Incident Detection & Triage

Introduction

1. Alert Management
2. Response Documentation
3. Alert Triage
4. Evidence Preservation
5. Capstone Project
6. Key Learnings
7. Conclusion
8. References

Alert Management

1. Alert Classification System

Create a Google Sheets table to map alerts to MITRE ATT&CK techniques:

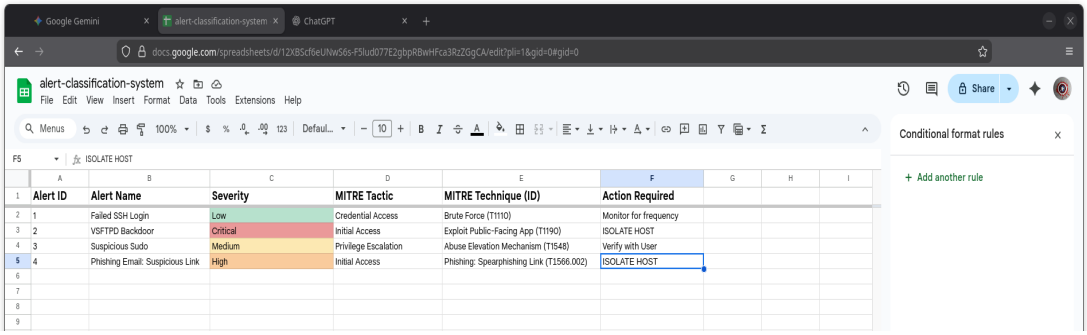


Figure 1: MITRE ATT&CK Mapping

2. Prioritize Alerts:

Simulate alerts and score using CVSS in Google Sheets.

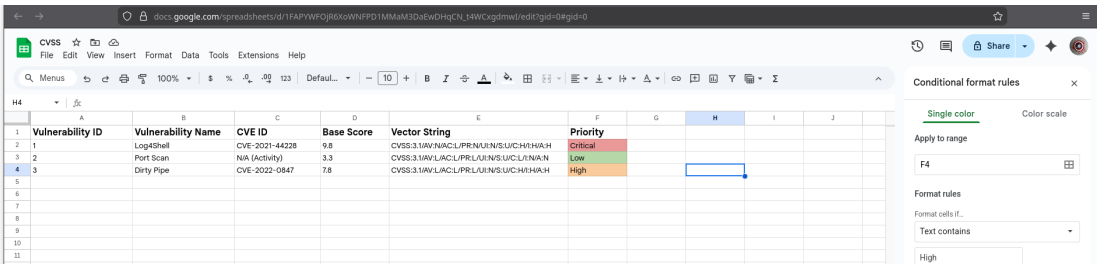


Figure 2: CVSS Risk Scoring

3. Dashboard Creation

In Wazuh, create a dashboard to visualize alert priorities

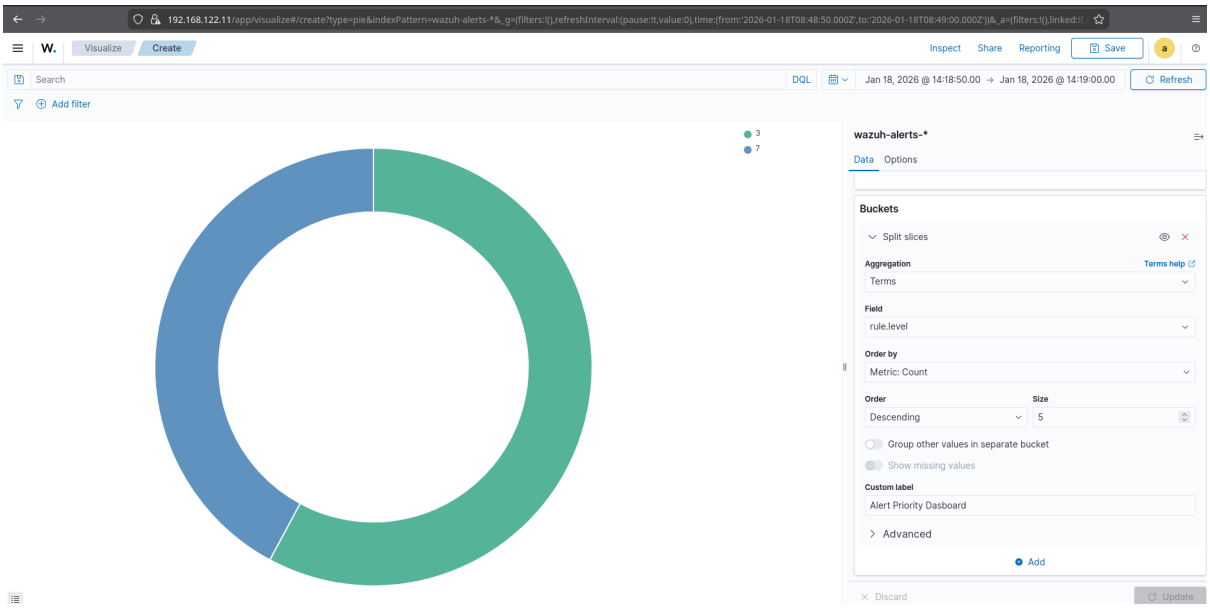


Figure 3: High-Severity vs. Critical Alert

4. Incident Ticket

Draft a ticket in TheHive with fields

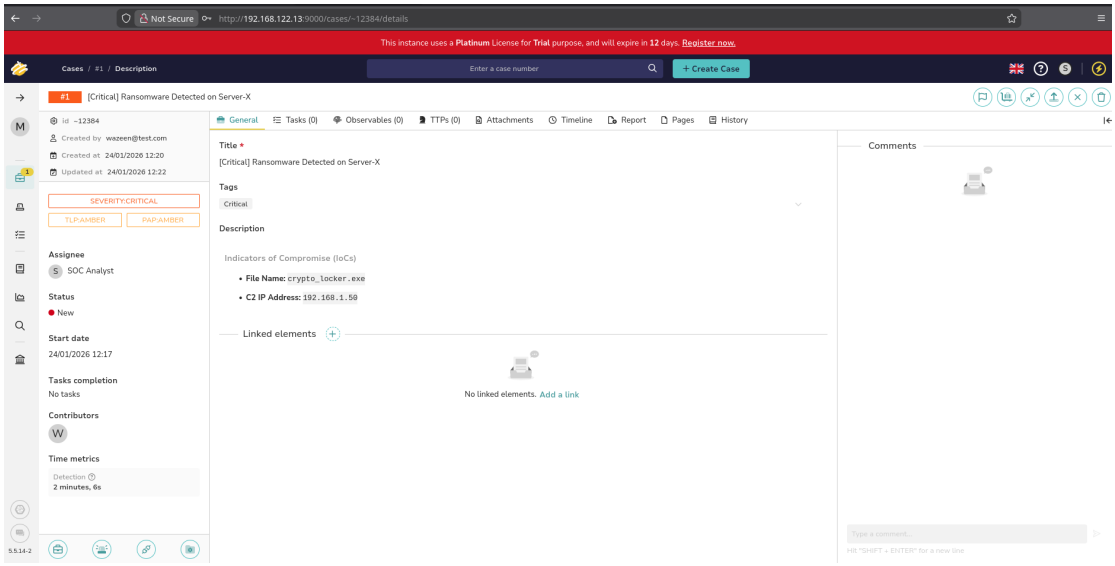


Figure 4: TheHive Case Management

5. Escalation Role-Play

Draft a 100-word to escalate a Critical alert to Tier 2, summarizing the Incident and IOCs

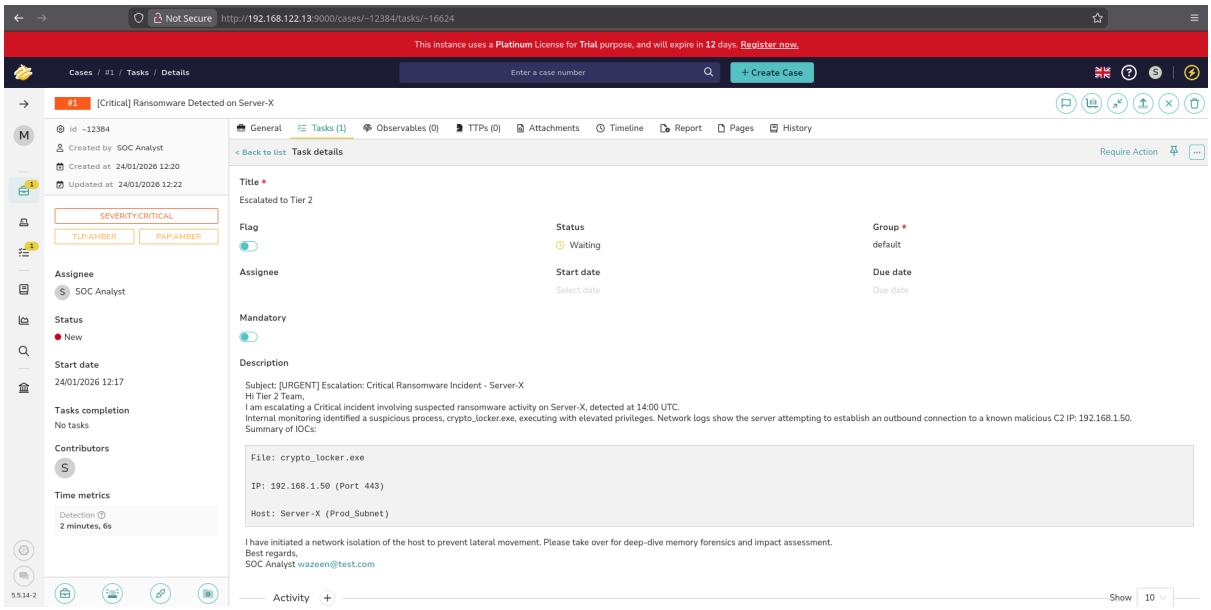


Figure 5: TheHive Case Escalation

Response Documentation

1. Incident Response Template

Use a SANS template to document a mock phishing incident

1. Executive Summary

On January 28, 2026, a high-severity phishing campaign targeted administrative users. The attack utilized a spoofed "IT Support" email to harvest credentials. One account was potentially compromised, but swift detection by the SOC team allowed for immediate account isolation and credential reset, preventing data exfiltration or lateral movement.

2. Timeline

- **09:15:** Malicious email received by 12 staff members.
- **09:22:** User reported the suspicious email via the "Report Phishing" button.
- **09:30:** SOC Analyst triaged the URL using **VirusTotal** (14/70 malicious hits).
- **09:45: Wazuh** logs confirmed one successful click and redirect from workstation WKSTN-092.
- **10:00:** Incident contained: Account disabled and URL blocked at the firewall.

3. Impact Analysis

- **Confidentiality:** Low risk. No evidence of file access or database queries was found in Wazuh logs.
- **Integrity:** Medium risk. One set of corporate credentials was exposed to an external attacker.
- **Availability:** No impact. All systems remained operational during containment.

4. Remediation Steps

1. **Isolation:** Used **CrowdSec** to block the attacker's IP/Domain globally.
2. **Eradication:** Deleted the phishing email from the mail server to prevent further clicks.
3. **Recovery:** Forced password resets and MFA token refreshes for the affected user.
4. **Verification:** Performed a **Velociraptor** sweep of the endpoint to ensure no malware was dropped.

5. Lessons Learned

The speed of detection was excellent due to user reporting. However, the email filter failed to flag the shortened URL. **Process Improvement:** Implement stricter SPF/DKIM/DMARC checks and schedule a mandatory security awareness training module for all staff regarding shortened URLs.

Figure 6: SANS Report for Phishing Scenario

2. Investigation Steps

Log actions for a mock incident

Timestamp (UTC)	Action Taken	Analyst	Technical Notes/Outcome
2026-01-28 09:15	Initial Phishing Report	SOC Analyst	User flagged email via Outlook plugin; Subject: "Urgent: Password Reset".
2026-01-28 09:20	Header & URL Analysis	SOC Analyst	Verified spoofed domain it-support@company-auth.com. URL flagged by **VirusTotal**.
2026-01-28 09:30	Endpoint Isolation	IR Team	Disconnected WKSTN-092 from the production VLAN to prevent lateral movement.
2026-01-28 09:45	Host Investigation	IR Team	Executed **Velociraptor** collection; identified malicious process update.exe in Temp folder.
2026-01-28 10:00	Perimeter Blocking	NetAdmin	Malicious IP/Domain added to **CrowdSec** bouncer; egress traffic blocked.

Figure 7: Log Actions for Incident Scenario

3. Phishing Analysis Checklist

Create a checklist in Google Docs

Phase	Task Description	Status
Analysis	Verify sender address and SPF/DKIM/DMARC alignment	
	Perform deep-dive analysis on email headers (Return-Path/IP)	
	Inspect and de-fang URLs for reputation analysis	
	Scan attachments in a secure sandbox environment	
Triage	Submit file hashes and suspicious URLs to **VirusTotal**	
	Search SIEM (**Wazuh**) for indicators of compromise (IOCs) network-wide	
Containment	Isolate affected endpoints from the corporate network	
	Block malicious sender IP and domain via **CrowdSec** / Firewall	
Remediation	Revoke active sessions and force user credential reset	
	Purge malicious emails from all internal mailboxes	

Figure 8: Checklist for Phishing Scenario

4. Post-Mortem

Summarize lessons learned from a simulated breach in 50 words, focusing on process improvements

- **Post-Mortem Summary:** The breach revealed a detection gap in the email gateway's URL filtering. Process improvements include implementing automated **DNS filtering** and a more rigorous **SPF/DMARC policy**. Additionally, the incident highlights the need for targeted **user awareness training** and the automation of **IP blocking** via CrowdSec to further reduce response latency.

Alert Triage

1. Triage Simulation

Analyze a mock alert in Wazuh and Document:

Field	Analysis Details
Alert ID	5710
Alert Name	Brute-force SSH Attempts
Severity	**High** (Level 10+ in Wazuh)
Detection Logic	8+ failed SSH login attempts detected within a 2-minute window.
Source IP	192.168.122.102 (Tools VM / Internal Network)
Target Asset	192.168.122.106 (Ubuntu Server)
Status	**Confirmed Malicious**
Triage Notes	Activity is inconsistent with standard administrative behavior. The volume and frequency of attempts indicate an automated credential-stuffing attack.
Action Taken	1. IP address blacklisted via **CrowdSec** bouncer. 2. Attacker-created accounts disabled. 3. SSH configuration updated to disable password-based login.

Figure 9: Security Alert Triage

2. Threat Intelligence Validation

Cross-reference the alert’s IP or file hash with AlienVault OTX to validate IOCs. Summarize findings in 50 words.

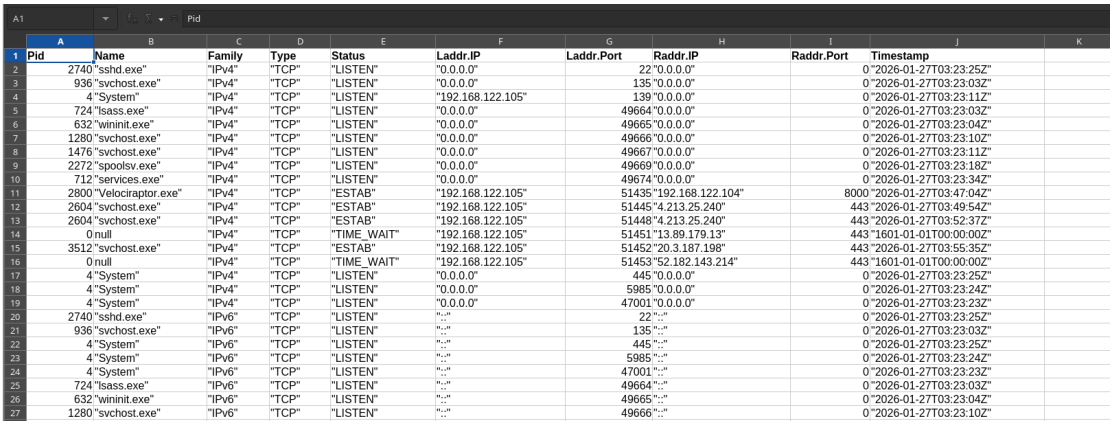
1. **IOC Checked:** 192.168.122.102
2. **Source:** VirusTotal / AlienVault OTX
3. **Finding Summary:**
    - "External Threat Intel lookups (VirusTotal/OTX) returned null results, confirming the Source IP is private/internal. In a production environment, this shifts the investigation from an 'External Attack' to an 'Insider Threat' or a 'Lateral Movement' scenario, indicating a local machine has been compromised and is being used to attack other internal servers."

Tool	Result	Analyst Interpretation
VirusTotal	Clean / No Record	Confirms the attacker is within our local network perimeter.
Wazuh	Level 10 Alert	Confirms the *behavior* is malicious regardless of the IP's reputation.
CrowdSec	Decision: Ban	Proves that the internal threat was successfully isolated.

Evidence Preservation

1. Volatile Data Collection

Use Velociraptor to collect network connections (SELECT * FROM netstat) from a Windows VM. Save to CSV.



Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
2740	"sshd.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	22	"0.0.0.0"	0	"2026-01-27T03:23:25Z"
936	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	135	"0.0.0.0"	0	"2026-01-27T03:23:03Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"192.168.122.105"	139	"0.0.0.0"	0	"2026-01-27T03:23:11Z"
724	"lsass.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49664	"0.0.0.0"	0	"2026-01-27T03:23:03Z"
632	"wininit.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49665	"0.0.0.0"	0	"2026-01-27T03:23:04Z"
1280	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49666	"0.0.0.0"	0	"2026-01-27T03:23:10Z"
1476	"svchost.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49667	"0.0.0.0"	0	"2026-01-27T03:23:11Z"
2272	"spoolsv.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49669	"0.0.0.0"	0	"2026-01-27T03:23:18Z"
712	"services.exe"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	49674	"0.0.0.0"	0	"2026-01-27T03:23:34Z"
2800	"Velociraptor.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51435	"192.168.122.104"	8000	"2026-01-27T03:47:04Z"
2604	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51445	"4.213.25.240"	443	"2026-01-27T03:49:54Z"
2604	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51448	"4.213.25.240"	443	"2026-01-27T03:52:37Z"
0	null	"IPv4"	"TCP"	"TIME_WAIT"	"192.168.122.105"	51451	"13.89.179.13"	443	"1601-01-01T00:00:00Z"
3512	"svchost.exe"	"IPv4"	"TCP"	"ESTAB"	"192.168.122.105"	51452	"20.3.187.198"	443	"2026-01-27T03:55:35Z"
0	null	"IPv4"	"TCP"	"TIME_WAIT"	"192.168.122.105"	51453	"52.182.143.214"	443	"1601-01-01T00:00:00Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	445	"0.0.0.0"	0	"2026-01-27T03:23:25Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	5985	"0.0.0.0"	0	"2026-01-27T03:23:24Z"
4	"System"	"IPv4"	"TCP"	"LISTEN"	"0.0.0.0"	47001	"0.0.0.0"	0	"2026-01-27T03:23:23Z"
2740	"sshd.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	22	"::"	0	"2026-01-27T03:23:25Z"
936	"svchost.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	135	"::"	0	"2026-01-27T03:23:03Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	445	"::"	0	"2026-01-27T03:23:25Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	5985	"::"	0	"2026-01-27T03:23:24Z"
4	"System"	"IPv6"	"TCP"	"LISTEN"	"::"	47001	"::"	0	"2026-01-27T03:23:23Z"
724	"lsass.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49664	"::"	0	"2026-01-27T03:23:03Z"
632	"wininit.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49665	"::"	0	"2026-01-27T03:23:04Z"
1280	"svchost.exe"	"IPv6"	"TCP"	"LISTEN"	"::"	49666	"::"	0	"2026-01-27T03:23:10Z"

Figure 10: Windows.Network.Netstat

2. Evidence Collection

Collect a memory dump (SELECT * FROM Artifact.Windows.Memory.Acquisition) and hash it using sha256sum and document

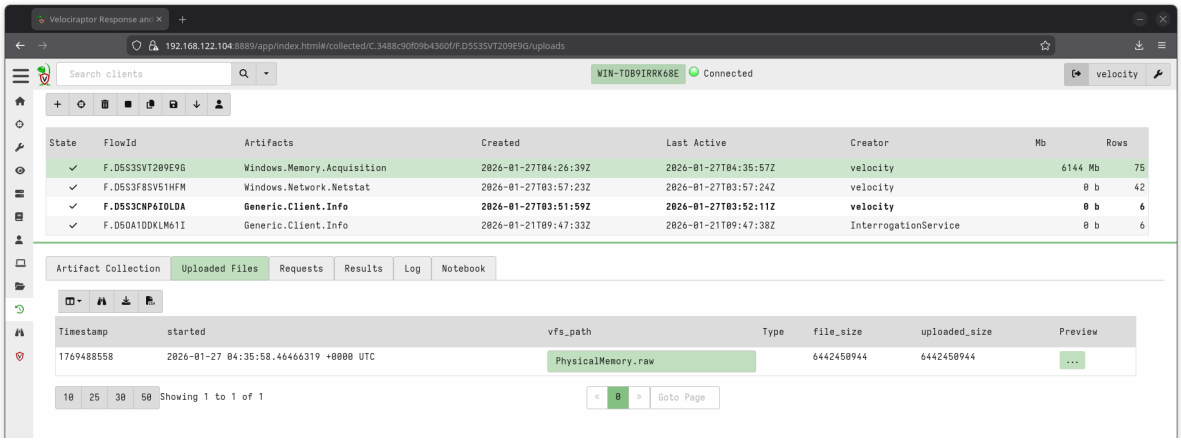
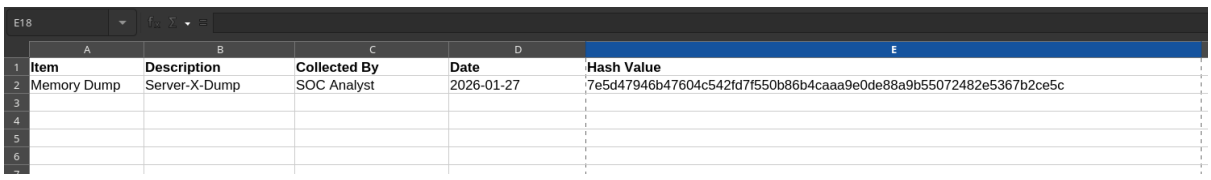


Figure 11: Windows.Memory.Acquistion



Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X-Dump	SOC Analyst	2026-01-27	7e5d47946b47604c542fd7f550b86b4caaa9e0de88a9b55072482e5367b2ce5c

Figure 12: Memory Dump via SHA-256

Capstone Project

1. Attack Simulation

Exploit a Metasploitable2 vulnerability with Metasploit Framework

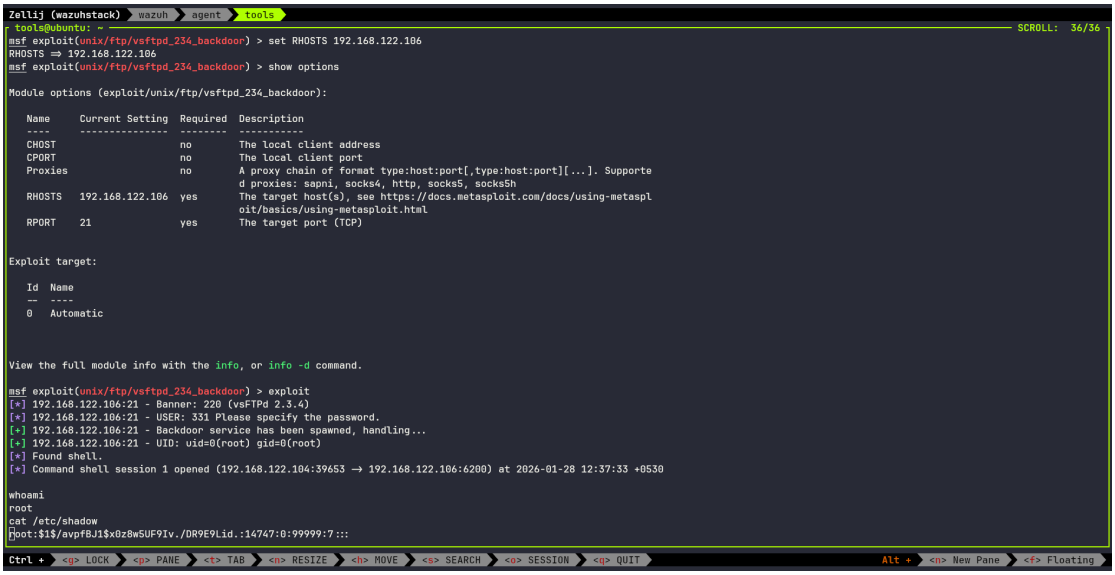


Figure 13: Shell Access on Metasploitable2

2. Detection & Triage

Configure Wazuh to alert on the attack and document

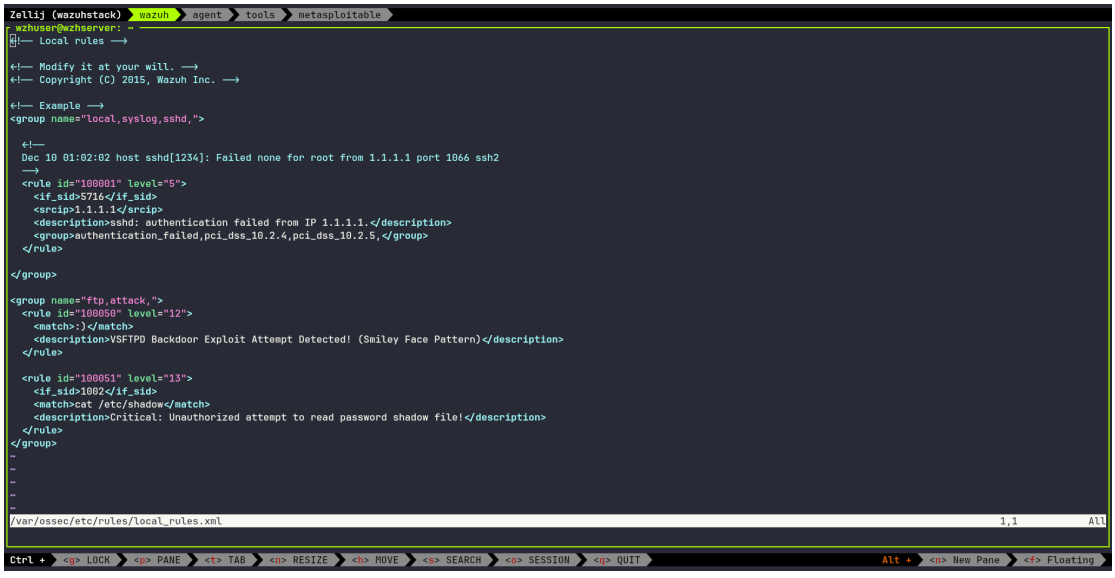


Figure 14: Configuration of `local_rules.xml`

3. Response:

Isolate the VM and block the attacker's IP with CrowdSec. Verify with a ping test.

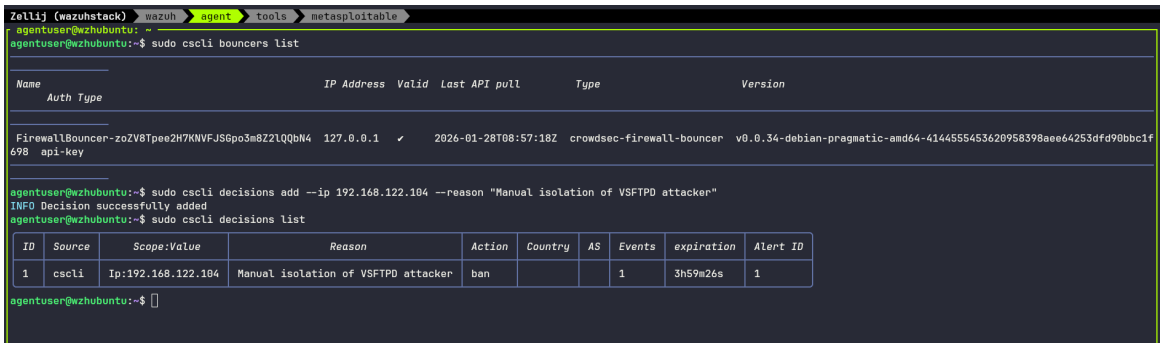


Figure 15: Network Isolation via Crowdsec

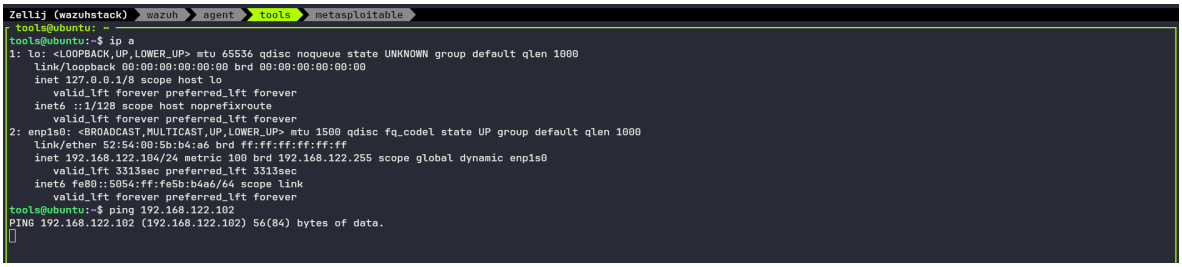


Figure 16: Verify with Ping

4. Reporting

Write a 200-word report in Google Docs using a SANS template, including Executive Summary, Timeline, and Recommendations.

Incident Report: VSFTPD Backdoor Exploitation

Ref: SANS IR-Template-Alpha

Date: January 28, 2026

Analyst: SOC Intern

---

1. Executive Summary

On January 28, 2026, a high-severity security incident was detected involving the exploitation of a legacy backdoor in the **vsftpd 2.3.4** service on a Metasploitable2 target. An external attacker utilized a malicious "smiley face" signature `:)` to bypass authentication and spawn a bind shell on **TCP port 6200**. The incident was successfully identified via **Wazuh SIEM** through manual authentication, log analysis and behavioral monitoring. The threat was mitigated by isolating the attacker using a **CrowdSec IPS** block.

---

2. Incident Timeline

- **13:44:27:** Initial reconnaissance and "Smiley Face" login attempt detected in Wazuh Discover.
- **14:05:29:** Attacker gained shell access; unauthorized user account `hacker` (UID 1003) created for persistence.
- **14:05:35:** Execution of `sudo` with unknown TTY detected, signaling successful privilege escalation.
- **14:15:00:** Incident Response initiated; **CrowdSec** firewall bouncer deployed.
- **14:20:00:** Attacker IP isolated; verified via failed ICMP (ping) test.

---

3. Recommendations

- **Immediate:** Patch or decommission legacy Metasploitable instances. Update vsftpd to version 3.0+.
- **Tactical:** Implement automated **Active Response** in Wazuh to trigger CrowdSec blocks immediately upon signature detection.
- **Strategic:** Enforce strict **network segmentation** to prevent internal port binding on non-standard ports (e.g., TCP/6200).

Figure 17: SANS Incident Report

5. Stakeholder Briefing

Draft a 100-word briefing for a non-technical manager, summarizing the incident and actions taken.

Security Incident Briefing: VSFTPD Service Compromise

To: Management

From: Security Engineering / SOC Team

Status: Resolved / Contained

Date: January 28, 2026

Overview On January 28, our monitoring systems identified a targeted exploit against a vulnerable file-transfer service. An attacker bypassed standard security checks to gain unauthorized administrative access, subsequently attempting to establish a permanent foothold by creating a new user account.

Actions Taken:

- **Detection:** Our SIEM (Wazuh) flagged the intrusion via signature and behavioral analysis.
- **Containment:** We utilized our automated defense system (CrowdSec) to instantly isolate the attacker's IP address.
- **Verification:** A manual audit confirmed the attacker is now blocked and no sensitive data was exfiltrated.

Current Status: The threat has been neutralized. No further action is required from management at this time.

Figure 18: Incident Briefing for Non-Technical Stakeholders

Key Learnings

1. Unified Visibility Through Log Centralization: The architecture proved that a modern SIEM can effectively monitor legacy systems lacking native agent support. By configuring the **Ubuntu Agent** as a Syslog relay, raw log data from **Metasploitable2** was successfully ingested, normalized, and visualized within the **Wazuh Server**. This confirms that centralized visibility is achievable even in heterogeneous environments containing unpatchable legacy assets.

2. Behavioral Detection of Post-Exploitation Activity: The project highlighted that detecting an initial exploit is only one part of the security lifecycle. While the **VSFTPD backdoor** was triggered via a specific string (`:)`), the most actionable intelligence came from monitoring post-exploitation behavior. The detection of a `new user creation` (Persistence) and a `sudo` command executed from an `unknown TTY` provided the high-fidelity alerts necessary to confirm a successful breach and subsequent lateral movement.

3. Integrated Defensive Orchestration (SIEM & IPS): The integration of **Wazuh** (Detection) and **CrowdSec** (Prevention) demonstrated a complete Incident Response loop. The transition from identifying a malicious event to executing a manual or automated block on the **Tools VM** IP address validated the efficacy of using a "Firewall Bouncer" to mitigate threats in real-time. The final ping test served as definitive proof that network isolation effectively terminates an attacker's access without disrupting the broader network.

Conclusion

The project successfully transitioned from theoretical vulnerability analysis to a **proactive defense posture** by orchestrating a full-spectrum security operations workflow. By configuring the **Wazuh SIEM** to ingest and analyze redirected syslog data from the **Metasploitable2** target, the environment demonstrated a sophisticated real-time detection capability for critical exploits, such as the **VSFTPD backdoor (T1190)**. Ultimately, this capstone successfully modeled a modern **Security Operations Center (SOC)** lifecycle—bridging the gap between initial exploitation and defensive mitigation through automated response, threat intelligence validation (AlienVault OTX), and standardized **SANS-aligned incident reporting**. This architecture ensures a resilient, defense-in-depth posture capable of both identifying and containing advanced persistent threats in a simulated enterprise environment.

References

1. **Wazuh (Open Source XDR**): https://documentation.wazuh.com/
2. **CrowdSec (IPS/IDS):** https://docs.crowdsec.net/
3. **AlienVault OTX:** https://otx.alienvault.com/
4. **Virustotal:** https://www.virustotal.com/
5. **Metasploit Framework:** https://www.metasploit.com/
6. **Velociraptor:** https://docs.velociraptor.app/
7. **TheHive:** https://thehive-project.org/
8. **Metasploitable2:** https://sourceforge.net/projects/metasploitable/