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.

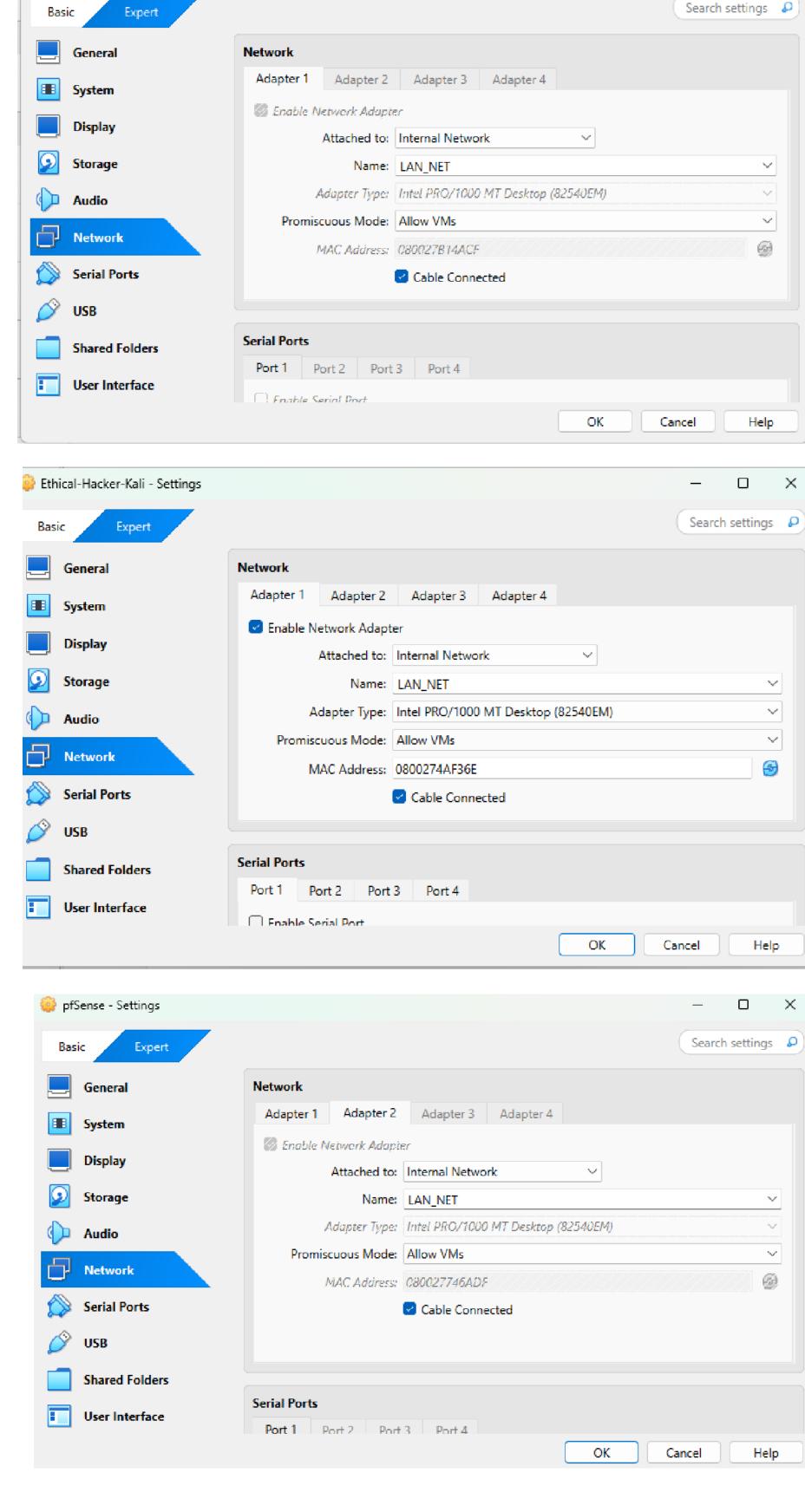
Project 1: Step-by-Step pfSense + Suricata Homelab Setup

• pfSense (router/IDS)

Step 1: Create Virtual Machines in VirtualBox

• Created three VMs:

- Kali Linux (attacker) • Windows 10 (target)
- All VMs connected to the same Internal Network: LAN_NET
- 🙀 Windows 10 Settings



*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

Step 2: Install and Configure pfSense

• Adapter 1: NAT for Internet

Adapter 2: Internal Network

• Enabled DHCP for automatic IP assignment

Configured LAN interface with static IP 192.168.1.1

WAN (wan)

• Assigned two adapters:

v6/DHCP6: fd17:625c:f037:2:a00:27ff:fee5:4da1/ LAN (lan) -> em1 -> v4: 192.168.1.1/24

3) Reset webConfigurator password

4) Reset to factory defaults

Rule Signature ID (SID) Enable/Disable Overrides

Rule Signature ID (SID) Enable/Disable Overrides

2260001

Apply

SID Actions

Rules View Filter

Legend: O Default

Enabled

Enabled

 \checkmark

 \checkmark

Ruleset: Default Rules

decoder-events.rules

dhcp-events.rules

dnp3-events.rules

dns-events.rules

files.rules

was enabled

up (0.0033s latency). scanned ports on 192.168.1.101 are in ignored states. s: 1000 filtered tcp ports (no-response) ess: 08:00:27:81:4A:CF (Oracle VirtualBox virtual NIC)

5) Reboot system

6) Halt system

-> em0

- 9) pfTop 0) Logout (SSH only) 10) Filter Logs 1) Assign Interfaces 2) Set interface(s) IP address Restart webConfigurator
- 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 090.252457 [842] iflib_netmap_config txr 1 rxr 1 txd 102 4 rxd 1024 rbufsz 2048 390.252475 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz 090.252483 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz Step 3: Install and Enable Suricata on pfSense • Installed Suricata via pfSense package manager Set Suricata to Alert mode on LAN interface

-> v4/DHCP4: 10.0.2.15/24

12) PHP shell + pfSense tools

14) Enable Secure Shell (sshd)

15) Restore recent configuration

13) Update from console

Default Auto-disabled by SID Disabled user Mgmt **DPort**

State Action GID SID Proto Destination

Auto-enabled by SID

2260000 SURICATA Applayer any any Mismatch protocol both directions

• Enabled default decoder, stream, and application-layer event rules

C Reset Curren

Action/content modified by SID

When finished, click APPLY to save and send any SID state/action changes made on this tab to Suricata.

Rule action is

Rule action is

alert

drop

Enable All

Rule contains noalert

🕛 Rule action is reject

SURICATA Applayer

Snort Rules are not enabled.

Last 250 Alert Entries. (Most recent entries are listed first)

Alert Log View Filter

05/20/2025

05/20/2025 🔔

16:34:09

https://192.168.1.1/suricata/suricata_alerts.php

Command Decode

Protocol

Generic

Protocol

Command

192.168.1.101 54141 147.235.20.72 443

192.168.1.101 50707 147.235.20.72 443

192.168.1.101 50707 147.235.20.72 443

192.168.1.101 62327 34.36.137.203 443

-5 sudo nmap -51 192.1981.101
sudol password for kali:
starting haup 7.94 (https://nmap.org) at 2025-05-20 15:36 UTC
map scan report for 192.168.1.101
nost is up (0.0000Has latency).
tt 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 (litered top ports (no-response)
MC Address: 08:00:27:81:4A:CF (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 21.22 seconds

—(kali⊕Kali)-[-] 5 nc -nvlp 4444 istening vn [any] 4444 ... onnect to [192.168.1.100] from (UNKNOWN) [192.168.1.101] 55092

- (mail o Nath) - [-] -5 nc mulp 4444 istening on [any] 4444 ... onnect to [192.168.1.100] From (UNKNOWN) [192.168.1.101] 55250

Network integrity

ensured

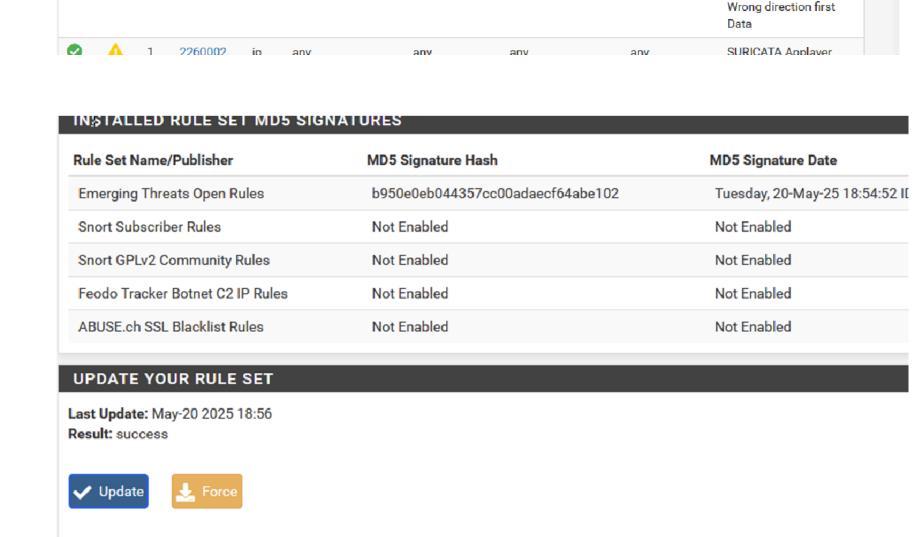
Q # E

Q 🌐 🕀

option

Message

0



Ruleset:

Ruleset: ET Open Rules

emerging-botcc.rules

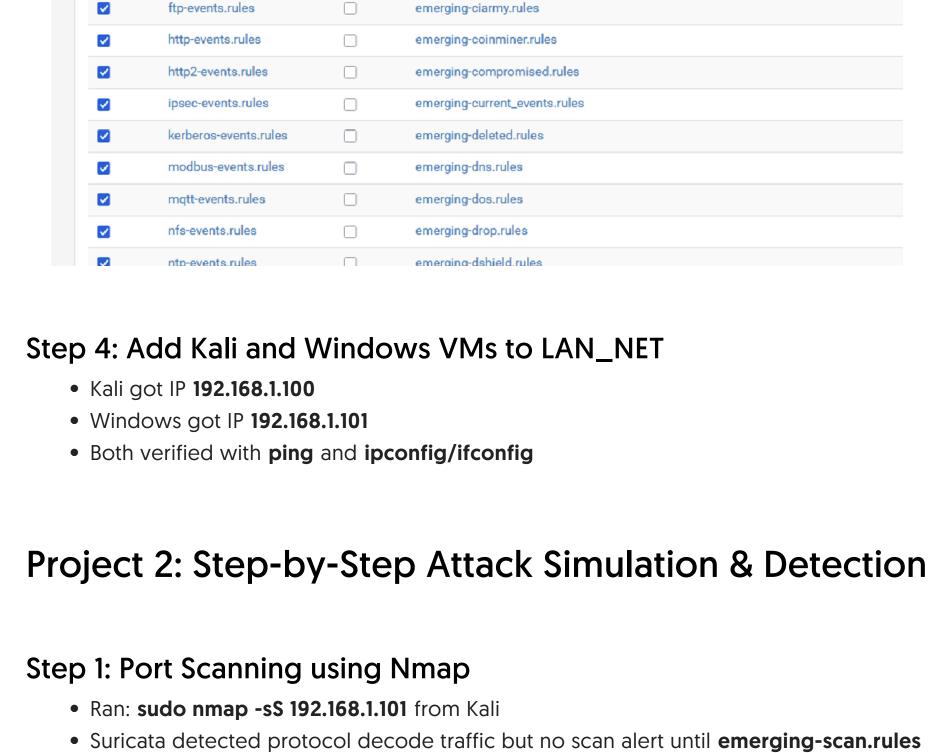
emerging-chat.rules

emerging-adware_pup.rules

emerging-attack_response.rules

emerging-botcc.portgrouped.rules

Enabled



05/20/2025 🛕 16:32:25

• Ran PowerShell payload on Windows to connect to Kali

• Connection established, verified with **whoami** in Kali

Step 2: Brute Force using Hydra

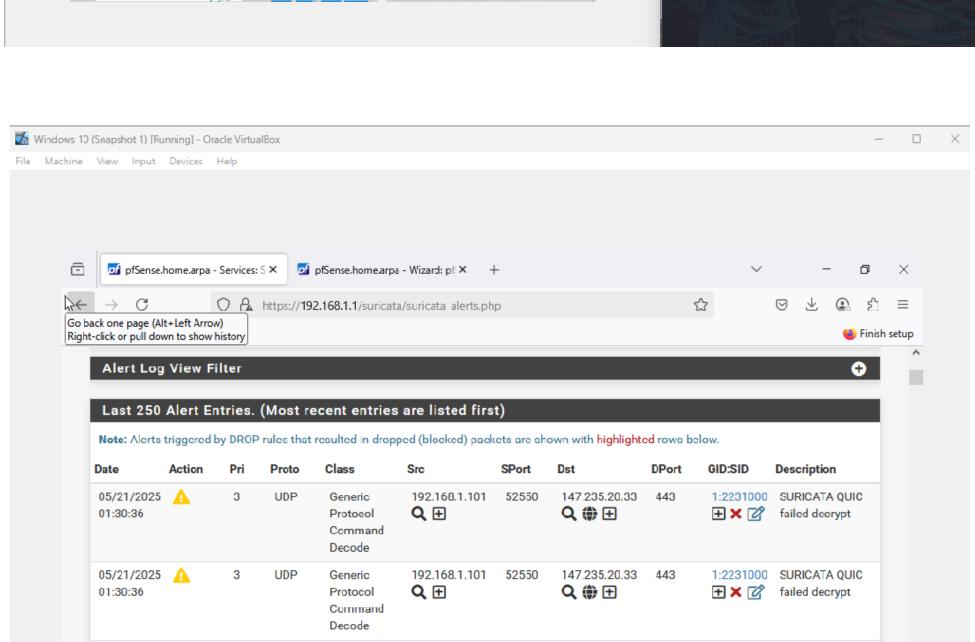
Step 3: Reverse Shell Simulation

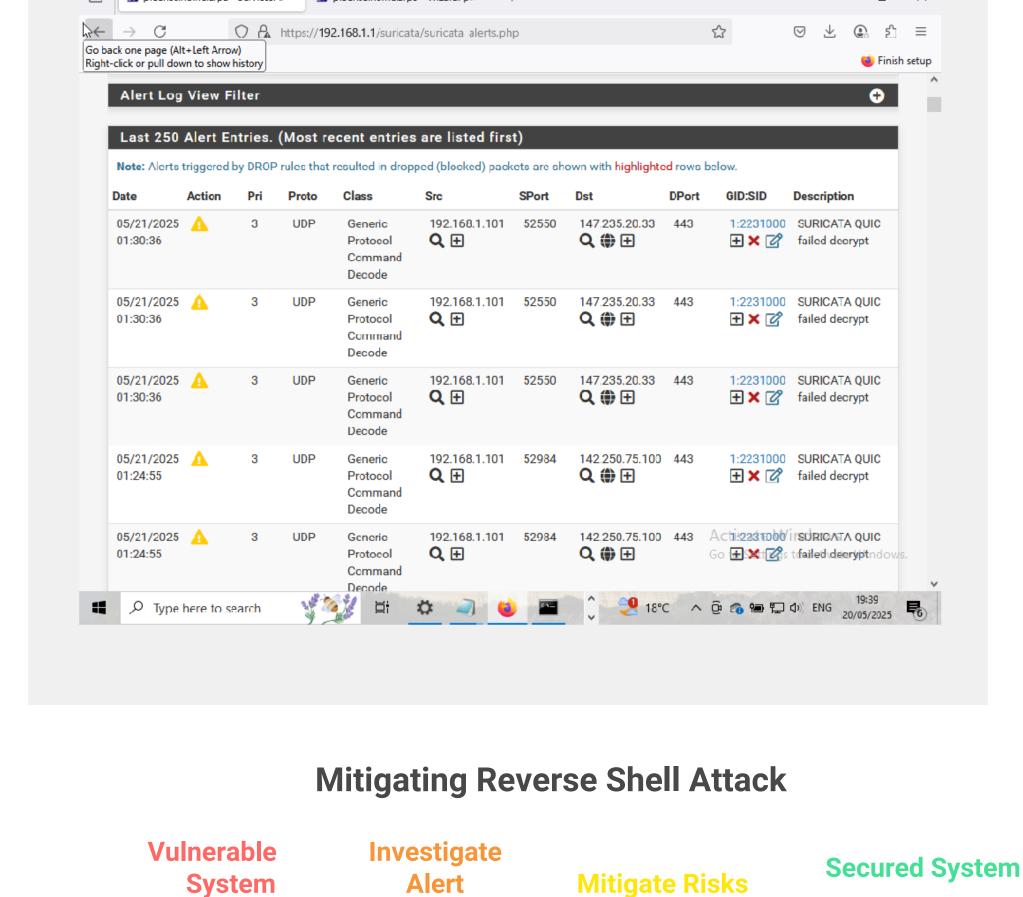
• Started Netcat on Kali: nc -nvlp 4444

• Suricata did not alert on this until shellcode rules were enabled

• 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







Secure the network

comprehensive monitoring and alerting for potential threats.

Alert

Identify the source

System

System under attack