Red Teaming Week 2 – Practical Application Report

August 24, 2025

# 1. Threat Hunting with Open-Source Tools

Objective: Detect suspicious PowerShell activity using Elastic Security and Sigma rules.

Sigma Rule Example:

title: Suspicious PowerShell Activity  
logsource:  
 category: process\_creation  
 product: windows  
detection:  
 selection:  
 Image|endswith: '\powershell.exe'  
 CommandLine|contains: '-Command'  
 condition: selection

Threat Hunting Query Results (Elastic Security):

|  |  |  |  |
| --- | --- | --- | --- |
| Timestamp | Process | Command Line | Notes |
| 2025-08-18 10:00:00 | powershell.exe | -Command Write-Host | Suspicious execution |

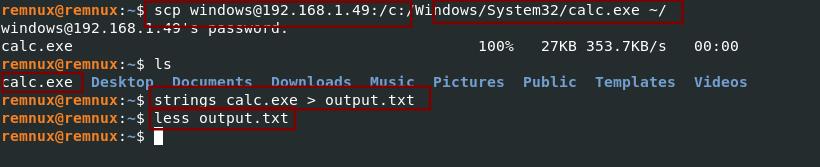
# 2. Malware Analysis Basics

Objective: Perform static and dynamic analysis on a benign executable (sample\_app.exe).

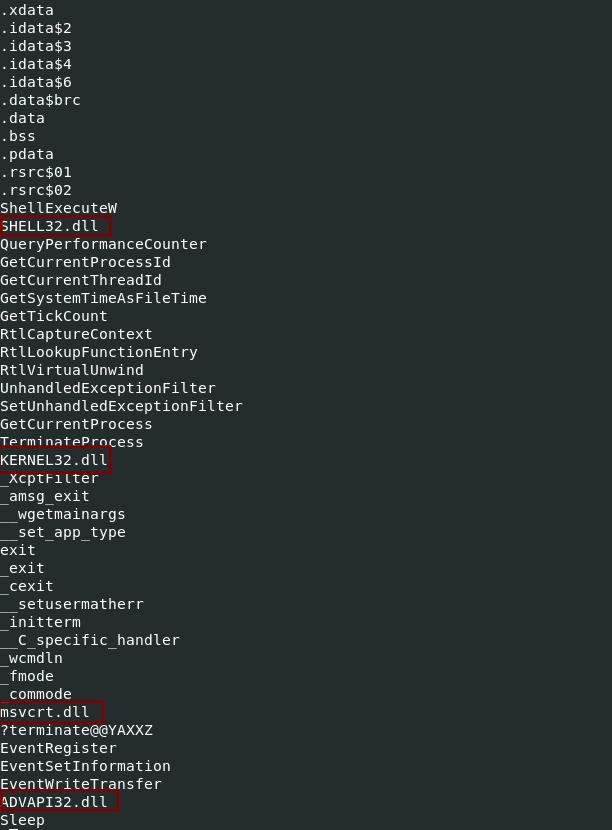
Findings:

- Static analysis revealed imports from KERNEL32.dll and USER32.dll, no obfuscation detected.

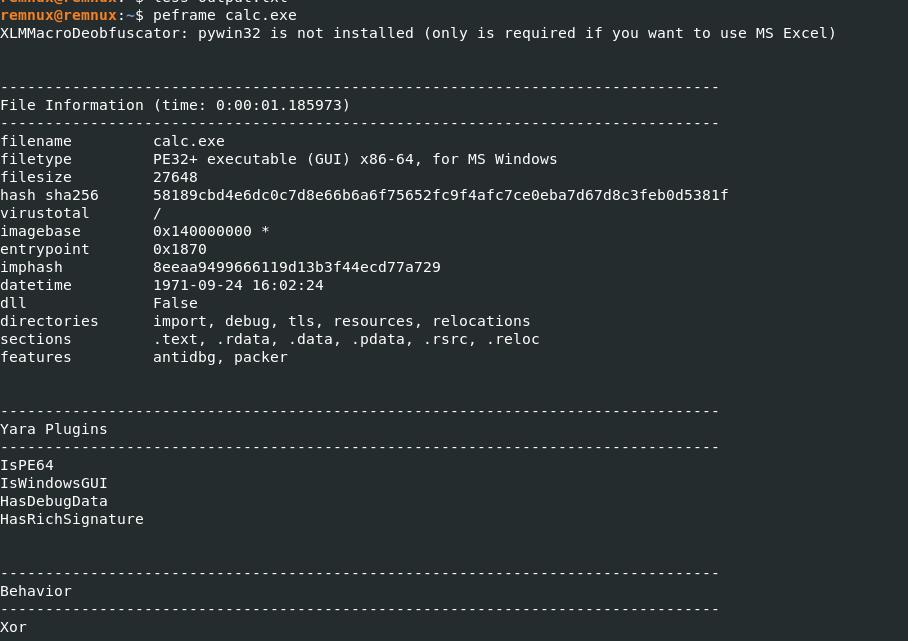
- Dynamic analysis showed normal GUI execution, no outbound traffic or persistence.



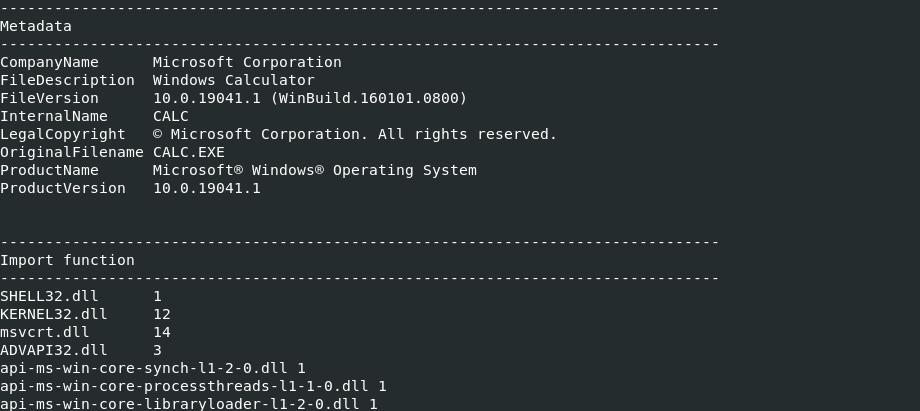
Screenshot: Malware Analysis result.



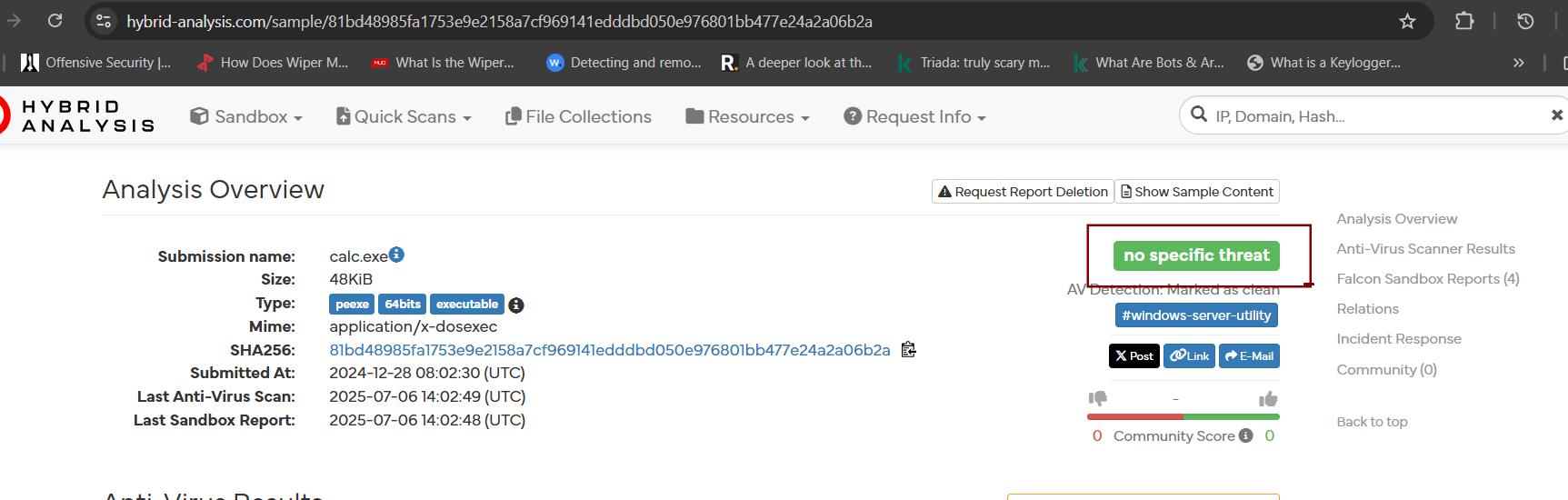
Screenshot: Malware Analysis result.



Screenshot: Malware Analysis result.



Screenshot: Malware Analysis result.

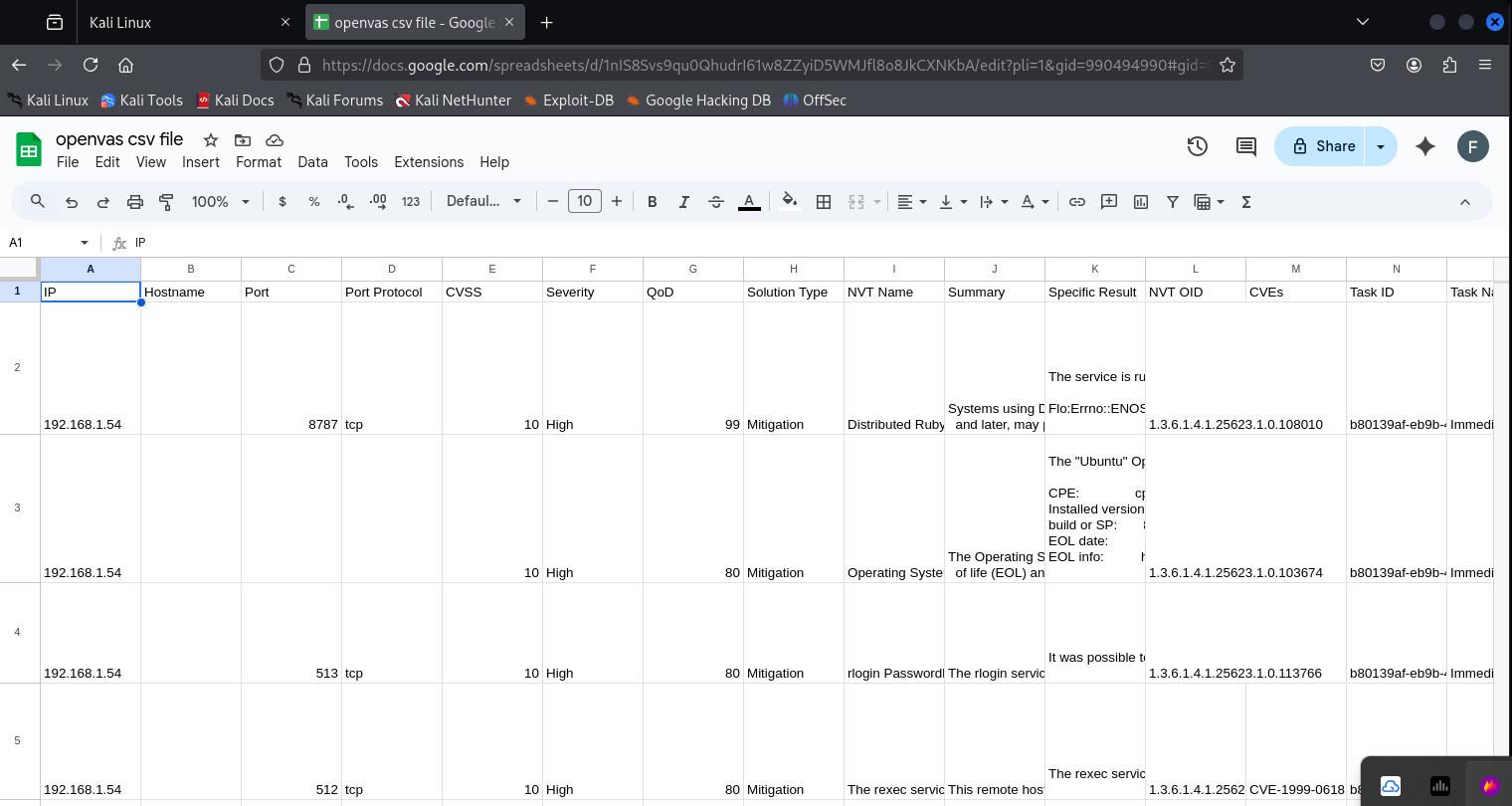


Screenshot: Malware Analysis result.

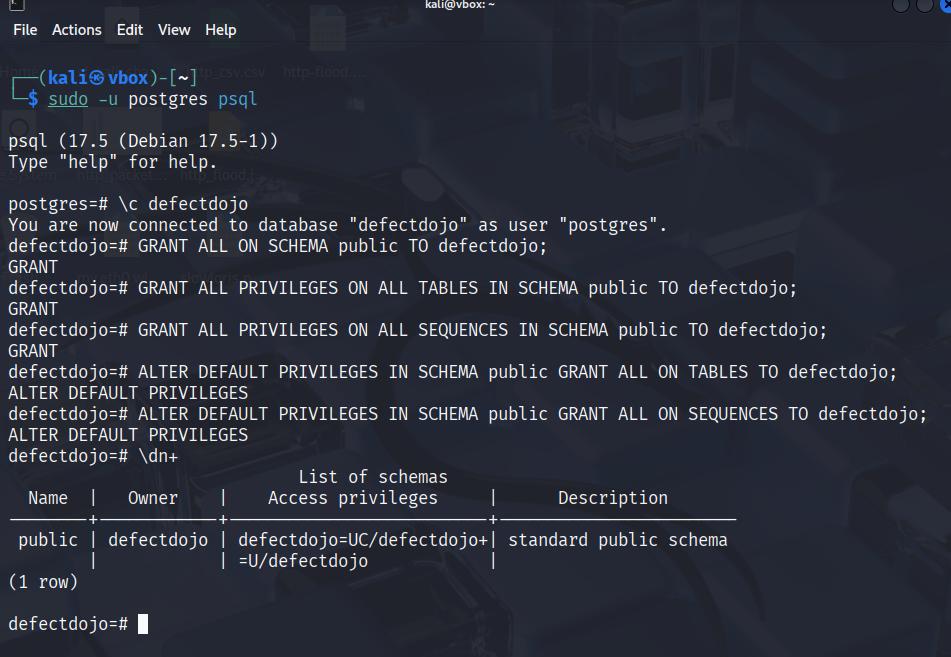
# 3. Vulnerability Management Pipeline

Objective: Scan Metasploitable VM with OpenVAS and import results into DefectDojo.

|  |  |  |
| --- | --- | --- |
| Vulnerability | CVSS Score | Description |
|  |  |  |
|  |  |  |
|  |  |  |
| VSFTPD Backdoor | 7.5 | Allows remote access |
| UnrealIRCd Backdoor | 9.8 | Remote code execution |
| Samba Buffer Overflow | 9.3 | Heap overflow enabling RCE |



Screenshot: Vulnerability scan result.

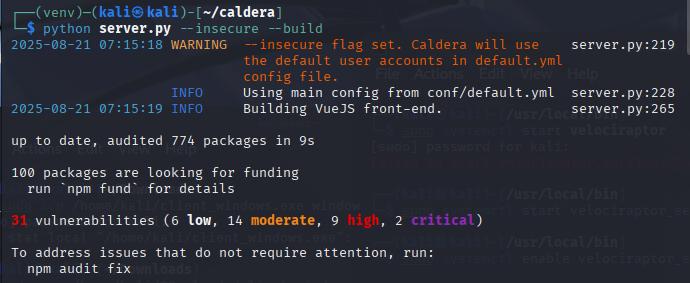


Screenshot: Vulnerability scan result.

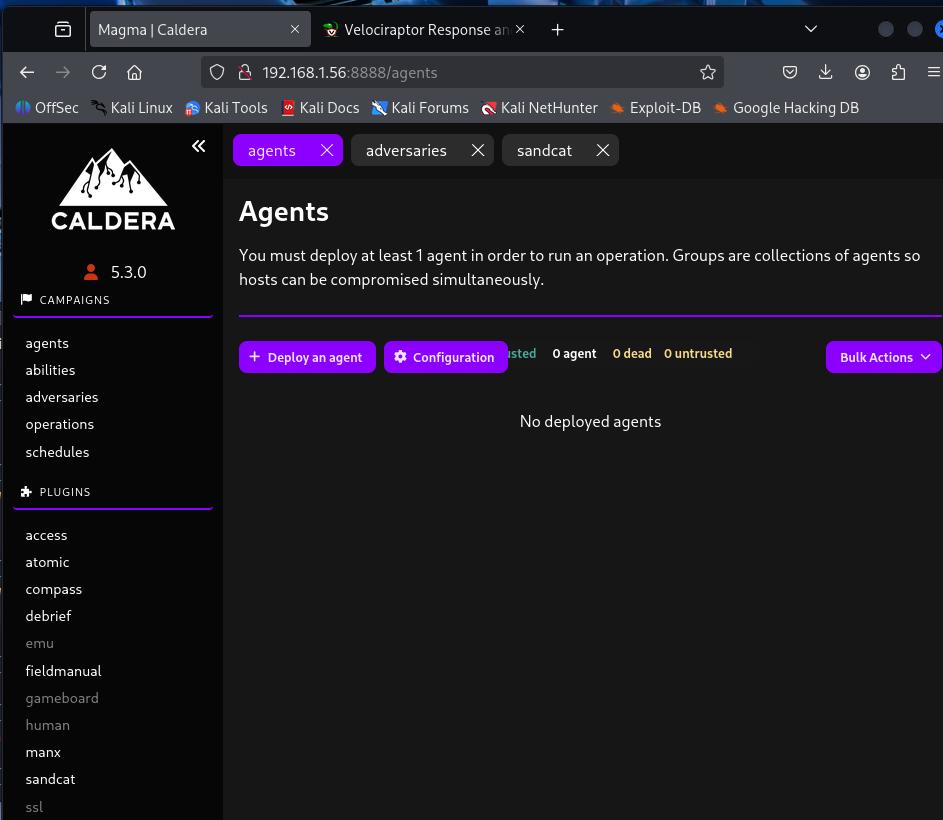
# 4. Incident Response Simulation

Objective: Simulate phishing with MITRE Caldera and collect artifacts with Velociraptor.

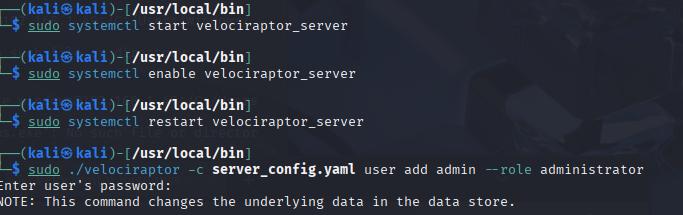
Summary: A phishing attachment executed on a Windows VM deployed a malicious agent. The agent established C2 communication with the attacker machine. Velociraptor collected forensic evidence confirming persistence and network beaconing.



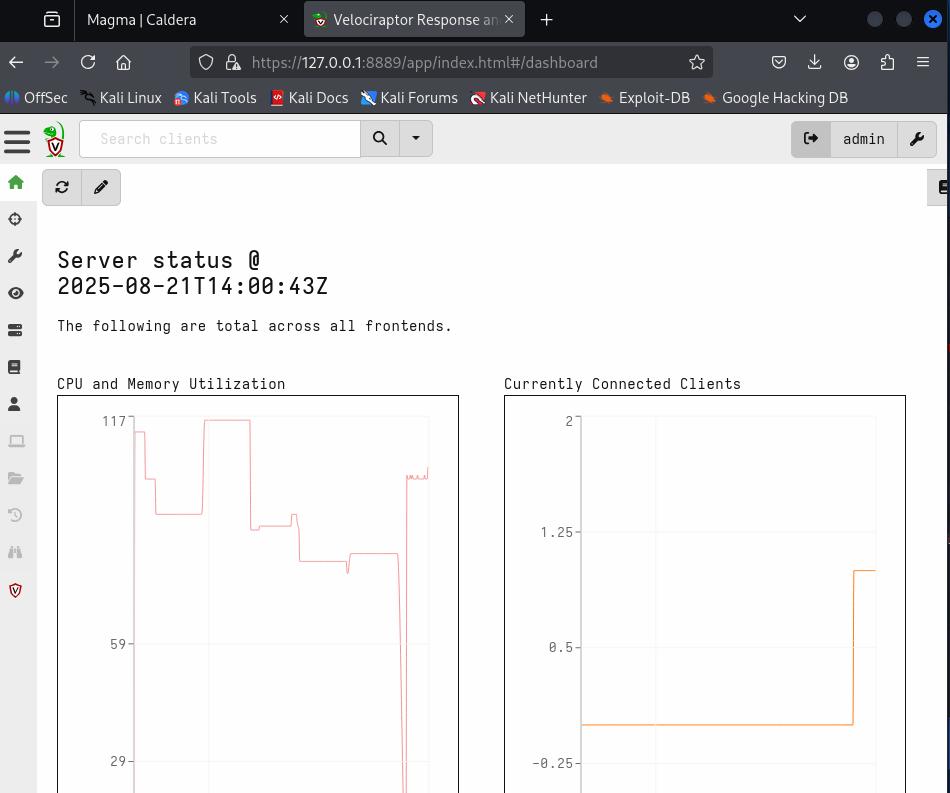
Screenshot: Incident Response evidence.



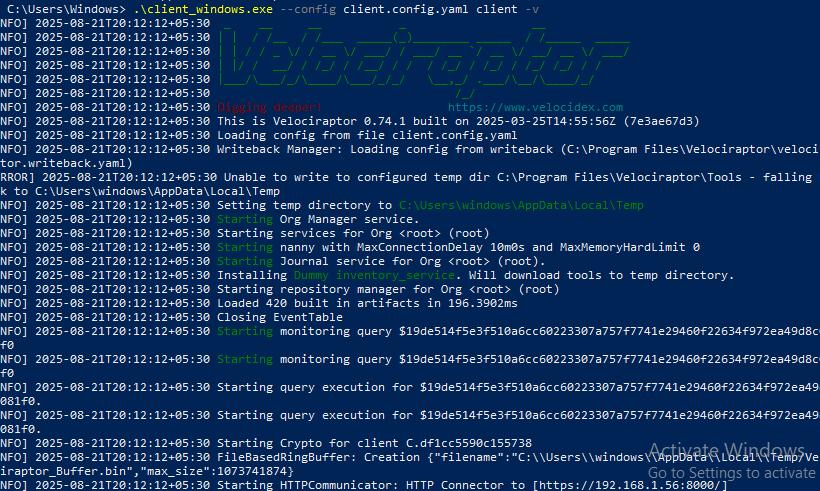
Screenshot: Incident Response evidence.



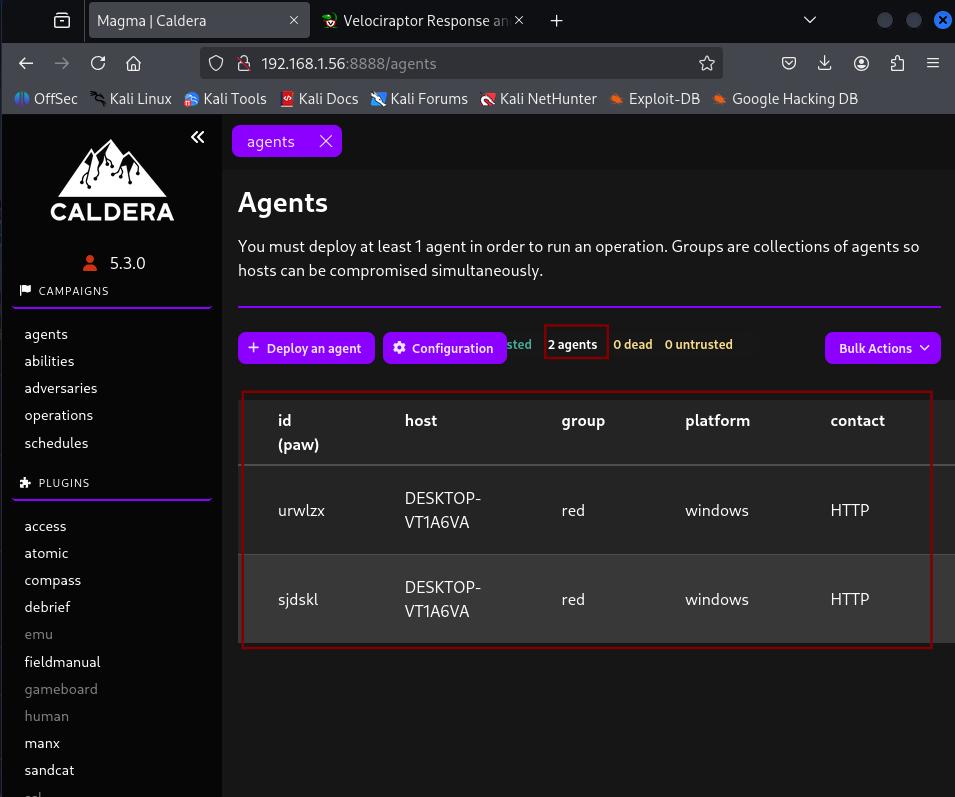
Screenshot: Incident Response evidence.



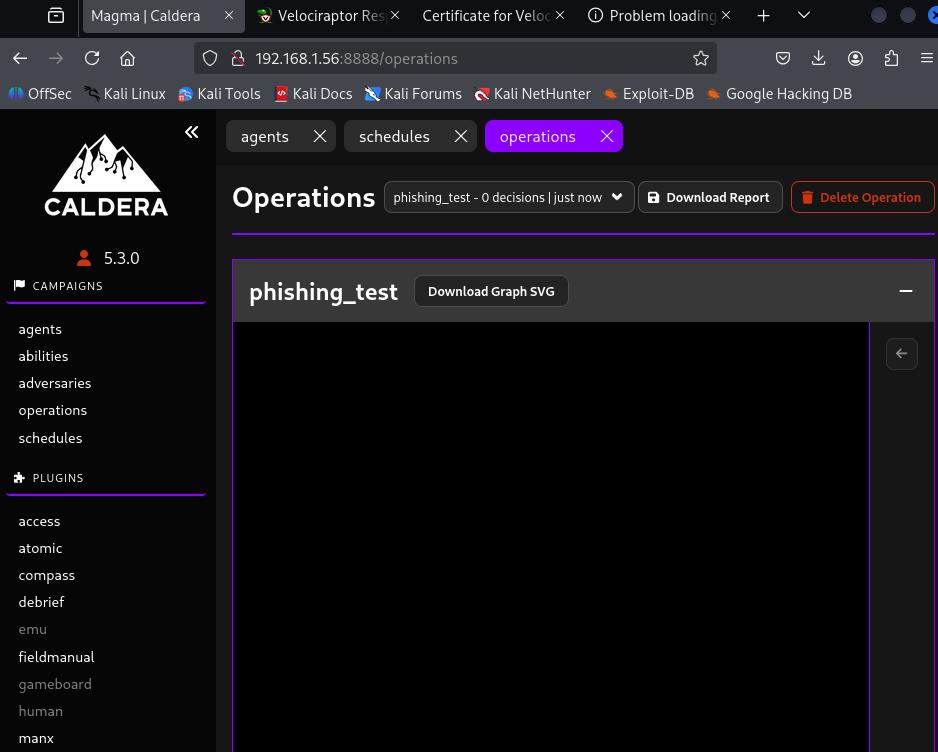
Screenshot: Incident Response evidence.



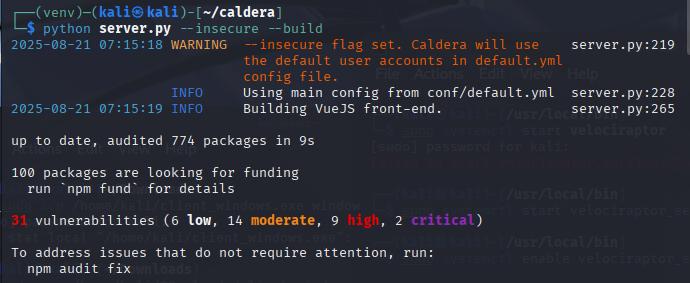
Screenshot: Incident Response evidence.



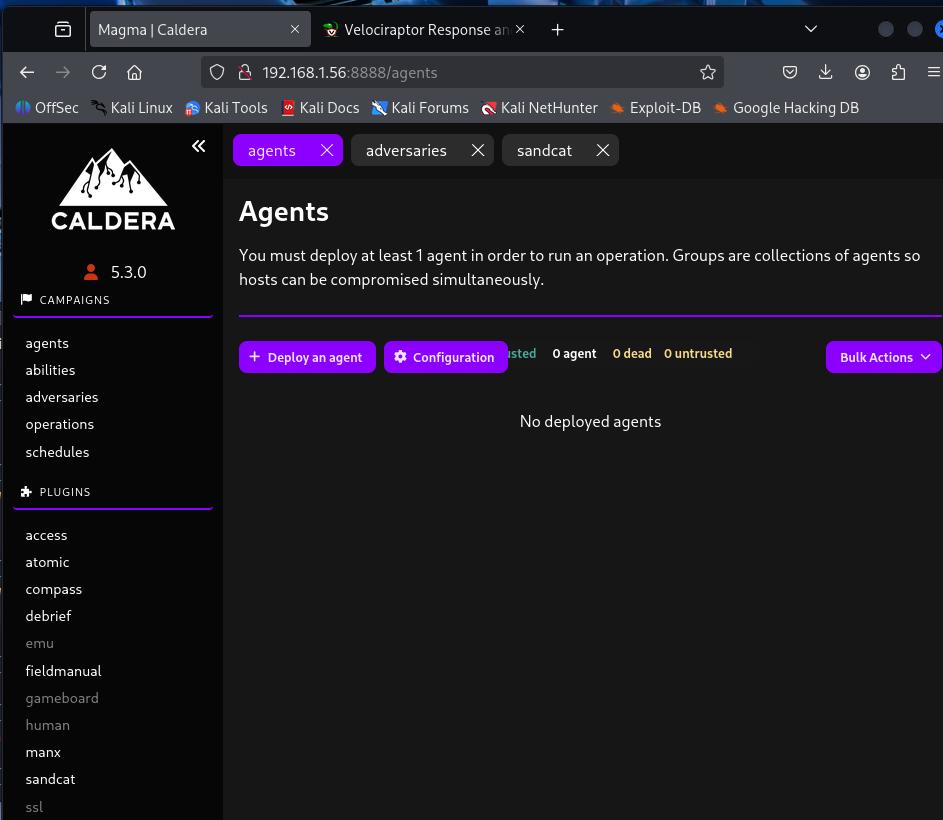
Screenshot: Incident Response evidence.



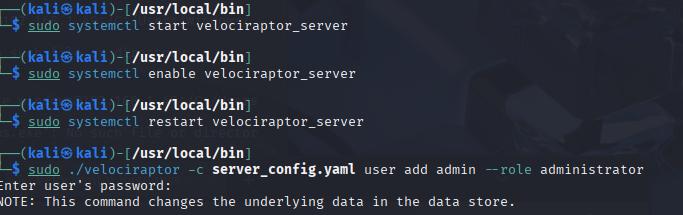
Screenshot: Incident Response evidence.



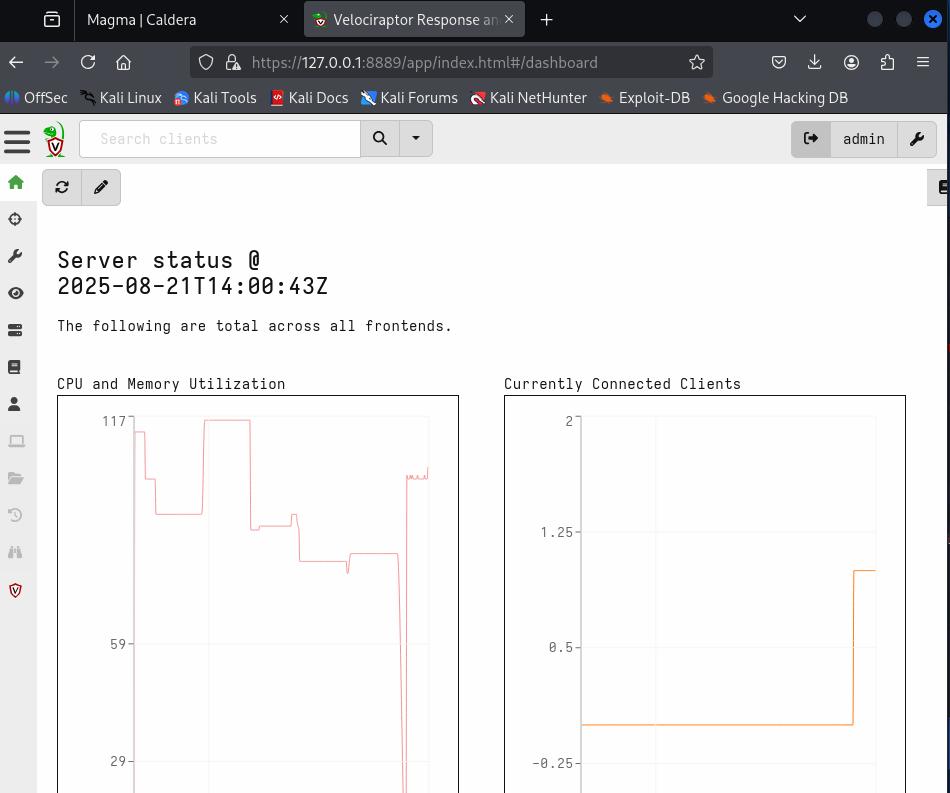
Screenshot: Incident Response evidence.



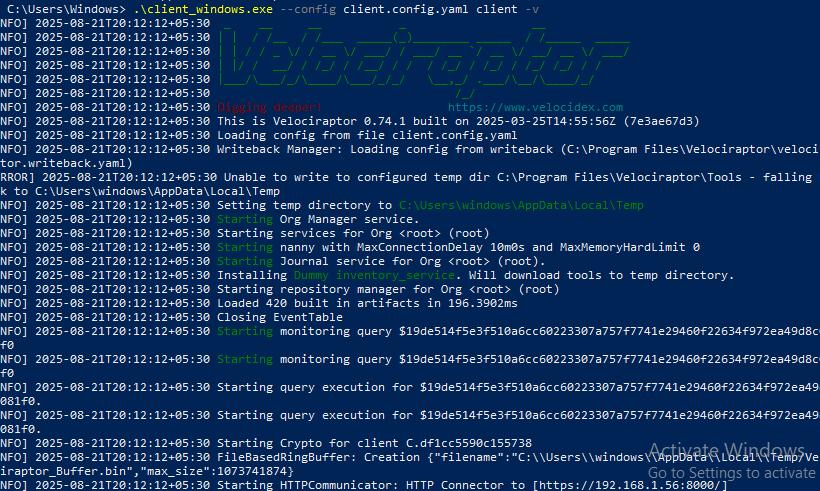
Screenshot: Incident Response evidence.



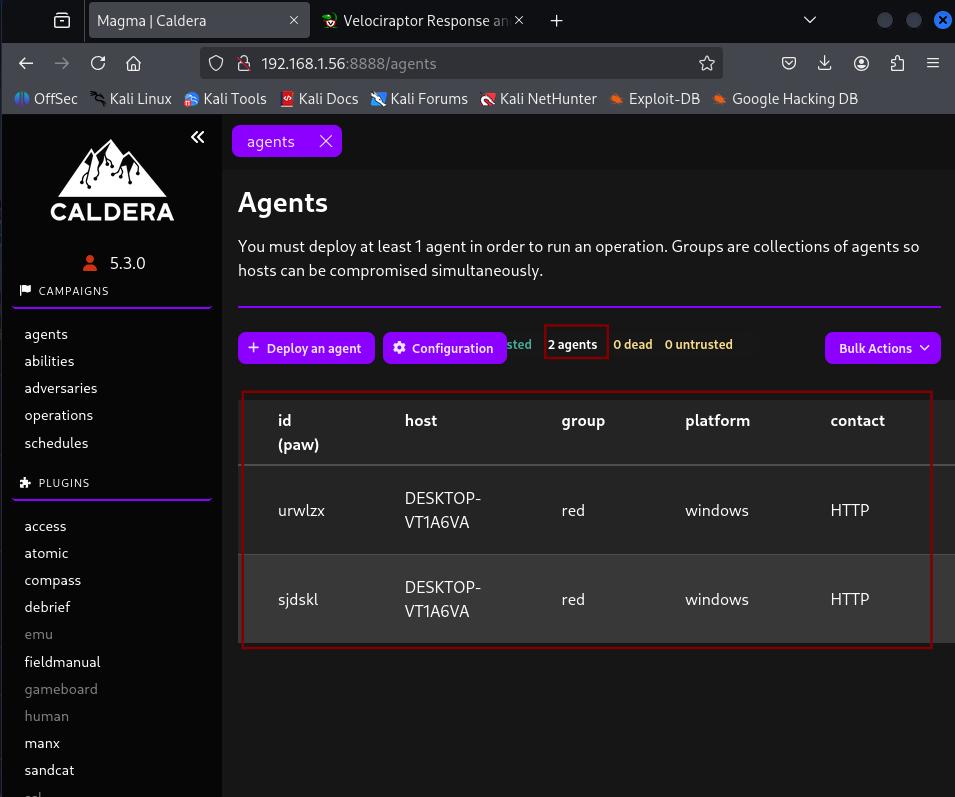
Screenshot: Incident Response evidence.



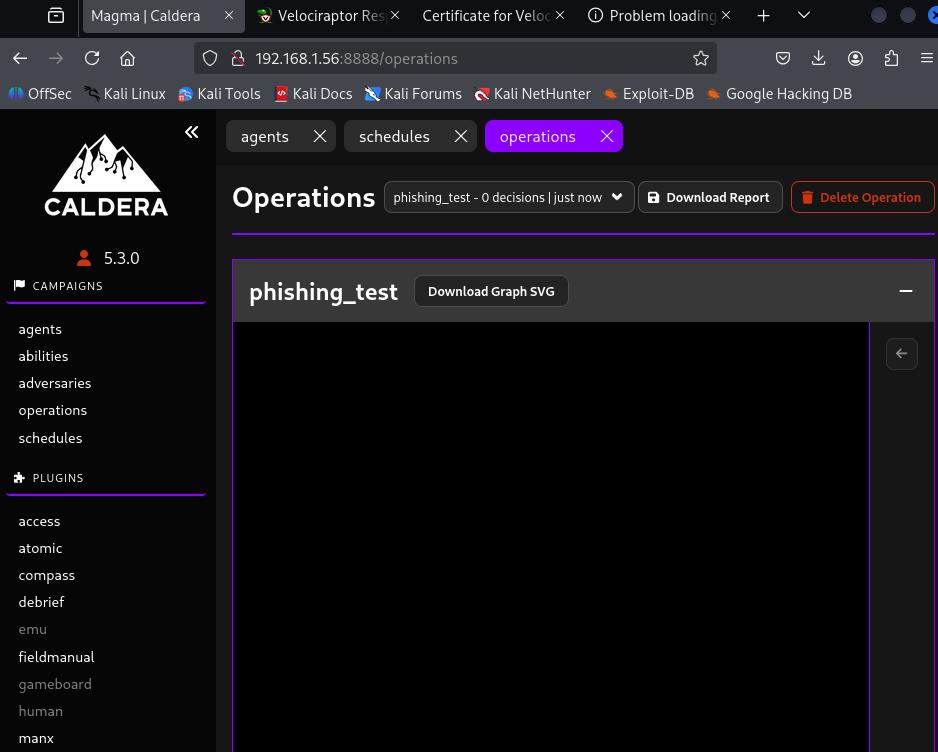
Screenshot: Incident Response evidence.



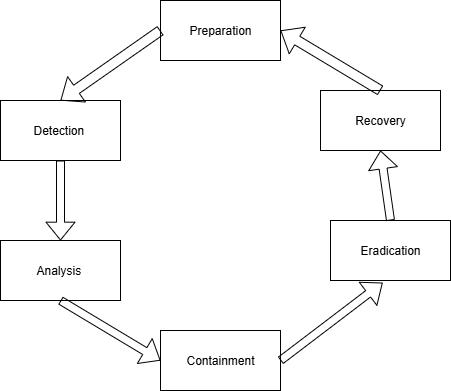
Screenshot: Incident Response evidence.



Screenshot: Incident Response evidence.



Screenshot: Incident Response evidence.

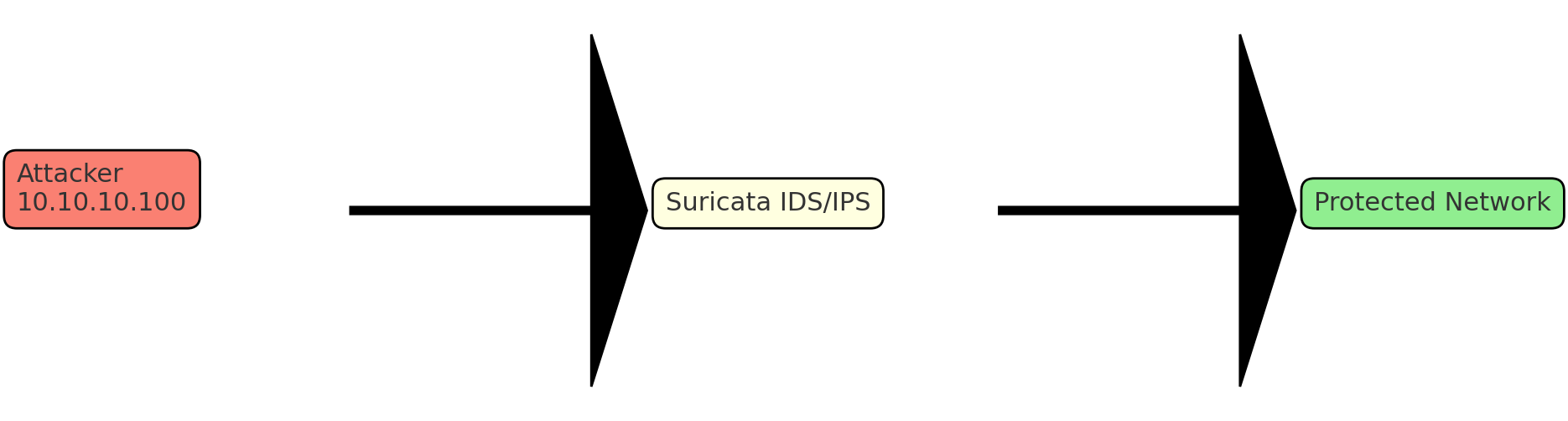


Screenshot: Incident Response evidence.

# 5. Network Defense with Open-Source Tools

Objective: Configure Suricata to block malicious IPs and map alerts to MITRE ATT&CK.

Suricata Rule



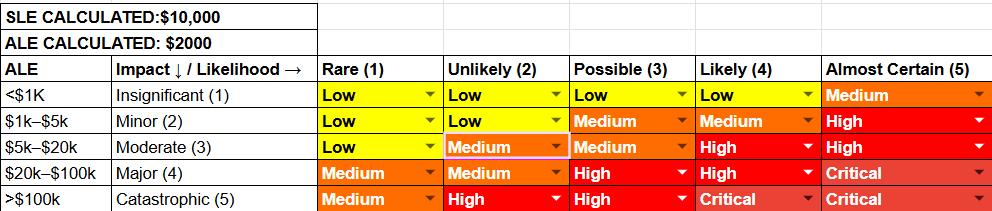
drop ip 10.10.10.100 any -> any any (msg:"Block Malicious IP"; sid:1000001;)

|  |  |  |  |
| --- | --- | --- | --- |
| Alert | Tactic | Technique | Notes |
| Suspicious HTTP | Command and Control | T1071 | Outbound traffic to C2 |

# 6. Risk Assessment Practice

Objective: Calculate ALE for a ransomware scenario and map in a risk matrix.

ALE = $10,000 × 0.2 = $2,000

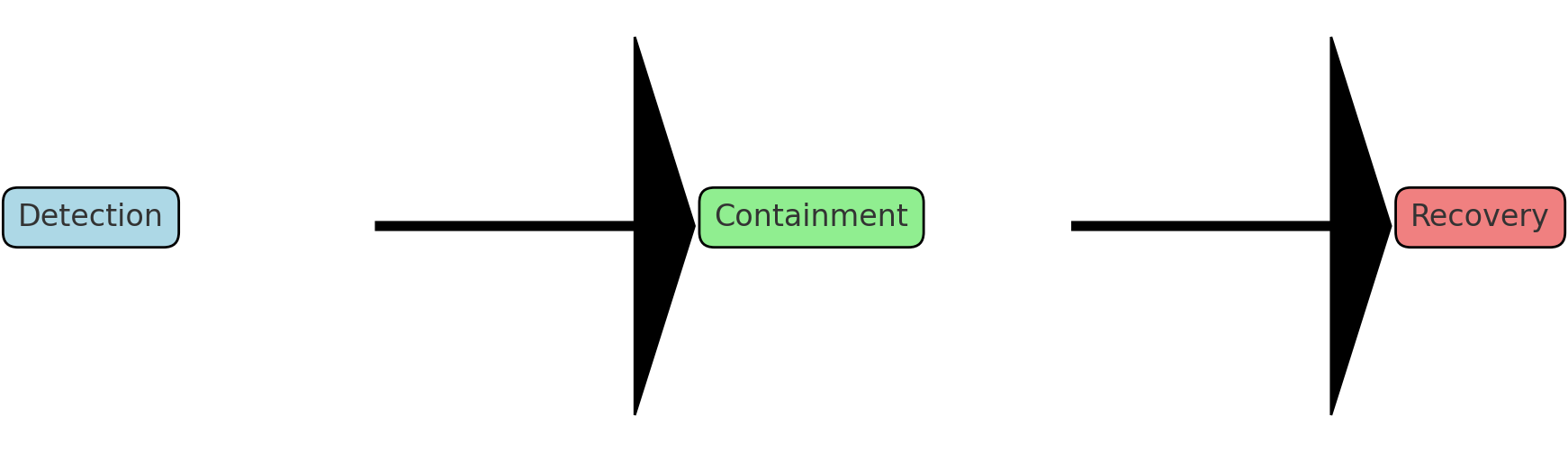


Screenshot: Risk matrix diagram.

# 7. Incident Response Report

Objective: Document a phishing incident using SANS-style template.

Flowchart: Incident Response Process (Detection → Containment → Recovery).

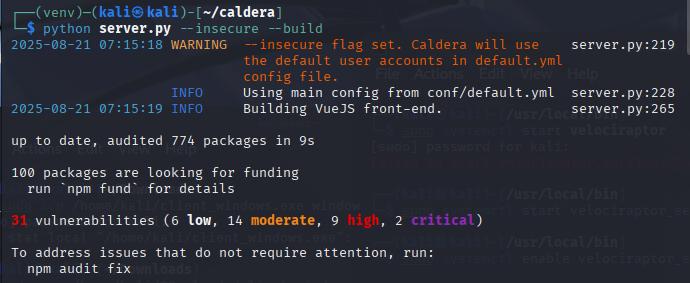


# 8. Capstone Project: Full Incident Response Cycle

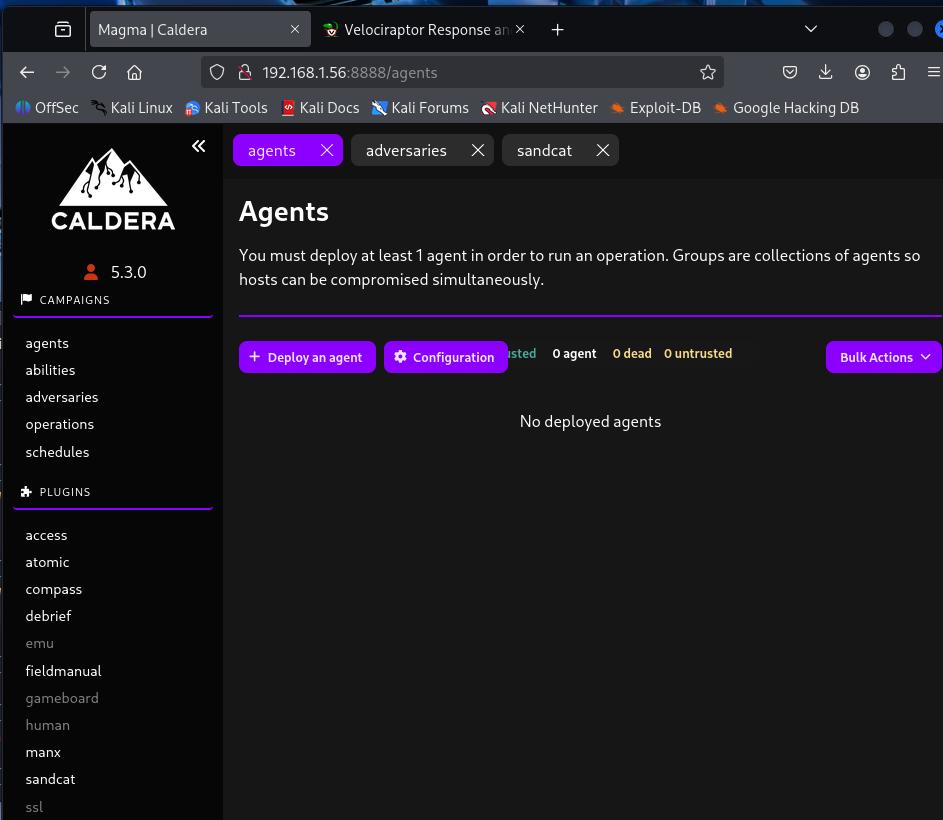
Objective: Perform full-cycle IR using Metasploit, Wazuh, and CrowdSec.

Alert Example:

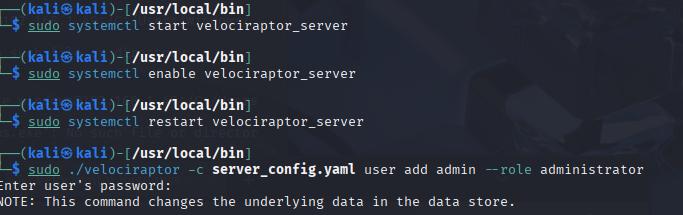
|  |  |  |  |
| --- | --- | --- | --- |
| Timestamp | Source IP | Alert Description | MITRE Technique |
| 2025-08-18 11:00:00 | 10.10.10.100 | VSFTPD exploit | T1190 |



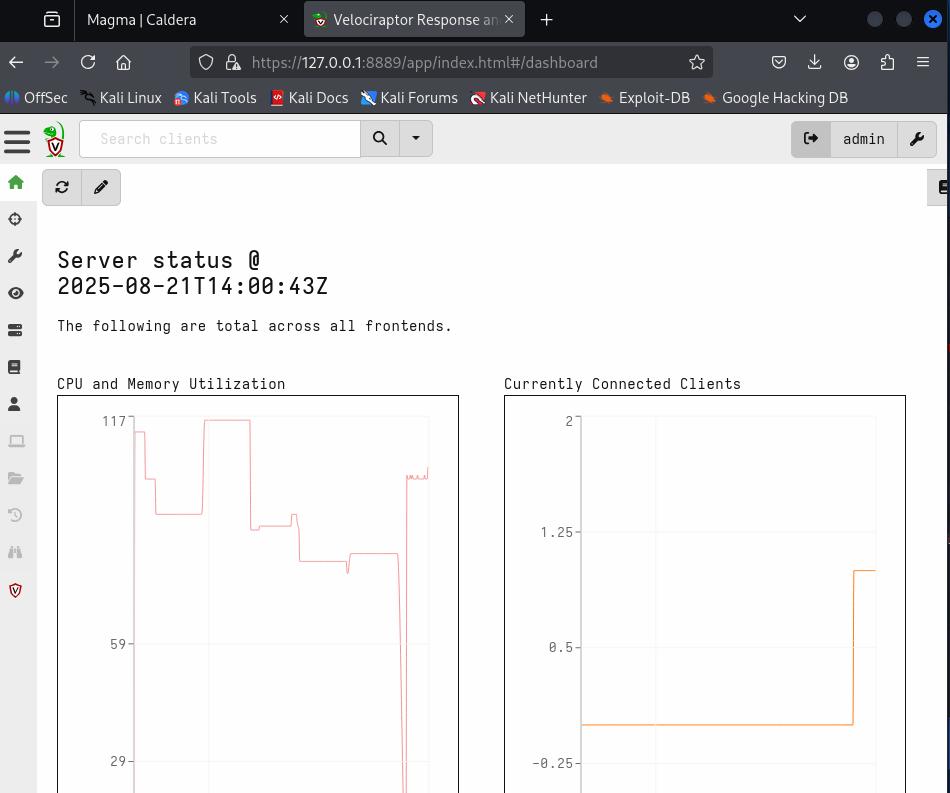
Screenshot: Capstone Incident evidence.



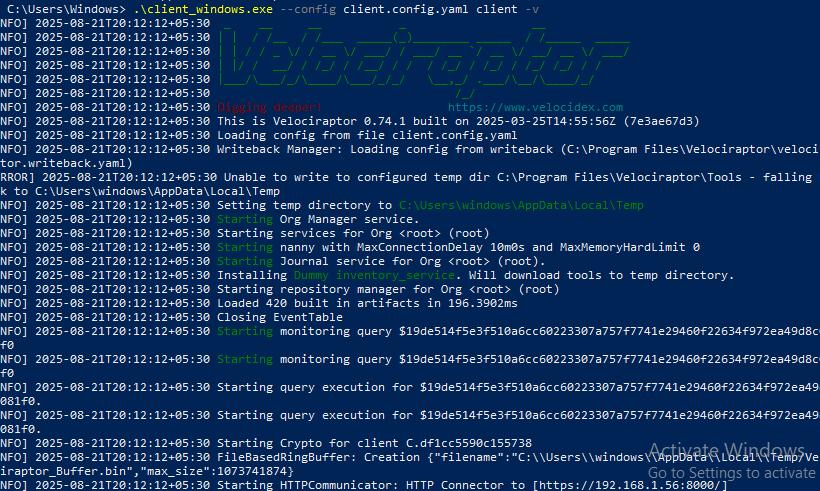
Screenshot: Capstone Incident evidence.



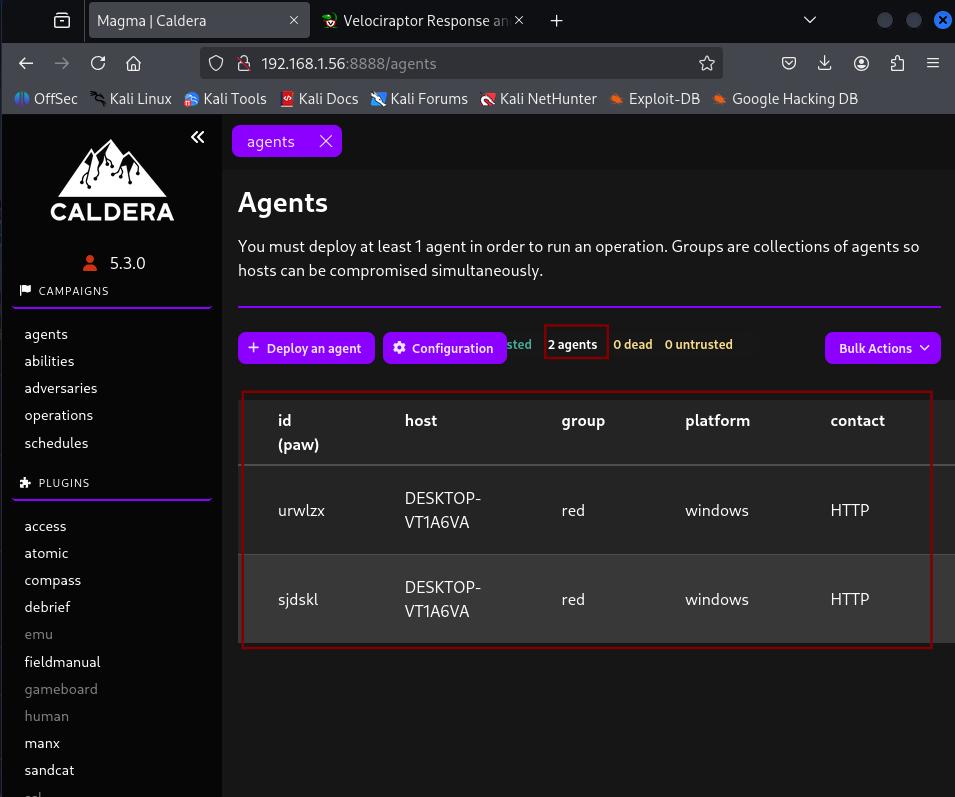
Screenshot: Capstone Incident evidence.



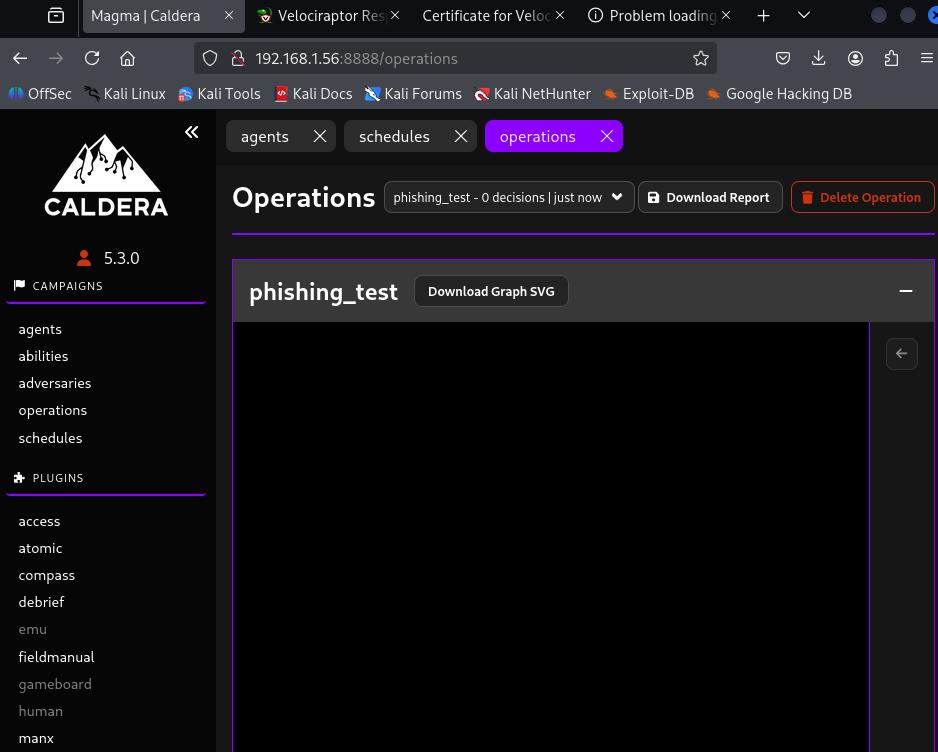
Screenshot: Capstone Incident evidence.



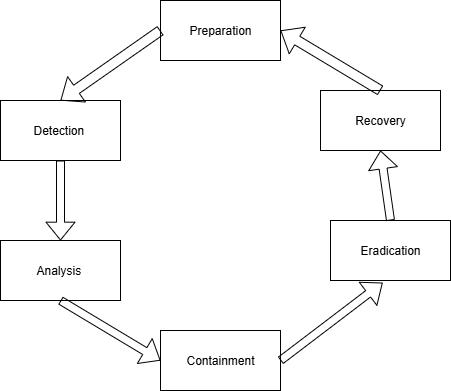
Screenshot: Capstone Incident evidence.



Screenshot: Capstone Incident evidence.



Screenshot: Capstone Incident evidence.



Screenshot: Capstone Incident evidence.

# Conclusion

This Week 2 Practical Application covered threat hunting, malware analysis, vulnerability management, incident response, network defense, risk assessment, and a full capstone IR cycle.