Incident handler's journal

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.

Scenario

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Additionally, employees also reported that a ransom note was displayed on their computers.

Date: 07/01/2024 Record the date of the journal entry.	**Entry: #1**
Description	Employees at a U.S. health care clinic were locked out of their files by a ransomware attack.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who: A group of unethical hackers** • **What: A ransomware attack** • **When: Tuesday at 9:00 AM** • **Where: At a small health clinic in the U.S.**

	• **Why: A group of unethical hackers were able to use a phishing attack to gain access to the companies systems. After gaining access, the unethical hackers launched their ransomware and encrypted critical files. On the ransomware note, they demanded a large amount of money for the decryption key.**
Additional notes	It would be recommended for the company to provide training on social engineering techniques for their employees to help prevent further incidents like this in the future.

Scenario

In this lab activity, you'll learn how to open and analyze a packet capture file using Wireshark.

Date: 07/02/2024	**Entry:** #2
Description	Analyze a packet capture file using Wireshark
Tool(s) used	Wireshark - A network protocol analyzer that uses a GUI.
The 5 W's	N/A
Additional notes	It was very exciting to use Wireshark for the first time, having never used a Cybersecurity program before. Having prior experience using databases like MySQL I believe helped me understand the GUI and outputs easier.

Scenario

Date: July 25 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	Tcpdump was used to capture and analyze network traffic. This is a network protocol analyzer that's accessed using a CLI, as opposed to a GUI like Wireshark.
The 5 W's	**N/A**
Additional notes	Having prior experience using Git Bash I believe helped me use it effectively to capture and analyze network traffic. It was still a bit confusing at times, but I didn't feel as overwhelmed as I had expected to.

Scenario

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Date: 07/05/2024	**Entry:** #3
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal - An investigative tool that analyzes files and URLs for viruses, trojans, worms, etc.
The 5 W's	Capture the 5 W's of an incident. • **Who**: An unknown malicious actor • **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: An employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	It would be wise to provide employees with training regarding security awareness and various forms of social engineering attacks.