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: **12/8/2023**	**Entry: #1**
Description	**A small health care clinic experienced a security incident on Tuesday at 9:00 am, where critical files are encrypted by unethical hackers and they are demanding ransom.**
Tool(s) used	**None were used**
The 5 W's	Capture the 5 W's of an incident. ● **Who: A group of unethical hackers.** ● **What: A group of unethical hackers are demanding ransom in exchange for decryption of critical information.** ● **When: Tuesday, 9:00 am.** ● **Where: A small U.S. health care clinic.** ● **Why: Unethical hackers sent phishing emails to employees where once opened, ransomware was deployed and encrypted the organization's important files.**
Additional notes	- **How will several other organizations respond to this incident? Should the small health care clinic pay this ransome?** - **How will the small health care clinic adapt to this situation to make**

	sure it won't happen again?

Date: 12/8/2023	**Entry: #2**
Description	**Analyzing a packet using Wireshark**
Tool(s) used	**I practiced using the network protocol analyzer, Wireshark, to analyze a packet capture file sample and filter network traffic data.**
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	**This was my first experience using Wireshark to analyze network traffic data and it definitely was a bit confusing, however at the same time, I had fun trying to decipher the output as if I was an actual security analyst.**

Date: 12/8/23	**Entry: #3**

Description	**Capturing a packet using tcpdump, command line interface**
Tool(s) used	**I practiced using tcpdump via the command line interface to capture and analyze network traffic and its contents.**
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	**I am relatively comfortable with the command line interface due to some experience with linux, butI wasn't used to the tcpdump outputs. However, with the step by step process provided, I was able to complete and understand each step, successfully capturing my first packet using tcpdump.**

Date: 12/8/23	**Entry: #4**
Description	**Investigating a suspicious file hash**
Tool(s) used	**I used Virustotal to capture details about whether the file is malicious by using posts from the cybersecurity community. In this case, Virustotal was used to analyze a hash, which was indeed considered malicious by a large chunk of contributors.**

The 5 W's	Capture the 5 W's of an incident. ● **Who: A malicious threat actor** ● **What: An employee was sent a malicious email that downloaded a file, which needed a password to get in. Upon entering the password, a malicious payload was entered on the computer. The file has a hash of: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b** ● **When: At 1:20 PM, the IDS detected executable files and send out alerts to SOC** ● **Where: At an employee's work station at a financial services company.** ● **Why: An employee downloaded a malicious file sent via email.**
Additional notes	**Important to practice security awareness and understand fraudulent vs official emails.**

Date: 12/8/23	**Entry: #5**
Description	**Practice using a playbook to respond to a phishing incident**
Tool(s) used	**I used the organization's playbook (with flowchart) to identify the necessary steps to deal with phishing.**

The 5 W's	Capture the 5 W's of an incident. ● **Who: Unknown malicious actor (Alias: Def Communications/Clyde West)** ● **What: Received a phishing alert about a suspicious file being downloaded on an employee's computer** ● **When: 7/20/22 at 9:30 AM was when the email was sent.** ● **Where: At an employee's workstation at a financial services company.** ● **Why: An employee downloaded a malicious file from a phishing email.**
Additional notes	**Important to practice security awareness and understand fraudulent vs official emails.**

Date: 12/12/23	**Entry:#6**
Description	**Performing a query with Chronicle**
Tool(s) used	**I used the cloud-native tool, Chronicle, to investigate a security incident relating to phishing. Chronicle is a SIEM tool used to collect, analyze, and report on data from different sources. Similar to Splunk, but Chronicle uses a unified data model.**
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	**It was interesting seeing the differences between Chronicle and Splunk. While Splunk is a search processing language, Chronicle uses a unified data model to store multiple sources. This is helpful because it tells me a general summary of domains.**

Reflections/Notes: **It was interesting to learn all of these necessary cybersecurity tools. They were all challenging in their own way, but understanding tcp dumping was definitely the most challenging. Though hard to grasp at first, I now understand the general use and output meaning. I enjoyed using Chronicle and Splunk the most due to its nature of investigation.**