Incident Detection and Analysis Documentation

1. Overview This document presents detailed analysis conducted within the IR environment using Wazuh. It covers methodology and findings from reviewing Parrot OS and macOS logs, investigates a specific suspicious login event, correlates related logs, builds a timeline, validates alerts, and classifies three distinct security incidents using a severity matrix.

---

2. Analysis Methodology

- **Log Sources:**
  - Parrot OS: `/var/log/auth.log`, `/var/log/syslog`
  - macOS: Remote syslog forwarded entries
- **Tool Used:** Wazuh Dashboard and CLI tools
- **Approach:**
  - Use Wazuh rules and queries to isolate events
  - Filter based on keywords like `sshd`, `login`, `usb`, `su`
  - Correlate host and network events using timestamps

---

3. Suspicious Login Attempt Investigation

3.1 Identified Event:

- Alert in Wazuh: **Unauthorized SSH login attempt (Rule ID: 100101)**
- Host: Parrot OS
- Timestamp: `2024-11-22 03:14:57`

3.2 Correlated Logs:

- `/var/log/auth.log` (Parrot OS):

sshd[2048]: Failed password for invalid user test from 192.168.1.5 port 55422 ssh2

- macOS logs:

ssh connection request to ParrotOS from Terminal.app

3.3 Event Timeline:

- **03:14:55** - Connection initiated from macOS (192.168.1.5)
- **03:14:57** - Failed password attempt on Parrot OS
- **03:14:59** - Wazuh alert generated and displayed

3.4 Alert Validation:

- Triggered rule: `local_rules.xml` (ID: 100101)
- Validated via raw log review + dashboard alert

---

4. Security Incident Classification Using the taught severity matrix:

Incident 1: Unauthorized SSH Login Attempt

- **Type:** Brute-force attempt
- **Severity:** High (multiple failures, from unrecognized IP)
- **Impact:** Potential credential stuffing

Incident 2: USB Device Detection

- **Log:** `/var/log/syslog` shows USB mass storage insertion
- **Severity:** Medium (insider threat risk)
- **Impact:** Data exfiltration possibility

Incident 3: Root Shell Execution

- **Log:** `session opened for user root`
- **Severity:** High
- **Impact:** Privilege escalation, potential compromise

---

5. Methodology Documentation

- **Log Filtering:** Custom queries used on Wazuh dashboard
- **Event Correlation:** Timestamps and source/destination matching
- **Alert Cross-check:** Used both local rules and default rulesets
- **Severity Assignment:** Followed the CIA-based severity matrix

---

6. Implications and Recommendations

- Repeated SSH login attempts suggest brute-force reconnaissance
- USB insertions can bypass network DLP controls
- Root access logins must be controlled and audited more strictly

Recommendations:

- Enforce SSH rate-limiting and 2FA

- Disable USB mounting unless explicitly approved
- Use sudo with audit policies for all root activity

End of Document