Incident handler's journal

Date: 11/26/2024	**Entry:** Entry: #1
Description	Documenting a cybersecurity incident.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Unethical hackers. • **What** happened? Employee opening phishing email and causing ransomware to be deployed. • **When** did the incident occur? Tuesday 9:00AM • **Where** did the incident happen? Small U.S. healthcare clinic. • **Why** did the incident happen? Employees falling for phishing emails. The unethical hackers were able to access the system and deploy ransomware. The hackers encrypted files and demanded money for the decryption key.
Additional notes	Situation could have been avoided with employee education. Employees need to be aware of security threats. Hackers gained access and launched ransomware on the systems and encrypting important files. The motivation was financial related.

Date: 11/26/2024	**Entry:** Entry #2
Description	Documenting a cybersecurity incident.
Tool(s) used	I used VirusTotal. This is a tool that allows analysis of files and URLs from malicious content. This tool is great for checking if there are any hints of compromise. The user is able to see if websites or files have been reported malicious. This occurred at the detection and analysis phase. I had to investigate a suspicious file hash. I had to analyze if this alert was a high risk.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Unethical hacker utilizing phishing. • **What** happened? Malicious payloads were executed with the use of a phishing email. • **When** did the incident occur? 1:11p.m-1:20pm • **Where** did the incident happen? Financial Service company via an employee workstation. • **Why** did the incident happen? Employee downloading malicious files.
Additional notes	Analyzing VirusTotal, I found that 59 vendors flagged the SHA256 file hash as malicious. Community score is -219 meaning likely malicious. Security vendor's analyst has many exclamation points showing that it is malicious. This incident could have been avoided with proper training regarding suspicious emails and links.

Date: 11/26/2024	**Entry:** Entry #3
Description	Documenting a cybersecurity incident.
Tool(s) used	Phishing Playbook
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Employee and unethical hacker. • **What** happened? Employee downloaded a malicious file. It was a known malicious file hash. • **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM • **Where** did the incident happen? Employee workstation. • **Why** did the incident happen? Employee had trouble identifying a phishing email.
Additional notes	Known malicious file hash. Many typos in the email body. Strange email address. Strange IP address. Links attached to email.

Date: 12/2/24	**Entry:** Entry #4
Description	Explore any failed SSH logins for the root account.

Tool(s) used	Splunk is a tool for collecting, indexing, and analyzing machine-generated data from various sources. In this case, Splunk played a key role in investigating the failed login attempts and identifying potential security threats.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Potential malicious users attempting to get into the admin account. • **What** happened? 300+ failed login attempts with time filters to “All time” • **When** did the incident occur? 2/27/23 - 3/26/23 • **Where** did the incident happen? Host is ‘msv’. • **Why** did the incident happen? Likely someone trying to login using brute force.
Additional notes	This incident involved 326 failed login attempts to the host 'msv'. Using Splunk, I was able to filter and isolate the relevant data, enabling a focused analysis of the events related to this case.

Date: 12/11/2024	**Entry:** Entry #5
Description	Analyzing a packet capture file
Tool(s) used	Wireshark is a powerful tool used for analyzing packet capture files. With its graphical user interface, Wireshark enabled me to efficiently capture and

	analyze network traffic, providing deeper insights into data flow and network behavior.
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	This was an excellent opportunity to gain hands-on experience with Wireshark, a powerful tool that facilitates the detailed analysis and understanding of network traffic

---

Date: 12/11/2024.	**Entry:** Entry #5
Description	Captured packet using tcpdump.
Tool(s) used	I utilized tcpdump to capture and analyze network traffic through the Linux command line. This tool enables analysts to capture, filter, and thoroughly examine network traffic for deeper insights.
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	This exercise provided valuable hands-on experience with the command-line interface. After reviewing the necessary commands, I was able to effectively capture and analyze network traffic.

This journal gave me practice with responding to incidents and utilizing various tools, enabling me to discover their strengths and weaknesses. I learned what to look for when capturing and analyzing data, and I now feel more confident in recording and responding to incidents.

Filling out this incident handlers journal, I learned the benefits and trade-offs of different traffic analysis tools. Tcpdump proved invaluable for fast network troubleshooting without requiring a heavy GUI, though it can be less intuitive for beginners. Wireshark's user-friendly GUI made it easy to visually analyze packets, but it demanded significant system resources for large data sets. Splunk streamlined the collection and real-time analysis of log data from multiple sources, offering powerful search capabilities through its search processing language (SPL). VirusTotal provided free and comprehensive malware scanning, analyzing files, URLs, and IP addresses, though its reliance on third-party tools may occasionally lead to false positives.

This exercise deepened my understanding of traffic analysis and network forensics while reinforcing my ability to document incidents systematically. It has prepared me to handle real-world scenarios with greater confidence and proficiency.