Incident handler's journal

Task:

In this activity, you will review the details of a security incident and document the incident using your incident handler's journal.

Scenario:

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident

	This incident occurred in the two phases: 1. **Detection and Analysis:** The scenario describes how the organization initially identified the ransomware incident. During the analysis phase, the organization reached out to multiple external organizations for technical support. 2. **Containment, Eradication, and Recovery:** The scenario outlines the actions taken to contain the incident, such as shutting down computer systems. However, as the company could not handle eradication and recovery on its own, it sought help from several other organizations.
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 incident occurred when malicious hackers gained access to the company's systems through a phishing attack. Once inside, they deployed ransomware that encrypted critical files. The attackers' motives seem to be financial, as the ransom note they left requested a significant amount of money in exchange for the decryption key.
Additional notes	1. How could the healthcare company prevent an incident like this in the future? 2. Should the company pay the ransom to retrieve the decryption key?

Task:

In this lab activity, you'll learn how to open and analyze a packet capture file using Wireshark.

Date: July 25 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this task, I used Wireshark to analyze a packet capture file. Wireshark is a

	network protocol analyzer with a graphical user interface. It is valuable in cybersecurity because it enables security analysts to capture and examine network traffic, which helped in detecting and investigating malicious activity.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	Since this was my first time using Wireshark, I was excited to dive into analyzing a packet capture file. The interface looked a bit complex at first, but I now see how useful it is for examining network traffic.

Task:

In this lab activity, you'll capture and analyze live network traffic using tcpdump. You'll use Linux commands in the Bash shell to complete these steps.

Date: July 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 operates through the command line. Like Wireshark, tcpdump is valuable in cybersecurity because it lets security analysts 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	Since I'm still learning to use the command-line interface, capturing and filtering network traffic was a bit challenging. I encountered a few setbacks when I used the wrong commands, but after carefully following the instructions and revisiting some steps, I was able to complete the activity and successfully

	capture network traffic.

Task:

In this activity, you'll analyze an artifact using VirusTotal and capture details about its related indicators of compromise using the Pyramid of Pain.

Date: July 27 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, an investigative tool that checks files and URLs for malicious content like viruses, worms, trojans, and more. It's a useful tool for quickly determining if an indicator of compromise, such as a file or website, has been flagged as malicious by others in the cybersecurity community. In this case, I used VirusTotal to analyze a file hash that had been reported as malicious. This incident took place during the Detection and Analysis phase. In the scenario, I acted as a security analyst at a SOC investigating a suspicious file hash. After the security systems flagged the file, I conducted a deeper analysis to determine whether the alert indicated a genuine 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 we prevent this incident from happening again in the future? Should we enhance security awareness training to ensure employees are more cautious about what they click on?

Reflections/Notes:

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

I found the tcpdump activity challenging because I'm new to the command line, and learning its syntax was tough. Initially, I struggled with getting the right output, but after redoing the activity, I figured out my mistakes. This experience taught me the importance of carefully following instructions and taking my time.

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

This course has significantly expanded my understanding of incident detection and response. Initially, I had a basic grasp of the concepts, but I didn't fully appreciate the complexity. As I worked through the course, I learned about the incident lifecycle, the critical role of plans, processes, and people, and the tools involved. Overall, I now have a deeper and more comprehensive understanding of incident detection and response.

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

I really enjoyed learning about network traffic analysis and using network protocol analyzer tools for the first time. It was both challenging and exciting to capture and analyze network traffic in real time. The experience sparked my interest in the topic, and I'm eager to continue learning and become more skilled with these tools in the future.