Personal SOC Lab Portfolio – Pruthviraj Chavan

# 1. Introduction

I am highly dedicated to the field of cybersecurity, with a strong foundation built through real hands-on experience and formal certifications.   
I have completed the STAR Cyber Security Certification, CompTIA A+, Network+, and hold a Red Hat certification for Linux systems.  
  
In my previous role, I managed and configured Sophos firewalls, giving me direct exposure to network security in a corporate environment.  
  
Driven by my passion to grow deeper into the world of detection and response, I’ve built my own SOC lab at home.   
This lab allows me to simulate real-life scenarios, understand how security events are generated, and practice how alerts are handled,   
investigated, and mitigated — just like in a real-world Security Operations Center.  
  
My goal is to become a professional SOC Analyst with strong skills in log analysis, threat detection, and incident response.

# 2. Lab Setup Overview

To gain real-world, hands-on experience in monitoring and incident response, I set up a virtual SOC lab using VirtualBox on my host machine.   
The lab is fully isolated and uses static IPs within the 192.168.5.1/24 network.

Lab Components:  
- Wazuh Manager (Ubuntu Server): SIEM and dashboard  
- Windows 11: Endpoint with Wazuh Agent and Sysmon  
- Kali Linux: Attacker VM with Hydra, Nmap, etc.  
  
Key Features:  
- Sysmon on Windows for deep logging  
- Wazuh agents on all endpoints  
- Wazuh dashboard monitoring real-time logs

# 3. Wazuh Deployment

To centralize event collection and alerting, I deployed Wazuh on an Ubuntu Server VM as the core of my SOC lab.  
  
- Operating System: Ubuntu Server (no GUI)  
- Wazuh Version: 4.x (offline installation)  
- Installation Method: wazuh-install.sh script  
- Deployment Type: All-in-one (Manager, Dashboard, Filebeat, Elasticsearch)  
- Ports Used: 1514/UDP, 1515/TCP  
  
Dashboard Access:  
- Accessed via browser over HTTPS  
- Admin credentials reset securely

# 4. Windows Agent + Sysmon Integration

Wazuh agent was installed on Windows 11 and registered using a key from the manager.   
Sysmon was installed and configured with SwiftOnSecurity’s configuration file for deep system-level logging.  
  
Collected Events:  
- Event ID 1 – Process Creation  
- Event ID 3 – Network Connections  
- Event ID 10 – Process Access  
- Event ID 4625 – Failed Logon  
  
Tested Encoded PowerShell Command:  
powershell -EncodedCommand aGVsbG8gd29ybGQ=

# 5. Simulated Attack & Detection

Simulated a brute-force attack using Hydra from Kali Linux to SMB on Windows 11.  
  
Command Used:  
hydra -l administrator -p WrongPass123 -t 4 smb://192.168.5.11  
  
Detection:  
- Windows Event ID 4625 captured  
- Source: NtLmSsp and AuthenticationPackageName: NTLM  
- Detected by Wazuh using rule ID 18107 (invalid login)  
- Alert Level: 5

# 6. Roadmap & Next Steps

I plan to expand the lab with:  
  
MITRE ATT&CK Mapping:  
- Map detection rules to real-world adversary tactics and techniques  
  
Custom Detection Rules:  
- Build Sigma-based and manual Wazuh rules to detect:  
 - PowerShell abuse  
 - Registry persistence  
 - Suspicious network activity

# 7. Conclusion

Building this SOC lab has been a powerful learning experience.   
It has helped me simulate attacks, analyze log data, and create meaningful detections using open-source tools.  
  
I now have hands-on experience with SIEM technology, threat detection, and incident response workflows.   
I will continue refining my skills with frameworks like MITRE ATT&CK and rule writing to grow into a professional SOC Analyst.