**Mini SOC Lab - Detailed Setup and Documentation**

**Table of Contents**

1. Introduction
2. Lab Architecture Overview
3. Environment Setup
   * VirtualBox Installation
   * VM Creation: Kali Linux and Ubuntu
4. Installing and Configuring Wazuh
   * Installing Wazuh Manager and ELK Stack on Ubuntu
   * Installing and Configuring Wazuh Agent on Ubuntu
   * Installing and Configuring Wazuh Agent on Kali Linux
5. Connectivity Verification
6. Attack Simulation and Detection
7. Monitoring and Analysis in Kibana
8. Incident Response Workflow
9. Troubleshooting Tips
10. Future Enhancements
11. References

**1. Introduction**

This document guides you through building a Mini Security Operations Center (SOC) lab environment using Kali Linux as the attacker, Ubuntu as the victim, and Wazuh as the SIEM and monitoring platform. The lab aims to provide practical hands-on experience with attack simulation, log collection, alerting, and incident response.

+-------------------+ +-------------------+

| Kali Linux | | Ubuntu Linux |

| (Attacker VM) | ---> | (Victim VM with |

| | | Wazuh Agent & |

| | | Wazuh Manager + |

+-------------------+ | ELK Stack) |

+-------------------+

|

|

+-------------------+

| Wazuh Manager |

| + ELK Stack |

| (Centralized SIEM)|

+-------------------+

**2. Lab Architecture Overview**

The lab consists of three main components:

* **Attacker:** Kali Linux VM, used to launch penetration testing and attacks
* **Victim:** Ubuntu Linux VM, running Wazuh agent to monitor system activity
* **SIEM:** Wazuh Manager installed on the Ubuntu VM along with the ELK stack for centralized log storage, analysis, and visualization

**3. Environment Setup**

**3.1 VirtualBox Installation**

Download and install VirtualBox from https://www.virtualbox.org/. VirtualBox allows you to create and manage virtual machines on your host system.

*Insert screenshot of VirtualBox installation or dashboard.*

**3.2 VM Creation: Kali Linux**

* Download Kali Linux ISO from https://www.kali.org/get-kali/
* Create a new VM with at least 2GB RAM, 20GB disk space
* Install Kali Linux by booting the VM with the Kali ISO

*Insert screenshots of VM creation steps and Kali Linux installation.*

**3.3 VM Creation: Ubuntu Linux**

* Download Ubuntu ISO from <https://ubuntu.com/download/desktop>
* Create a new VM with similar specs (2GB+ RAM, 20GB disk)
* Install Ubuntu OS

**4. Installing and Configuring Wazuh**

**4.1 Installing Wazuh Manager and ELK Stack on Ubuntu**

* Use the following command to install Wazuh Manager and ELK stack on Ubuntu:

bash

CopyEdit

curl -s https://packages.wazuh.com/install.sh | bash

* After installation, start the Wazuh manager and ELK services:

bash

CopyEdit

sudo systemctl start wazuh-manager

sudo systemctl start elasticsearch

sudo systemctl start kibana

**4.2 Installing and Configuring Wazuh Agent on Ubuntu**

* Install the Wazuh agent on the Ubuntu victim machine using the same install script.
* Configure the agent to communicate with the Wazuh manager by editing /var/ossec/etc/ossec.conf and adding the manager’s IP address.
* Start the agent service:

bash

CopyEdit

sudo systemctl start wazuh-agent

*Insert configuration file snippets and command outputs screenshots.*

**4.3 Installing and Configuring Wazuh Agent on Kali Linux**

* Repeat the agent installation on the Kali Linux VM.
* Edit the agent’s ossec.conf to point to the Wazuh Manager IP.
* Start the Wazuh agent service.

**5. Connectivity Verification**

* Log in to the Wazuh Manager dashboard (via Kibana web UI) and verify that both Kali and Ubuntu agents are connected and reporting data.
* Confirm the agent status and last check-in time.

**6. Attack Simulation and Detection**

**6.1 Running Basic Attacks from Kali Linux**

* Use tools like nmap for network scanning and hydra for brute force attempts targeting the Ubuntu VM.
* Example:

bash

CopyEdit

nmap -sS <Ubuntu\_IP>

hydra -l user -P /usr/share/wordlists/rockyou.txt ssh://<Ubuntu\_IP>

*Add screenshots of attack commands and terminal output.*

**6.2 Detecting Alerts in Wazuh**

* Observe generated alerts in Kibana under the Security Events or Wazuh App dashboard.
* Alerts will indicate suspicious activities like port scans, brute force attempts, or unauthorized access.*.*

**7. Monitoring and Analysis in Kibana**

* Use Kibana dashboards to filter and analyze events by severity, source IP, or event type.
* Demonstrate querying logs and drilling down into alert details.

**8. Incident Response Workflow**

* Upon detecting an alert, analyze the log details to understand the attack vector.
* Document findings and isolate the threat if possible.
* Practice creating an incident report including timeline and mitigation steps.

**9. Troubleshooting Tips**

* Ensure agents have network connectivity to Wazuh Manager.
* Verify firewall settings on VMs are not blocking necessary ports (default Wazuh port: 1514 UDP/TCP).
* Check service statuses if logs are not appearing.

**10. Future Enhancements**

* Add more victim machines for diverse attack scenarios.
* Integrate automation tools like Shuffle SOAR for incident response.
* Implement advanced correlation rules in Wazuh.

**11. References**

* Wazuh Documentation
* [ELK Stack Guide](https://www.elastic.co/guide/)
* Kali Linux
* [Ubuntu](https://ubuntu.com/)
* VirtualBox