Incident handler's journal

Date: 29-06-2024	**Entry:** #1
Description	Documenting a cybersecurity incident ● The company first detected the incident because several employees reported that they were unable to access files and software needed to do their job. ● And there is report of ransom note displayed on their computers ● The company realized that the attacker gained access to the company's network through targeted phishing emails. The phishing emails contained malicious attachments that encrypted critical files. ● The containment, eradication, and recovery steps the company took to handle this incident involved shutting down their computer systems, and contacted several other organizations for assistance.
Tool(s) used	List any cybersecurity tools that were used. ● None
The 5 W's	● **Who:** An organized group of unethical hackers ● **What:** A ransomware security incident ● **When:** Tuesday 29-06-2024 at 9 AM ● **Where:** Several employees computers at a health care company ● **Why:** A phishing email launched by a group of hackers that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. The attacker's motivation is financial because they left the ransom note demanding a large sum of money in exchange for the decryption key.

Additional notes	Include any additional thoughts, questions, or findings. ● The group are known to target organizations in healthcare and transportation industries ● They had to contact several organizations to report the incident and receive technical assistance ● How could the company prevent phishing attacks from happening again in the future ● Should the company pay the ransom to retrieve the decryption key

---

Date: 30-06-2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	I used a graphic user interface packet sniffer tool called Wireshark. It can display all the data inside the packet to help me analyze it thoroughly.
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 have never used Wireshark before, so I was excited but also nervous to begin using it. At first I was overloaded with the amount of information that it displays, making me confused as to where do I need to focus my attention. But overtime, reading them and getting familiar with the interface helps me

	navigate the application to find the information that I need. And it helps me understand more about network traffic.

Date: 01-07-2024	**Entry:** 3
Description	Capturing my first packet with tcpdump
Tool(s) used	I used tcpdump, a command line interface application to capture, 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	I have used bash and command line terminal before so some of the commands are familiar to me. Still, tcpdump is a new tool that I have never used before. It does take some time to get familiar with it and play around with the commands to see different results. But overall it was a very productive activity and I learned a lot more about network traffic.

Date: 02-07-2024	**Entry:** 4
Description	Investigating a phishing attempt possible download of malware
Tool(s) used	For this investigation I used VirusTotal. It is an investigation tool tat can analyze files and URLs for malicious contents like viruses, worms, trojans, and more. It is an easy and quick way to check if an indicator of compromise like a website or file has been reported as malicious in the cybersecurity community. This time I am investigating a hash file, which was reported to be malicious. In this incident, my role is to perform a deeper investigation of a hash file that a security team has detected. My task is to determine if the alert signified a real threat or not
The 5 W's	Capture the 5 W's of an incident. ● **Who:** Unknown malicious actor ● **What:** An email sent from this email address 76tguyhh6tgftrt7tg.su was opened by an HR employee at Ignergy. The email contained a malicious file attachment with the SHA-256 file hash of “54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab27f6b” ● **When:** At 1:20p.m, an alert was sent to the organization’ SOC after the system detected the file ● **Where:** From an Ingergy employee’s computer, Ingergy is a financial service company ● **Why** did the incident happen? The incident happened because the employee was trying to open the attached file from that email, thinking that it’s a resume and cover letter
Additional notes	The name of the email and the name of the sender is different The file is already confirmed to be malicious

	There is grammar error found in the email The file is an executable file not a doc file

---

Reflections/Notes:

- Some of the activities are challenging as someone who is just starting to learn cybersecurity. Using Wireshark and tcpdump for the first time was a challenge. Both of them have high learning curves for me. What made me get through the activities and get a better understanding of how to use these tools are patience, and humility to learn something new. Starting slow works best for me when exposed to something new.
- My understanding and impression of the cybersecurity world changed a lot throughout this program. Specifically in the incident detection and response stages. All thought it requires a lot of attention to detail, critical thinking and problem solving skills in time sensitive situations, and a solid understanding of a complex topic such as network traffic. This program makes me realize that there’s a lot of tools and resources out there that can help me learn and improve myself jumping into this career path. Overall these activities makes me feel the cybersecurity field to be less daunting.
- I enjoyed it the most when using network protocol analyzer tools. They can be overwhelming at first but overtime I really appreciate how useful these tools are to help me learn and practice my skills in the cybersecurity field. There’s a lot of interesting things that can be found and learn from using these kind of tools too which makes it more intriguing for me to keep trying.