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: 12/4/25	**Entry: 1**
Description	A healthcare company had to shut down operations due to a ransomware attack that encrypted patient health files.
Tool(s) used	none
The 5 W's	Capture the 5 W's of an incident. ● **Who** A group of unethical hackers ● **What** Emails containing malware was sent to employees. ● **When** 9am 12/4/25 ● **Where** A small healthcare clinic ● **Why** employees falling prey to phishing email scams and downloading unknown attachments. Critical files then became encrypted and held for ransom by the group who sent the phishing emails.
Additional notes	How can the employees be better trained to not fall for phishing scams? Can the files be retrieved without payment?

Date: 12/6/25	**Entry: 2**
Description	An employee received an email containing a file that required a password to access. The password was in the email and the employee entered it and malware was executed and began installing files onto the employees PC.
Tool(s) used	**VirusTotal, Alert Ticket, Play Book**
The 5 W's	● **Who** an unknown sender ● **What** a trojan virus sent via email ● **When** 1:13pm 12/6/25 ● **Where** A financial services company ● **Why** An employee downloading and opening an unknown file from an unknown sender.
Additional notes	What damage was caused by the files that were downloaded by the trojan?

Date: 12/6/25	**Entry: 3**
Description	Capture a packet
Tool(s) used	tcpdump
Additional notes	Tcpdump was used to capture network traffic in order to later be analyzed in depth.

Reflections/Notes: These include some labs I completed working to get my certifications. I am still learning all the ins and outs of all the different systems and it is a lot of information, but it is exciting at the same time figuring things out 1 step at a time.