**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:**  2023-10-30 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Initial Incident Documentation | | |
| Tool(s) used | N/A | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who caused the incident?** An organized group of unethical hackers. * **What happened?** The health care clinic experienced a security incident involving ransomware, triggered by a phishing email that contained a malicious attachment. * **When did the incident occur?** The incident took place on a Tuesday morning at approximately 9:00 a.m. * **Where did the incident happen?** The incident occurred within the small U.S. health care clinic specializing in primary-care services. * **Why did the incident happen?** The incident happened due to employees falling victim to a targeted phishing email, leading to the deployment of ransomware by the hackers who demanded a ransom for file decryption. | | |
| Additional notes | This incident highlights the critical need for cybersecurity awareness and training among employees in healthcare organizations, as well as the importance of a robust incident response plan to minimize disruption and protect sensitive patient data. It's crucial to promptly address such incidents to safeguard patient confidentiality and maintain business continuity. | | |

| **Date:**  2023-10-30 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | In this exercise, I leveraged Wireshark to delve into the analysis of a packet capture file. Wireshark, as a network protocol analyzer with a graphical user interface, proved to be an invaluable asset for comprehending network traffic. This experience served as a refresher from my university days, and I was excited to reacquaint myself with its capabilities. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who: N/A** * **What: N/A** * **Where: N/A** * **When: N/A** * **Why: N/A** | | |
| Additional notes | As I revisited Wireshark, I found the interface to be initially overwhelming, but its power in unraveling network traffic soon became evident. | | |

| **Date:**  2023-10-30 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | My First Packet Capture | | |
| Tool(s) used | For this task, I decided to immerse myself in the world of packet capture using tcpdump. Tcpdump is a command-line network protocol analyzer, which distinguishes it from the graphical interface of tools like Wireshark. Its significance in the realm of cybersecurity lies in its capability to empower security analysts to not only capture but also effectively filter and analyze network traffic. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** N/A * **What** N/A * **When** N/A * **Where** N/A * **Why** N/A | | |
| Additional notes | As someone still relatively new to the command-line interface, the endeavor of capturing and filtering network traffic using tcpdump presented its challenges. I encountered a few roadblocks, particularly due to my occasional reliance on incorrect commands. However, through meticulous following of instructions and the occasional do-over, I successfully navigated this activity and achieved my goal of capturing network traffic. | | |

| **Date:**  2023-10-30 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Investigating a suspicious file hash | | |
| Tool(s) used | I employed VirusTotal, a versatile investigative tool that assesses files and URLs for potentially malicious content, including viruses, worms, trojans, and more. It serves as a valuable resource for swiftly verifying whether indicators of compromise, such as websites or files, have been previously flagged as malicious within the cybersecurity community. In this instance, I utilized VirusTotal to scrutinize a file hash that had raised suspicions. This incident unfolded during the Detection and Analysis phase, placing me in the role of a security analyst within a Security Operations Center (SOC). My task was to investigate a suspicious file hash that had triggered an alert from the organization's security systems, with the objective of ascertaining the validity of the potential threat. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** The malevolent actor behind this incident remains unidentified. * **What:** An email dispatched to an employee contained a malevolent file attachment, accompanied by the SHA-256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * **Where:** The compromise occurred on an employee's computer within a financial services company. * **When:** At 1:20 p.m., the organization's SOC received an alert after the intrusion detection system flagged the file. * **Why:** The incident transpired due to an employee downloading and executing a malicious file attachment received via email. | | |
| Additional notes | To prevent similar incidents in the future, it is advisable to consider enhancing security awareness training programs. Empowering employees with the knowledge and vigilance to discern potentially hazardous email attachments and links can significantly bolster the organization's overall security posture. | | |

| **Date:**  2023-10-30 | **Entry:**  5 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| Reflections/Notes:   1. **Did you encounter any specific challenges during the activities? If so, what were they and how did you overcome them?**   The activity involving tcpdump proved to be quite challenging for me. My familiarity with the command line was limited, and grasping the syntax of a tool like tcpdump presented a significant learning curve. Initially, I felt a sense of frustration as I struggled to obtain the desired output. However, I decided to redo the activity, meticulously following the instructions and working through the process at a deliberate pace. This experience reinforced the importance of careful instruction reading and methodical problem-solving.   1. **How has your perspective on incident detection and response evolved throughout the course?**   Upon completing this course, my perspective on incident detection and response has undergone a substantial transformation. Initially, I possessed a rudimentary understanding of these concepts, but the complexity involved had yet to fully manifest. As the course progressed, I delved into the intricacies of the incident lifecycle, recognizing the significance of comprehensive plans, well-defined processes, and the role of individuals. Moreover, I gained insights into the array of tools employed in this field. Overall, my comprehension has deepened, and I now possess a broader knowledge base and heightened awareness of incident detection and response.   1. **Was there a particular tool or concept that captured your interest the most? If so, why?**   I was particularly captivated by the realm of network traffic analysis and the practical application of knowledge through network protocol analyzer tools. This was my inaugural exposure to network traffic analysis, which offered both challenges and excitement. The ability to employ tools for real-time capture and analysis of network traffic fascinated me. I am now keen on delving deeper into this domain, with aspirations of enhancing my proficiency in utilizing network protocol analyzer tools. |
| --- |