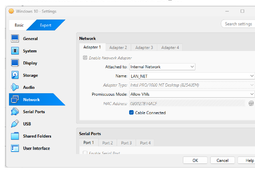
Cybersecurity Homelab & Attack Simulation - Detailed Report

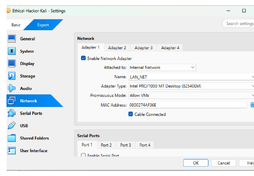
This document provides a comprehensive overview of a cybersecurity homelab setup and the subsequent attack simulations conducted within that environment. The report details the step-by-step process of configuring a pfSense router with Suricata for intrusion detection, as well as the execution of various attack simulations using tools like Nmap, Hydra, and Netcat. The goal is to demonstrate the effectiveness of the homelab setup in detecting and responding to common cybersecurity threats.

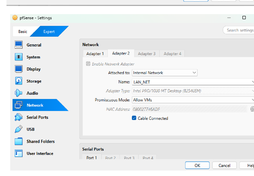
Project 1: Step-by-Step pfSense + Suricata Homelab Setup

Step 1: Create Virtual Machines in VirtualBox

- Created three VMs:
  - **pfSense** (router/IDS)
  - **Kali Linux** (attacker)
  - **Windows 10** (target)
- All VMs connected to the same Internal Network: **LAN_NET**

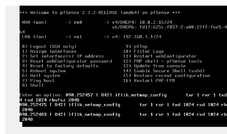






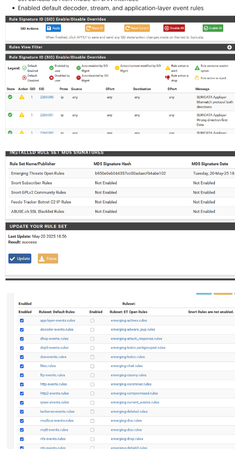
Step 2: Install and Configure pfSense

- Assigned two adapters:
  - **Adapter 1**: NAT for Internet
  - **Adapter 2**: Internal Network
- Configured LAN interface with static IP **192.168.1.1**
- Enabled DHCP for automatic IP assignment



Step 3: Install and Enable Suricata on pfSense

- Installed Suricata via pfSense package manager
- Set Suricata to Alert mode on LAN interface
- Enabled default decoder, stream, and application-layer event rules



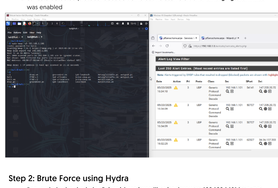
Step 4: Add Kali and Windows VMs to LAN_NET

- Kali got IP **192.168.1.100**
- Windows got IP **192.168.1.101**
- Both verified with **ping** and **ipconfig/ifconfig**

Project 2: Step-by-Step Attack Simulation & Detection

Step 1: Port Scanning using Nmap

- Ran: **sudo nmap -sS 192.168.1.101** from Kali
- Suricata detected protocol decode traffic but no scan alert until **emerging-scan.rules** was enabled

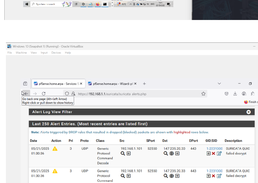


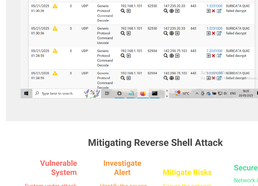
Step 2: Brute Force using Hydra

- Ran: **sudo hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.101 http-get**
- Suricata generated an alert once **http-events** and **auth.rules** categories were active

Step 3: Reverse Shell Simulation

- Started Netcat on Kali: **nc -nvlp 4444**
- Ran PowerShell payload on Windows to connect to Kali
- Connection established, verified with **whoami** in Kali
- Suricata did not alert on this until **shellcode rules** were enabled





This report outlines the successful setup and testing of a cybersecurity homelab, demonstrating the capabilities of pfSense and Suricata in detecting various attack vectors. The findings highlight the importance of enabling specific rules within Suricata to ensure comprehensive monitoring and alerting for potential threats.