**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

|  |  |
| --- | --- |
| **Date:** 06/10/2023 | **Entry:** #1 |
| Description | A small U.S health care clinic experienced a security incident on Tuesday at 9:00am which severely disrupped their business operations. The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed which encrypted the organization's computer files. An organized group of unethical hackers left a ransom note stating the company's files were encrypted and demanded money in exchange for the decryption key. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of unethical hackers * **What** happened? Ransonmware encrypted critical files that made the company unable to access critical patient data, causing major distruption 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. * **When** did the incident occur? Tuesday at 9:00am * **Where** did the incident happen? At a health care company * **Why** did the incident happen? A group of unethical hackers were able to gain access to the company's systems by ushing a phishing attack. After gaining access, the attackers launched ransomeware that encrypted critical patient files. The attackers' motivation appears to be financial because of the ransom note that they left demanding larg sums of money for the decryption key. |
| Additional notes | 1. How can the health care company prevent incidents like this from happening in the future?  2. Should the company pay the ransom fee to retrieve the decryption key? |

|  |  |
| --- | --- |
| **Date:** 06/10/2023 | **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**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I've never used Wireshark before, so I was curious to begin this exercise and analyze a packet capture file. At first, it was slightly overwhelming due to lots of different fields and options, but I eventually gained my footing and started understanding the different parts. I can see why this is such a powerful tool. |

|  |  |
| --- | --- |
| **Date:** 06/10/2023 | **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**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I luckily had a bit of a background with using the command-line interface, so it wasn't completely starting from scratch, but this was the first time I used it to capture and filter network traffic. I got stuck a couple of times because I made a few typos here and there, but after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. |

|  |  |
| --- | --- |
| **Date:** 06/11/2023 | **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, and trojans. 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? |