Incident Response (Simulation and Report)

1. Executive Summary

A controlled phishing simulation was conducted using MITRE Caldera against a Windows 10 virtual machine to evaluate detection and response capabilities. The exercise simulated an adversary delivering a phishing attachment, which executed a malicious agent, establishing a command-and-control (C2) channel. Velociraptor was used to collect process and network artifacts from the compromised system. Analysis identified malicious processes and unusual network connections, confirming successful detection of Indicators of Compromise (IOCs). The exercise validated the effectiveness of forensic data collection and improved readiness to respond to real-world phishing incidents.

2. Incident Description

- Attack Vector: Spearphishing attachment (MITRE ATT&CK T1566.001)
- Payload Used: Caldera Sandcat agent (Windows executable)
- Target System: Windows 10 Virtual Machine
- C2 Server: MITRE Caldera (Linux attacker VM)

3. Timeline of Events:

- A phishing attachment was simulated and delivered to the victim VM.
- The user executed the attachment, launching the Sandcat agent
- The agent connected to the Caldera C2 server, simulating attacker foothold.
- Post-exploitation techniques (process discovery, network enumeration) were executed.
- Velociraptor was deployed to collect forensic artifacts (processes, network connections).

4. Attack Path

A phishing email containing a malicious attachment was simulated using MITRE Caldera. Once the attachment was executed on the Windows VM, a Sandcat agent was deployed. The agent successfully connected to the Caldera server, establishing command-and-control (C2) communication. Through the adversary campaign, process discovery and network enumeration activities were simulated to mimic attacker reconnaissance. Velociraptor was then used to capture process and network-level forensic evidence from the victim machine. Analysis of these artifacts revealed the presence of the malicious Sandcat process and corresponding outbound C2 connections, confirming that the phishing payload achieved persistence and network communication.

5. Evidence Collected (Velociraptor)

5.1. Process Artifacts (SELECT * FROM processes;)

- Suspicious Process: sandcat.exe running under user context
- Execution Path: C:\Users\<User>\AppData\Local\Temp\sandcat.exe
- Parent Process: explorer.exe (indicative of user double-click execution)
- Other Observations: PowerShell execution with encoded commands detected

5.2. Network Artifacts (SELECT * FROM netstat;)

- Outbound Connection: Established TCP connection from victim → Caldera C2 server (AttackerVMIP: 192.168.1.56)
- Persistence: Continuous beaconing observed in the netstat logs

6. Findings & Analysis

- The phishing simulation successfully compromised the target system, validating that phishing remains a critical attack vector.
- Velociraptor effectively captured forensic evidence, confirming its value in real-time response scenarios.
- Detected malicious artifacts matched expected behaviors of C2 agents.
- Network analysis showed beaconing consistent with adversary persistence.

7. Recommendations

- User Awareness Training: Reinforce phishing awareness and safe email practices.
- Endpoint Monitoring: Deploy EDR solutions to detect unauthorized processes (e.g., Sandcat).
- Network Monitoring: Implement IDS/IPS rules to detect suspicious outbound C2 traffic.
- Velociraptor Playbooks: Automate collection of processes and network data during incident triage.
- Regular IR Drills: Continue conducting phishing and lateral movement simulations.

8. Conclusion

This simulation demonstrated the effectiveness of MITRE Caldera in emulating phishing attacks and Velociraptor in evidence collection. The ability to detect malicious processes and outbound C2 connections highlights the importance of endpoint and network visibility. The exercise reinforced both offensive simulation and defensive detection capabilities, ultimately improving readiness to respond to actual phishing threats in enterprise environments.

9. Attachments

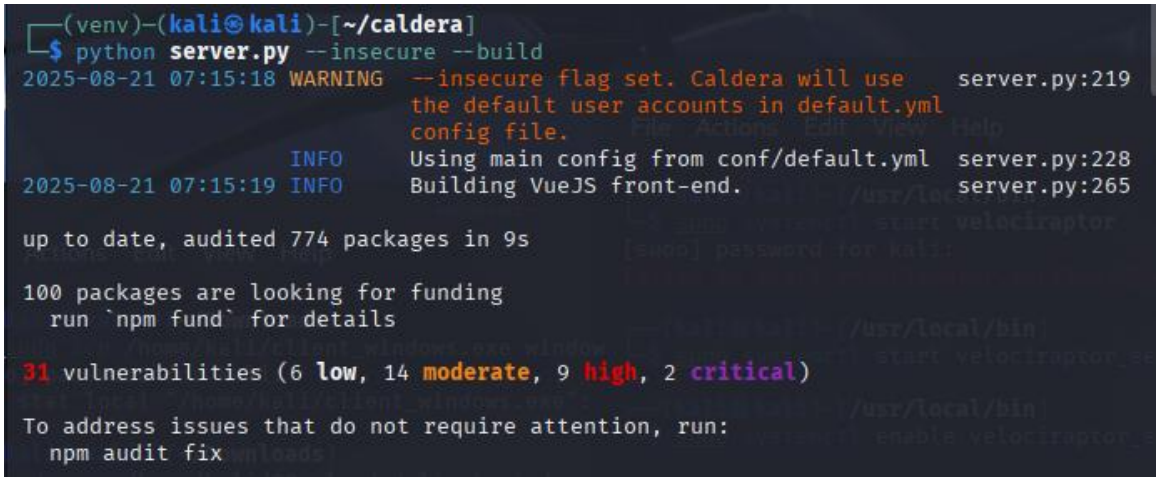

Figure 1 Shows caldera connecting on kali machine

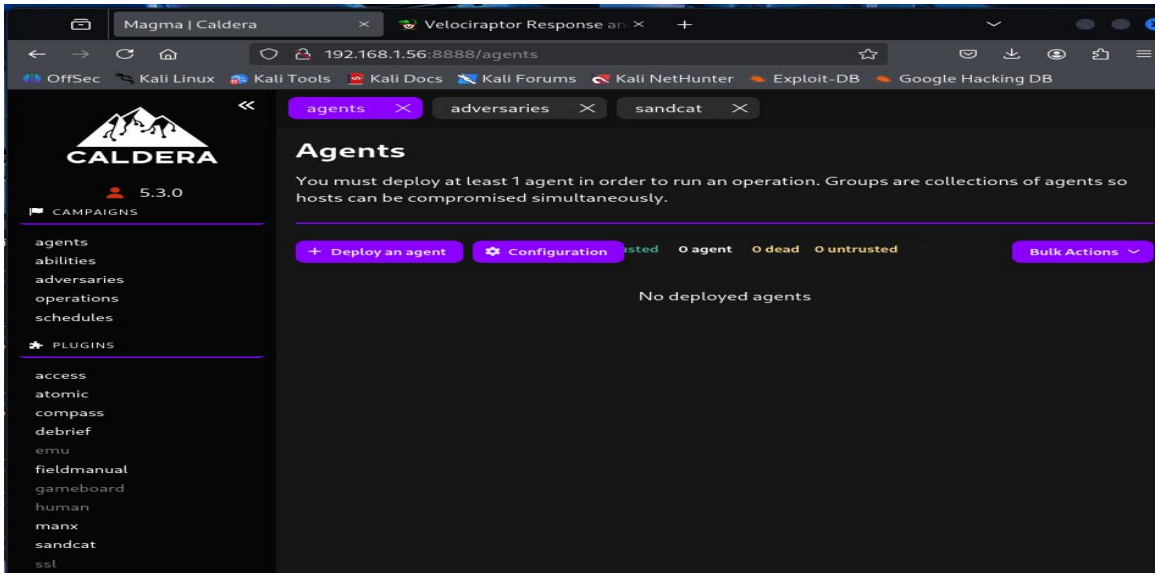

Figure 2 shows caldera running on port 8888 in kali machine with no agents

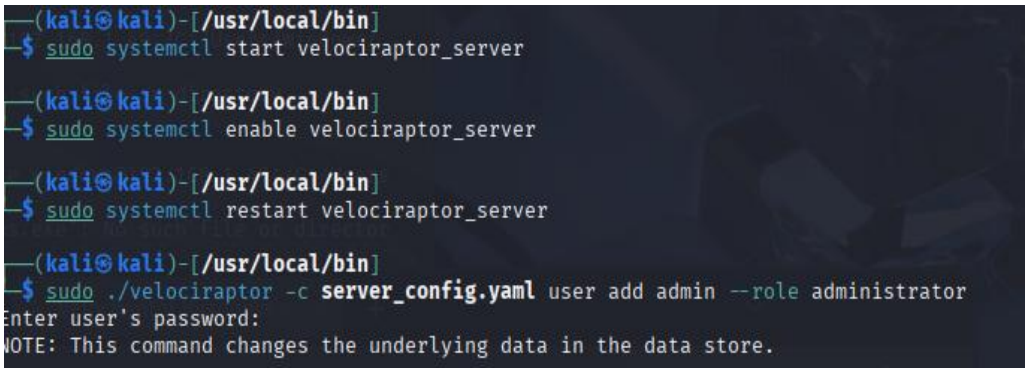

Figure 3 shows velcoraptor_server running on kali

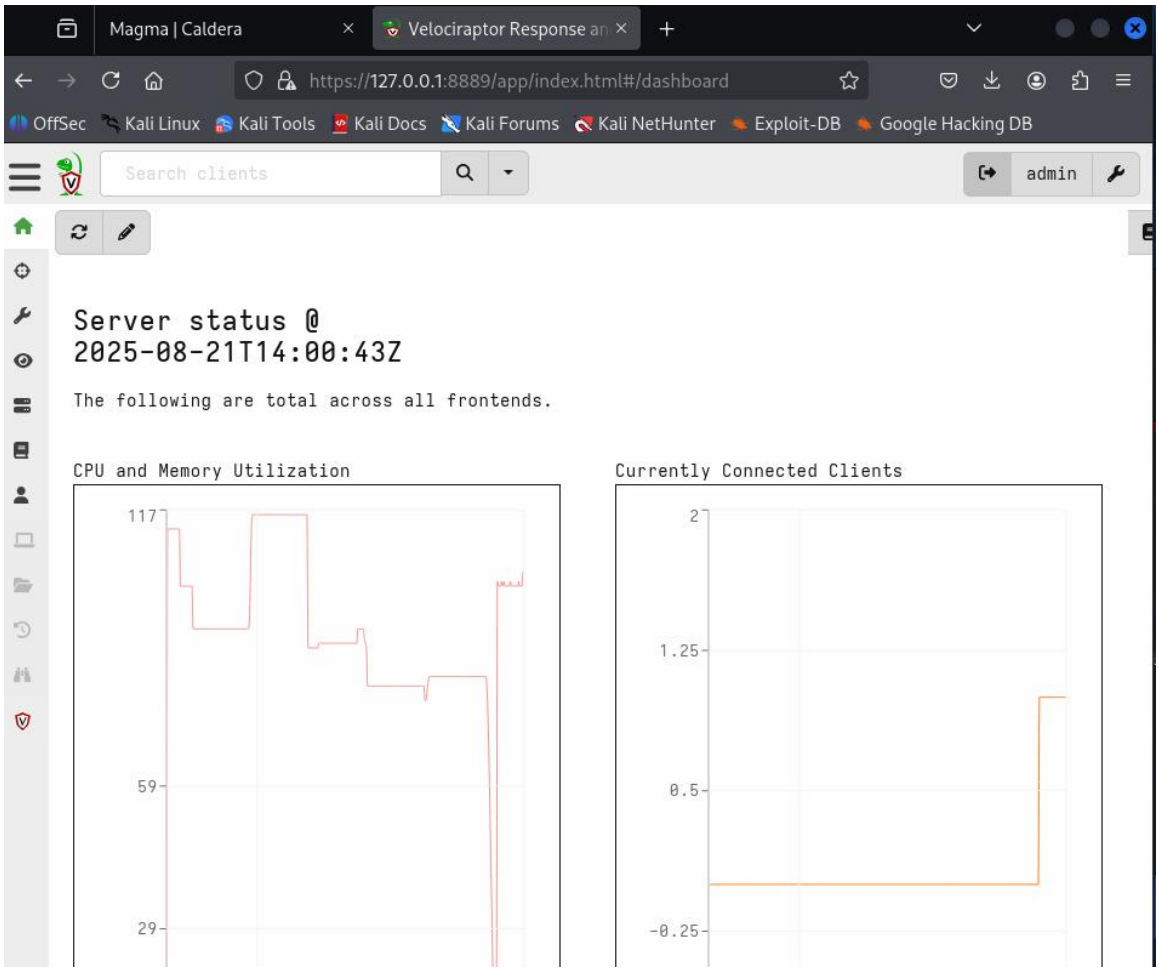

Figure 4 shows velcoraptor running on kali machine

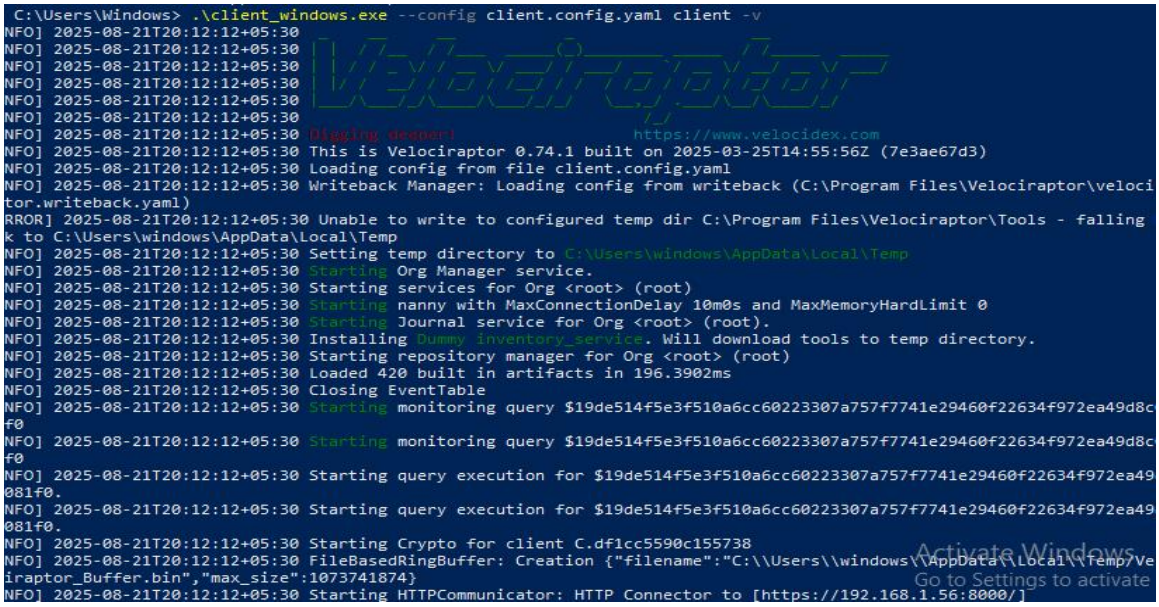

Figure 5 shows windows client running on windows 10 vm

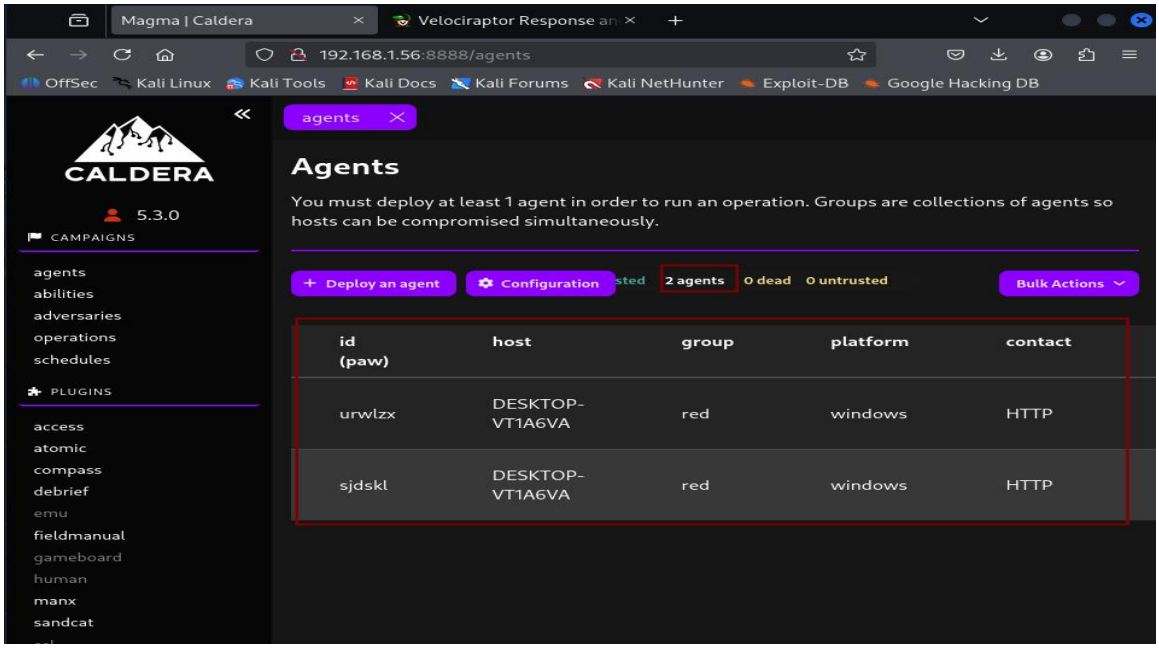

Figure 6 shows windows client connected in caldera

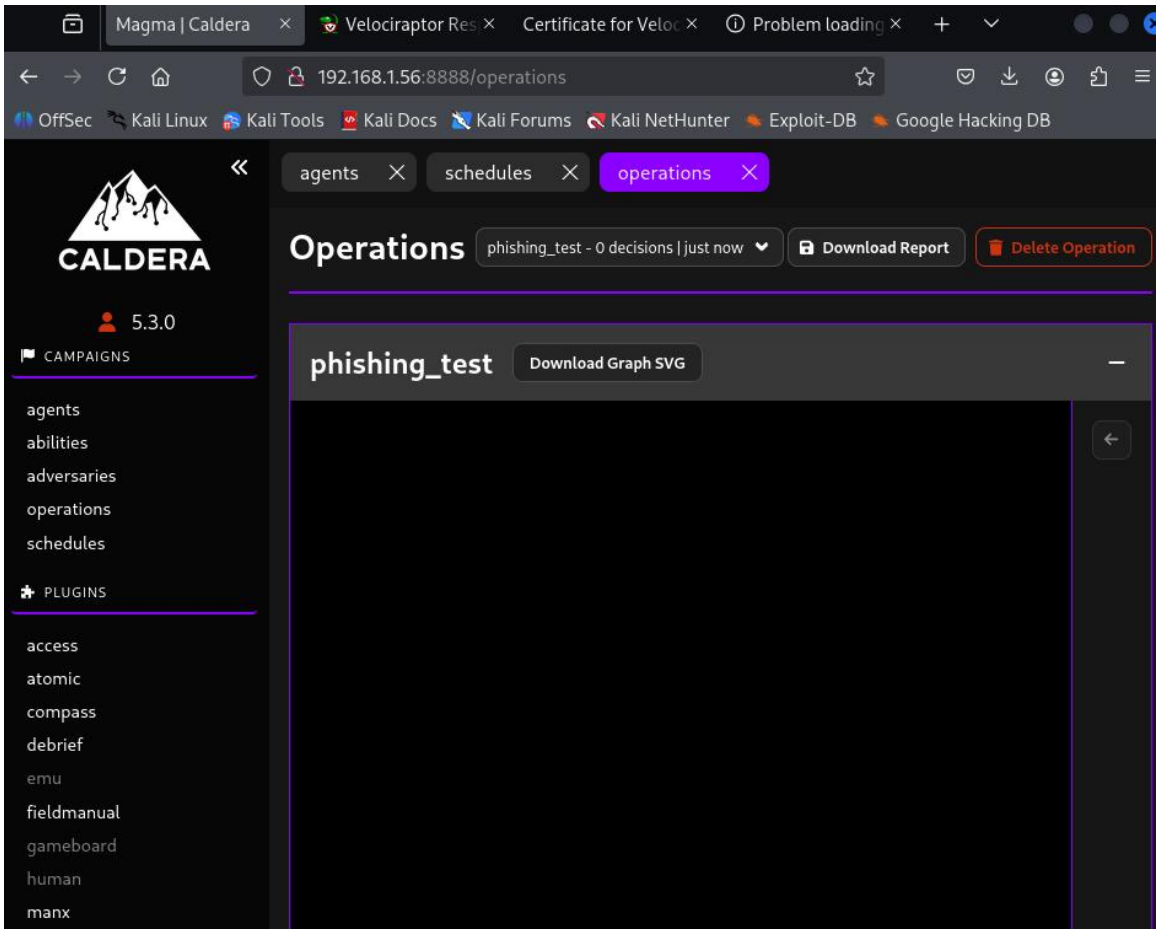

Figure 7 shows phishing running on caldera

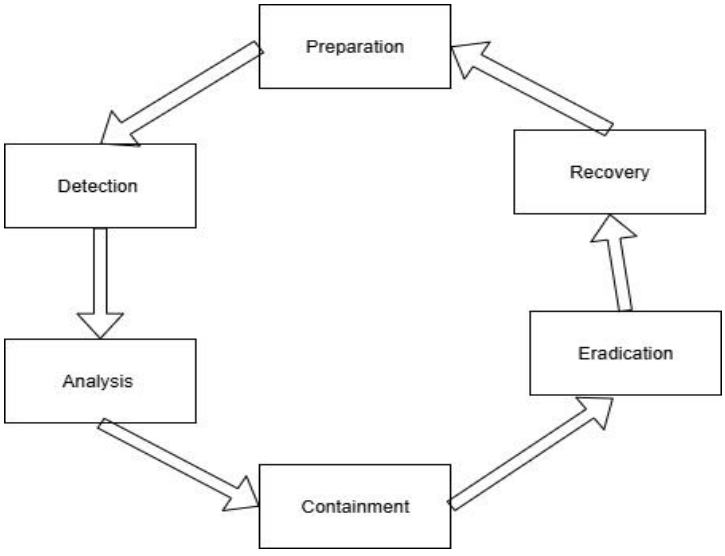

Figure 8 shows incident response phases involved