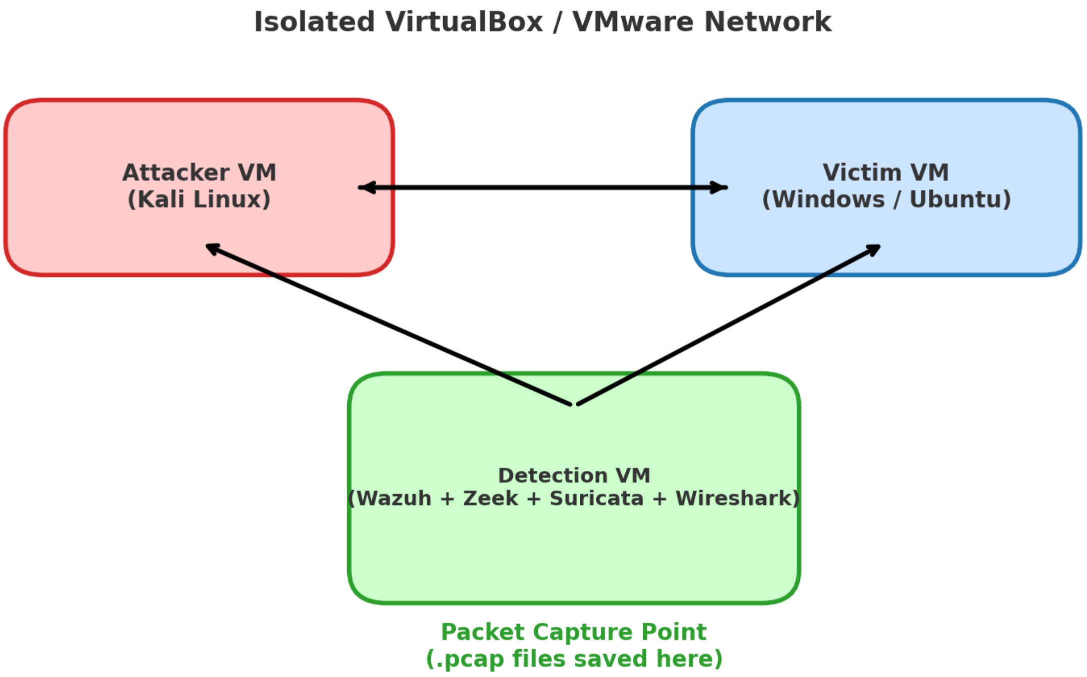
SOC Lab & Packet Capturing Project – Full Enterprise-Grade Documentation

This **complete project deliverable** contains everything needed to showcase your skills as a **SOC Analyst** or **Threat Hunter**. It includes your **SOC lab setup**, **packet capturing workflow**, **bash commands**, **Sigma detection rules**, and a **GitHub-ready README**.

■ SOC Lab Setup Overview

- Runs on **VirtualBox** or **VMware** in an isolated environment.
- **Attacker VM** → Kali Linux for scanning, exploitation, and payload testing.
- **Victim VM** → Windows 11 / Ubuntu to simulate endpoints.
- **Detection VM** → Wazuh + Zeek + Suricata + Wireshark for detection and analysis.
- Generates `.pcap` files, triggers IDS alerts, and visualizes findings in Wazuh dashboards.

■ SOC Lab Network Diagram


Isolated VirtualBox / VMware Network
Attacker VM (Kali Linux)
Victim VM (Windows / Ubuntu)
Detection VM (Wazuh + Zeek + Suricata + Wireshark)
Packet Capture Point (.pcap files saved here)

■ Packet Capturing Commands

Wireshark Capture Filters

```
# Capture only your device traffic by IP
host 192.168.0.105

# Capture only your device traffic by MAC
ether host 08:00:27:36:1b:5a
```

tcpdump Commands

```
# Capture traffic by IP address
sudo tcpdump -i wlan0 host 192.168.0.105 -w my_device_traffic.pcap

# Capture traffic by MAC address
sudo tcpdump -i wlan0 ether host 08:00:27:36:1b:5a -w my_device_traffic.pcap

# Open captured packets in Wireshark
wireshark my_device_traffic.pcap
```

■ Wireshark Filters Cheat Sheet

Goal	**Capture Filter**	**Display Filter**
My device only	host 192.168.0.105	ip.addr == 192.168.0.105
My device only (MAC)	ether host 08:00:27:36:1b:5a	eth.addr == 08:00:27:36:1b:5a
Only DNS traffic	port 53	dns
Only HTTPS traffic	port 443	tls

■■■■■ Custom Sigma Detection Rules Pack

Nmap Scan Detection via Zeek

```
title: Nmap Scan Detection via Zeek
id: 001-jaysolex-nmap-scan
logsource:
  product: zeek
  service: conn
detection:
  selection:
    history|contains: "S"
    conn_state: "S0"
    orig_bytes: 0
    resp_bytes: 0
  condition: selection
level: high
tags: [attack.discovery, attack.t1046]
```

PowerShell Reverse Shell Detection

```
title: PowerShell Reverse Shell Indicators
id: 002-jaysolex-reverse-shell
logsource:
  product: windows
  service: powershell
```

```
detection:
  selection:
    EventID: 4104
    ScriptBlockText|contains:
      - "New-Object Net.Sockets.TCPClient"
      - "Invoke-Expression"
      - "FromBase64String"
      - "IEX"
  condition: selection
level: critical
tags: [attack.command_and_control, attack.t1059.001]
```

Suspicious Packet Capture Activity

```
title: Suspicious Packet Capture Activity
id: 003-jaysolex-pcap
logsource:
  product: linux
  service: sysmon
detection:
  selection:
    EventID: 1
    Image|endswith:
      - "/tcpdump"
      - "/tshark"
    TargetFilename|contains:
      - "/home"
      - "/tmp"
  condition: selection
level: medium
tags: [attack.collection, attack.t1040]
```

DNS Tunneling or C2 Beaconing

```
title: DNS Tunneling or Beaconing
id: 004-jaysolex-dns
logsource:
  product: zeek
  service: dns
detection:
  selection:
    query|re: '([A-Za-z0-9]{30,}\.){3,}'
  condition: selection
level: high
tags: [attack.command_and_control, attack.t1071]
```

■ GitHub README Template

```
# ■■ SOC Lab & Packet Capturing Project

![Wireshark](https://img.shields.io/badge/Wireshark-Packet_Analysis-007ACC?logo=wireshark)
![tcpdump](https://img.shields.io/badge/tcpdump-Capture_Traffic-FF9800?logo=linux)
![Zeek](https://img.shields.io/badge/Zeek-Network_Analysis-009688?logo=gnu-bash)
![Suricata](https://img.shields.io/badge/Suricata-IDS/IPS-FF5722?logo=suricata)
![Wazuh](https://img.shields.io/badge/Wazuh-SIEM-673AB7?logo=wazuh)

## ■ Project Overview
This project simulates **real cyberattacks** using **Kali Linux** against **Windows/Ubuntu victims** and cap

## ■ SOC Lab Architecture
Include the diagram: `SOC_Lab_Network_Diagram.png`

## ■ Sigma Detection Rules
```

```
- Nmap Scan Detection
- PowerShell Reverse Shell
- Suspicious `.pcap` Captures
- DNS Tunneling Detection

## ■ Download Documentation
[■ SOC_Lab_Packet_Capturing_Project_With_Sigma_Rules.pdf](SOC_Lab_Packet_Capturing_Project_With_Sigma_Rules.
```

This upgraded project now includes **custom Sigma detection rules**. Upload this PDF, your `.pcap` files, diagram, and Sigma rules to GitHub for a **portfolio-ready SOC project**.