MANJIRA DAS

FIELD: SOC

DAY 01 REPORT

INDEX

SOC FUNDAMENTALS & OPERATIONS

Introduction

This section documents the purpose, structure and core functions of s Security Operations Centre (SOC). It also summarizes how the team applied two standard frameworks— *NIST* and *MITRE ATT&CK* as well as workflow simulation using **Splunk Phantom** to validate detection and response playbooks in a lab environment.

Overview of SOC Fundamentals

A security operation centre is a command centre to monitor, detect, analyse and respond to security threats in an organization. Its principal goals are,

- Identifying alerts and open incidents – Threat Detection
- Investigate the root cause and impact – Incident Response
- Recommend mitigations and remove threat.
- Constantly adapting to process and technology to improve real time as incidents occur and to reduce risk over time.

Roles In A SOC

- **Tier 1 Analyst:** This first line of defence in an organization's SOC functions known as the Triage Specialist are the initial responders to security alerts and potential threats. They collect the raw data to confirm, determine or adjust the criticality of alerts.
- **Tier 2 Analyst:** These Incident Responders serve as the bridge between initial alert triage and advance threat hunting. They review the higher-priority security incidents escalated by Triage Specialists and do a more in-depth assessment using threat intelligence such as indicators of compromise, updated rules etc. These individuals are responsible for designing and implementing strategies to contain and recover from an incident.
- **Tier 3 Analyst:** These analysts aka Threat Hunters represents the highest level of technical expertise within the security operation hierarchy. They handle major

incidents escalated to them by Incident Responders. Their work involves detailed forensic analysis, malware reverse engineering and the development of custom tools and techniques to combat evolving threats.

- **SOC Manager:** They supervise and manage the security operation team including hiring, training and evaluating team members, creating processes, assessing incident reports and developing, implementing necessary crisis communication plans. They also oversee stuff activities and review team's performances.
- **Threat Hunter:** These are the Tier 2 analysts who proactively looks fir threats inside the organization. They specialize in log review, threat hunting and research outside of the organization by analysing publicly available threat intelligence.

Key SOC Functions

- **Log Analysis:** It is the process of computer-generated event logs i.e., collecting, parsing, indexing and visualizing data to monitor systems, detect security threats or other risks. It ingest and correlate logs from network devices, endpoints, servers and cloud services. Effective log analysis improves troubleshooting, enhance organization's cyber security capabilities as well as improves customer experience.
- **Alert Triage:** It is a key process within SOC that entails the systematic evaluation, prioritization and response to security alerts. It involves swiftly assessing the threat level of a security alert and determining the appropriate course of action. This process includes reviewing, confirmation and prioritization of security alerts generated by monitoring systems.
- **Threat Intelligence Integration:** It is the process of incorporating threat days, analysis and insights into an organization's security operations to enhance their ability to detect, analyse and respond to cyber threats.

SOC Frameworks

NIST Cybersecurity Framework (CFS): The core functions of NIST CFS are—

1. **Identify:** To protect against cyber-attacks, the team needs a thorough understanding of the organization's business environment, governance, risk assessment, risk management strategy and supply chain risk management.
2. **Protect:** This function covers much of the technical and physical security controls for developing and implementing appropriate protections. These categories are identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology.
3. **Detect:** This implements measures that alert an organization to cyber-attacks. It includes anomalies and events, security, continuous monitoring and detection processes.
4. **Respond:** This function ensures the appropriate response to cyber-attacks and other cyber security events including planning, communications, analysis, mitigation and improvements.
5. **Recover:** It implements plans for cyber resilience and ensure business continuity in the event of a cyber-attacks, security breach or other events. It helps restoring operations through recovery planning, continuous improvement and communications.

MITRE ATT&CK

This framework is a universally accessible, continuously updated knowledge base for modelling, detecting, preventing and fighting cyber security threats based on criminals' known adversarial behaviours. MITRE ATT&CK use cases—

- **Detection Engineering:** enables security teams to design detections around behaviour and regardless of toolset. Teams can identify which techniques are already detected and which lack visibility, helping them prioritize sensor deployment, log enrichment, or new detection rules based on tactical risk.
- **Threat Hunting:** Hunting teams use MITRE ATT&CK to focus hypotheses. Instead of relying on broad anomaly detection, hunters align their queries to high-priority techniques observed in relevant campaigns. Because each technique includes

example procedures, data sources, and detection recommendations, ATT&CK provides a starting point for crafting hunts with operational focus.

- **Threat Intelligence Mapping:** ATT&CK creates a shared language for expressing adversary behaviour. Cyber threat intelligence teams enrich reports by tagging tactics and techniques used by threat groups. This structure allows faster triage. When a new report mentions a technique your organization already detects, you can validate coverage immediately.
- **Security Gap Assessment:** ATT&CK helps red teams emulate adversaries more accurately. Rather than relying on generic scripts, they build campaigns aligned to known actors using the same techniques, mapped across tactics. Purple teams use the same mapping to validate controls. They track detection efficacy by technique and identify which alerts were blocked, missed, or misclassified. MITRE ATT&CK becomes the blueprint for adversary simulation and response validation.

References

- https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc
- https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities
- https://radiantsecurity.ai/learn/soc-tier-1-vs-tier-2-vs-tier-3/
- https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/log-analysis/
- https://www.splunk.com/en_us/blog/learn/log-analysis.html
- https://www.ibm.com/think/topics/nist
- https://www.cisco.com/site/us/en/learn/topics/security/what-is-nist-cybersecurity-framework-csf.html
- https://www.cisco.com/site/us/en/learn/topics/security/what-is-nist-cybersecurity-framework-csf.html
- https://www.ibm.com/think/topics/mitre-attack
- https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack

SECURITY MONITORING BASICS

Introduction

This document provides an overview of the fundamentals of security monitoring, focusing on the detection of anomalies, unauthorized access, and policy violations. It outlines the key objectives, essential tools, and practical steps to set up a lab environment for security monitoring. Using sample data such as PCAP files and Indicators of Compromise (IOCs), this guide aims to facilitate learning through hands-on analysis and detection of suspicious activities.

Tools Overview

- **SIEM Tools:** Elastic SIEM (part of Elastic Stack) and Splunk are centralized platforms used to collect, correlate, and analyse security events from diverse sources. They provide real-time alerting and dashboards to monitor organizational security posture.
- **Network Traffic Analysers:** Wireshark is a powerful tool for capturing and inspecting network packets. It helps identify suspicious communication patterns, protocols, and anomalies at the packet level using PCAP files.
- **Supporting Tools:** Firewall logs track allowed or blocked network connections, IDS/IPS detect intrusions and suspicious activities, and endpoint logs provide system-level information. These tools complement SIEM and traffic analysers to provide a holistic security monitoring solution.

Setting Up a Lab Environment

- **Installing Elastic Stack:** Set up Elasticsearch, Logstash, and Kibana on Kali Linux to collect and visualize logs.
- **Enable Elastic Security / SIEM Module:**
  Activate the security module within Kibana to access detection rules and dashboards.
- **SIEM (Security Information and Event Management):** Platforms like Splunk or Elasticsearch collect, normalize, and correlate logs from various systems,

applications, and network devices. SIEMs enable real-time alerting, historical analysis, and visualization of suspicious activities.

- **Network Traffic Analyzers:** Tools like Wireshark capture and inspect network traffic at a granular level. They help identify abnormal communication patterns, unexpected protocols, or unauthorized connections that might indicate malicious activity.

Key Metrics:

- **False Positives/Negatives:** Measure the accuracy of detection. High false positives can overwhelm analysts, while false negatives represent missed threats.
- **Mean Time to Detect (MTTD):** Tracks the average time taken to detect a security event. Lower MTTD indicates faster threat recognition and a more effective monitoring setup.

Collecting Sample Logs

- Importing various log formats (syslog, Windows Event Logs) into the Elastic Stack.
- Using network capture files (PCAPs) analysed with Wireshark to identify suspicious packet flows.

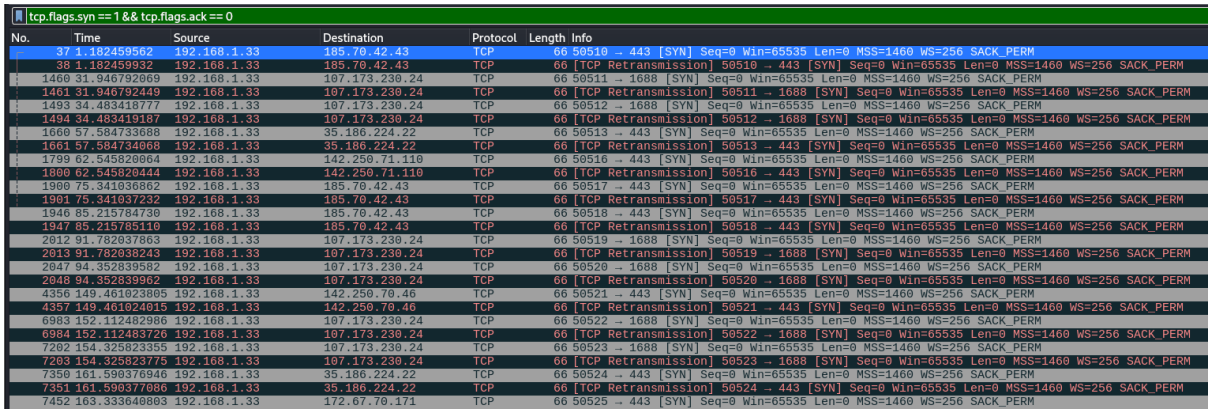
Analyse Logs for Suspicious Patterns

- **Failed Login Attempts:**

  Detect repeated authentication failures which may indicate brute force attacks or credential misuse.
- **Unusual IP Addresses:**

  Monitor for external or internal IP addresses communicating unexpectedly or generating high traffic volumes.
- **Traffic Spikes:**

  Identify sudden bursts in network traffic that may suggest scanning, denial-of-service attacks, or data exfiltration.


tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
37	1.182459562	192.168.1.33	185.70.42.43	TCP	66	50510 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38	1.182459932	192.168.1.33	185.70.42.43	TCP	66	[TCP Retransmission] 50510 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1460	31.946792069	192.168.1.33	107.173.230.24	TCP	66	50511 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1461	31.946792449	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50511 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1493	34.483418777	192.168.1.33	107.173.230.24	TCP	66	50512 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1494	34.483419187	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50512 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1660	57.584733688	192.168.1.33	35.186.224.22	TCP	66	50513 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1661	57.584734068	192.168.1.33	35.186.224.22	TCP	66	[TCP Retransmission] 50513 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1799	62.545820064	192.168.1.33	142.250.71.110	TCP	66	50516 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1800	62.545820444	192.168.1.33	142.250.71.110	TCP	66	[TCP Retransmission] 50516 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1900	75.341036862	192.168.1.33	185.70.42.43	TCP	66	50517 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1901	75.341037232	192.168.1.33	185.70.42.43	TCP	66	[TCP Retransmission] 50517 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1946	85.215784730	192.168.1.33	185.70.42.43	TCP	66	50518 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1947	85.215785110	192.168.1.33	185.70.42.43	TCP	66	[TCP Retransmission] 50518 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2012	91.782037863	192.168.1.33	107.173.230.24	TCP	66	50519 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2013	91.782038243	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50519 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2047	94.352839592	192.168.1.33	107.173.230.24	TCP	66	50520 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2048	94.352839962	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50520 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4356	149.461023805	192.168.1.33	142.250.70.46	TCP	66	50521 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4357	149.461024015	192.168.1.33	142.250.70.46	TCP	66	[TCP Retransmission] 50521 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
6983	152.112482986	192.168.1.33	107.173.230.24	TCP	66	50522 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
6984	152.112483726	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50522 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7202	154.325823355	192.168.1.33	107.173.230.24	TCP	66	50523 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7203	154.325823775	192.168.1.33	107.173.230.24	TCP	66	[TCP Retransmission] 50523 → 1688 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7350	161.590376946	192.168.1.33	35.186.224.22	TCP	66	50524 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7351	161.590377086	192.168.1.33	35.186.224.22	TCP	66	[TCP Retransmission] 50524 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7452	163.333640803	192.168.1.33	172.67.70.171	TCP	66	50525 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

1: SYN Spikes in Wireshark captured

- **Indicators of Compromise (IOCs):**

  Use threat intelligence to search for known malicious IPs, domains, file hashes, or behaviour patterns.

Use Pre-recorded Attack Scenarios

- Download datasets such as “Boss of the SOC” from public repositories.
- Replay attack scenarios in your lab to test detection capabilities of your SIEM and network analysers.
- Validate alert generation and incident response workflows based on real attack data.

1. **Loading the Dataset**
   - The *Boss of the SOC* dataset was used as it contains a variety of simulated attacks including DDoS, brute force, and malware activity.
   - The dataset files (CSV or log format) were placed in the lab environment on the Kali Linux machine for ingestion.
2. **Ingesting Data into the SIEM**
   - **Logstash** was configured to read the dataset file as input.
   - A **CSV filter** was applied to parse important fields such as:
     - saddr / daddr – source and destination IPs
   - The parsed data was sent to **Elasticsearch** using the Elasticsearch output plugin.
   - Timestamps were converted to @timestamp using the **date filter** to ensure proper time-series indexing in Kibana.

3. **Indexing and Validation**
   - The bots_ddos index was created in Elasticsearch to store the ingested data.
   - A _refresh command was issued to make the events searchable immediately.
   - Sample queries were run to ensure events were indexed correctly. For example:
   - curl -X GET "localhost:9200/bots_ddos/_search?size=5&pretty"
   - Key fields like stime, proto, sport, dport, and pkts were verified in the index mappings.

2: DDoS Attack Simulation

References

- https://www.elastic.co/guide/index.html
- https://www.wireshark.org/docs/
- https://github.com/bots-of-the-soc/bots-of-the-soc
- https://github.com/SigmaHQ/sigma
- https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices?resource=download

LOG MANAGEENT FUNDAMENTALS

Introduction

Log management is a critical component of IT security and operations. It involves the systematic collection, normalization, storage, retention, and analysis of log data to monitor system health, detect anomalies, and support incident response. This document provides an overview of the log lifecycle, common log types, and hands-on practices for managing and analyzing logs.

Log Lifecycle

The **log lifecycle** consists of the following stages:

1. **Collection:** Gathering logs from various sources such as servers, network devices, and applications.
2. **Normalization:** Converting logs into a standard format (e.g., JSON or CEF) for consistency and easier analysis.
3. **Storage:** Saving logs in a centralized location, often a log management system or SIEM.
4. **Retention:** Keeping logs for a defined period according to organizational policy or compliance requirements.
5. **Analysis:** Querying and visualizing logs to detect trends, anomalies, and security incidents.

Common Log Types

- **Windows Event Logs:** System, security, and application logs from Windows machines.
- **Syslog:** Standardized logs from Unix/Linux systems, network devices, and routers.
- **HTTP Server Logs:** Access logs, error logs, and performance logs from web servers.

Failed Logins Analysis in Kibana

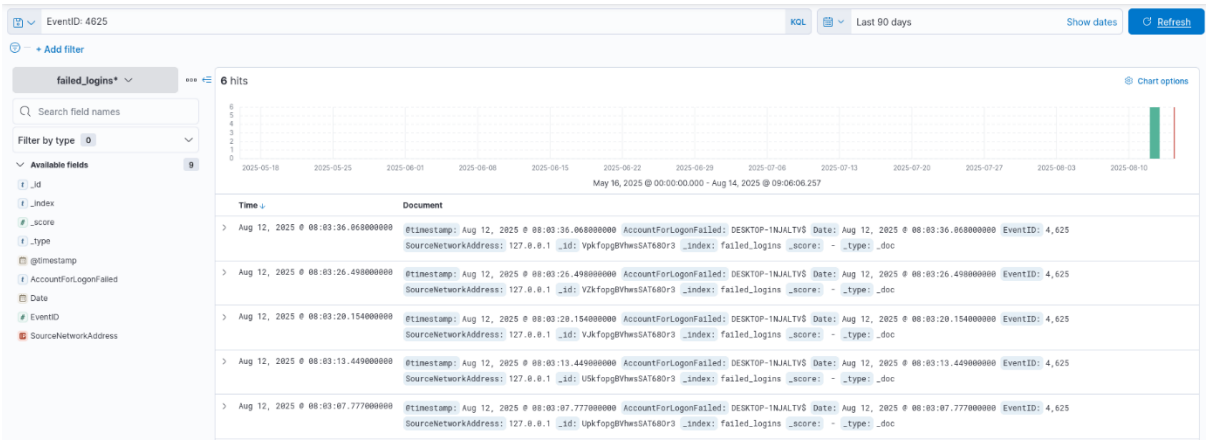
- **Upload CSV to Kibana**

    1. Open Kibana (http://localhost:5601).
    2. Navigate to **Discover → Upload File**.
    3. Use Logstash to send CSV to Elasticsearch with a config like:

```
    output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "failed_logins"
  }
}
```

4. Ensure the **timestamp field** is detected as a date.
5. Kibana will automatically create an **index** for the data.
6. Go to **Discover**, select the failed_logins index.
7. Enter KQL in the search bar:

   EventID: 4625



3: KQL Query Practice

References

- https://www.elastic.co/docs/explore-analyze/discover
- https://www.elastic.co/docs/explore-analyze/query-filter/languages/kql
- https://docs.fluentd.org
- https://learn.microsoft.com/en-us/azure/sentinel/query-logs

SECURITY TOOLS OVERVIEW

Introduction

This document provides an overview of essential cybersecurity tools, their purposes, learning approaches, and practical exercises for hands-on experience. It is intended for beginners and intermediate learners to understand and experiment with SIEM, EDR, IDS/IPS, vulnerability scanning, and endpoint monitoring tools.

Key Tools

- **SIEM (Security Information and Event Management):**
  - **Tools:** *Splunk, QRadar*
  - **Purpose:** Centralizes logs from multiple sources, monitors security events, and helps in threat detection and incident response.
- **EDR (Endpoint Detection and Response):**
  - **Tool:** *CrowdStrike*
  - **Purpose:** Detects, investigates, and responds to endpoint threats in real time.
- **IDS/IPS (Intrusion Detection/Prevention System)**
  - Tool: *Snort*
  - Purpose: Monitors network traffic to detect or block malicious activity.
- **Vulnerability Scanner**
  - Tool: *Nessus*
  - Purpose: Identifies security weaknesses and misconfigurations in systems.
  -

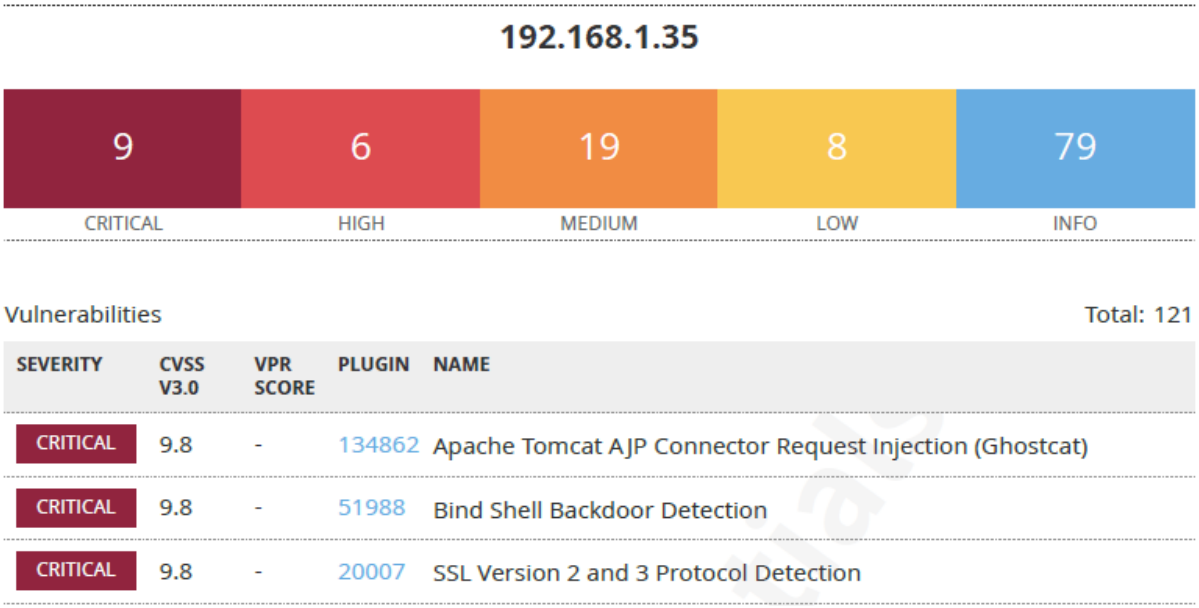
Snort Rule Testing

1. **Create a rule** to detect HTTP requests to malicious.com:
2. alert tcp any any -> any 80 (msg:"Malicious Domain"; content:"malicious.com"; http_uri; sid:1000001;)
3. **Test the rule** using:

4. curl http://malicious.com
5. **Verify** that Snort generates an alert for the request.

Nessus Scan

- Scan a **Metasploitable2 VM**. IP: 192.168.1.35
- Export the scan report and list the top 3 vulnerabilities by CVSS score.



: Nessus Scan Report

Snort Rule Testing

Tools Used

- **Snort 3.9.2.0** – Intrusion Detection and Prevention System
- **Netcat (nc)** – Tool for sending raw TCP/UDP packets
- **Curl** – HTTP client for testing (optional)
- **Kali Linux VM** – Test environment

Prepare the Rule File

1. Create the local.rules file in the Snort community rules folder:

nano ~/snort3/snort3-community-rules/local.rules

2. Add the following rule:

alert tcp any any -> any 80 (msg:"Malicious Domain"; content:"malicious.com"; sid:1000001;)

Run Snort in Console Mode

1. Used the following command to start Snort with live packet capture on the interface eth1:

sudo ~/snort3/build/src/snort -c ~/snort3/etc/snort.lua -i eth1 -A console

- -i eth1 → Specify the network interface
- -A console → Print alerts directly to the terminal

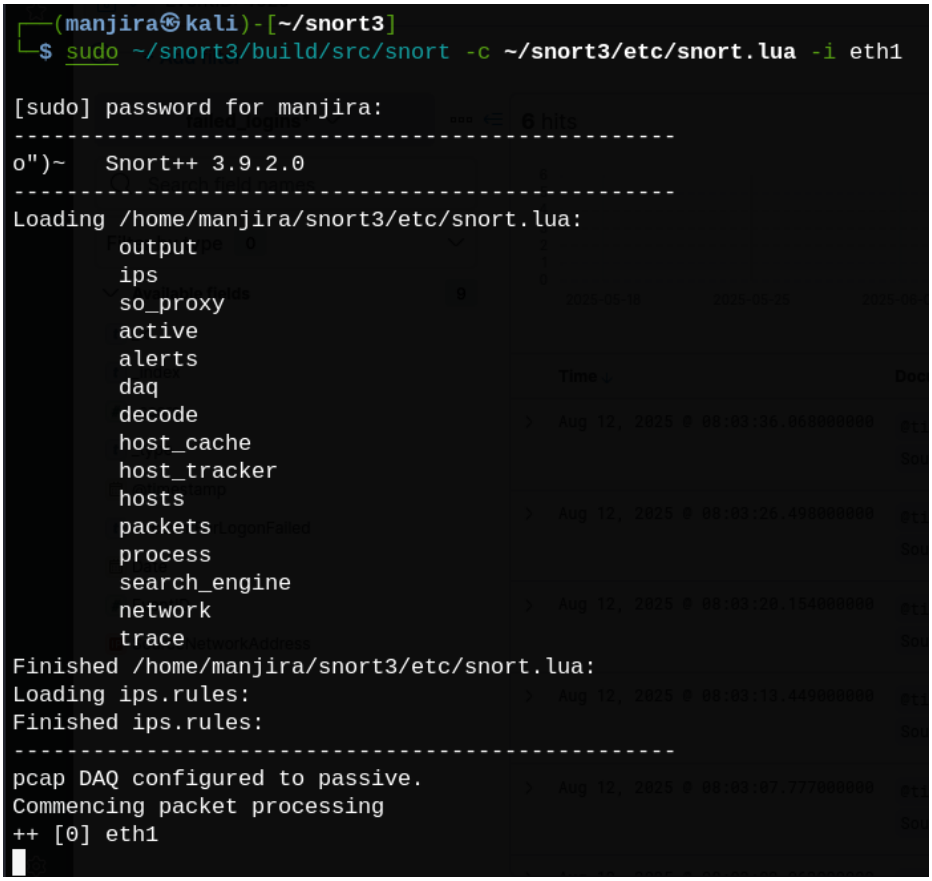
Test the Rule

Used Netcat to send a controlled HTTP request containing malicious.com:

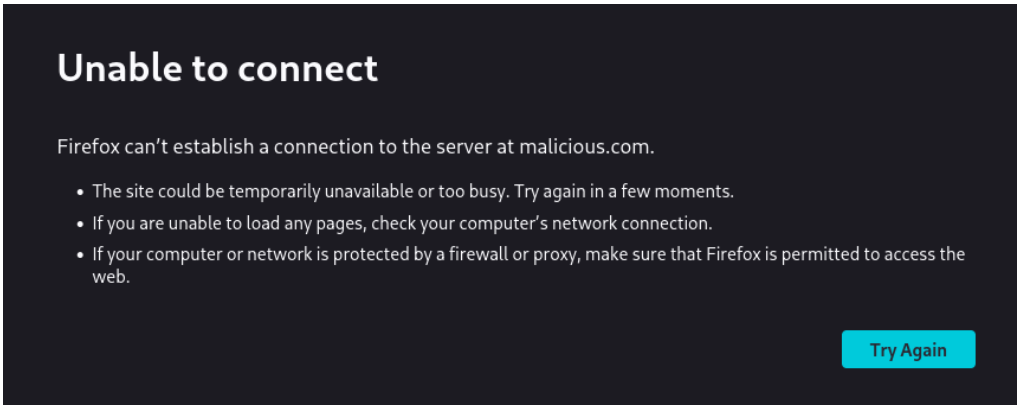
echo -e "GET / HTTP/1.1\r\nHost: malicious.com\r\n\r\n" | nc -v -w 1 192.168.1.39 80

Output

- Did not get the desired output as the Malicious domain was unable to connect.



4: Snort Successfully Running



5: Could Not Connect Malicious Domain

References

- https://www.snort.org
- https://www.snort.org/documents
- https://docs.splunk.com/Documentation/Splunk
- https://www.ibm.com/security/security-intelligence/qradar
- https://wazuh.com
- https://www.crowdstrike.com/resources/
- https://www.tenable.com/products/nessus/nessus-essentials
- https://information.rapid7.com/metasploitable-download.html

BASIC SECURITY CONCEPTS

Introduction

This section covers fundamentals security concepts essential for understanding information security principles. It explains key terminology such as **CIA Triad**, the differences between threats, vulnerabilities and risks; modern security models like defence-in-depth and zero trust.

CIA Triad

- **Confidentiality:** Ensures that sensitive date is accessible only to authorized users and protected from unauthorized access
- **Integrity:** Maintains the accuracy and trustworthiness of data, ensuring it has not been tampered with by any unauthorized individual
- **Availability:** Guarantees that data and systems are accessible when needed by authorized users, minimizing downtime or disruptions.

Threat vs. Vulnerability vs. Risk

Threat	Vulnerability	Risk
Potential malicious actors, events or circumstances that could exploit vulnerabilities to cause harm or disruption.	Weaknesses or gaps in an organization's people, process or technology that can be exploited.	The potential for loss or damage when threat exploits a vulnerability, assessed by evaluating both the likelihood and impact.

Learning

- Using flashcards to memorize and reinforce terminology and definitions.
- Studying *Equifax breach* case study which highlights the consequences of failed vulnerability management.

References

- https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/
- https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html
- https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

SECURITY OPERSTIONS WORKFLOW

Introduction

This document provides a comprehensive guide to the Security Operations workflow, specifically focusing on handling a phishing email incident. It outlines the stages of detection, triage, investigation, and response, and provides step-by-step guidance on simulating workflows using incident response platforms.

Overview of Security Operations Workflow

Security Operations (SecOps) teams are responsible for monitoring, detecting, and responding to security threats. The workflow generally involves the following stages:

- **Detection:** Alerts are generated from security tools like SIEM (Security Information and Event Management) or EDR (Endpoint Detection and Response).
- **Triage:** Incidents are prioritized based on severity, potential impact, and urgency.
- **Investigation:** Analysts correlate logs, hunt for indicators of compromise (IOCs), and gather relevant evidence.
- **Response:** Actions are taken to contain the threat, eradicate malicious elements, and recover affected systems.

Step-by-Step Guide for Phishing Email Incident

- **Detection**
    1. **Alert Generation:**
        a. SIEM detects suspicious email patterns, such as phishing links or malware attachments.
        b. EDR tools flag unusual user behavior after interacting with the email.
    2. **Initial Notification:**
        a. Analysts receive alert notifications through dashboards, emails, or mobile alerts.
- **Triage**
    1. **Severity Assessment:**
        a. Evaluate the risk level based on the email content, attachment type, and targeted users.

b. Classify the incident (e.g., low, medium, high, critical).

2. **Prioritization:**
   a. Prioritize incidents affecting high-value assets or multiple users.
   b. Determine if immediate containment is required.

- **Investigation**

1. **IOC Correlation:**
   a. Extract indicators of compromise such as suspicious URLs, IP addresses, sender domain, or file hashes.
   b. Use threat intelligence feeds to check known phishing campaigns.
2. **Log Analysis:**
   a. Correlate email server logs, endpoint logs, and SIEM data to trace the phishing attempt.
   b. Identify affected users and systems.
3. **Simulation with Incident Response Platform:**
   Use platforms like **TheHive** to simulate the workflow:
   a. Create a case for the phishing incident.
   b. Assign tasks to team members.
   c. Track evidence and investigation status.

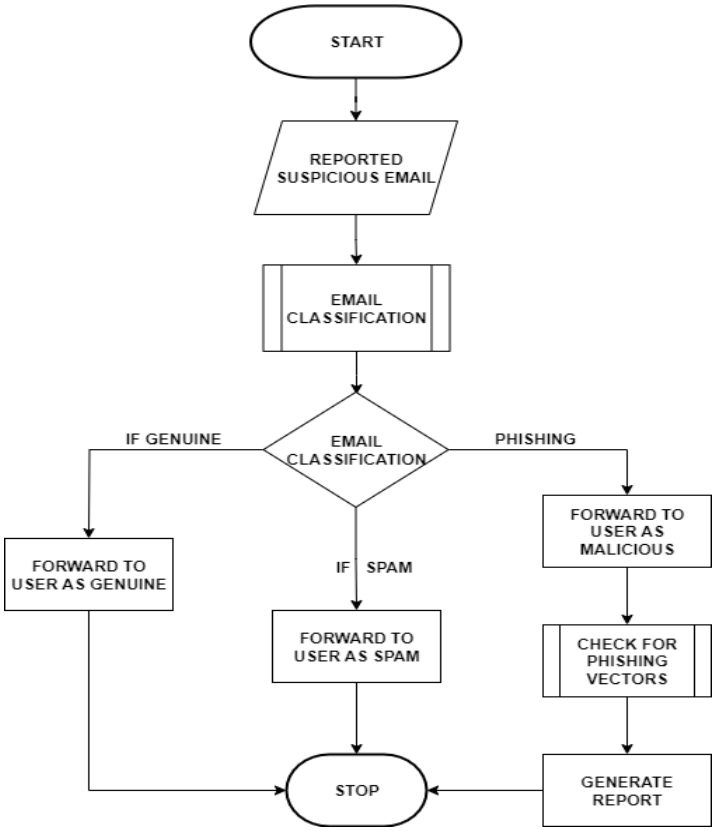
- Response

1. **Containment:**
   a. Quarantine affected endpoints.
   b. Block malicious URLs or sender domains.
   c. Reset credentials if user accounts are compromised.

- **Eradication:**
  a. Remove phishing emails from mailboxes.
  b. Delete malicious files or scripts.
  c. Apply security patches if needed.
- **Recovery & Communication:**
  a. Restore systems from clean backups.
  b. Notify stakeholders and affected users.

c. Conduct user awareness training to prevent recurrence.

Flowchart: Phishing Email Incident Response



6: Phishing Email Incident

References

- NIST Special Publication 800-61: *Computer Security Incident Handling Guide*
- TheHive Project: https://thehive-project.org/
- SIEM and EDR Documentation (Vendor-specific manuals)
- Curtailing Phishing Attacks
- Phishing Investigation | Microsoft Learn
- https://share.google/tnvNu2RenLnoOIUUq

INCIDENT RESPONSE BASIC

Introduction

Incident Response (IR) is a structured approach to managing and mitigating the impact of security incidents. It aims to quickly identify, contain, and recover from threats while learning to improve future defences.

IR Lifecycle

- **Preparation:** Establish policies, tools, and team readiness before an incident occurs.
- **Identification:** Detect and verify potential security incidents.
- **Containment:** Limit the spread and impact of the incident.
- **Eradication:** Remove the root cause of the incident from the environment.
- **Recovery:** Restore and validate system functionality and operations.
- **Lessons Learned:** Analyse the incident to improve future response and security posture.

NIST SP 800-61 Framework

The NIST Special Publication 800-61 Revision 2 is the industry-standard guide for Computer Security Incident Handling. It provides a comprehensive framework for organizations to:

- Establishing effective incident response programs.
- Preparing to handle incidents with well-defined roles and tools.
- Detect and analyze cybersecurity events.
- Contain, eradicate, and recover from incidents efficiently.
- Document lessons learned to enhance security posture.

Following this framework helps organizations respond consistently and minimize damage during incidents.

Learnings

- Studying the NIST SP 800-61 guide for detailed incident response processes.

- Conducting Tabletop Exercises simulating scenarios like ransomware attacks to practice coordination and decision-making in a safe environment.

References

- https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- SANS Incident Handler's Handbook
- https://tryhackme.com/room/cybergovernanceregulation
- https://tryhackme.com/room/windowsthreatdetection1

DOCUMENTATION STANDARD OVERVIEW

Introduction

This document provides a brief overview of essential documentation standards used in cybersecurity and IT operations. It covers key types of documentation including incident reports, runbooks, standard operating procedures (SOPs), and post-mortems. Following these standards ensures consistent, clear, and actionable documentation for effective incident response and operational continuity.

Incident Reports

Incident reports detail the nature, timeline, and impact of a security event or incident. They document the detection, investigation, mitigation, and recovery steps taken, providing a formal record for communication and review.

Runbooks

Runbooks are step-by-step guides for routine operational tasks or specific incident responses. They enable consistent execution of procedures, reduce errors, and speed up resolution times.

Standard Operating Procedures (SOPs)

SOPs define standardized processes and policies for performing various IT and security functions. They ensure all personnel follow best practices and organizational policies.

Post-Mortems

Post-mortems analyze incidents after resolution to identify root causes, successes, and areas for improvement. They support continuous learning and process enhancement.

Documentation Of A Mock DDoS Attack

- Using established templates such as the SANS Incident Handler’s Handbook.

- Practice writing documentation through exercises, such as creating mock incident reports.
- Ensuring documentation is clear, concise, and factual.
- Reviewing and updating documents regularly to keep them relevant.
- Including (mock) timelines, impact assessments, and lessons learned where applicable.

Incident Report: DDoS Attack

Incident Handler: Manjira Das
Date/Time of Report: 13-Aug-2025 14:00 IST
Incident ID: DDoS-2025-08-13-001

1. Summary

On 13-Aug-2025, at approximately 11:40 IST, multiple internal monitoring systems detected unusually high traffic to the corporate web servers. The traffic was identified as a Distributed Denial of Service (DDoS) attack targeting the public-facing web application. The incident caused intermittent service disruption but no data breach was observed.

2. Incident Classification

a. **Type:** Distributed Denial of Service (DDoS)

b. **Severity:** Medium

c. **Impact:** Availability of web application temporarily degraded; no data loss detected

d. **Category:** Network Attack

3. Detection and Identification

a. **Detection Method:**

- Network monitoring tools (NetFlow, IDS/IPS) flagged abnormal traffic patterns.

- Web application monitoring tools reported high response times and packet loss.

b. **Indicators of Compromise (IOCs):**

- Source IPs: 192.168.58.0/24, 203.0.65.51, multiple unknown international IPs
- Traffic spike: 5x normal baseline within 10 minutes
- High SYN and UDP packet rates

4. Timeline of Events

Date/Time IST	Event
11:40	Alert from IDS: abnormal traffic detected
11:50	Web application response time increases
11:55	Network team confirms high inbound traffic from multiple sources
12:00	Firewall rules adjusted to block top offending IPs
12:30	Mitigation via cloud-based DDoS protection activated
13:15	Traffic returns to baseline levels
13:30	Initial incident analysis completed

5. Containment, Eradication, and Recovery

a. **Containment:**

- Temporary IP blocks applied to the most aggressive source IPs
- Connection throttling enabled at the firewall

b. **Eradication:**

- DDoS traffic filtered via cloud-based mitigation service (e.g., Cloudflare, AWS Shield)
- Malicious bot traffic identified and blacklisted

Recovery:

- Web services restored to normal operation within 90 minutes
- Logs and packet captures preserved for further analysis

6. Root Cause Analysis

The attack was a **volumetric DDoS** originating from multiple compromised systems (botnet) across international locations. The attack targeted HTTP/S ports and DNS resolution requests, overwhelming server resources. No system compromise or data exfiltration occurred.

7. Lessons Learned / Recommendations

a. **Monitoring:** Enhance network traffic monitoring and alert thresholds for early detection.
b. **Mitigation:** Maintain active DDoS protection solutions (cloud-based or on-premise).
c. **Incident Response:** Ensure IR team has pre-approved firewall and mitigation playbooks.
d. **Communication:** Notify stakeholders promptly; provide external communication guidance.
e. **Future Prevention:** Conduct regular DDoS simulation exercises to validate defenses.

8. References / Evidence

a. IDS logs: /var/log/snort/alert
b. Firewall logs: /var/log/ufw.log
c. Traffic captures: ddos_capture_2025-08-13.pcap
d. Monitoring dashboards: Kibana and NetFlow charts

Note: All IP addresses and data in this report are **mock/fake**, safe for documentation and training purposes. The structure follows the **SANS Incident Handler's Handbook** template.

End of mock document.

References

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

LOG ANALYSIS PRACTICE WITH DOCUMENT SECURITY EVENTS

Introduction

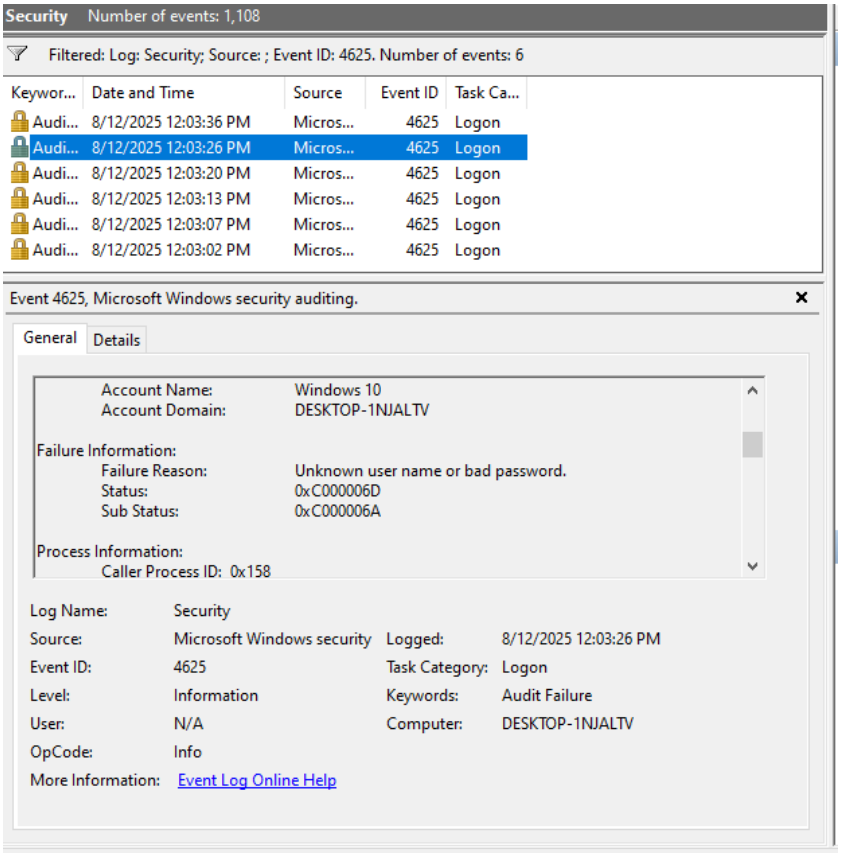
This document provides a step-by-step guide to perform practical log analysis tasks on a Windows virtual machine (VM). It covers simulating failed login attempts to generate security logs, analysing Windows Event Viewer logs for brute-force detection, and parsing Chrome browser history using specialized forensic tools. The goal is to help users practice incident detection and data parsing using both built-in and third-party tools.

Log Analysis Practice

Windows security logs capture critical events such as failed login attempts (Event ID 4625). Analysing these events helps identify brute-force attacks and unauthorized activities. Browser history analysis uncovers potentially malicious URL visits.

Simulating Failed Logins

- **Generating Event ID 4625 entries in Windows Security logs.**
    1. Setting password on Windows VM user account
    2. Locking Windows screen
    3. **Attempting to login with an incorrect password:** Enter wrong password 6 times to trigger failed login events.
    4. **Verifying logs in Event Viewer:** On Windows Run: eventvwr.msc. Navigate to Windows Logs → Security. Filter current log by Event ID 4625.



7: Windows Security Logs

- **Exporting Event Logs to CSV**

1. On Windows PowerShell Admin, running command: Get-WinEvent -FilterHashtable @{Id=4625} | Export-Csv -Path "C:\Temp\failed_logins.csv" –NoTypeInformation
2. Open the CSV file with Excel or a text editor for analysis.

	A	B	C	D
1	Date	EventID	AccountForLogon Failed	SourceNetwork Address
2	2025-08-12T12:03:02.0630000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
3	2025-08-12T12:03:07.7770000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
4	2025-08-12T12:03:13.4490000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
5	2025-08-12T12:03:20.1540000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
6	2025-08-12T12:03:26.4980000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
7	2025-08-12T12:03:36.0680000Z	4625	DESKTOP-1NJALTV$	127.0.0.1
8				

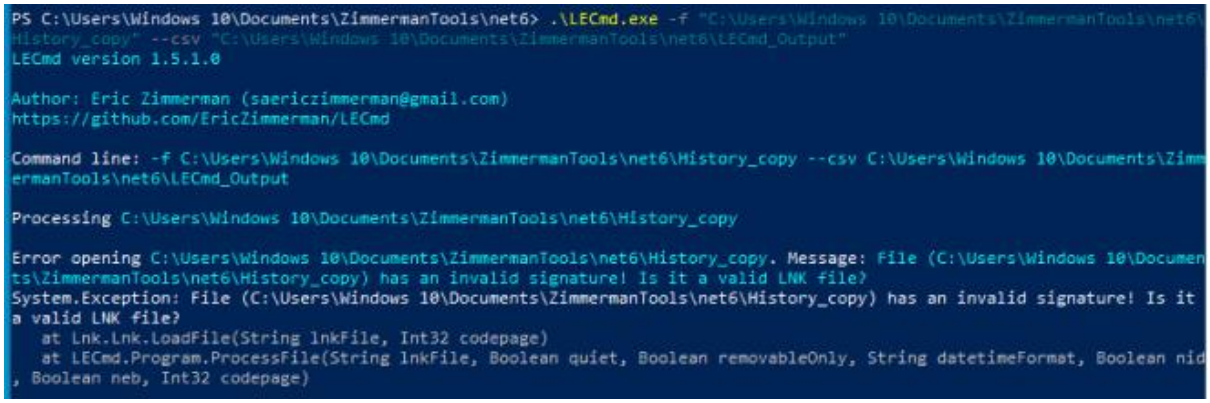
8: Event Logs in CSV

Chrome Browser History Analysis

Chrome stores browsing history in a locked SQLite database file. Forensic analysis requires accessing a copy of this file and using specialized tools to parse URLs and visit timestamps.

- **Tool Selection and Limitations**

Initially, LECmd by Eric Zimmerman was supposed to using for parsing the Chrome History file. However, the tool is designed to process Windows shortcut (.lnk) files and could not handle the Chrome History SQLite database, resulting in "invalid signature" errors.
Due to this limitation, the open-source tool ChromeHistoryView by NirSoft was used instead. This tool is specifically built to read and analyse Chrome browsing history files efficiently.



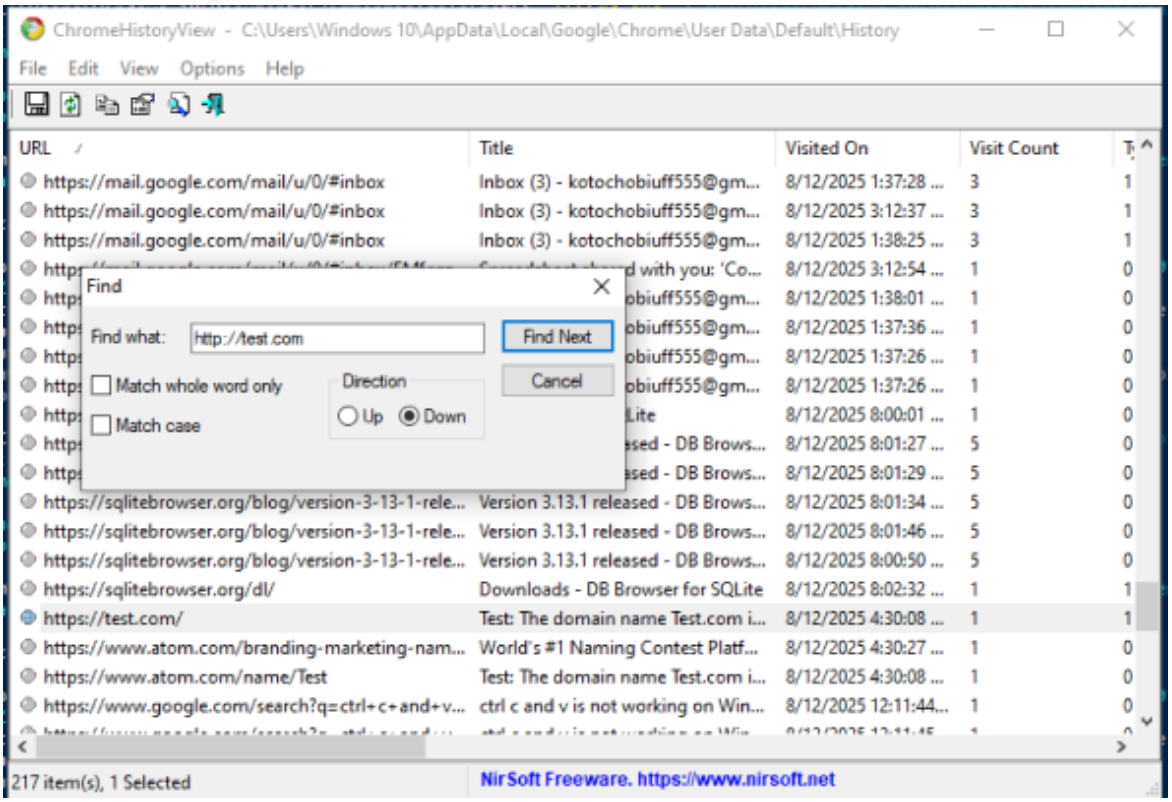
9: Zimmerman Tool Didn't Execute

- **Preparing the History File**

1. Closing Chrome completely to release file locks (checking Task Manager to ensure no chrome.exe processes are running).
2. Copying the History file
   Path: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History
   Paste the copy in a working directory (e.g., C:\Users\Windows 10\Documents\ZimmermanTools\).

- **Using ChromeHistoryView**

1. Download ChromeHistoryView from NirSoft: https://www.nirsoft.net/utils/chrome_history_view.html
2. Extracting the ZIP and run ChromeHistoryView.exe.
3. In the tool, select File →Select History File, then browse to the copied History file.
4. The tool displays URLs, visit count, and timestamps.
5. Use Find (Ctrl+F) to search for specific URLs (e.g., http://test.com).



10: ChromeHistoryView

Detailed Failed Login Attempts

Following is the detailed documentation of individual failed login attempts detected from the Windows Security logs. Each attempt is listed with its precise timestamp.

Date/Time	Source IP	Event ID	Description	Action Taken
2025-08-12 12:03:02	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.
2025-08-12 12:03:07	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.
2025-08-12 12:03:13	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.
2025-08-12 12:03:20	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.
2025-08-12 12:03:26	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.
2025-08-12 12:03:36	127.0.0.1	4625	Failed login attempt for user "Windows 10" on local machine.	No action taken yet; logs recorded for investigation.

Reference

- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625
- https://learn.microsoft.com/en-us/powershell/
- https://www.nirsoft.net/utils/chrome_history_view.html
- https://ericzimmerman.github.io/

SET UP MONITORING DASHBOARD

Introduction

This document provides a detailed overview of setting up monitoring dashboards to visualize critical network activity. It explains the steps taken, tools used, and challenges faced during the process. The focus is on creating visualizations for top source IPs and critical events using Kibana, as Sigma rule integration could not be completed.

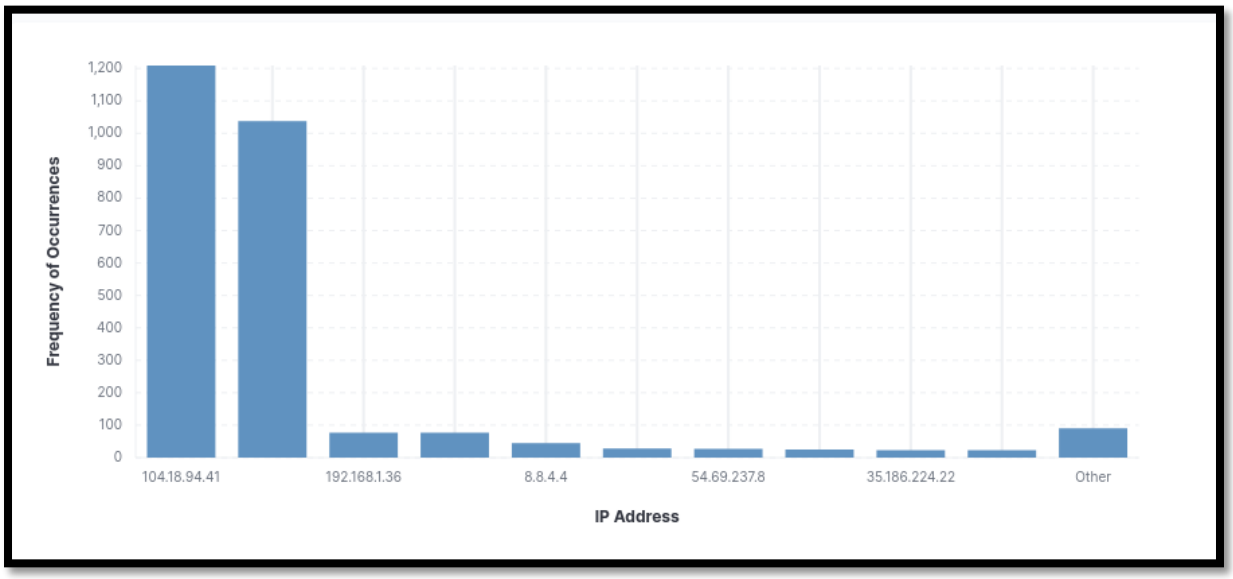
Step-by-Step Guide

- **Uploading Data to Kibana**

    1. Export network traffic data to a CSV file.
    2. Ensure timestamps are correctly formatted in ISO 8601 to be compatible with Kibana.
    3. Open Kibana and navigate to Stack Management → Index Patterns.
    4. Create a new index pattern pointing to the uploaded CSV data.
    5. Verify that all fields, including frame.time_full, are correctly mapped.

- **Creating Visualizations**

    1. Go to Kibana → Visualize Library.
    2. Create a new Bar Chart or Pie Chart for: - Top 10 source IP addresses. - Frequency of critical Event IDs.
    3. Configure the aggregation: - X-axis: IP addresses - Y-axis: frequency of occurrences.
    4. Save each visualization.



11: Visualization of IP Address Activity

- **Building the Dashboard**

1. Navigate to Kibana → Dashboard.
2. Add the saved visualizations to the dashboard.
3. Arrange and resize visualizations for clarity.
4. Save the dashboard for ongoing monitoring.

Sigma Rule Integration

c. Sigma is a generic signature format for SIEM systems that allows rules to detect suspicious activities across different platforms.

d. Challenges faced:

- Sigma CLI (sigmac) was not accessible due to version incompatibilities and Python environment issues.
- Docker images for Sigma could not be pulled because the repository sigmahq/sigma does not exist or requires authentication.
- Attempts to install older pySigma versions resulted in dependency conflicts with required pyparsing versions.

References

- https://www.elastic.co/guide/en/kibana/current/index.html
- https://github.com/SigmaHQ/sigma
- https://www.iso.org/iso-8601-date-and-time-format.html

Incomplete Tasks

1. **Logstash Automation / Splunk Automation Start-up**
    - **Task:** Start and automate Logstash/Splunk tasks for data ingestion.
    - **Reason Not Completed:** T there were prior issues with Splunk automation setup, including permission errors and directory ownership problems that were not fully resolved.

2. **Wazuh Docker Agent Log Collection Testing**
    - **Task:** Verify Wazuh single-node Docker setup for collecting agent logs and test alerts.
    - **Reason Not Completed:**
        - Encountered persistent errors in agent control (Cannot find 'queue/db/wdb') and the system could not process logs properly; testing was postponed.
        - Also due to low RAM and storage issues, causing both Windows and Ubuntu VMs to run very slowly and unstably.