IR Documentation & Reporting

1. Incident Response Playbook

1.1 Common Incidents & Response Procedures

- **Unauthorized SSH Attempt:**
  - Identify source IP using `journalctl -u ssh` or `/var/log/auth.log`
  - Block IP using `iptables` or `ufw`
  - Alert SOC and monitor for recurring patterns
- **USB Device Insertion:**
  - Detect via `dmesg | grep usb`
  - Log device ID and time
  - Disable USB ports if unauthorized
- **Privilege Escalation (root shell):**
  - Detect via `/var/log/auth.log` or `auditd`
  - Correlate with user login history
  - Lock account and isolate system

1.2 Tool-Specific Commands (Parrot OS)

- Wazuh CLI: `/var/ossec/bin/ossec-control status`
- Log Review: `less /var/log/auth.log`, `journalctl -xe`
- Memory Dump: `insmod lime.ko path=/root/memdump.lime format=lime`
- Network Monitoring: `tcpdump`, `wireshark`

1.3 Evidence Collection Steps

- Logs: Copy `/var/log/*` files and Wazuh alerts
- Memory: Use LiME to capture and Volatility to analyze
- Network: Export `.pcap` files from Wireshark
- Screenshots of alerts and logs

---

2. Incident Tracking System

Format Example:

Incident ID	Date	System Affected	Summary	Action Taken	Timeline

IR-SSH-001	2024-11-22	Parrot OS	Unauthorized SSH attempt	IP blocked, alert triggered	03:14 login attempt, 03:16 alert

- Tool: Markdown table + Wazuh integration notes

---

3. Complete Incident Report (Example)

Title: Unauthorized SSH Login Attempt

Incident ID: IR-SSH-001 **Date:** 2024-11-22 **System:** Parrot OS (VirtualBox)

Summary: A brute-force SSH login attempt was made from IP 192.168.1.5. The attempt was logged in `/var/log/auth.log` and detected by Wazuh custom rule.

Detection:

- Log: `sshd[2048]: Failed password for invalid user test`
- Alert ID: 100101

Response Actions:

- Source IP blocked using `ufw`
- Logs preserved and exported
- Notified security team

Timeline:

- 03:14:55 – Attempt initiated
- 03:14:57 – Failed login recorded
- 03:15:00 – Alert triggered
- 03:16:00 – IP blocked

Lessons Learned:

- Need to enforce 2FA
- Add alerting thresholds for rapid escalation

---

4. IR Tools Documentation (Parrot OS)

4.1 Wazuh Agent

- Monitors system logs, file integrity, and threat detection
- Command: `sudo systemctl status wazuh-agent`

4.2 Wireshark

- Captures and filters live traffic
- Usage: Apply filters like `tcp.port == 22` to isolate SSH

4.3 Volatility Framework

- Performs memory analysis on `.lime` dumps
- Usage: `vol.py -f memdump.lime --profile=LinuxParrot pslist`

4.4 Syslog / Auditd

- Collects login, process, and file access logs
- Commands: `journalctl`, `ausearch`, `auditctl`

End of Document