**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:**  November 26th, 2023 | **Entry: 1** |
| Description | A small US health care clinic experienced a security incident on Tuesday at 9AM which severely interrupted business operations.  There were two phases for this incident:  **Detection & Analysis:** The scenario describes how the health care clinic detected the ransomware attack. The clinic contacted different organizations for technical assistance in order to analyze the incident.  **Containment, Eradication, and Recovery:** To contain the incident, the company shut down their computer systems. They contacted other organizations to help them eradicate and recover from the incident. |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? This incident was caused by an organized group of unethical hackers. * **What** happened? Ransomware was deployed on the organization’s systems through a phishing attack. * **When** did the incident occur? This occurred at 9AM on Tuesday. * **Where** did the incident happen? This happened at the health care clinic, specifically on employee computers. * **Why** did the incident happen? This happened because unethical hackers gained access to the organization’s system from a phishing attack. Once access was gained, they deployed ransomware on the organization’s systems, cutting off access to files critical for business operations. The hackers’ motivation seems to be financial as they claim to be targeting healthcare and transportation industries, demanding payment in exchange for decryption of files. |
| Additional notes | * I’m curious if this happened because employees may not have been informed enough on how to prevent such an attack from happening. * What are the pros and cons of paying the ransom? |
| Date:  November 27th, 2023 | Entry: 2 |
| Description | Analyzing a packet capture file |
| Tool(s) used | I used Wireshark, a network protocol analyzer, to analyze a packet capture file. This is a tool to help analysts capture and analyze network traffic. It is especially helpful and user-friendly because it uses a GUI. |
| 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 | This was the first time I used Wireshark, but the GUI made it relatively easy to navigate. I know with practice this can be a great tool for analyzing network traffic. |

|  |  |
| --- | --- |
| **Date:**  November 26th, 2023 | **Entry: 3** |
| Description | Capturing a packet |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. This is a good tool to analyze data relatively quickly via a command-line interface. |
| 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 | * I am still getting used to using the command-line, and remembering all the commands and what their functions are. This was good practice and the guidelines throughout the activity helped me to understand it all a bit better. |

|  |  |
| --- | --- |
| **December 2, 2023** | **Entry: 4** |
| Description | An employee working for a financial services company downloaded a malicious file from an e-mail they received, executing malware on their computer.  **Detection & Analysis:** In this scenario, the suspicious file had already been detected by the organization. I was required to analyze and investigate the incident to determine the threat level of the incident. |
| Tool(s) used | VirusTotal. This is a tool that helps professionals such as myself investigate files to see if anyone else in the cybersecurity world has determined them as malicious. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? BlackTech (FlagPro) * **What** happened? Malware was executed on an employee’s computer through a malicious attachment * **When** did the incident occur? 1:15pm * **Where** did the incident happen? On an employee’s computer at a financial services company * **Why** did the incident happen? This happened because an employee downloaded a malicious file from an email causing malware to be deployed on the computer. This threat actor could be trying to hack this financial services’ company’s information. |
| Additional notes | After looking through the VirusTotal reports I can see that this is indeed a known malicious hash file. It creates a DirectInput object which is essentially used for capturing keystrokes and can be used to gain access to web applications or internet services as an authenticated user without needing credentials. Moving forward we should hold trainings so that employees are more careful when interacting with e-mails to know which are suspicious and which aren’t. |

|  |  |
| --- | --- |
| **Date:**  December 2, 2023 | **Entry:**  5 |
| Description | Updating the previous entry |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? 76tguyhh6tgftrt7tg.su otherwise known as the threat actor * **What** happened? An employee in HR received an email that contained a malicious attachment, and deployed malware onto their computer from accessing the attachment * **When** did the incident occur? 09:30:14AM * **Where** did the incident happen? On an employee’s computer at a financial services company * **Why** did the incident happen? This happened because the employee failed to recognize the signs that this was a suspicious email, such as numerous typos. |
| Additional notes | This employee received an email from a known malicious file hash and it contains a malicious attachment. The sender claims to be “Clyde West” but the sender name is “Def Communications” and the email is “76tguyhh6tgftrt7tg.su”. There were many typos in the email and the email contained an attachment named “bfsvc.exe” that needed a password to be accessed, which the employee entered into the machine. This alert was reported as medium. Due to these findings, I escalated the ticket. |

|  |  |
| --- | --- |
| **Date:**  December 2, 2023 | **Entry:**  6 |
| Description | A mid-sized retail company experienced a security incident which breached the data of over one million users. This is a review of the final report. |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A Threat actor (no name or email/info provided) * **What** happened? A threat actor stole customer data and demanded payment in exchange for not releasing the data through a forced browser attack. * **When** did the incident occur? December 28, 2022 at 7:20PM. PT * **Where** did the incident happen? On an employee’s computer at the mid-sized retail company. * **Why** did the incident happen? This happened because a threat actor took advantage of a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exciltrated. |
| Additional notes | This could use a little more information such as the name, email or IP address so that we can make sure our records are a bit more accurate, although the actions taken to prevent future occurrences should block this and/or any other threat actor that might try this type of attack. |

|  |  |
| --- | --- |
| **Date:**  December 4, 2023 | **Entry:**  7 |
| Description | Analyzing failed login attempts for Buttercup Games to identify possible mail server security issues. |
| Tool(s) used | Splunk. This is a data analysis platform that can help you search, analyze and visualize security data. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? It is unclear who caused the incident as there are many different login attempts from various IP addresses and ports. * **What** happened? Multiple failed login attempts to Buttercup Games * **When** did the incident occur? 01:39:00AM on pretty much everyday * **Where** did the incident happen? Buttercup games website * **Why** did the incident happen? Someone could be trying to attack the website for malicious purposes. |
| Additional notes | We would need to explore this further or potentially escalate. The numerous IP addresses trying to gain access through various ports could be an indicator of a DdoS attack. We could look into only allowing access for the root account through the necessary ports and blocking the rest. |

|  |  |
| --- | --- |
| **Date:**  December 4, 2023 | **Entry:**  8 |
| Description | Analyzing a phishing attempt and determining if any other employees or the domain have been affected for a financial services company |
| Tool(s) used | Chronicle. This also a data analysis platform similar to Splunk used for search, analysis and visualization of security data. The difference is Chronicle already has data forwarded to it instead of having to upload information like Splunk. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Signin.office365x24.com * **What** happened? A known threat actor sent a phishing email which affected three different employees. * **When** did the incident occur? The three different incidents occurred on 01-31-2023 at 14:40:45, 14:42:45 & 14:50:14. * **Where** did the incident happen? On employees’ emails at a financial services company. The affected users were email-palmer-pc, ashton-davidson-pc & warren-morris-pc. * **Why** did the incident happen? This incident happened because employees received a phishing email that led them to a malicious domain. Although some employees clicked the domain, only 3 actually have POST requests, meaning these users had sensitive information that was submitted to the login page such as login credentials. |
| Additional notes | We should conduct a training on how to identify malicious emails to ensure employees are not visiting domains like these. Because of the incident, now this threat actor could gain access to our systems. We will have to update passwords to ensure the threat actor cannot gain access, as well as conduct an investigation to determine whether any additional damage was done. |

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

|  |
| --- |
| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   Honestly using Chronicle, Splunk, VirusTotal, tcpdump & Wireshark all provided unique challenges for me. The main challenge was getting used to using these tools as they are all new to me. It was a bit difficult trying to navigate and figure out where to find all the correct information. I enjoyed the challenge though, and I know that with practice using these tools will become easier over time. The instructions throughout the activities helped as well, it was just a bit overwhelming.   1. **Has your understanding of incident detection and response changed after taking this course?**   I definitely learned a lot more about incident detection and response after taking this course. I initially thought it was going to be mostly based on using cybersecurity tools and responding to incidents through them, but I wasn’t aware of all the other aspects involved Some of these include the heavy use of documentation, the tools used and the overall process of an incident response.   1. **Was there a specific tool or concept that you enjoyed the most? Why?**   I enjoyed using Splunk & Chronicle the most. I can see how these tools can be very useful when investigating an incident and analyzing malicious activities when a security incident has occurred. They both have relatively user-friendly interfaces and that made me feel a bit more at ease when using them even though they are new tools for me. |