Incident handler's journal

Date: May 25 2024	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario describes how the ransomware incident was discovered by the organization. The organization made technical assistance requests to multiple entities for the analysis step. 2. **Containment, Eradication, and Recovery**: The scenario outlines the actions the organization did to keep the crisis under control. For instance, the business terminated its computer networks. But, they reached out to a number of other organizations for support because they were unable to work alone to eliminate and recover from the catastrophe. 3.
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The issue occurred as a result of phishing attacks used by dishonest hackers to gain access to the company's systems. Critical files were encrypted by the attackers' ransomware after they had access to the company's computers. Given that the ransom note the attackers left demanded a substantial payment in exchange for the decryption key, it would seem that their purpose was financial in nature.
Additional notes	1. How could the healthcare provider ensure that anything similar doesn't happen again? 2. Does the business need to pay the ransom to have the decryption key back ?

Date: May 25 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this exercise, I examined a packet capture file using Wireshark. A network protocol analyzer with a graphical user interface is called Wireshark. The ability for security analysts to record and examine network traffic is what makes Wireshark valuable in the field of cybersecurity. Investigating and identifying harmful activities may be aided by this.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	Wireshark is new to me, so I was eager to start this exercise and examine a packet capture file. The interface seemed incredibly confusing at first. It makes sense why it's such an effective tool for deciphering network traffic.

Date: May 25 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.

The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	Using the command-line interface to capture and filter network traffic was difficult for me because I'm still learning how to use it. I used the incorrect commands a few times, which caused me to get stuck. However, I was able to complete this task and record network traffic after closely following the directions and going through several of the procedures again.

Date: May 27 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	I utilized VirusTotal, an investigative program, for this task. It scans files and URLs for harmful information, including trojans, worms, and viruses. If you want to quickly see whether a website or file that may be a sign of compromise has been flagged as malicious by other members of the cybersecurity community, this is a very useful tool. I utilized VirusTotal to examine a file hash that was flagged as harmful for this task. This occurrence happened during the period of detection and analysis. I was placed in the position of a security analyst at a SOC looking into a questionable file hash in this scenario. I had to conduct further research and analysis once the security measures in place identified the suspicious file in order to ascertain whether the warning actually represented a threat.
The 5 W's	• **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**: An employee's computer at a 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	How can anything similar be avoided in the future? Should we think about enhancing security awareness training to encourage staff to use caution when clicking on links?

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

The tcpdump activity was pretty difficult for me. It took me a while to get used to the syntax of a tool like tcpdump because I'm new to utilizing the command line. I was first really annoyed because I wasn't receiving the desired results. I corrected my mistakes and completed the task again. This taught me to carefully study the directions and proceed cautiously with the process.

2. **Has your understanding of incident detection and response changed after taking this course?**

My comprehension of incident detection and response has undoubtedly changed as a result of taking this course. I had a rudimentary understanding of detection and reaction at the start of the course, but I was unaware of the complexity required. As the course went on, I gained knowledge of the event lifecycle, the significance of people, procedures, and plans, as well as the tools that were employed. In general, I believe that my perspective has evolved and that I now know and comprehend incident detection and response better.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

Using network protocol analyzer tools to apply what I learnt about network traffic analysis was a truly fun experience for me. It was fascinating and challenging because it was my first experience learning about network traffic analysis. Being able to use technologies to record and analyze network traffic in real time really piqued my interest. I have a strong desire to learn more about this subject and eventually aim to master the use of network protocol analyzer tools.