Incident handler's journal

Author: Betim Sejdiu

Date: October 7, 2024	**Entry:** #1
Description	The incident unfolded in two phases: 1. **Detection and Analysis**: This phase describes how the organization initially identified the ransomware incident. During the analysis, the organization reached out to several external entities for technical support. 2. **Containment, Eradication, and Recovery**: This phase outlines the measures taken to contain the incident, such as shutting down their computer systems. However, because they needed additional help to effectively eradicate the threat and recover, they sought assistance from several other organizations.
Tool(s) used	N/A
The 5 W's	• **Who**: A coordinated group of unethical hackers • **What**: A ransomware security incident • **Where**: At a healthcare company • **When**: Tuesday at 9:00 a.m. • **Why**: The incident occurred because the hackers gained access to the company's systems through a phishing attack. Once inside, they deployed ransomware to encrypt critical files. The attackers seem to be motivated by financial gain, as evidenced by the ransom note they

	left, which demanded a substantial sum of money for the decryption key.
Additional notes	1. Should you ever in cases such as these pay the ransom to get the decryption key?

Date: October 8, 2024	**Entry:** #2
Description	Analyzing a packet capture file.
Tool(s) used	For this activity, I utilized Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer with a graphical user interface. Its value in cybersecurity lies in its ability to capture and analyze network traffic, aiding security analysts in detecting and investigating malicious activities.
The 5 W's	N/A
Additional notes	I've used Wireshark once before in a class project. I am excited to know that some of the knowledge is being brought up again and I've even strengthened it in this exercise.

Date: October 8, 2024	**Entry:** #3
Description	Capturing a packet using tcpdump.
Tool(s) used	For this activity, I employed tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that operates through the command-line interface. Like Wireshark, tcpdump is valuable in cybersecurity because it enables security analysts to capture, filter, and analyze network traffic.
The 5 W's	N/A
Additional notes	I've used a command-line interface before; however, I've never used it to capture a packet before so that was new to me. It was a little challenging to capture a packet and figure out all the different aspects of one. I was able to get through this activity following the directions and the notes of packets that I've previously recorded.

Date: October 9, 2024	**Entry:** #4
Description	Investigating a suspicious file hash
Tool(s) used	For this activity, I utilized VirusTotal, an investigative tool that examines files and URLs for malicious content, including viruses, worms, trojans, and more. It's an invaluable resource for quickly checking if an indicator of compromise, such as a website or file, has been flagged as malicious by others in the

	cybersecurity community. In this instance, I used VirusTotal to analyze a file hash that was reported as malicious. This incident took place during the Detection and Analysis phase. The scenario positioned me as a security analyst at a Security Operations Center (SOC) investigating a suspicious file hash. After the security systems detected the suspicious file, I needed to conduct a thorough analysis to determine whether the alert indicated a genuine threat.
The 5 W's	• **Who**: An unidentified malicious actor • **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: On an employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was triggered and sent to the organization's SOC after the intrusion detection system identified the file • **Why**: An employee was able to download and execute the malicious file attachment from the email.
Additional notes	How can we improve security awareness through training to prevent employees from clicking on malicious links?