Incident handler's journal

Maria Audu

Date: July 23, 2024	**Entry:** #1
Description	Documentation of a cybersecurity incident Two phases: **Phase I: Detection and Analysis** The ransomware incident was first detected at **9:00 a.m. on Tuesday** when employees at a healthcare company were unable to access critical files and received a ransom note demanding payment. Initial alerts indicated abnormal file encryption activity across multiple systems. During the analysis phase, the organization determined that the attack originated from a **phishing email** that allowed an organized group of unethical hackers to gain access to the network. To better understand the scope and technical details of the attack, the organization contacted external cybersecurity experts and relevant authorities for technical assistance and guidance on mitigating the threat. **Phase II: Containment, Eradication, and Recovery** To contain the ransomware, the company **shut down affected computer systems** to prevent further spread of the malware. However, the organization lacked sufficient resources and expertise to fully eradicate the ransomware and recover encrypted files on its own. As a result, the company **engaged external organizations** specializing in incident response and cybersecurity recovery. These experts assisted in safely

	removing the ransomware, restoring encrypted files from backups where possible, and implementing enhanced security controls to prevent future attacks.
Tool(s) used	None
The 5 W's	**Who:** An organized group of unethical hackers. **What:** A ransomware attack that encrypted critical files on the healthcare company's systems. **Where:** A healthcare company's network and computer systems. **When:** Tuesday at 9:00 a.m. **Why:** The attackers gained access through a phishing email. After compromising the system, they deployed ransomware to encrypt files, demanding a ransom for the decryption key. The motive appears to be financial gain.
Additional notes	1. Were there any **indicators of compromise (IOCs)** that could have alerted the security team earlier, such as unusual login attempts or suspicious network traffic? 2. How quickly were the **incident response and disaster recovery plans** activated, and were they effective in minimizing system downtime and data loss?

Date: July 25 2024	**Entry:** #2

Description	Analyzing a packet capture file
Tool(s) used	For this activity, I utilized **Wireshark** to examine a packet capture file. Wireshark is a **graphical network protocol analyzer** that allows analysts to monitor and investigate network traffic in real time. It is a valuable tool in cybersecurity because it helps identify unusual patterns or suspicious activity, enabling analysts to **detect potential threats, troubleshoot network issues, and support incident response efforts**.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I have never used **Wireshark** before, so I was excited to try it out and look at a packet capture file. At first, the interface was a bit overwhelming, but I can see why it's such a **powerful tool** for checking and understanding 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 **command-line network protocol analyzer** that allows security analysts to **capture, filter, and inspect network packets**. Like Wireshark, it is valuable in cybersecurity because it provides detailed insight into network activity, helping analysts **identify suspicious behavior and investigate potential security incidents**.
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 **tcpdump** to capture packets. The command-line interface was a bit tricky, and all the raw output with hex and flags was hard to follow at first.

Date: July 27 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real 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 this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? 1. **Containment:** Isolate affected workstation from the network. 2. **Block IoCs:** Add identified domains, IPs, and file hashes to security tools and firewall. 3. **Remediation:** Remove malicious files from the workstation; perform full endpoint scan. 4. **Reporting:** Escalate to Tier 2/3 SOC for further investigation. 5. **User Awareness:** Educate employee about phishing and password-protected attachments.

Reflections/Notes:

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

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

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

After taking this course, my understanding of **incident detection and response** has significantly evolved. Initially, I had a basic idea of what it involved, but I didn't fully grasp the complexity. As the course progressed, I learned about the **incident lifecycle**, the critical role of **plans, processes, and people**, and the various **tools** used in response. Overall, I now feel much more knowledgeable and better equipped to handle incidents effectively.

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

I really enjoyed learning about **network traffic analysis** and applying it using network protocol analyzer tools. It was my first time exploring this area, so it was both **challenging and exciting**. I

found it fascinating to **capture and analyze network traffic in real time**. This experience has increased my interest in the topic, and I hope to become more proficient in using these tools in the future.