Incident handler's journal - Omar Alami

Date: 2/6/24	**Entry: 1**
Description	This scenario outlines how unethical hackers have deployed ransomware into the internal network of a healthcare organization through targeted phishing emails to several employees. The hackers left a ransom note stating that the company's files were encrypted, and demanded money in exchange for the decryption key.
Tool(s) used	Anti-virus software
The 5 W's	● **Who** - Unethical group of hackers ● **What** - Ransomware attack on internal network ● **When** - Tuesday at 9:00am ● **Where** - Small U.S. healthcare clinic ● **Why** - Staff clicked on links from targeted phishing emails
Additional notes	The operations team should hold a meeting to educate employees on how to spot phishing emails, and other cyber threats. Audits on company security controls should also be conducted. A back-up of company needs to be kept to recover from this incident.

Date: 2/8/24	**Entry: 2**
Description	For this activity, an alert was investigated stating an employee received a phishing email in their inbox. A suspicious domain name is contained in the email's body: **signin.office365x24.com**. It was discovered that 6 company assets have accessed the domain which has been flagged as malicious. Assets: **ashton-davidson-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023 **bruce-monroe-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023 **coral-alvarez-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023 **emil-palmer-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023 **jude-reyes-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023 **roger-spence-pc** First accessed: January 31, 2023 Last accessed: July 09, 2023
Tool(s) used	Chronicle SIEM tool, VirusTotal website

The 5 W's	● **Who** - Employees who had received the phishing email ● **What** - Employees accessed a suspicious domain ● **When** - 2023-01-31 ● **Where** - Employee pc’s on company premises ● **Why** - Employees clicked on a phishing link
Additional notes	POST requests to the /login.php page have been found. This indicates the possibility of malicious phishing attempts being successful.

Date: 2/11/24	**Entry: 3**
Description	In this scenario, an alert was received regarding a suspicious file being downloaded onto an employee's computer.
Tool(s) used	VirusTotal website
The 5 W's	● **Who** - Unknown threat actor ● **What** - An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab5 27f6b ● **When**: ● 1:11 p.m.: An employee receives an email containing a file attachment.

	- 1:13 p.m.: The employee successfully downloads and opens the file. - 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. - 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC. - **Where** - Employee computer on company premises - **Why** - The employee who had received the phishing email clicked on a link that was attached which then started the download of the malicious payload.
Additional notes	Findings should be passed onto the L2 SOC analyst for further investigation.

Date: 2/16/24	**Entry: 4**
Description	In this activity, I am tasked to identify whether there are any possible security issues with the mail server of an e-commerce store "ButterCupGames." Failed SSH logins for the root account must be investigated.
Tool(s) used	Splunk SIEM tool
The 5 W's	- **Who** - Users of various company endpoints - **What** - An investigation to identify possible security issues

	● **When** - 2023-03-06 at 1:39pm ● **Where** - On company premises ● **Why** - Multiple failed login attempts were found on the company mail server.
Additional notes	Over 300 failed login attempts were found for the root account on the mail server. There is a possibility a data breach has occurred.

Date: 2/17/24	**Entry:** #5
Description	Capturing my first data packet.
Tool(s) used	Tcpdump was used to capture and analyze network traffic. Tcpdump is a network protocol analyzer that uses a command-line interface. Similar to Wireshark, tcpdump allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	I'm still new to using the command-line interface, so capturing and filtering network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. However, after carefully following the instructions and redoing some steps I was able to successfully capture network traffic, and gain more confidence in using tcpdump.

Reflections/Notes:

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

I found the activity using tcpdump challenging.Since I am new to using the command line, learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

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

After taking this course, my understanding of incident detection and response has significantly improved. In the beginning of the Google Cybersecurity Professional Certificate course I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of frameworks, processes, people, and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

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

I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. Although it was my first time learning about network traffic analysis, it was both interesting and exciting. I am definitely more interested in learning more about this topic, and I hope to one day become more proficient in using network protocol analyzer tools.