Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: September 3,2023	**Entry:** #1. Tuesday morning, at 9:00 a.m
Description	Documenting a cybersecurity incident
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who**: A group of unethical Hacker • **What :** Ransomware Attack • **When**: Tuesday morning 9:00 am • **Where**: At a health care company • **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 and 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: December 28, 2022,	**Entry: #2** 7:20 p.m., PT
Description	Documenting a cybersecurity incident
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.
The 5 W's	Capture the 5 W's of an incident. ● **Who** : An Individual ● **What** : An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When** : At 3:13 p.m., PT, on December 22, 2022, ● **Where** :An employee's computer at a financial services company ● **Why** :The incident happened because an individual was able to access the customer personal identifiable information (PII) and financial information due to vulnerability in the e-commerce web application. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated and then demanded a large sum of money.
Additional notes	1. How can this incident be prevented in the future? 2. Should we consider improving security awareness training so that employees are careful with what they click on?

Date: September 9,2023	**Entry: #3**
Description	Analyzing a packet capture file
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. Wireshark allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	• **Who** N/A • **What** N/A • **When** N/A • **Where** N/A • **Why** N/A
Additional notes	I've never used Wireshark before, At first glance, the interface was very overwhelming. I got stuck a couple of times but , I was able to get through this activity and analyze network traffic