Incident handler's journal

Date: July 23, 2024		**Entry:** #1
Description		Documenting a cybersecurity incident 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 entities for technical support in understanding and assessing the attack. 2. **Containment, Eradication, and Recovery:** The scenario outlines specific actions the organization took to contain the incident, such as shutting down its computer systems. Recognizing the complexity of the situation, the organization sought assistance from various external organizations to effectively eradicate the threat and begin recovery efforts.
Tool(s) used		None
The 5 W's		• **Who:** An unidentified malicious actor. • **What:** A phishing email was sent to an employee and contained a malicious file attachment. The file was identified with the SHA-256 hash: `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`. • **Where:** The incident occurred on an employee's workstation at a financial services company.

		• **When:** At 1:20 p.m., the organization's Security Operations Center (SOC) received an alert from the intrusion detection system after the malicious file was detected. • **Why:** The incident occurred because the employee downloaded and executed the malicious file from the email attachment. • **How can this be prevented in the future?** The organization should consider enhancing its security awareness training to reduce the risk of similar incidents. Educating employees on how to recognize phishing attempts and the risks of opening unexpected attachments can significantly improve overall cybersecurity posture.
Additional notes		The motive behind the attack appears to be financial, as the ransom note demanded a substantial payment in exchange for the decryption key. 1. **How can the Financial Services Company prevent similar incidents in the future?** To prevent future incidents, the company should implement a multi-layered security approach, including regular employee cybersecurity training, stronger email filtering, endpoint protection, routine system backups, and continuous monitoring for suspicious activity. 2. **Should the company pay the ransom to obtain the decryption key?** Paying the ransom is generally discouraged, as it does not guarantee data recovery and may encourage further attacks. Instead, the company should focus on restoring systems from secure backups and reporting the incident to the appropriate authorities.

Date: July 23, 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	I used Wireshark to analyze a packet capture (PCAP) file. Wireshark is a network protocol analyzer with a graphical user interface that enables detailed inspection of network traffic. In cybersecurity, Wireshark is a valuable tool for capturing, monitoring, and analyzing network data, helping security analysts detect and investigate potential malicious activity.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	This was my first time using Wireshark, so I was excited to begin the exercise and analyze a packet capture file. Initially, the interface felt overwhelming, but it quickly became clear why Wireshark is such a powerful tool for understanding and analyzing network traffic.

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's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in

	cybersecurity lies in its ability 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	As someone still new to using the command-line interface, capturing and filtering network traffic presented a challenge. I encountered a few setbacks due to incorrect commands, but by carefully following the instructions and repeating certain steps, I was ultimately able to complete the activity and successfully capture network traffic.

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 scans files and URLS for malicious content such as viruses, worms, and trojans. It's particularly useful for quickly checking if an indicator of compromise, such as a file or website, has been flagged by others in the cybersecurity community. In this case, I used VirusTotal to analyze a file hash, which was confirmed to be malicious. This incident took place during the Detection and Analysis phase of the incident response process. The scenario placed me in the role of a security analyst working in a Security Operations Center (SOC), tasked with investigating a suspicious file hash. After the file was detected by existing security systems, I conducted further analysis to determine whether the alert represented a legitimate 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**:** An unidentified malicious actor. • **What:** A phishing email was sent to an employee containing a malicious file attachment. The file was identified by its SHA-256 hash: `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`. • **Where:** The incident occurred on an employee's workstation at a financial services company. • **When:** At 1:20 p.m., the organization's Security Operations Center (SOC) received an alert from the intrusion detection system after the malicious file was detected. • **Why:** The employee unknowingly downloaded and executed the malicious attachment from the phishing email, triggering the security alert. • • **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 this incident be prevented in the future?** To prevent similar incidents, the organization should consider enhancing its security awareness training programs. Educating employees on how to recognize phishing attempts and the risks of clicking on suspicious links or attachments can significantly reduce the likelihood of successful attacks

Reflections/Notes

Were there any specific activities that were challenging for you? Why or why not?
One of the most challenging activities for me was using **tcpdump**. As someone new to the command-line interface, learning the syntax and functionality of this tool was a significant learning curve. Initially, I felt frustrated because I couldn't produce the correct output. However, after carefully reviewing the instructions and repeating the steps, I was able to identify my mistakes and complete the task successfully. This experience taught me the value of patience, attention to detail, and methodical problem-solving.

Has your understanding of incident detection and response changed after taking this course?
Absolutely—my understanding of incident detection and response has deepened considerably. Before taking this course, I had a basic awareness of what these concepts involved, but I didn't fully grasp the complexity and structure required for effective incident management. Throughout the course, I learned about the full lifecycle of an incident, the critical role of planning and defined processes, and the importance of the people and tools involved. I now feel more confident in my knowledge and better prepared to participate in real-world incident response scenarios.

Was there a specific tool or concept that you enjoyed the most? Why?
I particularly enjoyed exploring **network traffic analysis** and working with network protocol analyzer tools. This was my first introduction to analyzing live network data, and although it was challenging, it was also incredibly engaging. I found it fascinating to see how much information can be gathered from monitoring network traffic in real time. This experience sparked a genuine interest in the topic, and I'm motivated to continue building my skills and become more proficient with these tools in the future.