Project of Mohammad Aminul Islam

Name: Mohammad Aminul Islam

Project Title: Incident Handling & Network Threat Detection Using SIEM and Packet Analysis Tools.

Professional Summary:

I am **Mohammad Aminul Islam**, a cybersecurity practitioner with hands-on experience in **incident response**, **threat detection**, and **network traffic analysis**. Through real-world simulations and investigative use of industry tools, I have developed a strong skill set in identifying and mitigating cyber threats such as **phishing attacks**, **malware infections**, and **data exfiltration**.

My expertise includes working with tools like **Chronicle SIEM**, **Splunk**, **Wireshark**, and **Suricata** to analyze security events, uncover anomalies, and strengthen organizational defenses. I follow structured methodologies such as the **NIST Incident Response Framework**, ensuring a complete cycle of **detection**, **containment**, **eradication**, and **post-incident analysis** to continuously improve security posture.

Objective:

The goal of this project was to simulate and document real-world cybersecurity incidents to enhance practical response capabilities. This involved detecting and analyzing phishing attacks, malware infections, and suspicious network activity using a range of forensic and monitoring tools. The objective was to **strengthen threat visibility**, sharpen investigative skills, and **develop incident handling techniques** aligned with professional cybersecurity operations and best practices.

Incident Handling & Threat Investigation Journal

Date: 05-02-2024	**Entry: 01**
Description	Analyzed a phishing email incident to determine affected assets and potential compromise.
Tool(s) used	Chronicle SIEM
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Unknown attacker using a phishing email campaign. • **What** happened? Employees received a phishing email containing a suspicious domain. Some accessed the link, potentially exposing credentials. • **When** did the incident occur? January 30, 2024, at 10:45 AM UTC. • **Where** did the incident happen? Emails were sent to multiple employees within the organization. • **Why** did the incident happen? The phishing email bypassed email security filters and was opened by users.
Additional notes	Chronicle was used to investigate affected assets, the domain's reputation, and HTTP POST requests that indicated potential credential theft. Next steps include containment and implementing stricter email filtering policies.

Date: 01-02-2024	**Entry: 02**

Description	Investigated a suspicious file hash using VirusTotal and Splunk.
Tool(s) used	VirusTotal, Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Potential attacker distributing a malicious file via email. • **What** happened? An employee downloaded an attachment that triggered an alert. • **When** did the incident occur? January 31, 2024, at 2:15 PM UTC. • **Where** did the incident happen? Affected endpoint was an employee's laptop (HOST-123). • **Why** did the incident happen? The employee downloaded an unknown executable file that bypassed basic endpoint security.
Additional notes	The file hash was analyzed in VirusTotal and flagged by multiple vendors as malware. Splunk logs confirmed execution attempts. The file was quarantined, and the employee's system was reimaged.

Date: 28-01-2024	**Entry:0 3**
Description	Performed packet capture analysis to detect unauthorized network traffic.
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident?

	Captured network traffic using Wireshark for 10 minutes. • **What** happened? Applied filters to analyze suspicious outbound connections. • **When** did the incident occur? Identified high-volume data exfiltration to an unknown IP address. • **Where** did the incident happen? Cross-referenced IP in threat intelligence databases; confirmed as a known C2 server. • **Why** did the incident happen? Alerted the SOC team for immediate containment.
Additional notes	A compromised endpoint was exfiltrating data to a remote server. The host was isolated, credentials were reset, and logs were archived for further forensic analysis.

Date: 25-01-2024	**Entry: 04**
Description	Created and tested a custom Suricata rule to detect suspicious HTTP traffic.
Tool(s) used	Suricata
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Defined a rule to trigger alerts on HTTP GET requests containing suspicious keywords. • **What** happened? Applied rule to test environment and replayed a malicious traffic sample.

	• **When** did the incident occur? Verified rule triggered expected alerts in eve.json. • **Where** did the incident happen? Adjusted rule sensitivity to reduce false positives. • **Why** did the incident happen? Successfully deployed rules into the production IDS for monitoring.
Additional notes	The rule significantly improved detection accuracy for phishing-related web traffic. Future improvements include refining detection logic for broader coverage.

Reflections/Notes:

1. Yes, investigating packet captures in Wireshark was challenging at first due to the large volume of data and the need for filtering techniques. However, after practicing with different filters and understanding network protocols, I became more comfortable analyzing traffic.

2. Yes, I now understand the importance of structured incident response using the NIST framework. Previously, I focused on detection, but now I realize how containment, eradication, and post-incident analysis are equally important.

3. I enjoyed working with SIEM tools like Splunk and Chronicle. Their powerful search and correlation features made it easier to analyze large datasets and uncover security incidents. I also liked how Splunk's SPL queries allowed for fine-tuned searches.

Conclusion: This project not only deepened my technical abilities but also enhanced my understanding of structured incident response. Initially, working with tools like Wireshark was challenging due to the complexity and volume of network data, but through consistent practice, I gained confidence in filtering and protocol analysis. I also came to appreciate the full cycle of the NIST Incident Response Framework—realizing that detection is just the beginning, and that containment, eradication, and recovery are equally critical. Leveraging SIEM tools like Splunk and Chronicle gave me firsthand experience in correlating events and uncovering security incidents through advanced querying and analysis. Overall, this hands-on project has prepared me for real-world roles in cybersecurity operations and solidified my passion for threat detection and response.