**Incident handler's journal**

| **Date:** 16-07-2024 | **Entry: 1** | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident which happened U.S health care clinic | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   The incident was caused by an organized group of unethical hackers.   * **What** happened?   A ransomware was spread through a phishing email.   * **When** did the incident occur?   The incident occurred on Tuesday, 9:00 AM.   * **Where** did the incident happen?   The incident took place in a health care clinic.   * **Why** did the incident happen?   The incident happened because a group of unethical hackers were able to gain access to the company’s system by using a phishing attack which was sent through an email, which contained an attachment, when downloaded installed a ransomware which encrypted the organization’s critical files. The attackers intentions appears to be financial gain as they left a note conveying that the organization must pay a large sum of money in exchange for the decryption keys. | | |
| Additional notes | 1. How can the organization prevent similar situations from happening again? 2. Should the organization pay the ransom money to the hackers? | | |

| **Date:** 17-07-2024 | **Entry: 2** | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | 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 | Capture the 5 W's of an incident.   * **Who** caused the incident?   N/A   * **What** happened?   N/A   * **When** did the incident occur?   N/A   * **Where** did the incident happen?   N/A   * **Why** did the incident happen?   N/A | | |
| Additional notes | Successfully used wireshark to analyze and understand a packet capture file and use it to understand network traffic. | | |

| **Date:** 17-07-2024 | **Entry: 3** | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   N/A   * **What** happened?   N/A   * **When** did the incident occur?   N/A   * **Where** did the incident happen?   N/A   * **Why** did the incident happen?   N/A | | |
| Additional notes | It was challenging to capture a network packet using tcpdump but after following the instructions and rectifying some steps, I was able to capture network traffic using tcpdump. | | |

| **Date:** 17-07-2024 | **Entry: 4** | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | 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. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Unknown malicious actor   * **What** happened?   A malicious file attached to an email sent to an employee with the file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b   * **When** did the incident occur?   At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file   * **Where** did the incident happen?   An employee's computer at a financial services company   * **Why** did the incident happen?   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? | | |