Step-by-Step Implementation Guide for SOC Lab Setup and Configuration

Phase 1: Lab Planning and Diagram Creation

1. **Define Objectives**
   - The lab will simulate an **SOC workflow** with **Wazuh, The Hive, and Shuffle** for threat detection, case management, and automation.
2. **Connect Components Logically**
   - **Windows 10 Client** → **Wazuh Manager** (send security events)
   - **Wazuh Manager** → **Shuffle** (alerts enrichment)
   - **Shuffle** → **The Hive** (case creation)
   - **Shuffle** → **SOC Analyst** (email notifications)
   - **SOC Analyst** → **Shuffle** → **Wazuh** (response action execution)

Phase 2: Install Applications and Virtual Machines

2.1 Install VirtualBox and Create Windows 10 VM

1. **Download VirtualBox** from VirtualBox.org
2. **Verify SHA-256 checksum** to ensure file integrity.
3. **Install VirtualBox** and resolve dependencies (e.g., **Microsoft Visual C++ 2019**).
4. **Download Windows 10 ISO** using the **Media Creation Tool**.
5. **Create Virtual Machine (VM) in VirtualBox**:
   - Name: **Windows10-Client**
   - RAM: **4GB**
   - CPU: **1 Core**
   - Storage: **50GB**
   - Attach **Windows 10 ISO** as the bootable disk.
6. **Install Windows 10** (Select **Custom Installation**).

2.2 Install Sysmon on Windows 10

1. **Download Sysmon** from Microsoft Sysinternals.
2. **Download sysmonconfig.xml** from the SwiftOnSecurity GitHub repo.

Install Sysmon:

```
sysmon64.exe -accepteula -i sysmonconfig.xml
```

3. **Verify Sysmon installation** via:
   - **Services.msc** → Look for **Sysmon**.

- **Event Viewer** → Navigate to **Applications and Services Logs** → **Microsoft** → **Windows** → **Sysmon** → **Operational**.

2.3 Deploy Wazuh and The Hive in the Cloud

2.3.1 Setup Wazuh Server

1. **Sign up on DigitalOcean** (or AWS, GCP, Azure).
2. **Create a Droplet**:
   - OS: **Ubuntu 22.04**
   - RAM: **1GB**
   - Storage: **50GB**
3. **Set up firewall rules**:
   - Allow **SSH** only from your **public IP**.
   - Open ports for Wazuh, The Hive, and Shuffle if necessary.

Connect to Wazuh via SSH: `ssh root@<WAZUH_PUBLIC_IP>`

4.

Install Wazuh:

```
curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh

sudo bash wazuh-install.sh
```

5.

Retrieve Admin Credentials:

```
cat /var/ossec/api/configuration/security/user.conf
```

6. **Access Wazuh Dashboard**:

Open a browser and navigate to: `https://<WAZUH_PUBLIC_IP>`

- Log in with **admin** and your password.

2.3.2 Setup The Hive Server

1. **Create another Droplet**:
   - OS: **Ubuntu 20.04**
   - RAM: **8GB**
   - Storage: **50GB**

Install dependencies:

```
sudo apt update && sudo apt install openjdk-11-jdk cassandra elasticsearch
```

2. **Configure Cassandra** (**`/etc/cassandra/cassandra.yaml`**):
   - Set **cluster_name**: `my_dfir`
   - Set **listen_address** and **rpc_address** to **The Hive's Public IP**.

Restart Cassandra: `systemctl restart cassandra`

3. **Configure Elasticsearch** (**`/etc/elasticsearch/elasticsearch.yml`**):
   - Set **cluster.name**: `hive`
   - Set **network.host**: `<HIVE_PUBLIC_IP>`
   - Enable **cluster.initial_master_nodes**.

Restart Elasticsearch: `systemctl restart elasticsearch`

4.

Install The Hive:

```
wget https://download.thehive-project.org/thehive-latest.deb
```

```
sudo dpkg -i thehive-latest.deb
```

5.

Start The Hive: `systemctl start thehive`

6.

Access The Hive Dashboard: `http://<HIVE_PUBLIC_IP>:9000`

Phase 3: Configure Wazuh and The Hive

Verify Services:

```
systemctl status cassandra
```

```
systemctl status elasticsearch
```

```
systemctl status thehive
```

1. **Configure The Hive** (**`/etc/thehive/application.conf`**):
   - Set **database.host** to **Cassandra's Public IP**.
   - Set **storage.path** to a writable directory.

Restart The Hive: `systemctl restart thehive`

2. **Enroll Windows 10 Client in Wazuh**:
   - Generate an agent key from Wazuh.
   - Install the Wazuh agent on Windows 10.

```
wazuh-agent.exe -i <WAZUH_PUBLIC_IP> -p 1514
```

Phase 4: Generate Telemetry and Detect Mimikatz

1. **Modify Wazuh Configuration (`ossec.conf`)**:
   - Add **Sysmon logs ingestion**.

Restart Wazuh Service: `systemctl restart wazuh-manager`

2. **Test Detection with Mimikatz**:
   - Exclude **Downloads folder** in **Windows Defender**.
   - Download and run **Mimikatz**.
   - `mimikatz.exe`
3.
   - Check Wazuh for alerts.

Phase 5: Integrate Shuffle for Automated Response

1. **Create an Account on Shuffle**.
2. **Create a New Workflow**:
   - Use **Webhook Trigger** for Wazuh alerts.

Copy Webhook URL and Add to Wazuh (`ossec.conf`):

```
<integration>

    <name>webhook</name>

    <hook_url>https://shuffle.io/webhook/...</hook_url>

    <rule_id>100002</rule_id>

</integration>
```

3.

Restart Wazuh:

```
systemctl restart wazuh-manager
```

4. **Test Automated Response**:
    - Generate a **Mimikatz alert**.
    - Verify **Shuffle receives alert**.
    - Ensure **Shuffle sends an email to the SOC Analyst**.

Final Steps

- **Confirm Wazuh, The Hive, and Shuffle communicate correctly**.
- **Test end-to-end detection-response workflow**.
- **Expand use cases with additional attack simulations**.