Chidubem Onochie-Onyetenu’s Incident Handler’s Journal

Date: 13th October 2023	**Entry:** #1
Description	Details about the security incident that the U.S. healthcare clinic experienced.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of hackers known to target the healthcare and transportation industries. ● **What** happened? The company’s files were encrypted, and the attackers demanded a large sum of money in exchange for the decryption key. This was a ransomware incident. ● **When** did the incident occur? At approximately 9:00 a.m. on a Tuesday. ● **Where** did the incident happen? At the clinic’s premises. ● **Why** did the incident happen? Employees downloaded a malicious attachment from a phishing email. This installed malware, which allowed the attackers to deploy ransomware that encrypted the organization’s files.
Additional notes	1. How could the healthcare company prevent an incident like this from happening again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: 16th October 2023	**Entry: #2**
Description	Details about a security incident that occurred at a financial services company
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An unidentified sender emailed a phishing message to an employee. ● **What** happened? An employee downloaded a malicious attachment from the phishing email. ● **When** did the incident occur? By 9:30 a.m. on a Wednesday. ● **Where** did the incident happen? At the company's premises. ● **Why** did the incident happen? A malicious file was sent in a phishing email, and the employee downloaded the attachment.
Additional notes	The alert showed that an employee downloaded and opened a malicious file from a phishing email. After investigating, I confirmed that the email and its attachment were malicious, so I escalated the ticket to a level-two security operations center analyst for further action.

Date: 30th November 2023	**Entry: #3**
Description	Description of an activity that was carried out in which I was tasked to

	analyze a packet.
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	N/A
Additional notes	I was given 5 tasks to carry out on this activity: • Task 1 was to explore data using Wireshark • Task 2 was to apply a basic Wireshark filter and inspect a packet • Task 3 was to use filters to select packets • Task 4 was to use filters to explore DNS packets • Task 5 was to use filters to explore TCP packets I had never used Wireshark before, so I was excited to analyze a packet capture file. I completed the activity successfully.

Date: 1st December 2023	**Entry: #4**
Description	Description of an activity that was carried out in which I was tasked to capture a 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	N/A
Additional notes	I was given 4 tasks to carry out in this activity: • Task 1 was to identify network interfaces • Task 2 was to Inspect the network traffic of a network interface with tcpdump • Task 3 was to capture network traffic with tcpdump • Task 4 was to filter the captured packet data I am still new to the command-line interface, so capturing and filtering network traffic was a challenge. I got stuck a couple of times because I used the wrong commands, but by following the instructions carefully and redoing some steps, I captured the network traffic. I completed the activity.

Date: 1st December 2023	**Entry: #5**
Description	Details about a security incident that occurred at a retail company.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A ransomware attacker, who gained access to the private data of the company's users. ● **What** happened? The company experienced a major security incident: a data breach affecting more than one million users.

	● **When** did the incident occur? At approximately 3:13 p.m. Pacific Time on December 22, 2022, and again on December 28, 2022, after which the attacker increased the ransom demand. ● **Where** did the incident happen? In the company's e-commerce web application. ● **Why** did the incident happen? A vulnerability in the e-commerce web application allowed the attacker to perform a forced browsing attack and gain access to customer transaction data.
Additional notes	To prevent a repeat, it was recommended that the company carry out regular vulnerability scans and penetration tests, and allow only authenticated users to access content.

Reflections/Notes:

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

   They were not challenging, because the scenarios were explained well and the tasks I was asked to carry out were mostly straightforward.

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

   My understanding of incident detection and response has changed for the better. I have gained much more knowledge of the subject since starting the course.

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

   I probably enjoyed using Linux the most because I had never used it before this exercise, and it was exciting to learn a new operating system.