Title : SOC Fundamentals & Operations :

Key Learnings :

a) **NIST Cybersecurity Framework** : Through NIST Framework we can learn about the lifecycle of the SOC that is

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

This Helps us understand how to respond to incidents that occur in SOC with proper approach.

b) MITRE Attack & Framework :

1) Learn about how tactics are used in real attacks
2) How alerts are used to detect attacks
3) How analysts classify and detect attacks

c) Workflow Simulations:

1) Through workflow simulations we understand how we can collect and receive auto logs, how auto tickets are created, how severity is decided for a particular incident or attack.

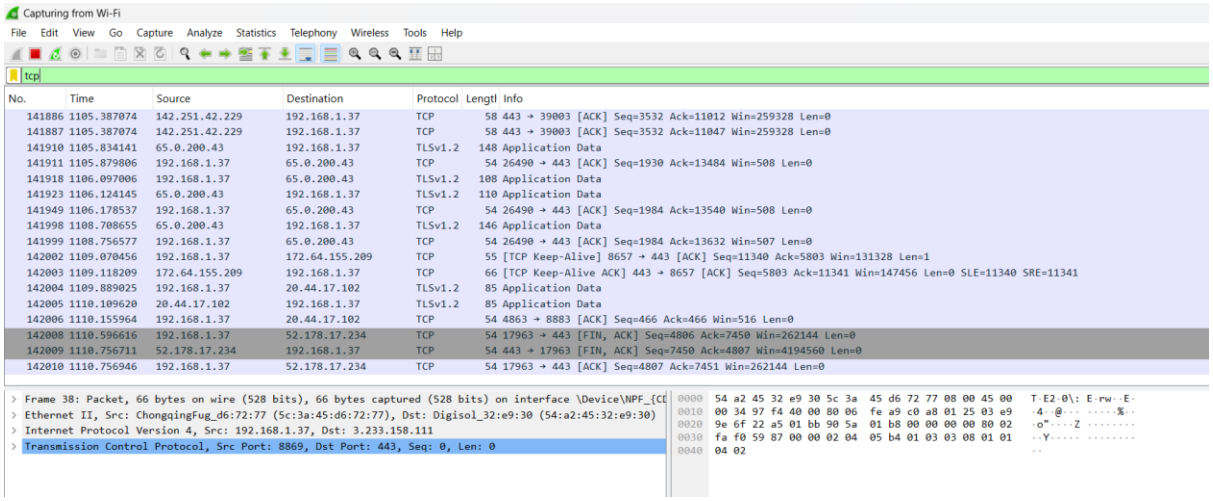
Security Monitoring Basics :

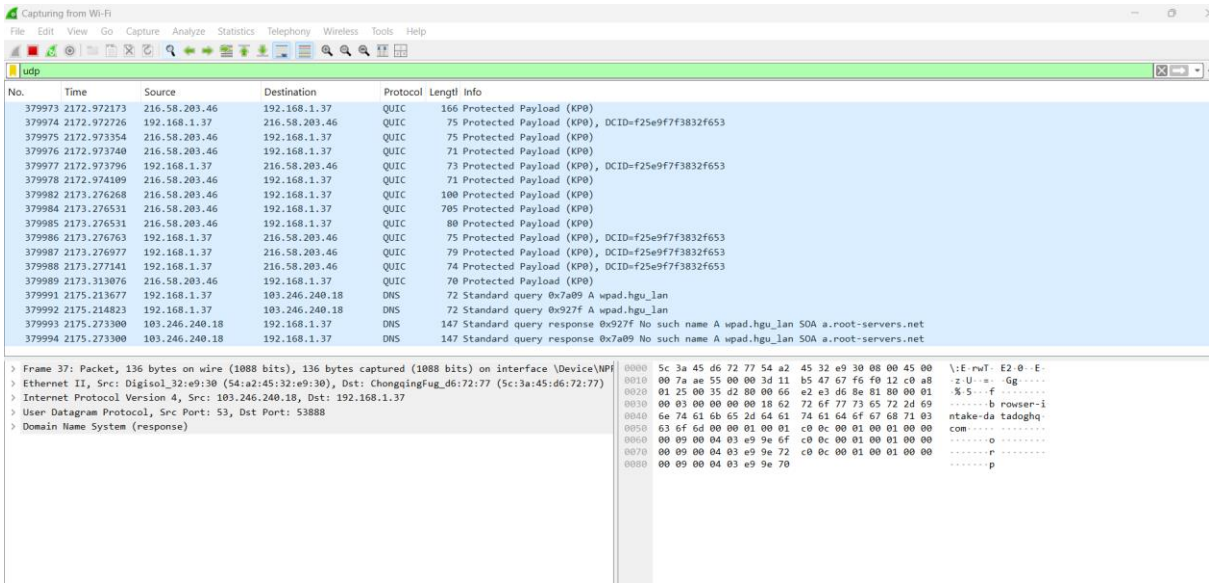
1) Through this task we can get information about spotting anomalies and strange logins
2) Noticing login failures from other countries
3) Detecting unusual traffic spike in Wireshark

- SIEM Tools : SIEM tools help collect logs, parse them and display them on dashboard through which we can figure out if there is any attack.
- Wireshark : It is tool which shows traffic packet by packet along with protocol. It is a important tool as we can see a rise in traffic if any attack happens and in this we can also filter the traffic.
- False Positive : Legitimate Event or authorised activity marked as attack or suspicious activity.
- False Negative : Attack or Suspicious activity not detected by system.
- Mean Time To Detect : How much time is taken to detect the attack.

Wireshark Traffic Captures :

Here are few traffic captures snapshots from the system with different filters :





- Through BOTS (Boss of the SOC) we can learn and identify about the attacks that happen in the SOC.

  We can learn this through the Attack Scenario Flow:

  a) Initial Access

b) Execution
c) Persistence
d) Command & Control
e) Lateral Movement
f) Impact

Through this tasks we can learn about the actual incidents that are handled in daily life in SOC and we can also think in the same way as a person handling the tasks.

- **Log Management Fundamentals** :

  There are 5 Stages of Log lifecycle

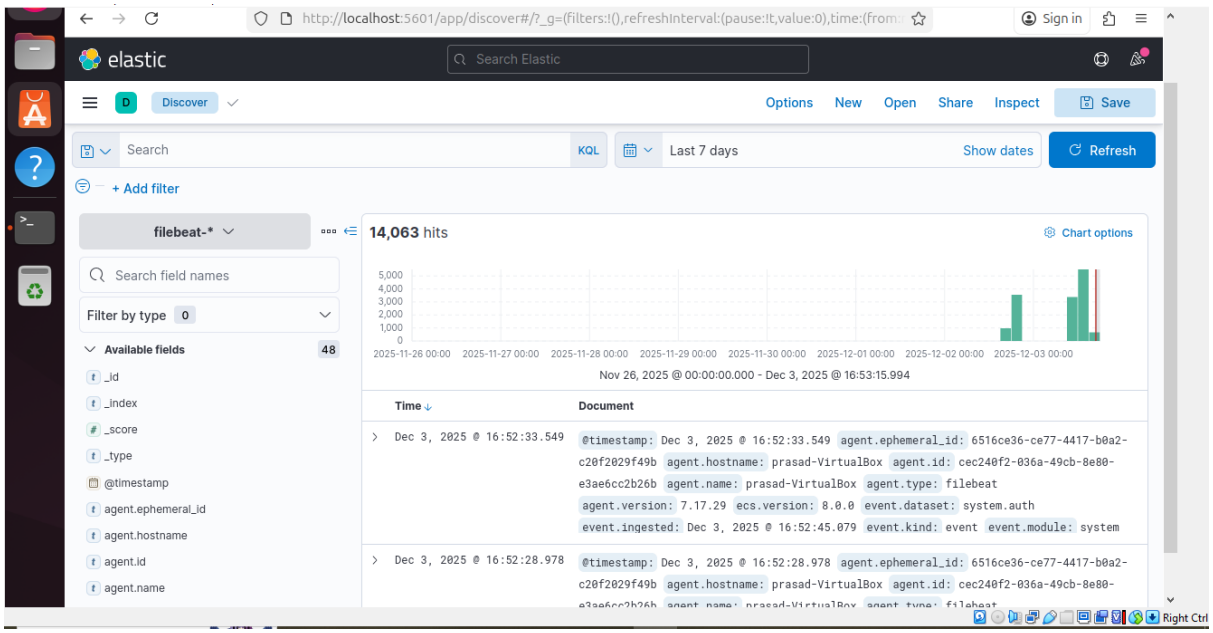
  a) Log Collection – Logs collected from Sources
  b) Normalisation – Logs converted into a consistent form
  c) Storage – Logs stored in proper format
  d) Retention – Logs kept for fixed duration of time
  e) Analysis – Analysis done from Logs to investigate alerts.

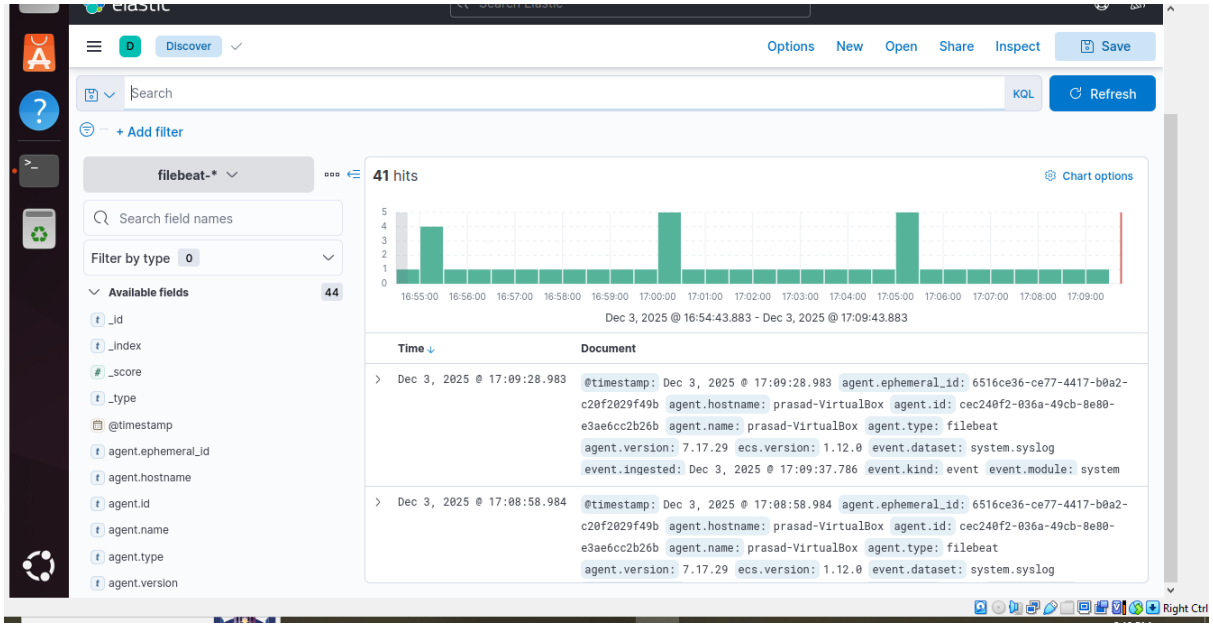
- **Practical :** Using Logstash in Ubuntu VM
  a) Update the system by **sudo apt update**
  b) Add elastic key that is needed for logstash installation
  c) Add elastic search repository
  d) Update the system
  e) Install logstash through **sudo apt install logstash -y**
  f) Create a simple log file for ingestion (logs)
  g) Add sample HTTP logs
  h) Create logstash pipeline configuration
  i) Run logstash using full path
  j) Below is the output structure :

```
eclare your desired ECS Compatibility mode.
{"message":"192.168.1.5 - - [11/Dec/2025:10:12:23 +0000] \"GET /login.php HTTP/1.1\" 200 532","@timestamp":"2025-12-03T0
5:56:32.816Z","@version":"1","path":"/home/prasad/logs/apache.log","host":"prasad-VirtualBox","tags":["_grokparsefailure
"]}{"message":"192.168.1.5 - - [11/Dec/2025:10:12:25 +0000] \"POST /login.php HTTP/1.1\" 401 123","@timestamp":"2025-12-
03T05:56:32.919Z","@version":"1","path":"/home/prasad/logs/apache.log","host":"prasad-VirtualBox","tags":["_grokparsefai
lure"]}^C[WARN ] 2025-12-03 11:43:57.303 [SIGINT handler] runner - SIGINT received. Shutting down.
```

- **Practice Task :**

a) Install and update kibana
b) After that in elastic search that is in menu at left side click explore
c) Click event analytics
d) After that select the correct data view (That is filebeat-*)
e) After that you will see the bar graphs on the view and you can filter the timestamp
f) Next step is to enter the query and you can see the graph on the scrren
g) The snapshot of bar chart are attached below.





- **Security Tools Overview**

a) The first step in Configure Snort rules to block mock attacks are

b) Install Snort in the VM (Ubuntu)

c) Verify Installation by **snort -V**

d) Create sandbox folder for custom rules

e) Open snort configuration and see if **$RULE_PATH/local.rules** is not commented

f) Create blocking rules, open local.rules and write the rule

g) The rule **drop icmp any any -> $HOME_NET any (msg:"ICMP ping blocked"; sid:1000001; rev:1;)** This rule blocks the ping packets

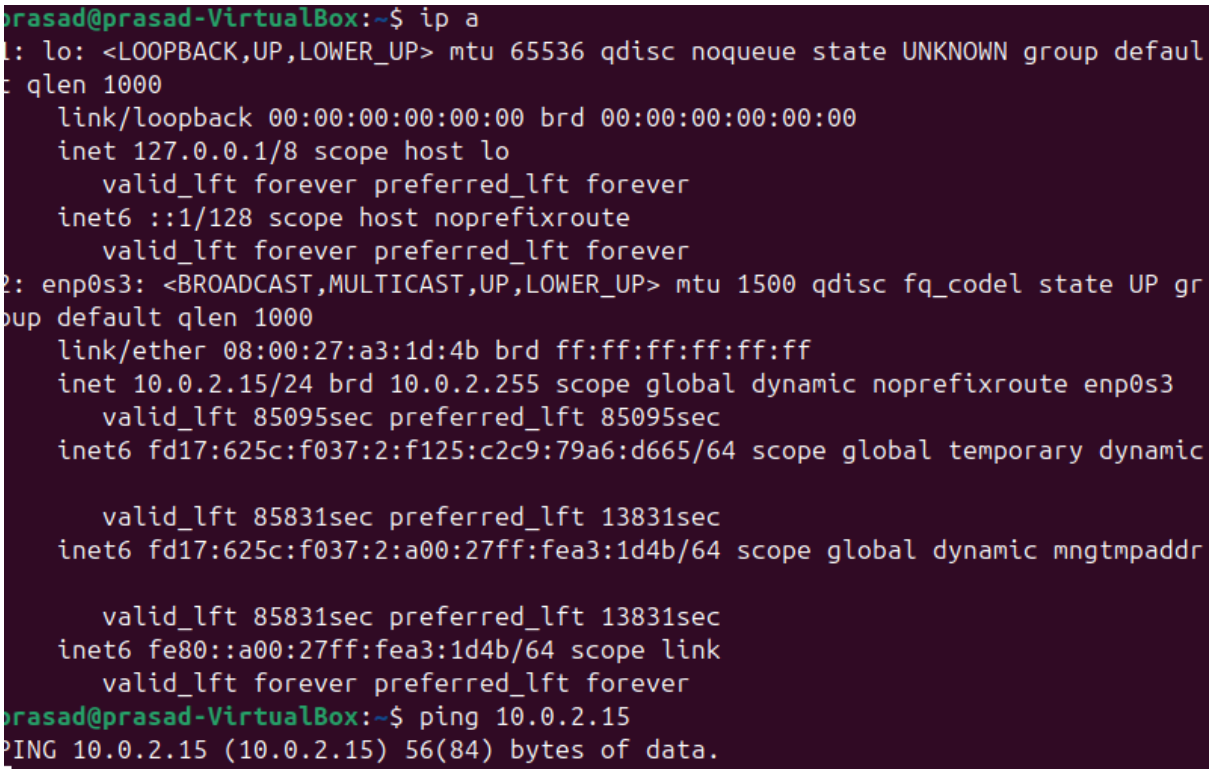
h) The next step is run snort in IPS mode as it requires NFQUEUE install it

i) The next step would be add IP table rules so that snort block traffic

j) The next step would be start snort in IPS mode

k) Then check the mock attack by ping the IP of VM

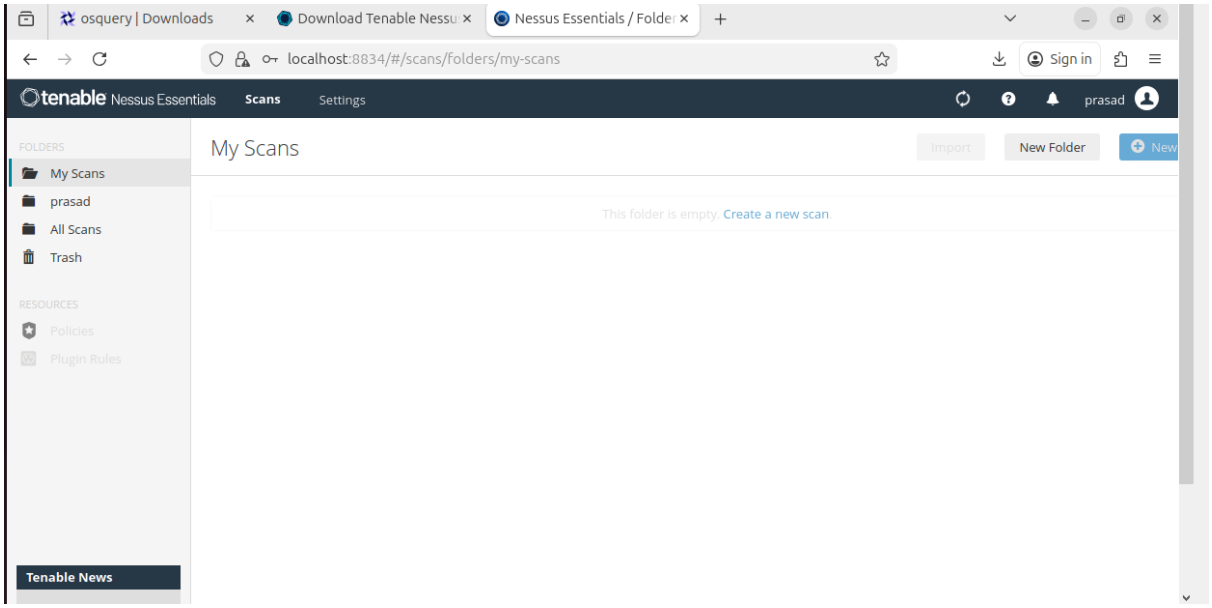
l) The output is attached in which it shows ICMP ping blocked.



- **Vulnerability Scanners (Nessus)**

  Vulnerability scanning can referred to as process of discovering a host machine and identifying the services running on it and matching it with the known vulnerabilities that is the CVE database and then assigning the severity to the vulnerability and upon that providing the remedy to it.

- Nessus can be referred to as the vulnerability assessment tool that scans machines, systems and networks to check and identify for the vulnerability like security configurations, missing patches, open ports, outdated services etc.
- Metasploitable is a vulnerable virtual machine which contains weak configurations, outdated software's etc.
- Through Nessus we can check open ports, services which are running on that and check the severity of that incidents. Below is the browser page of Nessus



- You must create a login to Nessus and sign in to it
- You can search **https://localhost:8834/** for Nessus
- After the webpage loads click on New scan and choose a template
- After that choose the name of scan and IP of vulnerable machine that is metasploit2
- Then you can choose the scan, save and launch the scan.
- Then it does the scans, vulnerability checks and port assessment.
- Then you can categorize the scan based on scores

- **Basic Security Concepts :**

a) **CIA Triad** : The CIA triad represents the core of security principles.
   1) Confidentiality : Ensuring that information is accessible to authorized users only like encrypted files, confidential documents of company.
   2) Integrity : Ensuring that the information is accurate and it has not been altered or changed at any point.
   3) Availability : Ensuring that authorized users have reliable access to the services and information.

b) Threat vs Vulnerability vs Risk
   1) Threat : Threat can be defined as the potential cause of an unwanted incident like a hacker trying to breach a server.
   2) Vulnerability : A vulnerability can be defined as a weakness or loop hole that can be exploited. Eg : weak passwords.
   3) Risk : Risk can be defined as the impact of threat exploiting the vulnerability. Eg : hacker gets access to the weak passwords of the users.

c) Defence in Depth & Zero Trust.
   1) Defence in depth can be defined as the layer wise security approach to prevent and detect attacks. For eg : Firewall + IDS + Antivirus + MFA + user training
   2) Zero Trust : It means never trust any device always verify user/device before granting access.

Learning from Equifax Breach: The main thing to understand is vulnerability exploitation due to unpatched software and teaches us that always stay updated in patch management and loopholes in that would lead to exploitation.

- **Security Operations Workflow :**
  Security Operations workflow can be defined as the structured flow of process followed by security analysts to handle security events. It helps us detect attacks or threats at a earlier stage, prioritize the events properly, investigate it and handle it. The workflow contains four core stages :

a) **Detection :** Identification of suspicious or malicious events through the security tools. For Eg : SIEM, EDR, Firewalls, IDS alerts etc.

b) **Triage :** It can be defined as identifying and classifying the incident or alerts based on severity, urgency and impact.

1) The first thing to look here is the alert or incident true or it may be false positive.
2) Determine the asset critically and then handle the incident
3) Assign the severity (Low/Medium/High Priority)
4) Escalate the incidents if required to higher authority

c) **Investigate :** Proper analysis of logs collected, endpoints and user behaviour to study and confirm the threat. The analysis can be :

1) Checking email headers
2) Analysing SIEM logs
3) Reviewing Endpoint behaviour
4) Crosschecking system logs

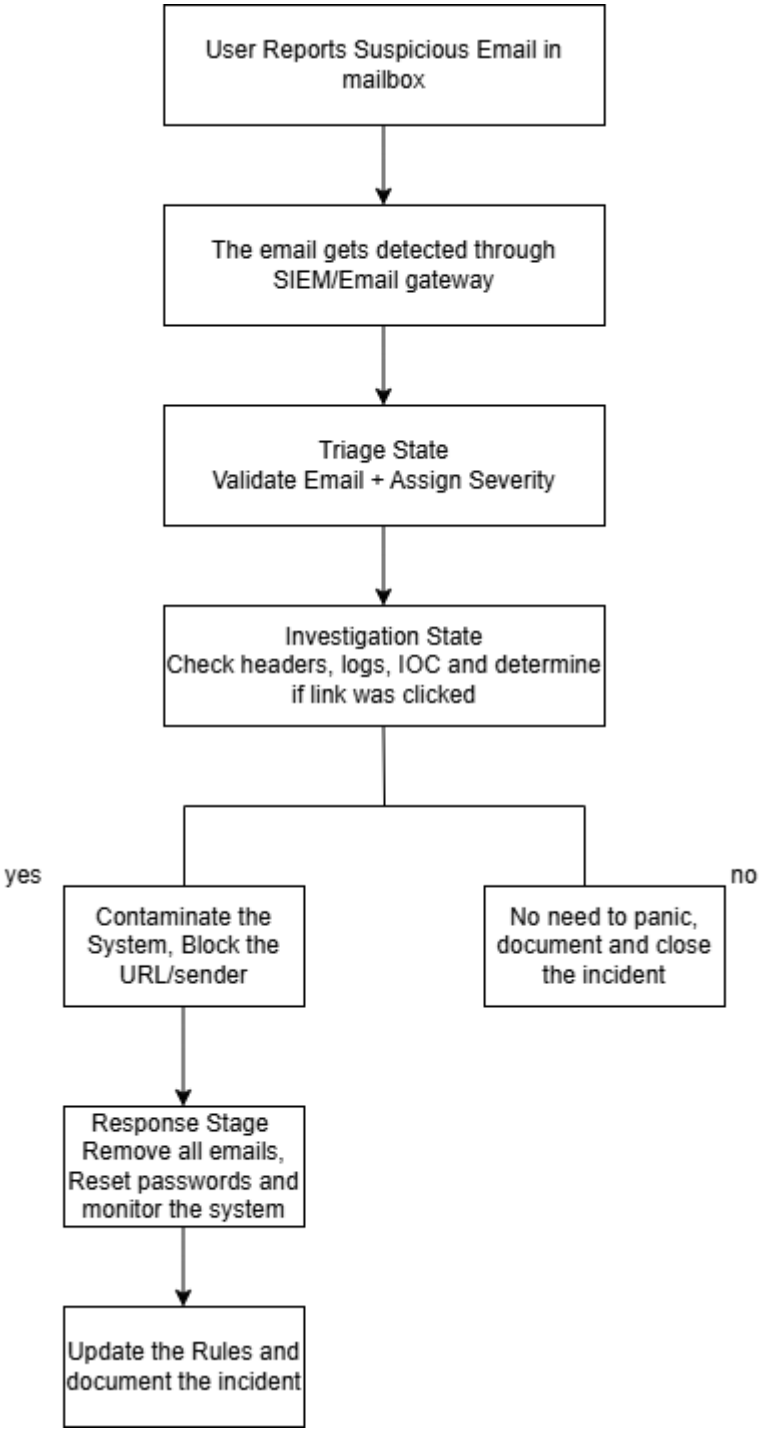
- **Response :** Response can be defined as the actions carried out to fight back the attack or malicious activity. It contains 3 parts

a) Contaminate – Block malicious IP/headers, remove fishing emails from mailbox

b) Eradicate – Delete malicious or infected files, recover the patches

c) Recover – Restore services back to normal, check if systems again get infected.

- **Flowchart for a Phishing email incident.**


User Reports Suspicious Email in mailbox
The email gets detected through SIEM/Email gateway
Triage State
Validate Email + Assign Severity
Investigation State
Check headers, logs, IOC and determine if link was clicked
yes
no
Contaminate the System, Block the URL/sender
No need to panic, document and close the incident
Response Stage
Remove all emails, Reset passwords and monitor the system
Update the Rules and document the incident

- **Incident Response Basics :**

  Incident response can be defined as the structured approach to detect, resolve and manage security incidents. The main objective is to minimize the damage through attack and recover as fast as possible.

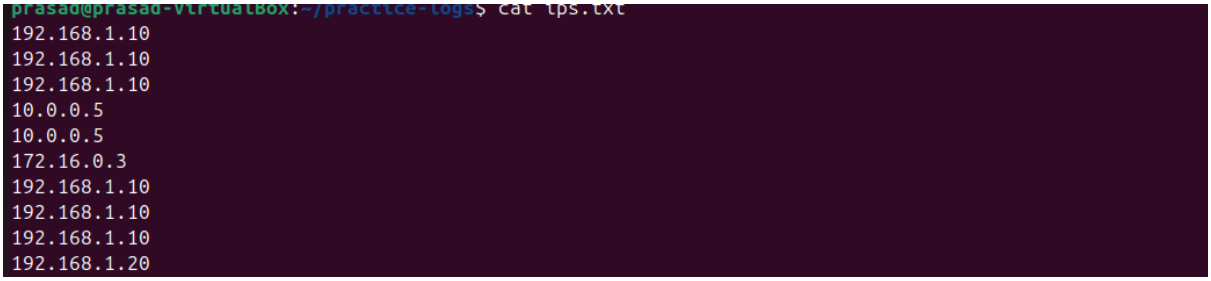
  The industry standard lifecycle follows NIST SP 800-61 Incident handling framework. The incident response lifecycle contains following stages.

  a) Preparation – Keeping the tools and processes up to date to handle incidents effectively.
  b) Identification – Analysing, Identifying, detecting and confirming that a security incident has occurred.
  c) Contaminate – Reducing the spread and impact of incident.
  d) Eradication – To eradicate/eliminate the root cause of the incident.
  e) Recovery – Restoring the affected systems and services back to normal operations.

- **Log Analysis Practice :**

In this task we are going to detect and filter the IP for failed login attempts (4625) and identify brute force attack from the logs.

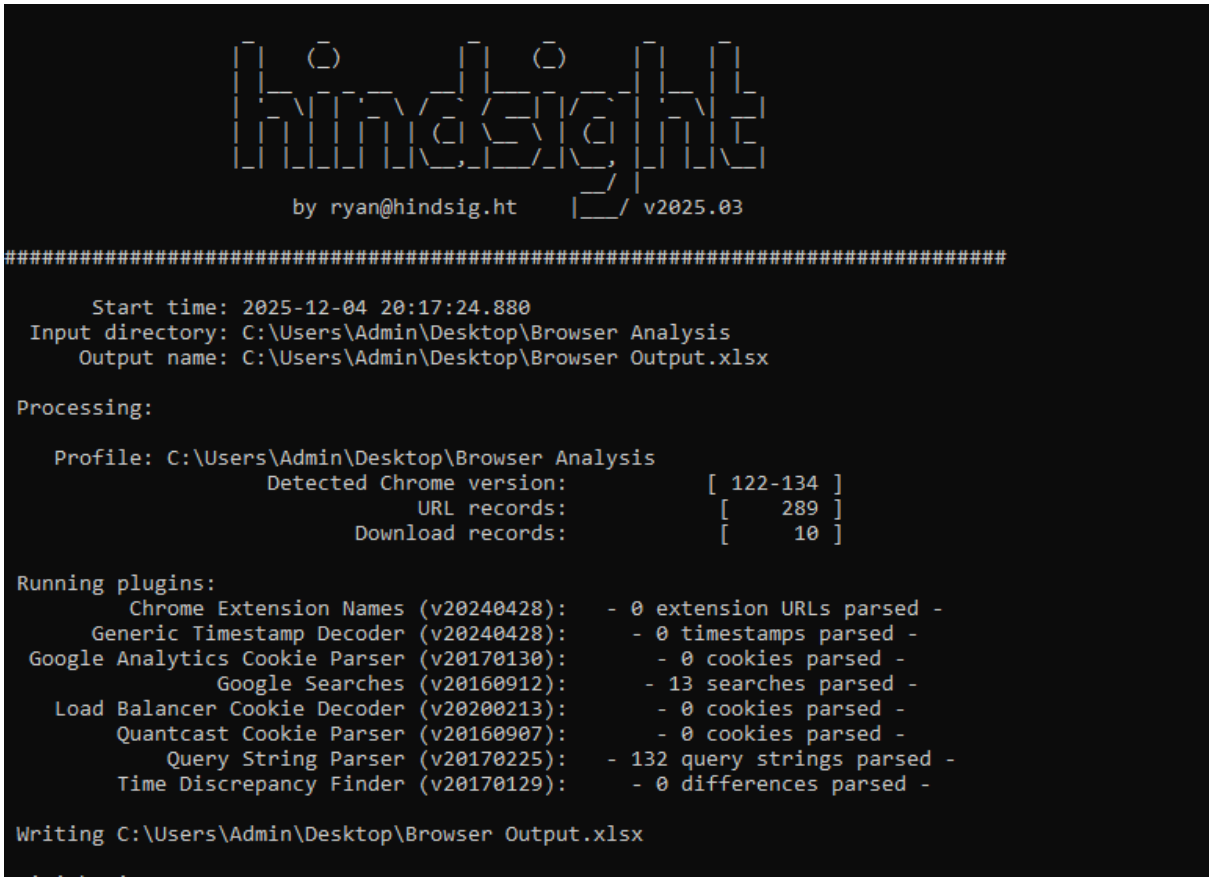
a) In this task we have taken a logs of Ips with event id, user type
b) After collecting the logs we have filtered the logs with failed attempt only.
c) Then after extracting the failed attempt only we filtered it with only IP of failed attempts. Below is snapshot of IP



d) And from this IP we have analysed for Brute force Attack with maximum attempts.

So from above snapshot we can confirm that IP **192.168.1.10** is trying for brute force attack.

- **Zimmerman Tools for analysing Chrome History :**
  a) Below are the steps for analysing chrome history using Zimmerman tools
  b) The first step is create folders for storing browser history and storing the output to another folder
  c) The next step would be installing Zimmerman from official website.
  d) Then download chrome history and store it in browse analysis
  e) Then store that downloaded and extracted files to another folder named Zimmerman to store files
  f) Copy chrome history to a folder created for analysis
  g) Run Hindsight to parse the logs of chrome history.
  h) Below is output after parsing logs



- **Security Event Documentation:**

  Security event documentation is essential for various reasons :

  1) Tracking suspicious activities
  2) Maintaining for further audits
  3) Investigating and Identifying incidents
  4) Providing reports to management

  b) The template of log would consist of:

  1) Date/Time - Exact date and Time of incident
  2) Source IP - IP address initiating the attack
  3) Event ID - Event type (Eg : 4625 – Multiple Failed Logins)
  4) Description – Explanation of what happened in the incident
  5) Action Taken – What all steps were performed when the incident occurred.

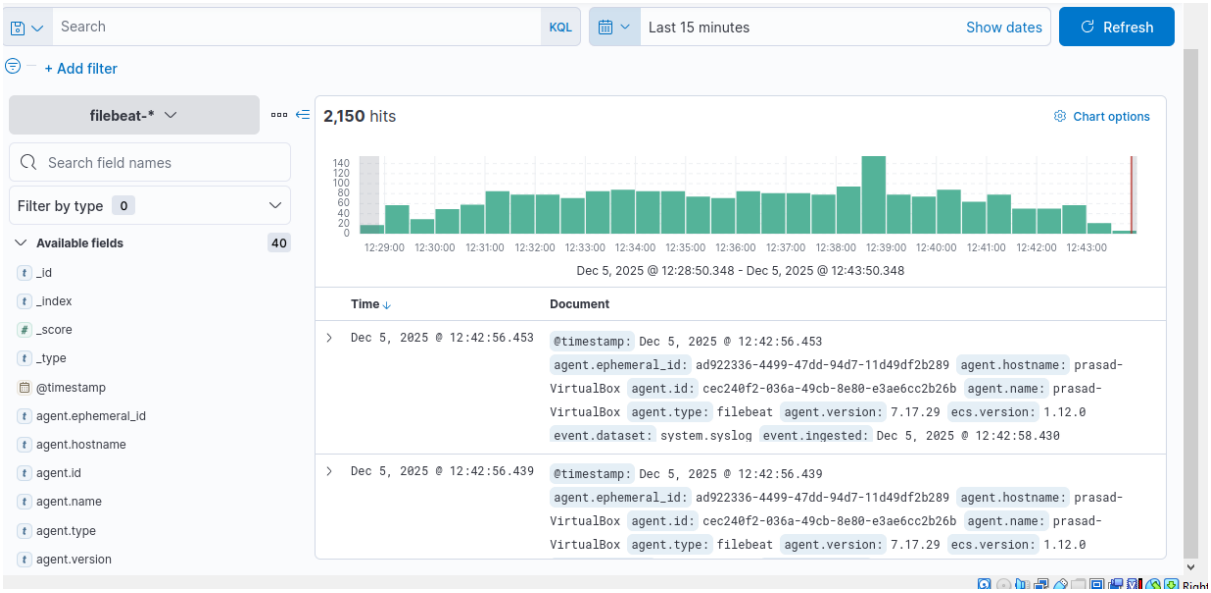
- **Mock Event Documentation :**

	Field	Value
1)	Event Date / Time	04/12/2025 14:32:24 IST
2)	Detection Time	04/12/2025 14:33:24 IST
3)	Source IP	192.168.1.10
4)	Username	root
5)	Event ID	4625 – Multiple Failed Login attempts
6)	Severity	High
7)	Description	SIEM detected multiple failed login Attempts from 192.168.1.10 within 5 minutes this indicated a potential Brute force attack.
8)	Action Taken	1. Blocked IP 192.168.1.10 2. Informed SOC lead
9)	Status	Resolved

- . **Set Up Monitoring Dashboards**

This task included generating alerts and monitoring traffic on dashboard as the traffic spikes. It includes following steps :

a) Start elasticsearch and check the status whether it is active or not
b) Start Kibana and check the status it should active and running
c) In this task we have given custom logs to the system of failed login attempts from IP
d) The next step is configure the filebeat and change enable status from false to true.
e) In configuration change the path to custom logs.
f) Save the configuration and exit it.
g) The next step is restart filebeat and check the status
h) The open kibana in VM browser.
i) In index pattern select filebeat-* and time field @timestamp
j) Then we can see a bar chart in the discover section of Analytics with hits. We can customize the timestamp. The snapshot is attached below



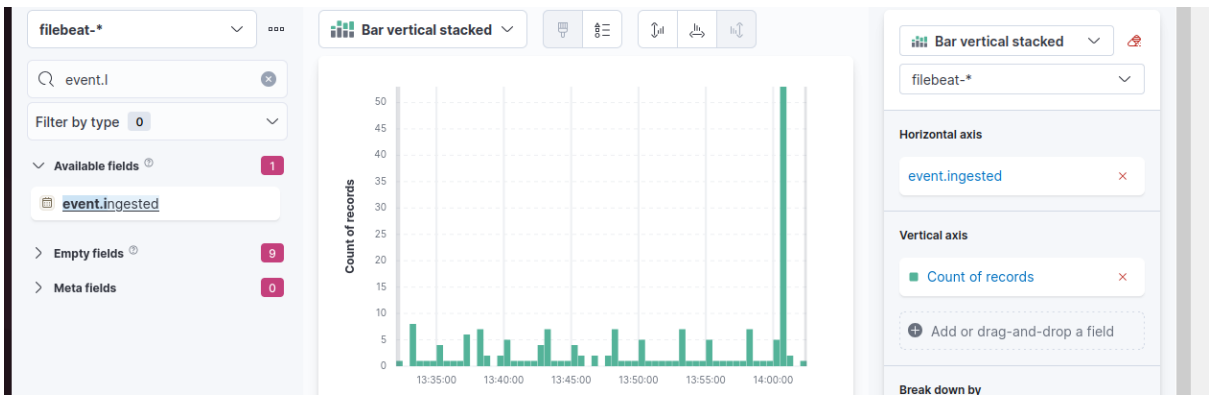
k) To visualize data we have to select the Visualize Library and in that Create Visualization and after that select lens.

l) In the lens select create new visualization and select filebeats, then select the source IP from dropdown menu and drag it.

m) This will generate the visualization of IP based count of maximum attempts with particular IP.

n) Then for Frequency of Critical Event ID select event code and evet ingested.

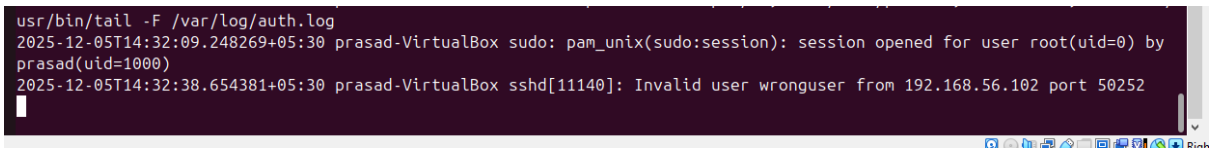
o) The snapshot is attached for event.ingested.



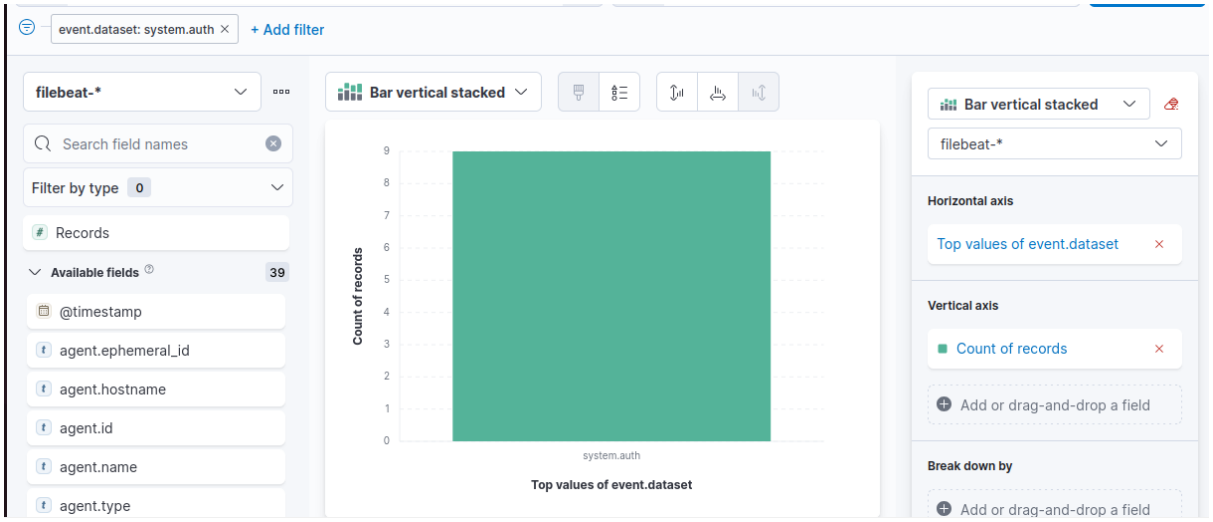
- **Configure Alert Rules :**

a) In Elastic use rules test for failed login attempts.

1) Below are the steps to be followed for the task.
2) Check elasticsearch and kibana are active and running in the VM
3) Filebeat is installed and sending logs to elasticsearch
4) Ensure that SSH is enabled and running on VM host.
5) Try to login through wrong user in another terminal and check if it pops invalid user login through a particular IP
6) The snapshot is attached below of wrong login.



7) The next step is open kibana and check for logs or hits within recent timestamp
8) Now create detection rules for 5+ failed login attempts.
9) In Kibana open security ->alerts->manage rules -> create rules
10) In create rules write a custom query and write the rule for greater than 5 attempts within 5 minutes.
11) The following is snapshot of system.auth for event dataset which shows the count for record



- **Custom Alert Rule :**

The following steps are to be followed for custom rule alert task using Wazuh.

1) The first step is to install Wazuh manager in VM machine
2) The next step is to install Wazuh Agent.
3) Verify the download status and log in to Wazuh to access the dashboard
4) The next step is to create a custom rule that is when 3 or more failed login attempts are made within 2 minutes it simulates a brute force attack.
5) The next step is to validate alert in the dashboard.
6) You can see the alerts generated in the dashboard.
7) The alerts were 3+ login attempts within 2 minutes which includes the source IP and username.
8) Mapping it with MITRE Attack the failed login attempts relate to
    a) T1110 – Brute force
9) It also demonstrates that how security teams or organizations classify the events
10) It also helps us identify attacker techniques and helps teams understand about security events and handling.