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: Record the date of the journal entry.	**Entry: # 1** **Ransomware** **12/05/2023**
Description	There has been a security breach, in the incident, the hacker was able to encrypt sensitive data and is requesting a ransom in order to provide a decryption key. This was done through a phishing email that the attacker sent to several of our employees.
Tool(s) used	No tools were used, it was done through a phishing email, and he's requesting a ransom.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A group of unethical hackers ● **What** happened? A group of unethical hackers was able to gain access to our sensitive files by sending a phishing email to several of our employees and now are requesting a ransom. ● **When** did the incident occur? Tuesday 9:00am. ● **Where** did the incident happen? At a U.S. health care clinic specialized in delivering primary-care services.

	● **Why** did the incident happen? Because the group of attackers wanted money they left a ransom note displayed on the employees computers requesting a huge amount of money.
Additional notes	We have to get help and see if there's a way that our company can decrypt these files or this company is going to have to pay to gain access to these files again by paying the ransom requested by these hackers and getting a decryption key, but we are not guarantee that this group of hackers won't come back for more, or give access to other groups of hackers to do the exact same thing again, Next We have to go through what we have learned as the incident response team and train all employees at this company to not click on any email and we have to keep this kind of training updated and keep updating employees to new attack strategies that are rising in the tech landscape

---

Date: Record the date of the journal entry.	**Entry: #2** **Analyzing packets with wireshark** **12/08/2023**
Description	Provide a brief description about the journal entry. I used Wireshark to analyze data packets. By using IP's in the top bar we can search for any IP and find what kind of activities happening on an organization network related to that IP, anything as to what time, what kind of protocol it used, the length and we can also see the source IP address and the destination IP address.
Tool(s) used	We used Wireshark. It is an open source tool that analyzes packets and network traffic, also known as a packet sniffer it also uses UDP.

The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A ● **Why** N/A ● We used different IP's to see what activities were performed on a network.
Additional notes	I'm very excited to be using Wireshark. It is such a helpful tool in the security world and very easy to use.

Date: Record the date of the journal entry.	**Entry: #3** **Capturing my first packet using tcpdump** **12/10/2023**
Description	I used different commands in tcpdump to filter out data and see what kind of activities that are happening on our network.
Tool(s) used	I used tcpdump to capture and analyze packets. Tcpdump is a packet analyzer that uses a command-line interface.
The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A

	● **Why** N/A
Additional notes	I was excited to know how to use tcpdump in order to capture and analyze packets and filter out data using a command line. I found it easy to use since it’s quite similar to using linux commands.

Date: Record the date of the journal entry.	**Entry: #4** **Investigated a suspicious file hash** **12/13/23**
Description	I used virus total in order to investigate a file that was downloaded by one of our employees, and i found out that this file has been flagged as malicious by other vendors
Tool(s) used	I used virus total which is used to search for URLs or files and can let you know if the URL or file that you are dealing with is malicious.
The 5 W's	Capture the 5 W's of an incident. ● **Who** : a malicious actor ● **What** happened?: an email was sent to one of our employees and there was an attached file that contained malicious codes. Once our employee opened it a malicious payload was then executed on their computer. SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When** did the incident occur? 1:11 p.m.: An employee receives an email containing a file attachment.

	1:13 p.m.: The employee successfully downloads and opens the file. 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC. ● **Where** did the incident happen? At a financial services company ● **Why** did the incident happen? An employee received an email and downloaded a malicious file that was attached to their computer.
Additional notes	We have to constantly remind our employees to not click on different links or unusual friendly or work related email that they weren't aware of or haven't experienced yet and the best way to do this is to constantly host security meetings and update all our employees to what the threat landscape looks like and we also have to keep our security team a step ahead in order to enhance our organization security.

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.