efficiency.