Incident handler's journal

Date: Oct. 16, 2024	**Entry: #1**
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers. • **What**: Ransomware attack • **When**: Tuesday at 9:00 a.m. • **Where**: A U.S. health care clinic • **Why**: Hackers sent a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.
Additional notes	Cause of the incident was social engineering. Employee training, data backup and port filtering on firewalls could help for future incidents. I am concerned about HIPAA regulations and data encryption.

Date: Oct. 16, 2024	**Entry: #2**
Description	Investigate an alert
Tool(s) used	VirusTotal
The 5 W's	• **Who:** Hacker • **What**: Phishing attack combined with malicious payload. • **When:** 1-1.20 p.m.

	• **Where**: Financial services company • **Why**: The employee opened the file, a malicious payload was then executed on their computer.
Additional notes	There is a mismatch between the sender's email address and the sender's name, it indicates that this is a phishing attack. It has malicious file attachment and the IP address of the sender is also malicious.

Date: Oct. 16, 2024	**Entry: #3**
Description	Review final report for a security incident
Tool(s) used	None.
The 5 W's	• **Who:** An individual • **What**: Unauthorized access • **When:** December 28, 2022, at 7:20 p.m. • **Where:** Retail company. • **Why**: A vulnerability in the e-commerce web application.
Additional notes	Perform routine vulnerability scans and penetration testing. Train staff to report suspicious emails.

Date: Oct. 17, 2024	**Entry: #4**

Description	Log analyze
Tool(s) used	Splunk - SIEM
The 5 W's	• **Who:** An attacker • **What**: Possible brute force attack on the mail server with the use of a botnet. • **When**: March 06, 2023, 01:39:51 • **Where:** E-commerce store - Buttercup Games • **Why**: The system did not implement the rate limiting.
Additional notes	All attempts occurred in the same timestamp, which indicates it is a botnet attack. Implementing MFA and rate limiting would help for future attacks.

Date: Oct. 17, 2024	**Entry: #5**
Description	Log analyze
Tool(s) used	Chronicle - SIEM
The 5 W's	• **Who**: Seven employees accessed the malicious domain: Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, Roger Spence and Warren Morris • **What**: A phishing attack • **When**: First access: January 31, 2023 and Last access: July 09, 2023 • **Where**: financial services company • **Why:** employees send “POST” requests to the malicious domain.

Additional notes	Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, Warren Morris and Roger Spence accessed the malicious domain, totaling seven employees. The first access occurred on January 31, 2023, and the last access on July 09, 2023. Only Ashton Davidson and Emil Palmer sent POST requests to the /login.php page, indicating possible successful phishing attacks. Additionally, Warren Morris sent a POST request to the IP address 40.100.174.34, which belongs to the same malicious domain. This suggests that his asset may have been phished as well. Totally 3 “POST” request to 40.100.174.34 IP address by employees. The domain 104.215.148.63 is also associated with the malicious domain, and login.office365x24.com is a sibling domain to the malicious domain.

Date: Oct. 17, 2024	**Entry: #6**
Description	Analyzing a network packet capture file
Tool(s) used	Wireshark
The 5 W's	• **Who**: N/A • **What**: N/A • **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	142.250.1.139 is the IP address for the DNS query for

	“opensource.google.com”. The Time to Live value of the packet as specified in the Internet Protocol Version 4 subtree is 64. Destination Address as specified in the Internet Protocol Version 4 subtree is 169.254.169.254. I find these and other information though implementing filters and analyzing the Wireshark file.

Date: Oct. 17, 2024	**Entry: #7**
Description	Capturing a packet
Tool(s) used	tcpdump
The 5 W's	• **Who**: N/A • **What**: N/A • **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	I used the ifconfig command to identify available network interfaces for capturing network packet data. Next, I utilized tcpdump with various options to filter and capture live network traffic. After capturing the network traffic, I applied filters to the packet data using tcpdump to focus on specific network events. Finally, I interpreted the packet information output by tcpdump, saved the captured packet data, and loaded it for further analysis at a later time.

Reflections/Notes:

I found the activity using tcpdump to be very exciting. Working with the command-line interface (CLI) is interesting for me. Before taking this course, I was more focused on the payload part of the packet. However, after the course, I realized that the header part of the packet is equally important and must be well protected.

One challenge for me has been documentation. Sometimes, I struggle to express myself clearly in writing. However, I believe I've made progress by writing more documentation and reading examples. I now understand how important documentation is for ensuring the chain of custody and for making my team's work, as well as others', more efficient and easier to manage.

Throughout the course, I learned about the incident lifecycle, and I now understand that handling incidents requires more than just tools—it requires knowledgeable people with experience and different perspectives. It's a deep and comprehensive topic. I find it fascinating that I can capture, analyze, and understand network traffic, and then create a narrative to comprehend the attack process and the TTPs (Tactics, Techniques, and Procedures) of attackers. I'm excited to continue learning and improving.