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: 5 November 2024	**Entry:** 1
Description	It is about a ransomware attack. **Detection and Analysis** The organisation identified a ransomware attack and initiated a formal request to several other organisations for urgent assistance in analysing the threat. **Containment, Eradication, and Recovery** To contain the threat, the company took decisive action by shutting down its computer systems. For eradication and recovery, they realised they needed external support and enlisted help from multiple organisations.
Tool(s) used	None.
The 5 W's	• **Who:** An organised group of unethical hackers. • **What:** Phishing was used to achieve a ransomware attack. • **When:** On a Tuesday morning, at approximately 9:00am.

	• **Where:** A small U.S health care clinic. • **Why:** Because an employee was deceived.
Additional notes	Thorough cybersecurity training should be administered to employees at regular intervals.

Date: 5 November 2024	**Entry:** 2
Description	It is about capturing my first packet.
Tool(s) used	Tcpdump was used to capture my first packet. This command-line tool is useful for capturing and displaying packet data in real time. It is often employed to analyse live network traffic.
The 5 W's	• **Who**: There is no incident indicated, therefore, whoever caused any incident isn't known. • **What:** Live network traffic is being captured and analysed using tcpdump. • **When:** No incident occurred but I captured my first packet in module 2 of this course. • **Where:** No incident happened anywhere, but I captured my first packet using tcpdump with respect to an organisation. • **Why:** No incident happened for any reason but I captured my first packet using tcpdump.
Additional notes	Tcpdump is a very useful tool as long as one understands Linux syntax.

	The fact that it captures and analyses live network traffic also makes it a useful tool.

Date: 5 November 2024	**Entry:** 3
Description	It is about analysing my first packet with Wireshark.
Tool(s) used	Wireshark was used to analyse my first packet. It is often used for troubleshooting network issues and examining protocols in real-time. This tool is invaluable for monitoring and examining network traffic effectively.
The 5 W's	• **Who**: It is not known if the user being investigated is malicious, however he or she is still being investigated. • **What**: Nothing in particular happened, but traffic to a website is being investigated. • **When**: There is no particular date about any incident that occurred. • **Where**: There is no sure incident, but if any happened, it would have happened on the website. • **Why:** There is no known incident that happened, therefore, this question cannot be answered.
Additional notes	Wireshark is good to use to investigate network traffic, once one has practised with it very well.

Date: 5 November 2024	**Entry:** 4
Description	A suspicious file hash is being investigated.
Tool(s) used	VirusTotal was used to analyse a suspicious file hash. This service allows users to examine files, domains, URLs, and IP addresses for potential malicious content. It aggregates threat intelligence from the global cybersecurity community, providing valuable insights into various security threats.
The 5 W's	• **Who**: An attacker who sent a phishing email. • **What**: A malicious file attachment was sent to an employee, and when he or she opened it, a malicious payload was executed on his or her computer. • **When**: The incident happened at 1:15pm. • **Where**: The incident happened at a financial services company. • **Why**: The incident happened because an unsuspecting employee opened a malicious email.
Additional notes	VirusTotal is a good tool for a SOC Analyst, because it helps the analyst to analyse suspicious files, domains, URLs, and IP addresses for malicious content.

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: 1. Were there any specific activities that were challenging for you? Why or why not? I didn't face any challenges, as I fully understood each task. My deep knowledge helped me engage effectively in all activities. Additionally, my ability to retain key information through active participation further supported my progress.

2. Has your understanding of incident detection and response changed since taking this course? My understanding has significantly deepened, thanks to the clarity of the incident detection and response content. The material was free of ambiguity, which helped me grasp the steps security teams take during these processes. I've especially started to appreciate the effectiveness of playbooks in streamlining responses.

3. Was there a specific tool or concept that you enjoyed the most? Why?
I found learning about the Pyramid of Pain really engaging and enlightening. It was easy to grasp, yet the concept conveys so much depth, which kept me excited and interested. The clear and expressive structure made it an enjoyable and impactful part of my learning experience.