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: 02/09/24	**Entry: #001**
Description	This journal entry covers a ransomware attack that occurred at a health care clinic in the U.S
Tool(s) used	N/A
The 5 W's	**Who**: The incident was caused by an employee who worked for the firm. **What**: The employee had downloaded a malicious attachment that had been delivered to them via a phishing email. The malicious attachment then installed ransomware on the victim's computer, which encrypted critical business documents. **When**: The incident occurred on a Tuesday morning, at 9:00 am. This resulted in a severe disruption of the business's operations, as critical patient data needed had been encrypted by the ransomware. **Where**: The incident occurred in a healthcare clinic in the United States. **Why**: The incident occurred because an employee had, perhaps mistakenly, downloaded an attachment from a phishing email that they had been sent onto their work computer. As this device was connected to the main business network, the ransomware was able to spread to the rest of the business.
Additional notes	• It is my strong recommendation that employers provide basic security

	training to their employees on the topic of computer security so that they are aware of the risks of opening attachments from unfamiliar emails. • Doing so would enhance the business' security posture, and reduce the likelihood of an event similar to the one described in this journal entry from reoccurring in the future.

Date: 03/09/24	**Entry: #002**
Description	In this journal entry, I investigated a suspicious file hash from a file downloaded by an employee at a financial services company
Tool(s) used	To analyse the suspicious file, I used the VirusTotal service
The 5 W's	**Who:** The incident was caused by one of the employees at the company **What:** The employee had downloaded a suspicious file from an email that they received, which infected their device with a malicious payload **When:** The incident occurred between the times of 1:11pm and 1:20pm, during which the employee received and downloaded the malicious file, and an alert was sent to the SOC **Where:** The incident occurred at the office of the financial services company, using a device connected to their network **Why:** The incident occurred because the employee had opened a file sent to them by a malicious actor while they were connected to the company network
Additional notes	• Using the VirusTotal service, it was determined that the file opened by the employee was of a malicious nature. • Indicators of compromise (IoCs) that were found during analysis of this file included a hash value, an IP address, and a domain name that the file contacted,

Date: 03/09/24	**Entry: #003**
Description	In this journal entry, I used a playbook to respond to a phishing incident that was identified in a previous journal entry
Tool(s) used	N/A
The 5 W's	N/A
Additional notes	• Having determined that the attachment in the ticket was of a malicious nature, I escalated the ticket as per step 3.2 of the phishing incident playbook • Having done this, I updated the ticket to the status of “Escalated”. I believe that the incident should have been escalated because my investigation showed that the content of the file attachment wa sof a malicious nature. • Additionally, as per step 3.2, I notified a L2 SOC analyst of the ticket escalation.

Date: 03/09/24	**Entry: #004**
Description	In this journal entry, I analysed a packet capture and applied filters to search for the necessary entries
Tool(s) used	To perform the tasks in this entry, I used the Wireshark packet capture tool.
The 5 W's	N/A

Additional notes	• During this lab exercise, I identified the source and destination IP addresses used in the communication • I examined the protocols that were used in connecting to the website, and I analysed the data packet to identify key aspects of the information sent, such as the type of the information sent and received by the two systems.

Reflections/Notes:

- **Were there any specific activities that were challenging for you? Why or why not?**
  - I did not find any of the activities particularly challenging, but I did find that some of the activities prompted my curiosity more so than other activities undertaken on the course.
- **Has your understanding of incident detection and response changed since taking this course?**
  - Since taking this course, my understanding of how incidents are handled in a cybersecurity context has greatly increased; now I am more aware of the processes and procedures that are carried out when detecting and responding to an incident.
- **Was there a specific tool or concept that you enjoyed the most? Why?**
  - The tool(s) that I enjoyed using the most during this course was Wireshark
  - This was because it was interesting to be able to deconstruct the packets as they were intercepted on the network and I could clearly see the way that the knowledge gained from previous courses in this certification were applicable.