Incident handler's journal

Date: 15/07/2024	**Entry: #**1
Description	Documenting a cybersecurity incident This incident unfolded in two main phases: 1. **Detection and Analysis:** The organization initially detected the ransomware incident and began analyzing it. For the analysis phase, they reached out to several other organizations for technical assistance. 2. **Containment, Eradication, and Recovery:** The organization took several steps to contain the incident, such as shutting down their computer systems. However, realizing they needed help to fully eradicate the ransomware and recover, they sought assistance from multiple organizations.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who:** An organized group of unethical hackers • **What:** A ransomware security incident • **Where:** At a health care company • **When:** Tuesday 9:00 a.m. • **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.

Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: 17/07/2024	**Entry: #2**
Description	Analyzing a packet capture file.
Tool(s) used	For this activity, I utilized Wireshark to examine a packet capture file. Wireshark, a network protocol analyzer with a graphical user interface, is invaluable in cybersecurity as it enables security analysts to capture and scrutinize network traffic. This capability is crucial for identifying and investigating malicious activities.
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA • **What**: NA • **When**: NA • **Where**: NA • **Why**: NA
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.

Date: 19/07/2024	**Entry:#3**
Description	Capturing my first network packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA • **What**: NA • **When**: NA • **Where**: NA • **Why**: NA
Additional notes	I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. Future note: -D for available network interfaces, -i to select interface, -c{n} no of packets.

Date: 21/07/24	**Entry: #4**

Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis phase**. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Sender: 76tguyhh6tgftrt7tg.su Sender IP: 114.114.114.114 • **What**: : An email was received by an employee containing a malicious file attachment. • **When**: Wednesday, July 20, 2022 09:30:14 AM • **Where**: : An employee's computer at a financial services company • **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

Date: 24/07/2024	**Entry: #5**
Description	Customer data was collected and exfiltrated by an attacker.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown individual • **What**: An individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. • **When**: December 28, 2022, at 7:20 p.m., PT • **Where**: At Webapp URL • **Why**: The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 26/07/2024	**Entry: #6**
Description	Exploring Signatures and Logs with Suricata
Tool(s) used	Suricata
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA

	• **What**: NA • **When**: NA • **Where**: NA • **Why**: NA
Additional notes	In this lab activity, I explored Suricata, an open-source IDS/IPS and network analysis tool. I delved into packet analysis, IDS signatures, and rule creation. By configuring Suricata to monitor network interfaces and analyzing log outputs like fast.log and eve.json files, I gained valuable insights into detecting and investigating network security threats.

Date:28/07/2024	**Entry: #7**
Description	Perform a query with Splunk
Tool(s) used	Splunk Cloud was used to investigate events
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA • **What**: Possibility of security issues in mail server • **When**: NA • **Where**: Multiple failed login attempts at mail server • **Why**: Possible brute force or password guessing.
Additional notes	NA

Date: 30/07/2024	**Entry: #8**
Description	Perform a query with Chronicle to investigate phishing alert

Tool(s) used	Chronicle was used to investigate security events.
The 5 W's	Capture the 5 W's of an incident. • **Who: 40.100.174.34** which resolves to signin.office365x24.com and signin.accounts-gooqle.com • **What:** Phishing attacks were carried out for employees credentials • **When**: It was done on 2 occasions dated 31/01/2023 and 09/07/2023 • **Where**: 6-8 pc users were affected at http://signin.office365x24.com/login.php • **Why** : post method was used on sign in page most probably credential harvesting of employees.
Additional notes	Request affected to change their passwords and evaluate damage caused.

Reflections/Notes: **1. Were there any specific activities that were challenging for you? Why or why not?**

The task involving `tcpdump` was particularly challenging for me. As I was relatively new to the command line, mastering the syntax of `tcpdump` presented a steep learning curve. Initially, I faced significant frustration because I wasn't getting the desired output. However, through perseverance and repeated attempts, I was able to identify my mistakes. This experience was a valuable lesson, highlighting the importance of carefully reading instructions and approaching tasks methodically and with patience.

2. Has your understanding of incident detection and response changed after taking this course?

After completing this course, my understanding of incident detection and response has significantly improved. At the beginning, my grasp of the fundamentals was quite basic, and I hadn't yet appreciated the complexity of the subject. As I worked through the course material, I gained insights into the entire incident lifecycle, including the importance of having well-defined plans, structured processes, and the essential role of human expertise. I also became familiar with key tools used in this field. Overall, my perspective has shifted considerably, leaving me better equipped with knowledge and a deeper understanding of incident detection and response.

3. Was there a specific tool or concept that you enjoyed the most? Why?

I particularly enjoyed learning about network traffic analysis and using network protocol analyzer tools. This was my first exposure to network traffic analysis, and I found it both challenging and exciting. It was fascinating to capture and analyze network traffic in real time using these tools. I am keen to delve deeper into this topic and aspire to become more proficient with network protocol analyzers in the future.