Practical Application 2

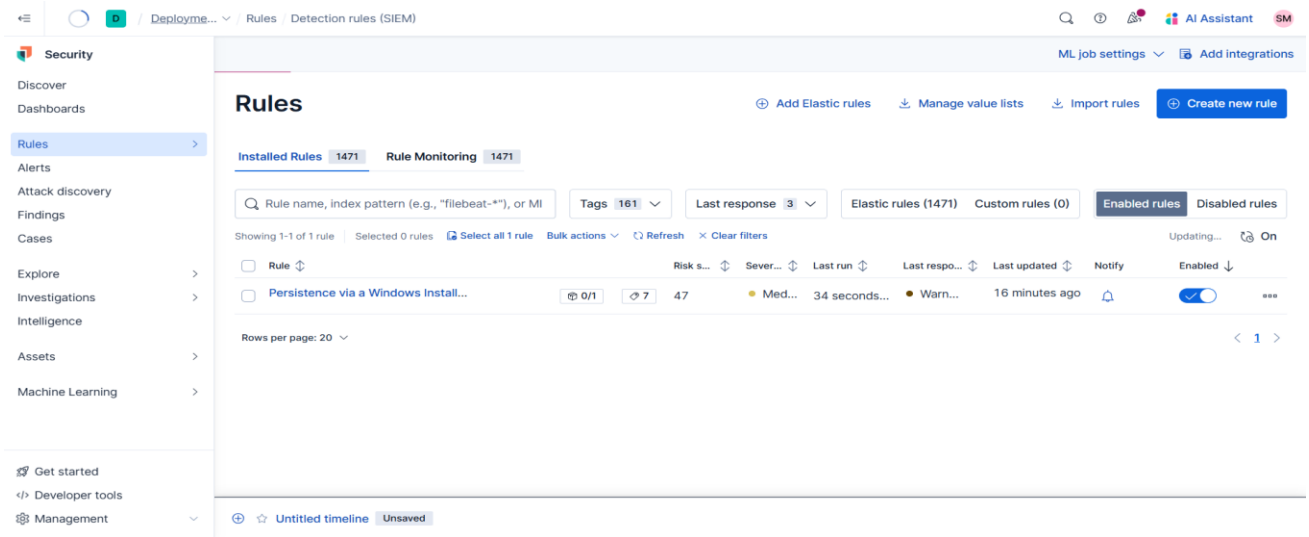
Index

(1) Theat Hunting with Open-Source Tools

Tools- Elastic Security, Security Onion, Sigma Rules.

Task- Ingest sample logs into Elastic Security and write a sigma rule to detect suspicious PowerShell activity.

Sigma Rule Sample-



Test with harmless windows script-

```
# PowerShell script to display basic system information

Write-Host "==== System Info ===="
Write-Host "Hostname: $($env:COMPUTERNAME)"
Write-Host "Username: $($env:USERNAME)"
Write-Host "OS Version: $((Get-CimInstance Win32_OperatingSystem).Caption)"
Write-Host "Architecture: $((Get-CimInstance Win32_OperatingSystem).OSArchitecture)"
Write-Host "Uptime: $([math]::Round((Get-CimInstance Win32_OperatingSystem).LastBootUpTime.ToUniversalTime() - (Get-Date).ToUniversalTime()).TotalDays * -1, 2)) days"
Write-Host "Logged-in Users:"
query user
```

Threat Hunting Query-

```
event.category:process and winlog.event_id:4688 and process.name:"powershell.exe"
```

(2) **Malware Analysis Basics**

Tool- REMnux, Hybrid Analysis

Task- Analyse a benign sample in REMnux using strings, peframe.

Enhanced Tasks-

Static Analysis:

(a) Basic Information fetch of calc.exe file

```
root@remnux:/mnt/hgfs/Downloads# file 'Windows Calculator Installer.exe'
Windows Calculator Installer.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windo
ws
root@remnux:/mnt/hgfs/Downloads#
```

(b) Strings Extraction

output.txt

pefile.txt

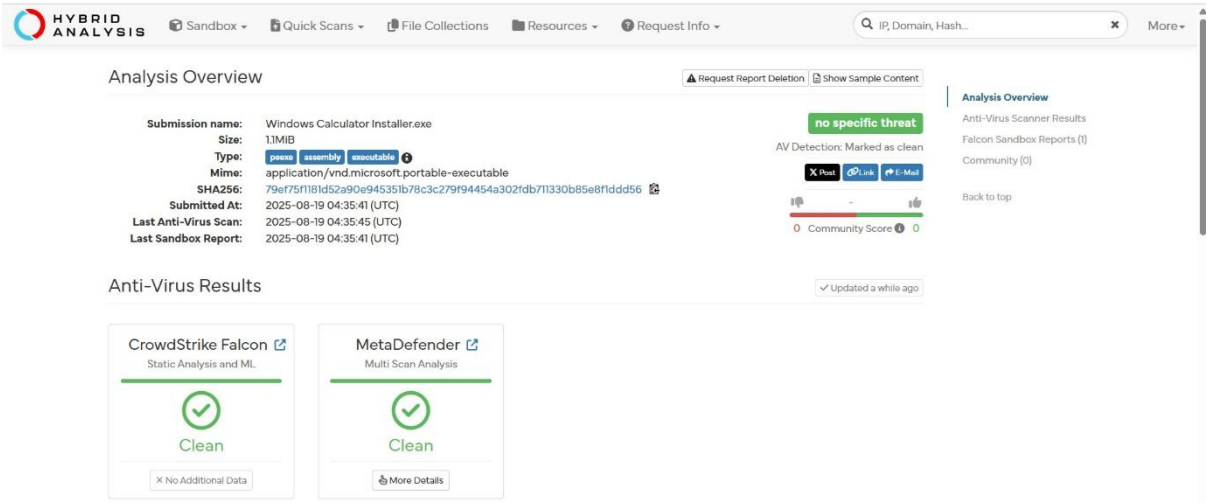
Summarize

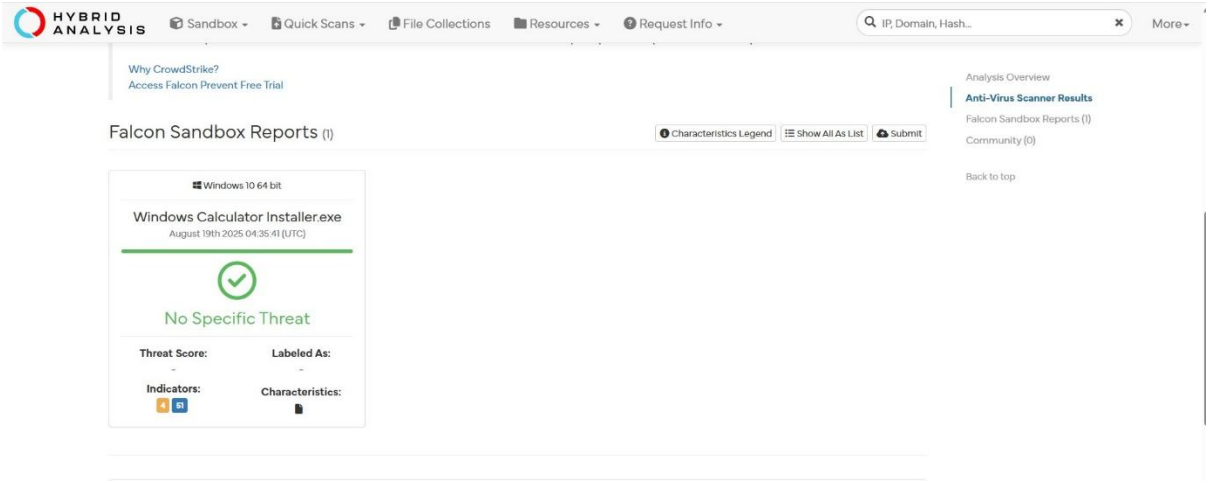
Version- 4.0.0.0

.NetFrameWork Version- 4.7.2

Colour

Dynamic Analysis-





Reports Comparison:

(1) when analyse with hybrid analysis it is showing nothing vulnerabilities. Same result showing from REMnux tool.

(2) Hybrid analysis of calc.exe done through sandboxes but REMnux analysis done through inbuilt sub tools like file, strings, pefile etc.

(3) REMnux showing details result of analysis in comparison with hybrid analysis.

(3) Build a Vulnerability Management Pipeline

Tools- OpenVAS, DefectDojo

OpenVAS Results

metasploitable-2.0-openvas.pdf

report.xml

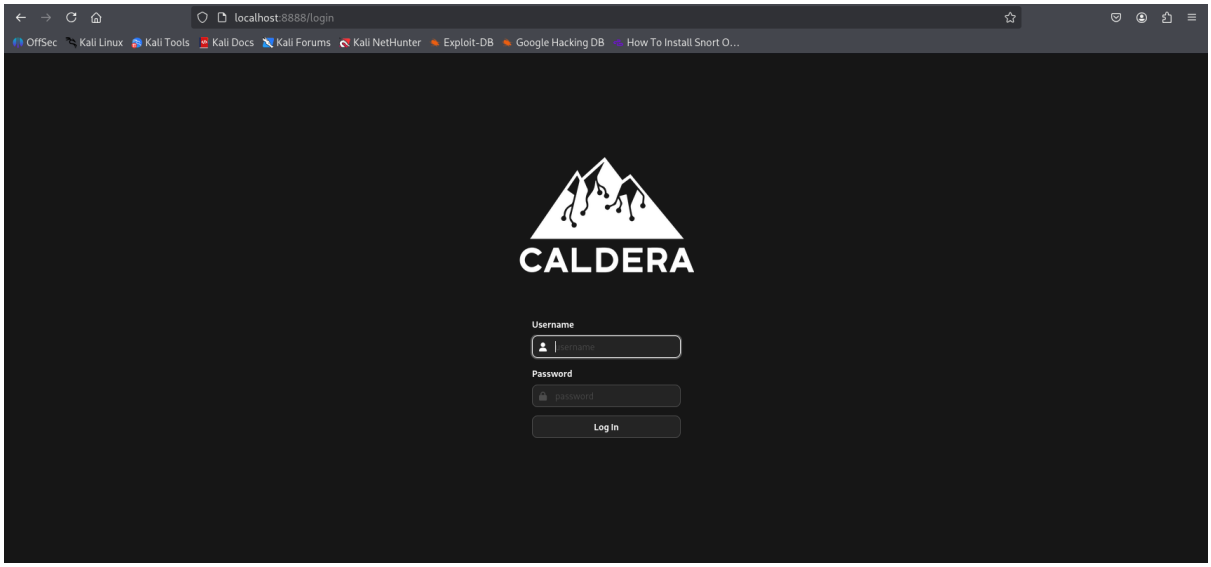
(4) Incident Response Simulation

Tool- Velociraptor, MITRE Caldera

Task- Simulate a phishing attack with Caldera and collect artifacts with Velociraptor.

Enhanced tasks-

Phishing Simulation-

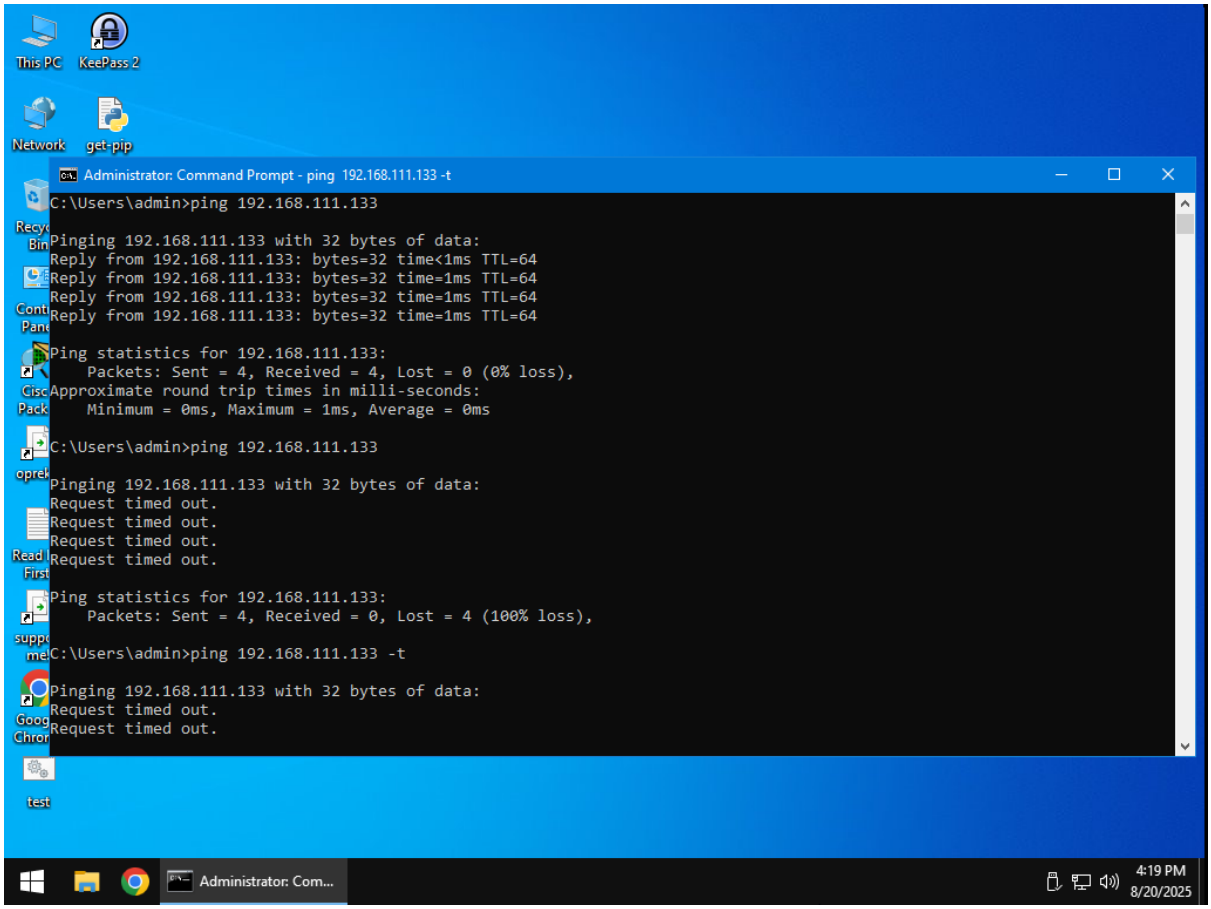


(5) Network Défense with Open-Source Tools

Tool- Suricata, Elastic SIEM,Crowdsec.
Task- Configure Suricata to block malicious Ips and map alerts to MITRE ATT&CK.

Enhanced Tasks-
Suricata Rule-

Test by pinging from another vm



Alert Logs-

ATT&CK Mapping-

```
alert ip 192.168.111.139 any -> any any (
  msg:"Dropped Malicious IP - Possible C2";
  metadata:attack_technique_id=T1071, attack_tactic=command-and-control;
  sid:1000002;
  rev:1;
)
```

(6) Risk Assessment Practice

Tool- Google Sheets

Task- Calculate ALE for a mock scenario

Enhanced Tasks-

ALE Calculation-

$$ALE = SLE \times ARO$$

Where:

- **ALE** = *Annualized Loss Expectancy* (expected loss per year in dollars)
- **SLE** = *Single Loss Expectancy* (loss per incident)
- **ARO** = *Annual Rate of Occurrence* (how often the event happens in a year)

If SLE = $10,000, ARO = 0.2

Then,

ALE = SLE x ARO

= 10,000 x 0.2

= $2000 per year

Risk Matrix-

	1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
5 - Almost Certain	Medium	High	High	Critical	Critical
4 - Likely	Medium	Medium	High	High	Critical
3 - Possible	Low	Medium	Medium	High	High
2 - Unlikely	Low	Low	Medium	Medium	High
1 - Rare	Low	Low	Low	Medium	Medium

Where row represents Likelihood and column represent Impact.

Score the Ransomware Scenario-

	1	2	3	4	5
5 (AC)	M	H	H	C	C
4 (Likely)	M	M	H	H	**C ←** ✔
3 (Possible)	L	M	M	H	H
2 (Unlikely)	L	L	M	M	H
1 (Rare)	L	L	L	M	M

- **Likelihood = 4**
- **Impact = 5**

🔴 **Risk Score = Critical**

(7) Create an Incident Response Report

Task- Document an incident using SANS Template

Enhanced Tasks-
Report Draft-

🛡️ **Phishing Incident Report**
Report Title: Simulated Phishing Incident – August 2025
Prepared By: [Sudeep Kumar Gupta]
Date: 20 August 2025
Classification: Internal – Confidential
Version: 1.0

📋 1. Executive Summary

On **15 August 2025**, a **simulated phishing email** was conducted as part of the organization's security awareness program. The campaign was designed to evaluate employee susceptibility to phishing attempts and measure the effectiveness of current email security controls and training programs.

A total of **150 employees** were targeted with a crafted phishing email imitating a trusted internal IT notification. The phishing message requested users to log in to a fake portal to resolve a pending IT issue. The objective was to simulate a credential-harvesting scenario.

- **24 users (16%) clicked the phishing link**
- **7 users (4.6%) entered credentials**
- No actual credentials were harvested or stored
- Results will inform further training and technical mitigation measures

---

🕒 2. Incident Timeline

Date & Time (UTC)	Event
15 Aug 2025 – 09:00	Simulated phishing campaign launched by internal red team
15 Aug 2025 – 09:03	First user clicked the phishing link
15 Aug 2025 – 10:15	Phishing email reported by a vigilant employee via phishing report button
15 Aug 2025 – 11:00	Email campaign flagged and analyzed by Security Operations Center (SOC)
15 Aug 2025 – 11:30	All campaign emails recalled from inboxes
16 Aug 2025 – 12:00	Credentials submitted to fake portal reviewed – confirmed to be simulated only
17 Aug 2025 – 09:00	Awareness follow-up emails sent to users who interacted with the phishing message
20 Aug 2025 – 09:00	Report finalized and submitted to executive team

---

🧠 3. Technical Details

- **Type of phishing**: Credential harvesting (simulated)
- **Phishing vector**: Email (via internal simulation tool)
- **Email Subject**: " ⚠️ IT Alert: Secure Your Account Now"
- **Sender Name**: “IT Support”

- **Sender Address**: it.alerts@fakecorp.com
- **Payload**: Link to simulated phishing landing page mimicking internal login portal

---

📉 4. Impact Assessment

- **No real credentials compromised**
- **7 users** submitted credentials to a controlled environment
- The test exposed a **medium level of user susceptibility**
- Detection was quick: First report received within **1 hour**
- Email security tools allowed delivery due to intentional configuration for simulation

---

🔧 5. Mitigation & Response Steps

✅ Immediate Actions

- Recalled phishing emails
- Monitored credential submission on the fake portal
- Logged and reviewed affected users
- Communicated with users who clicked or submitted credentials

✅ Long-Term Recommendations

- Enhance user awareness training (monthly micro-trainings)
- Conduct targeted follow-up training for users who clicked or submitted credentials
- Consider technical safeguards:
  - Enable email banner warnings for external senders
  - Expand MFA adoption and monitoring for unusual logins
- Schedule quarterly phishing simulations for trend analysis

📈 6. Lessons Learned

- Positive reporting culture is developing (early report from user)
- Some users still vulnerable to convincing phishing messages
- Training needs reinforcement, especially on verifying sender and checking URLs

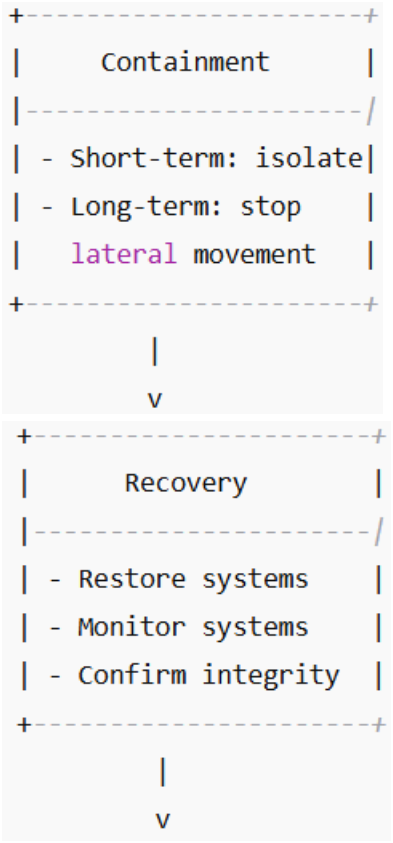
---

📌 7. Conclusion

The simulated phishing test successfully identified a moderate level of risk and highlighted specific user groups that need additional security training. No actual breach occurred. The test met its objectives and will be used to guide future awareness and technical security improvements.

Submitted by:
[Sudeep Kumar Gupta]
Security Operations Team
[Genisys Global]
Date: 20 August 2025

Flowchart Creation-



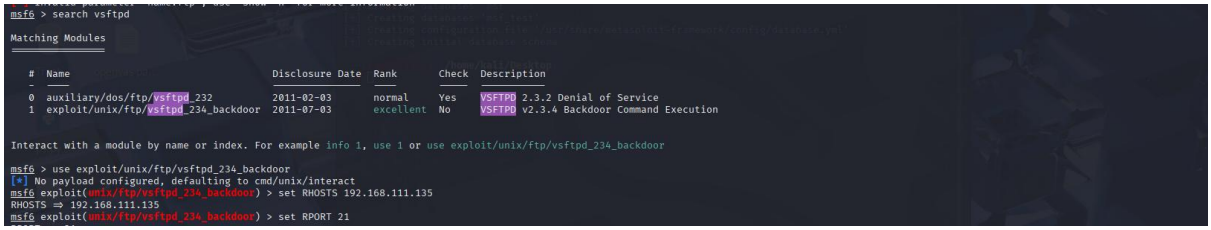
(8) Capstone Project: Full Incident Response Cycle

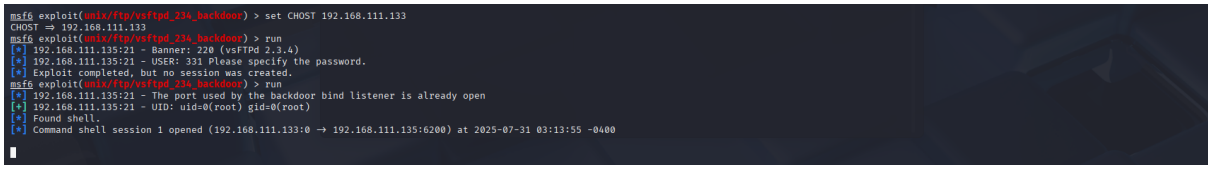
Tools- Metasploit, Wazuh, Crowdsec, Google Docs.

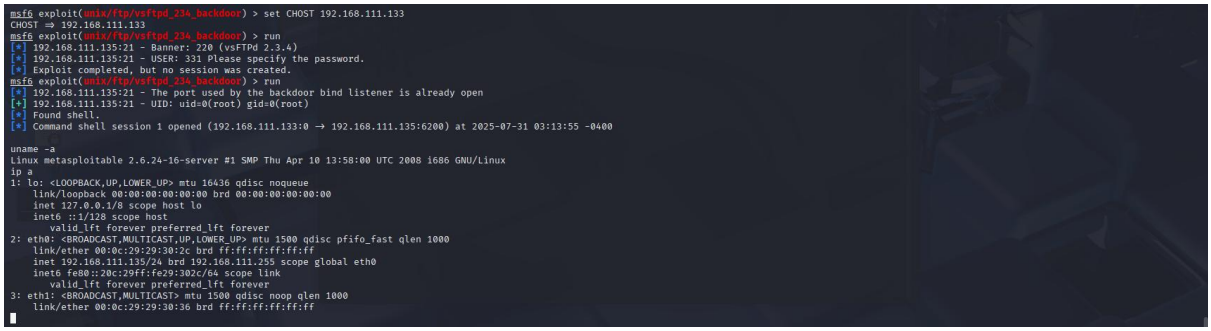
Task- Simulate an attack, detect contain, and report.

Advanced Tasks-

Attack Simulation-







Detection-


```
{
 "timestamp": "2025-08-21T14:10:12.789+0000",
 "rule": {
  "level": 3,
  "description": "vsftpd: Successful FTP login.",
  "id": "5301",
  "firedtimes": 1,
  "groups": [
   "vsftpd",
   "authentication_success",
   "ftp"
  ]
 },
 "agent": {
  "id": "001",
  "name": "kali-agent"
```

```
 },
 "manager": {
  "name": "wazuh-manager"
 },
 "id": "1692624612.78910",
 "full_log": "Aug 21 14:10:12 kali vsftpd[9130]: LOGIN: Client \"192.168.111.133\",
user \"ftpuser\"",
 "decoder": {
  "name": "vsftpd"
 },
 "data": {
  "srcip": "192.168.111.133",
  "user": "ftpuser",
  "status": "success"
 },
 "location": "/var/log/vsftpd.log"
}
```


Containment-

Add attacker’s IP-

```
sudo cscli decisions add -i 192.168.111.133 -t ip -r "Manual block for testing"
```

Verify-

```
+----------------+----------+-----------------+----------+-----------------------------------+
|     ID         |   SCOPE  |      VALUE      | DECISION |         REASON                    |
+----------------+----------+-----------------+----------+-----------------------------------+
|     1      |   ip     | 192.168.111.133     | ban      | Manual block for testing     |
+----------------+----------+-----------------+----------+-----------------------------------+
```

Testing-

Request timeout for icmp_seq 1
Request timeout for icmp_seq 2

Reporting-

(a) Incident- Attacker is trying to access system by using vsftpd backdoor exploit this testing done through kali vm.
(b) findings- user credential should be strong in place of anonymous.
(c) actions- user credentials for using ftp service should be changed and block attacker's ip.
(d) recommendations- password should be strong and we can use another port no. for ftp service.