**Incident handler's journal**

| **Date:** July 21,2025 | **Entry: #1** | | |
| --- | --- | --- | --- |
| Description | Documenting a cyber security incident. | | |
| Tool(s) used | No tools were used. | | |
| The 5 W's | * **Who** caused the incident? * It was caused by a group of unethical hackers. * **What** happened? * A ransomware security incident. * **When** did the incident occur? * The incident occurred on tuesday 9 a.m * **Where** did the incident happen? * At a healthcare company. * **Why** did the incident happen? * The incident occurred because unethical hackers were able to access the company’s systems through a phishing attack. They deployed ransomware, encrypting the company files and then leaving a note for ransom so that a decryption key would be provided to decrypt the data. | | |
| Additional notes | 1-How a similar incident can be prevented in future?  2- Were the employees given anti-phishing awareness and training in the past?  3- Should the company pay ransom to retrieve the decryption key? | | |

| **Date:**July 23, 2025 | **Entry: #2** | | |
| --- | --- | --- | --- |
| Description | Documenting a cyber security incident. | | |
| Tool(s) used | No tools were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * It was caused by Def Communications * **What** happened? * A phishing attempt. * **When** did the incident occur? * Occurred on Wednesday 09:30:14 AM * **Where** did the incident happen? * At a financial services company. * **Why** did the incident happen? * An employee received an email with an attachment. He clicked on the attachment and a malicious file was downloaded on his computer, accessing his system and stealing the company's sensitive info. | | |
| Additional notes | 1- What measures can be taken to prevent this type of incident in future?  2- What type of loss would the company face due to the incident? | | |

| **Date:** July 26,2025 | **Entry: #3** | | |
| --- | --- | --- | --- |
| Description | Documenting a cyber security incident. | | |
| Tool(s) used | No tools were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * An unethical hacker. * **What** happened? * Data Theft. * **When** did the incident occur? * Friday, 7:20 pm * **Where** did the incident happen? * At a mid-sized retail company. * **Why** did the incident happen? * The incident occurred due to a vulnerability in the company’s e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. The attacker left a note demanding payment as ransom for not releasing the data on public forums. | | |
| Additional notes | 1- Should the company pay ransom to prevent the attacker from releasing stolen data in public?  2- What measures can be taken to prevent this type of incident from happening in future?  3- Were there any security measures the company had implemented before the attack and why were they not successful in preventing the attack? | | |

| **Date:** July 27,2025 | **Entry: #4** | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet. | | |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. It 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 | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times, but I was able to get through this activity and capture network traffic. | | |

### 

### 

| **Date:** July 27,2025 | **Entry: #5** | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file. | | |
| Tool(s) used | I used wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer having a graphical user interface. It allows security analysts to capture and analyze network traffic, which can help in detecting and analyzing 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 | I used wireshark for the first time, the interface was overwhelming, but overall it was good and provided something new to learn. | | |

| **Date:**July 30,2025 | **Entry: #6** | | |
| --- | --- | --- | --- |
| 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. 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 cyber security community, so 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? * An unknown malicious actor. * **What** happened? * An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 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 | 1- How can the incident be prevented in the future?  2- Should we consider improving security awareness training so that employees are careful with what they click on? | | |