Incident handler's journal

Date: July 23, 2023
Entry:
#1
Description
Documenting a cybersecurity incident

This incident occurred in two phases:

- Detection and Analysis: The scenario outlines how the organization first detected the ransomware incident. In the analysis step, the organization contacted several entities for technical assistance.
- Containment, Eradication, and Recovery: The scenario details some measures that the organization took to contain the incident. For instance, the company halted their computer systems. However, since they could not independently work on eradicating and recovering from the incident, they enlisted the support of several other entities.

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 occurrence took place due to unethical hackers managing to infiltrate the company's systems through a phishing attack. Following successful access, the attackers initiated their ransomware on the company's systems, encrypting vital files. The motive behind the attackers seems to be financial in nature, as evident from the ransom note they left, which stipulated a substantial amount of money in exchange for the decryption key.

Additional notes

- How could the health care company prevent an incident like this from occurring again?
- Should the company pay the ransom to retrieve the decryption key?

Date: July 25 2023
Entry:
#2

Description
Analyzing a packet capture file
Tool(s) used
For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. Wireshark is useful in cybersecurity because it allows security analysts to capture and analyze network traffic. This can help 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
Being a newcomer to Wireshark, I embarked on the task with enthusiasm, eager to delve into the analysis of a packet capture file. Initially, the interface presented a somewhat intricate appearance, yet I did not let that stop me. It swiftly became evident why Wireshark enjoys its reputation as a potent instrument for comprehending network traffic dynamics; its capabilities are pretty impressive.

Date: July 25 2023
Entry:
#3
Description
Capturing my first packet
Tool(s) used
During this activity, I employed tcpdump to capture and assess network traffic. Tcpdump functions as a network protocol analyzer accessible via the command-line interface. Much like Wireshark, the significance of tcpdump in the realm of cybersecurity lies in its ability to enable security analysts to capture, filter, and scrutinize network traffic.
The 5 W's

- **Who**: N/A
- **What**: N/A
- **Where**: N/A
- **When**: N/A
- **Why**: N/A

Additional notes
Given my limited experience with the command-line interface, using it to capture and filter network traffic presented a challenge. I encountered a few stumbling blocks due to inaccurately inputting commands. Nevertheless, by diligently adhering to the instructions and retracing my steps, I successfully navigated through this activity and managed to capture network traffic.

Date: July 27 2023
Entry:
#4
Description
Investigate a suspicious file hash
Tool(s) used
During this activity, I utilized VirusTotal, an investigative tool designed to scrutinize files and URLs for potential malicious content, such as viruses, worms, trojans, and the like. This tool proves exceptionally valuable for swiftly verifying whether an indicator of compromise, like a website or file, has been flagged as malicious by other professionals in the cybersecurity community. In the context of this activity, I employed VirusTotal to analyze a file hash, which turned out to be reported as malicious.

This incident unfolded during the Detection and Analysis phase. Assuming the role of a security analyst at a Security Operations Center (SOC), I engaged in investigating a dubious file hash. After the security systems initially detected the suspicious file, I delved into comprehensive analysis and inquiry to ascertain whether the alert indicated an actual threat.

The 5 W's

- **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

How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

Reflections/Notes:

- **Were there any specific activities that were challenging for you? Why**

or why not?

Taking on the tcpdump activity was a real challenge for me. Given my limited experience with the command line, getting to grips with the syntax of tcpdump was a bit of a learning curve. At the start, I felt a bit frustrated since I wasn't getting the expected results. But I didn't give up; I decided to redo the activity and took my time to identify where I had made mistakes. This experience ended up being a great lesson in the value of careful instruction reading and working through tasks step by step. I'm feeling more confident after overcoming this hurdle!

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

Upon completing this course, my comprehension of incident detection and response has undeniably transformed. When I initially started, I possessed a rudimentary grasp of the concepts, but I was far from comprehending the intricacies involved. However, as I advanced through the course, I gained insights into the complete incident lifecycle, recognizing the significance of strategic plans, streamlined processes, and skilled personnel. Moreover, I delved into the array of tools utilized in this domain. Overall, I can confidently assert that my understanding has evolved significantly, leaving me better equipped with a wealth of knowledge about incident detection and response.

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

Exploring network traffic analysis and putting my newfound knowledge into practice through network protocol analyzer tools was an incredibly enjoyable experience for me. As a newcomer to the realm of network traffic analysis, I encountered both challenges and thrills along the way. Witnessing the capabilities of tools that enable real-time capture and analysis of network traffic was truly captivating. This exposure has certainly ignited a deeper interest in delving further into this domain. My aspiration is to enhance my proficiency in using network protocol analyzer tools, ultimately nurturing a comprehensive understanding of this subject matter.