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: 09/27/2023	**Entry:** 1
Description	Documenting an incident.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who**: Organized group of unethical hackers • **What**: Ransomware incident • **When**: Tuesday at approximately 9:00 AM • **Where**: Small U.S health care clinic • **Why**: Unethical hackers were able to take control of the company's systems via phishing attacks that caused malware to be downloaded through a malicious attachment. The hackers encrypted data for what appears to be the purpose of financial gain seeing as how they left a ransom note demanding money in exchange for the decryption key.
Additional notes	How can the health care clinic prevent this type of incident from happening again? How should they go about handling this situation?

Date: 09/27/2023	**Entry:** 2
Description	Analyzing a packet
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. • **Who**: I did • **What**: I opened saved packet capture files, view high-level packet data, and used filters to inspect detailed packet data • **When**: Approximately 2:50 PM • **Where**: Windows VM • **Why**: For the purpose of gaining experience with Wireshark
Additional notes	In what type of scenario would this tool be most useful?

Date: 09/28/2023	**Entry:** 3
Description	Investigating a suspicious file hash.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who**: A malicious threat actor • **What**: Malware downloaded • **When**: Between 1:11 PM and 1:20 PM

	• **Where**: An employee's computer at a financial services company. • **Why**: An employee opened an email with a password-protected spreadsheet file. The password was included in the email, and the employee downloaded the file and then entered the password. After opening the file, a malicious payload was then executed on their computer. The reason for the attack is unknown.
Additional notes	What type of training should be implemented for employees to prevent future incidents like this from occurring? Would restoring a backup fix this issue?

Date: 09/28/2023	**Entry:** 4
Description	Reviewing a final report.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who**: Threat actor • **What**: Data theft • **When**: Approximately 3:13 PM • **Where**: An organization • **Why**: A threat actor was able to steal data by exploiting a vulnerability in the e-commerce website by allowing the attacker to perform a forced browsing attack. The attacker was then able to access customer purchase confirmation pages. The attacker sought financial gain by demanding payment of first $25,000, and then $50,000, with a sample of proof of the stolen data.

Additional notes	Would identity protection services fix this? Are there any legal consequences?

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date	**Entry:** Record the journal entry number.

of the journal entry.	
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: