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: August 7, 2024	**Entry: #1**
Description	Documenting a cybersecurity incident.
Tool(s) used	N/A
The 5 W's	• **Who**: An organized group of unethical hackers • **What:** Ransomware attack • **When:** Tuesday 9:00 am • **Where:** A small health care clinic based in the U.S. • **Why:** The incident occurred via phishing attack (i.e. malicious attachment containing ransomware in phishing email). This was financially motivated as there was a ransom note demanding money in exchange for the decryption key of the company's files.
Additional notes	Education of all employees to carefully inspect each email could have helped prevent this situation. Also network segmenting and backing up data could help with mitigating risk of ransomware.

Date: August 7, 2024	**Entry: #2**
Description	Investigating a suspicious file hash
Tool(s) used	SHA256 file hash, VirusTotal
The 5 W's	• **Who**: Unethical hackers • **What**: Phishing email with malicious file • **When**: Today, at 1:20 pm • **Where**: Financial services company • **Why**: Capture user input for financial gain/information gathering purposes
Additional notes	By retrieving the malicious file and creating a SHA256 hash of the file, the file was able to be analyzed using VirusTotal to uncover indicators of compromise (IoCs) that are associated with the file. File appears to capture user input, which could potentially leak login credentials for the purpose of financial gain/information gathering. Increasing employee awareness could help prevent this in the future.

Date: August 8, 2024	**Entry: #3**
Description	Using Splunk to identify whether there are possible security issues with the mail server by exploring failed SSH logins for the root account.

Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who**: Malicious actor • **What**: Attempt access root account • **When**: September 8, 2022 • **Where:** e-commerce store Buttercup Games • **Why:** Take control of the root account for financial/political gain.
Additional notes	By analyzing log files using Splunk, we were able to locate that mailsv - Buttercup Games' mail server (root account) host had over 100 failed SSH login attempts. This could be a sign of a malicious hacker attempting to brute force into the mail server for financial gain.

Date: August 8, 2024	**Entry:#4**
Description	Financial services company had employees receive phishing emails with a suspicious domain and used their login credentials on the site, which allowed hackers to save credentials for financial/political gain.
Tool(s) used	Google Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who**: malicious hackers • **What**: phishing email contained a suspicious domain that was visited. • **When**: January 31, 2023 • **Where**: financial services company

	• **Why**: retrieve login information that was submitted to domain
Additional notes	By using Google's Chronicle SIEM, we were able to access threat intelligence reports on the domain, the assets that accessed the domain, evaluate HTTP events associated with the suspicious domain, and evaluate which assets submitted login information to the domain. After investigating, it was found that multiple assets may have been impacted by a phishing campaign as logs showed login information was submitted to the domain via Post requests.

Reflections/Notes:

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

I found using Google Chronicle difficult to navigate only because the instructions in the course were a bit unclear and using a "legacy interface." Although there is a GUI for Chronicle, it felt unfamiliar and not easy to navigate. Fortunately, there was an AI Gemini that was able to help with queries to resolve syntax issues I was having/navigating to exactly what was needed to analyze the data.

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

Yes, throughout the course, I was exposed to multiple tools to help analyze data or logs efficiently to determine the root cause of a problem that arises. I now have a better idea of incident detection and response and the basic framework/tools needed to properly handle incidents.

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

Splunk was especially useful as the SIEM tool took in data quickly, has a simple interface, and is easy to navigate. Also, the syntax for queries was simple and easy to use.