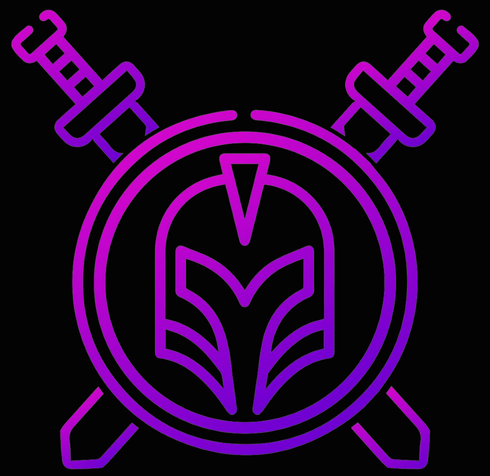
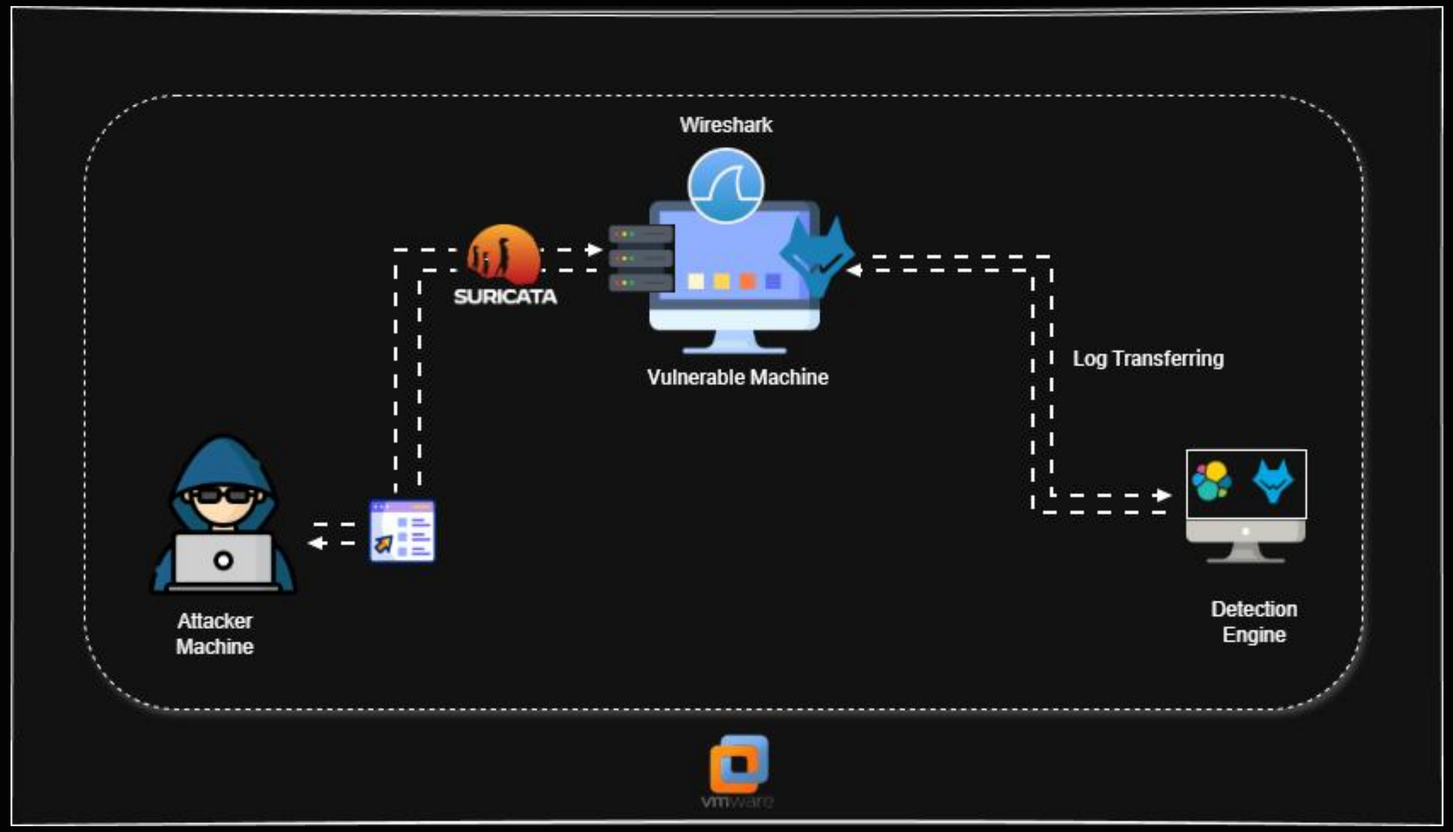
CWL
CyberWarFare Labs

Purple Team Fundamentals - Community Edition (PTF)



COMMUNITY EDITION

Purple Team Fundamentals - Community Edition (PTF) Architecture



CWL
CyberWarFare Labs

I. Introduction

II. Adversary Simulation and Detection Overview

2.1 Learning Red Team Perspective

2.2 Learning Blue Team Perspective

2.3 Adversary Simulation

2.4 Key aspects of Adversary Simulation

2.5 Adversary Detection

2.6 Key Aspects of Adversary Detection

III. Threat Intelligence and Defensive Frameworks

3.1 MITRE ATT&CK Framework

3.2 Understanding TTPs

3.3 Understanding IOC and IOA

3.4 MITRE D3FEND Framework

IV. Lab Planning and Setup

4.1 Lab Architecture

4.2 Lab Overview

4.3 Lab Requirement

4.4 Lab Setup and Deployment

4.5 VM Configuration and Deployment

4.6 Network Adaptor Configuration

4.7 Configuration of Bridged and Internal Network

V. Security Tools and Monitoring Setup

5.1 Security Solution Deployment

5.2 SIEM: Wazuh + ELK

5.3 Suricata: IDS/IPS

5.4 Wireshark: Network Monitoring

VI. Lab Exercise

6.1 Joint Operations in SImulated Lab

6.2 Web based Attack Detection

6.3 Network Based Attack Detection

CWL
CyberWarFare Labs

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live