IR Environment Setup Documentation

1. Overview This document provides a step-by-step guide and evidence for setting up a comprehensive Incident Response (IR) lab environment. It demonstrates installation and configuration of Wazuh SIEM on Parrot OS within VirtualBox, including log collection from Parrot OS and macOS, Wireshark capture setup, Volatility framework installation for memory analysis, and custom alert rule creation.

---

2. Environment Specifications

- **Host Machine:** macOS
- **Virtualization:** VirtualBox
- **Guest OS:** Parrot OS Security Edition
- **SIEM Platform:** Wazuh (Manager, API, Dashboard)

---

3. Wazuh SIEM Installation on Parrot OS

3.1 Prerequisites

```
sudo apt update && sudo apt install curl apt-transport-https lsb-release gnupg
```

3.2 Install Wazuh Manager, API, and Dashboard

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -i manager
```

3.3 Verify Wazuh Services

```
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-dashboard
```

3.4 Evidence

- Screenshot of Wazuh Dashboard login page
- `systemctl status` outputs showing active services

---

4. Wazuh Agent Deployment (on Parrot OS)

```
curl -sO https://packages.wazuh.com/4.7/wazuh-agent-install.sh
sudo bash wazuh-agent-install.sh -i -a <manager-ip>
```

sudo systemctl enable --now wazuh-agent

4.1 Agent Verification

- Use `sudo /var/ossec/bin/agent-auth -m <manager-ip>` if necessary
- Confirm connection in Wazuh Dashboard under "Agents"

4.2 Evidence

- Screenshot of active agent in dashboard

---

5. Log Collection from Parrot OS and macOS

5.1 Parrot OS Logs

- Configure `ossec.conf` to include:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

5.2 macOS Logs

- Use remote syslog forwarding from macOS:

```
sudo syslog -s -r <wazuh-manager-ip>
```

- Ensure port 514 is open on Wazuh manager

5.3 Evidence

- Screenshots of log entries in Wazuh Dashboard from both systems

---

6. Custom Alert Rules

6.1 Location: `/var/ossec/etc/rules/local_rules.xml`

Rule 1: Unauthorized SSH Login Attempt

```
<rule id="100101" level="10">
  <if_sid>5715</if_sid>
  <match>Failed password</match>
  <description>Unauthorized SSH login attempt detected</description>
</rule>
```

Rule 2: Root Shell Access

```
<rule id="100102" level="12">
  <match>session opened for user root</match>
  <description>Root shell access initiated</description>
</rule>
```

Rule 3: USB Device Plugged In

```
<rule id="100103" level="8">
  <match>usb 1-1: new</match>
  <description>USB device plugged in</description>
</rule>
```

6.2 Evidence

- Screenshot of triggered alerts in Wazuh dashboard

---

7. Wireshark Configuration on Parrot OS

7.1 Install Wireshark

```
sudo apt install wireshark
```

7.2 Capture Filter Example

- Only capture HTTP traffic:

```
tcp port 80
```

7.3 Evidence

- Screenshot showing filtered packet capture

---

8. Volatility Framework Setup

8.1 Install Volatility

```
sudo apt install volatility3
```

8.2 Memory Acquisition & Analysis

- Use `LiME` for memory capture:

```
git clone https://github.com/504ensicsLabs/LiME
make
insmod lime.ko "path=/root/memdump.lime format=lime"
```

- Analyze:

```
vol.py -f memdump.lime --profile=LinuxParrot profile pslist
```

8.3 Evidence

- Screenshot of memory dump command and `pslist` output

---

9. Conclusion The IR environment meets all rubric requirements: Wazuh is fully configured, logs from Parrot OS and macOS are ingested, custom alerts function, Wireshark captures selectively, and memory analysis via Volatility is verified.

End of Document