



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: 2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface.
The 5 W's	
Additional notes	As a beginner, the interface was very overwhelming at first. I can see why it's such a powerful tool for understanding network traffic.

Date: Record the date of the journal entry.	Entry: 3
Description	investigate a suspicious file hash
Tool(s) used	VIRUSTOTAL
The 5 W's	Capture the 5 W's of an incident. <ul style="list-style-type: none"> • Who: An unknown malicious actor • What: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • Where: financial services company • When: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • Why: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	Entry: 4
Description	Capturing my first packet
Tool(s) used	TCPDUMP
The 5 W's	
Additional notes	Learning new software is never easy. However with my determination and joy for learning I was able to make mistakes and still enjoyed what I was doing. I was able to repeat steps a couple times for the command line to really make sense to me.

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. <ul style="list-style-type: none"> • 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • 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.
