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: 11/22/24 Record the date of the journal entry.	**Entry:** Record the journal entry number. #1
Description	Documenting A CyberSecurity Incident 'Healthcare Clinic'
Tool(s) used	Email Security Filters, AntiVirus/Anti Malware Software, Intrusion Detection System, Ransomware Decrypting Tools
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers known to target healthcare and transportation industries. • **What** happened? Ransomware attack involving file encryption, triggered by malware installed via phishing emails. • **When** did the incident occur? Tuesday morning, approximately 9:00 a.m. • **Where** did the incident happen? Within the network of a small US healthcare clinic • **Why** did the incident happen?

	They were circumstances from successful phishing emails that lead to malware and ransomware being deployed
Additional notes	Include any additional thoughts, questions, or findings. The incident highlights the vulnerability of healthcare organizations to cyber attacks and ransomware. Shows the relevance of Phishing effectiveness, and targeting of emails. As well as business impact and data recovery. It emphasized the importance of cybersecurity measures and incident response plans. It also allows us to know how to recover patient data but depending on the availability of back ups and the decryption key specifically. Furthermore, it seems the clinic needs to vastly improve employee training on how to spot and avoid phishing emails.

Date: 1/13/25 Record the date of the journal entry.	**Entry:** Record the journal entry number. #2
Description	Provide a brief description about the journal entry. Analyzing a packet capture file on WireShark
Tool(s) used	List any cybersecurity tools that were used. For this specific scenario I was able to use WireShark to analyze a packet file on my computer. WireShark the app is considered a network protocol analyzer that uses a graphical user interface. The reason why WireShark is able to be

	utilized in CyberSecurity is that it allows analysts to monitor and analyze network traffic. This aids in detecting and investing malicious activity.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Me • **What** happened? I was able to capture specific packets in a list and examine its structure. I used a certain ip, and http GET REQUESTS to do so. • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings. A pretty sophisticated application, while being able to monitor network traffic and capture any issues, security threats or malware activity. Definitely a hidden gem that was fun to use.

Date: 2/27/25 Record the date of the journal entry.	**Entry:** Record the journal entry number. #3
Description	Provide a brief description about the journal entry. Capturing a network packet
Tool(s) used	List any cybersecurity tools that were used.

	I will be using tcpdump to capture files and analyze networks. Tcpdump is command-line packet analyzer thats most commonly used to network troubleshoot and security analysis.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Me • **What** happened? I was able to capture traffic to and from a specific host. As well as capture traffic on a specific port and network range. • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings. Fairly intricate for what the application is. I I got stuck in a loophole quite a few times. But after learning every time and trying something new. Taking notes we're essential. Eventually I was able to capture a few different network traffics.

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 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 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.

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: Record additional notes.