**Incident handler's journal**

| **Date:**  06/24/25 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | This scenario focused on how a healthcare company experienced and responded to a ransomware attack. The incident was broken down into two key phases: detection/analysis and containment/recovery. They had to involve outside organizations for support during the process. | | |
| Tool(s) used | None | | |
| The 5 W's | * **Who:** A group of malicious hackers * **What:** A ransomware attack * **Where:** A healthcare company * **When:** Tuesday, 9:00 a.m. * **Why:** Attackers used phishing to gain access and deployed ransomware to encrypt key files. Their goal appeared to be financial, as they demanded a large ransom for the decryption key. | | |
| Additional notes | The scenario raised important questions—should the company pay the ransom? And how can similar incidents be prevented going forward? Better phishing awareness and response planning are key areas to consider. | | |

| **Date:**  6/25/25 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. | | |
| The 5 W's | Who: N/A  What: Analyzed PCAP file  Where: N/A  When: N/A  Why: To learn how to identify and investigate malicious activity through network traffic | | |
| Additional notes | This was my first time using Wireshark to explore and analyze a packet capture (PCAP) file. The exercise introduced me to how cybersecurity professionals can examine network traffic to investigate potential threats. | | |

| **Date:**  6/26/25 | **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: Captured and analyzed packets * Where: N/A * When: N/A * Why: To learn how to use command-line tools for live traffic capture and filtering | | |
| Additional notes | Since I’m still new to the command line, I had to redo the activity after running into some syntax errors. But once I got the hang of it, it was very rewarding to successfully capture and review traffic. | | |

| **Date:**  6/27/25 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | For this task, I worked with VirusTotal, a tool that helps identify malicious content in files and URLs—things like viruses, trojans, or worms. It’s really useful for quickly checking whether something suspicious, like a file or website, has already been flagged by others in the cybersecurity world. In this case, I used VirusTotal to investigate a specific file hash that had been marked as malicious.  The scenario focused on the Detection and Analysis phase of incident response. I stepped into the role of a SOC analyst responding to an alert triggered by a suspicious file. Once the file was flagged by security tools, my job was to dig deeper and figure out whether it actually posed a threat. | | |
| The 5 W's | * **Who**: Unknown attacker * **What**: A phishing email containing a malicious file * **Where**: An employee’s workstation at a financial services company * **When**: 1:20 p.m., when the alert was triggered * **Why**: The file was downloaded and executed by the employee, causing a security alert | | |
| Additional notes | VirusTotal made it easy to cross-check the file hash against known threats. It also emphasized the importance of security awareness for employees. | | |

| Reflections/Notes: Record additional notes.   1. **Were there any specific activities that were challenging for you? Why or why not?**   The activity using tcpdump was the most challenging for me. I’m still new to using the command line, so learning the correct syntax for tcpdump took some time. I felt really frustrated at first because I wasn’t getting the right output. After redoing the activity and carefully going through the instructions, I finally figured out what I was doing wrong. It taught me how important it is to slow down and follow directions closely.   1. **Has your understanding of incident detection and response changed after taking this course?**   Yes, my understanding has definitely improved. At the beginning, I only had a basic idea of what incident detection and response involved. As I went through the course, I learned about the full lifecycle of an incident and how critical things like planning, processes, and teamwork are. I also got a better understanding of the tools used during each phase. I feel a lot more confident now and have a stronger grasp of how everything fits together.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   I really enjoyed learning about network traffic analysis. It was my first time exploring tools that let you capture and examine real-time network traffic. It was both challenging and exciting to see what’s going on behind the scenes. I thought it was fascinating, and it made me want to keep learning more about protocol analyzers like Wireshark and tcpdump. |
| --- |