**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:** 09/01/2023 | **Entry:** #1 |
| Description | Documentation of a cybersecurity incident. |
| Tool(s) used | NA. |
| The 5 W's | * **Who caused the incident?** An organized group of unethical hackers * **What happened?** A ransomware security incident. Hackers were able to access the company's systems using a phishing attack. * **When did the incident occur?** Tuesday at 9:00 a.m * **Where did the incident happen?** At a small U.S. health care clinic * **Why did the incident happen**? The incident happened because someone downloaded the malicious attachment from the phishing email, giving access to the unethical hackers.   The attackers' motivation appears to be financial because the ransom note they left demanded money in exchange for the decryption key. |
| Additional notes | The company has to discuss whether they should pay the ransom to retrieve the decryption key or not. Then, they should take measures to prevent an incident like this from happening again. |

|  |  |
| --- | --- |
| **Date:** 09/02/2023 | **Entry:** #2 |
| Description | Packet capture file analysis. |
| Tool(s) used | Wireshark, a network protocol analyzer that uses a graphical user interface. |
| The 5 W's | * **Who caused the incident?** NA * **What happened?** NA * **When did the incident occur?** NA * **Where did the incident happen?** NA * **Why did the incident happen**? NA |
| Additional notes | Having no prior experience with Wireshark, I approached this exercise with enthusiasm, eager to delve into packet analysis. Initially, the interface appeared complex and overwhelming, but I quickly grasped its potential as a robust tool for comprehending network traffic dynamics. |

|  |  |
| --- | --- |
| **Date:** 09/02/2023 | **Entry:** #3 |
| Description | Capturing a packet and analyzing network traffic. |
| Tool(s) used | Tcpdump, a network protocol analyzer that's accessed using the  command-line interface. (I used Linux for this activity) |
| The 5 W's | * **Who caused the incident?** NA * **What happened?** NA * **When did the incident occur?** NA * **Where did the incident happen?** NA * **Why did the incident happen**? NA |
| Additional notes | Using tcpdump for the first time, for capturing and filtering network traffic was an actual challenge. I encountered occasional setbacks due to syntax errors. However, by paying attention and diligently redoing some steps, I ultimately succeeded in completing the activity and effectively capturing network traffic. |

|  |  |
| --- | --- |
| **Date:** 09/03/2023 | **Entry:** #4 |
| Description | Investigating a suspicious file hash. |
| Tool(s) used | VirusTotal, an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. |
| The 5 W's | * **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. This incident occurred in the Detection and Analysis phase. * **Why did the incident happen**? An employee was able to download and execute a malicious file attachment via e-mail. |
| Additional notes | The company should consider improving security awareness training so that employees are careful with what they click on. They should take measures to prevent an incident like this from happening again. |

|  |  |
| --- | --- |
| **Date:** 09/03/2023 | **Entry:** #5 |
| Description | Using a playbook to respond to a phishing incident. |
| Tool(s) used | Phishing Playbook Version 1.0. |
| The 5 W's | * **Who caused the incident?** A malicious file hash. * **What happened?** The alert detected that an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su’” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was   downloaded and opened on the affected machine. Having previously investigated the file hash, it is confirmed to be a known malicious file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to  take further action.   * **When did the incident occur?** 09/05/2023, I received ticket A-2703 for the alert. * **Where did the incident happen?** Level one Security operations center (SOC) at a financial services company. * **Why did the incident happen**? An employee may have opened a   malicious email and opened attachments or clicked links. |
| Additional notes | The company should consider improving security awareness training so that employees are careful with what they click on. They should take measures to prevent an incident like this from happening again. |

|  |  |
| --- | --- |
| **Date:** 09/04/2023 | **Entry:** #6 |
| Description | Exploring signatures and logs. |
| Tool(s) used | Suricata, an open-source intrusion detection system, intrusion prevention system, and network analysis tool. |
| The 5 W's | * **Who caused the incident?** NA. * **What happened?** NA. * **When did the incident occur?** NA. * **Where did the incident happen?** NA.   **Why did the incident happen**? NA. |
| Additional notes | I created custom rules and ran them in Suricata, monitored traffic captured in a packet capture file, and examined the fast.log and eve.json output. |

|  |  |
| --- | --- |
| **Date:** 09/05/2023 | **Entry:** #7 |
| Description | Performing a query with Splunk. |
| Tool(s) used | Splunk platform and Spunk Cloud. |
| The 5 W's | * **Who caused the incident?** NA. * **What happened?** NA. * **When did the incident occur?** NA. * **Where did the incident happen?** NA.   **Why did the incident happen**? NA. |
| Additional notes | I activated a free trial of Spunk Cloud to upload data and performed basic searches while I was getting used to the plataform. I learned a couple of things like the fact that using short time ranges in the searches returns results faster and uses fewer resources. |

|  |  |
| --- | --- |
| **Date:** 09/06/2023 | **Entry:** #8 |
| Description | Investigating a suspicious domain used in a phishing email. |
| Tool(s) used | Chronicle. |
| The 5 W's | * **Who caused the incident?** NA. * **What happened?** NA. * **When did the incident occur?** NA. * **Where did the incident happen?** NA.   **Why did the incident happen**? NA. |
| Additional notes | I determined that the suspicious domain was involved in phishing campaigns. Multiple assets might have been impacted by the phishing campaign as logs showed that login information was submitted to the suspicious domain via POST requests. Finally, I identified two additional domains related to the suspicious domain by examining the resolved IP address. |