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: June 23, 2023	**Entry:** #1
Description	Documenting a cybersecurity incident; Phase: Detection and Analysis
Tool(s) used	None.
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: June 29, 2023	**Entry:** #2
Description	Documenting an phishing alert. Phase: Detection and Analysis

Tool(s) used	VirusTotal: Analyzing a suspicious attachment using its hash value.
The 5 W's	- **Who**: Def Communications (name: Clyde West, IP: 114.114.114.114) - **What**: A phishing email contains a malicious link (with a known malicious hash) - **Where**: At Inergy - **When**: Wednesday, July 20, 2022 09:30:14 AM - **Why**: A user was tricked into opening a malicious link sent by a threat actor pretending to be someone interested in the open Engineering role at the company. The malicious link may have downloaded malware onto the user's computer.
Additional notes	1. Ticket was escalated due to the download of malware. 2. More phishing identification training

Date: July 30, 2023	**Entry:** #3
Description	Analyzing a packet capture file
Tool(s) used	Wireshark: Wireshark is a network protocol analyzer, also known as a packet sniffer, with a GUI. Wireshark allows security analysts to capture and analyze network traffic, which helps in detecting and investigating malicious activity.
The 5 W's	- **Who**: N/A - **What**: N/A - **Where**: N/A - **When**: N/A - **Why**: N/A
Additional notes	I've never used Wireshark before, so it took some time getting used to the flow of the application. I can understand why Wireshark is so popular, as the program's functionality is simple and powerful.

Date: July 30, 2023	**Entry:** #4
Description	Capturing my first packet
Tool(s) used	tcpdump: tcpdump is a packet sniffer similar to Wireshark in purpose but uses a CLI instead of a GUI
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	tcpdump is certainly harder to read than Wireshark, but seems like it can be used at a faster pace after I gain more experience. I also mistyped the commands a few times, but after slowing down and taking the instructions step by step, I was able to easily find and analyze the packet data.

Date: July 3, 2023	**Entry:** #5
Description	Documenting a Chronicle analysis. NIST IRL phase: Post-incident Activity
Tool(s) used	Chronicle: Analyzing a suspicious domain's logs
The 5 W's	● **Who**: signin.office365x24.com ● **What**: A potentially malicious website ● **Where**: n/a ● **When**: January 31, 2023 ● **Why**: The website has been flagged as a dropsite for stolen login credentials.
Additional notes	● There are 6 assets that were affected. They all look like personal computers. ○ Ashton-davidson-pc (POST login.php) ○ bruce-monroe-pc ○ coral-alvarez-pc ○ Emil-palmer-pc (POST login.php) ○ jude-reyes-pc

	○ Roger-spence-pc ○ Warren-morris-pc (POST login.php); under resolved IPs ● The resolved IP 40.100.174.34 goes to two domains ○ signin.office365x24.com ○ signin.accounts-gooqle.com

Date: July 3, 2023	**Entry:** #6
Description	Documenting Suricata Logs; Phase: Preparation
Tool(s) used	Suricata: Analyzing logs
The 5 W's	● **Who**: signin.office365x24.com ● **What**: A practice file for running through Suricata called sample.pcap ● **Where**: n/a ● **When**: July 3, 2023 ● **Why**: To practice looking at logs in Suricata
Additional notes	● Used the command “sudo suricata -r sample.pcap -S custom.rules -k none” to have Suricata analyze sample.pcap ● Suricata created 4 different log files, I analyzed the eve.json and fast.log file ● Used the jq command to search for specific attributes of the eve.json file

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

Using Chronicle was difficult for me. I have never used any SIEM tools or the YARA-L language before. If there were not detailed instructions, then I would never have been able to use the tool properly. I would like to have more practice so that I can get over the hump of the learning curve, and get better at using SIEM tools in general.

2. **Has your understanding of incident detection and response changed after taking this course?**

I understand that preparation and adaptation are incredibly important. Many threats are urgent and require quick responses, so having playbooks and automated tools to assist people with threats will increase defense. Also, learning how to configure tools so that they are efficient at analysis prevents a lot of attacks while making other attacks easy to sniff out. Also, documentation, especially clear and concise documentation, is great because information is used so often everyday, and being able to understand and recall previous events and incidents gives the advantage to the defenders.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I think using Suricata was the most fun. I like using the command line because it is so simple and yet so powerful. I only wrote a few lines for Suricata, but I was able to have it analyze a specific package, create log files, and specifically analyze a few of those log files. Suddenly, logs didn’t seem so complicated and unreadable. They contain important info, and I just have to know how to read it to figure out lots of information.