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: 21 april,2024	**Entry:** #1
Description	Documenting a cybersecurity incident
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:An unethical hacking incident involving a phishing attack resulted in unauthorized access to the company's systems. Subsequently, the attackers launched ransomware, encrypting critical files. The apparent financial motivation of the attackers was evident in the ransom note they left, demanding a hefty 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: 7 april 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	In this activity, I utilized Wireshark, a network protocol analyzer with a graphical user interface, to analyze a packet capture file. The significance of Wireshark in cybersecurity lies in its ability to aid security analysts in capturing and analyzing network traffic. This capability is instrumental in detecting and investigating malicious activity.
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	Wireshark proved to be a captivating tool for network analysis, despite not being my initial encounter with it. Its capabilities as a software for examining captured files are truly remarkable.

Date: 20 april 2024	**Entry:** #3
Description	Capturing packet
Tool(s) used	I used tcpdump to capture and analyze network traffic.Tcpdump is a powerful command-line tool designed for capturing and analyzing network traffic on your computer.
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	Capturing and filtering network traffic proved challenging with Tcpdump. I faced obstacles due to incorrect command usage. However, by diligently following the instructions and repeating certain steps, I managed to navigate through this activity, successfully capturing network traffic.

Date: 29 april 2024	**Entry:** #4
Description	Investigate a suspicious file hash

Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the Detection and Analysis phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	Capture the 5 W's of an incident. ● Who: An unknown malicious actor ● What: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● Where: An employee's computer at a financial services company ● When: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● Why: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	To prevent future incidents, we should consider enhancing security awareness training. This would help employees become more cautious about the links they click on.

Date:	**Entry:**
4 june 2024	#5

Description	Using a playbook to respond to phishing incident
Tool(s) used	N/A
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	Playbooks are essentially rulebooks for your organization, outlining best practices and procedures. They offer a variety of benefits, streamlining operations and ensuring everyone's on the same page.They act as a shared reference point, fostering better communication and collaboration within teams. 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.

---

5 june 2024	#6

Description	Identifying possible security issues with mail server
Tool(s) used	Splunk
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	In my exploration of Splunk, I discovered several crucial fields, including "host," "source," and "sourcetype." The "host" field identifies the network host from which an event originated, while the "source" field indicates the file name associated with the event. The "sourcetype" determines how data is formatted. To locate any failed SSH login attempts for the root account, I utilized the following search query: **index=main host=mailsv fail* root.**

Reflections/Notes: I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools.it was both challenging and exciting. I found it really fascinating to be able to use tools to capture network traffic and analyze it in real time.Using splunk was quite interesting.