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: 13/03/2025	**Entry:** #1
Description	A healthcare clinic fell victim to a ransomware attack after phishing emails installed malware, encrypting crucial files and halting operations.
Tool(s) used	None.
The 5 W's	• **Who:** Unethical hackers targeting health and transport sectors. • **What:** Phishing emails led to ransomware installation and file encryption. • **When:** Tuesday morning, around 9:00 AM. • **Where:** The healthcare clinic's internal network. • **Why:** Lack of email security awareness and vulnerability to phishing.
Additional notes	• The clinic had no defense against phishing, disrupting patient care. • Security experts were contacted to restore data from backups. • Questions on improving cybersecurity to prevent future attacks were raised.

Date: 13/03/2025	**Entry:** #2
Description	A security analyst analyzed network traffic related to a user browsing a website using packet capture data. The analyst filtered and examined the data to identify the protocols, IP addresses, and content in the packets, including DNS queries and TCP traffic.
Tool(s) used	Wireshark
The 5 W's	• **Who**: The user interacting with a website using HTTP traffic. • **What**: Analysis of HTTP traffic to extract DNS and TCP packet data. • **When**: During an investigation, the time frame spans multiple tasks focusing on DNS queries and web traffic packets. • **Where**: The packets were captured from a system connecting to the website "opensource.google.com." • **Why**: To explore the network traffic, identify key information such as IP addresses, DNS queries, and TCP connections, ensuring proper network analysis for security purposes.
Additional notes	DNS queries revealed the IP address 142.250.1.139 for "opensource.google.com." TCP traffic on port 80 showed a TTL of 64 and a frame length of 54 bytes. Filters were applied to focus on DNS queries and TCP packets containing "curl" to identify HTTP requests.

Date: 13/03/2025.	**Entry:** #3
Description	I used **tcpdump** to capture HTTP traffic (port 80) on the **eth0** interface of a Linux virtual machine. The traffic was filtered and saved to a **capture.pcap** file for further analysis. I examined the captured packets, inspecting header and content data in hexadecimal and ASCII formats.
Tool(s) used	tcpdump
The 5 W's	• **Who**: The network analyst performing the packet capture and traffic analysis. • **What:** The analyst captured HTTP traffic on port 80, filtered the data using tcpdump, and saved the traffic into a `.pcap` file for further analysis. The traffic was generated using the `curl` command to simulate web browsing activity. • **When**: The tasks were performed on 13/03/2025 as part of a lab scenario focusing on packet capture and network analysis. • **Where**: The packet capture occurred on a Linux virtual machine, with the traffic being captured from the `eth0` network interface. • **Why**: The purpose was to practice network traffic analysis, capture HTTP traffic for review, and demonstrate how to filter, capture, and inspect packets using tcpdump.
Additional notes	TThe capture was successful, with 9 HTTP packets saved. I used the `-nn` option to prevent name resolution and focus on raw packet data. After capturing, I applied filters for HTTP traffic and used `-X` to display both hexadecimal and ASCII data, aiding in detailed packet analysis.

Date: 13/03/2025..	**Entry:** #4
Description	As a security analyst at Buttercup Games, I investigated SSH login failures to the root account on the email server using Splunk Cloud. I performed a filtered search to identify failed login attempts, focusing on the email server and the root account. The results revealed over 100 failed attempts, indicating a potential security risk.
Tool(s) used	Splunk Cloud
The 5 W's	• **Who:** The email server of Buttercup Games (mailsv). • **What:** SSH login failures to the root account on the email server. • **When:** During the investigation of security issues on the email server. • **Where:** In the Splunk Cloud instance associated with Buttercup Games' infrastructure. • **Why:** To identify unauthorized access attempts to the root account on the email server.
Additional notes	More than 100 failed SSH login attempts were found. The next step will be to investigate these attempts further and take corrective actions.

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.