**Kiernan Rodriguez**

**2/14/2024**

**Google Cyber security lab project:**

**Creating an incident handler’s journal**

**Scenario Overview**

In this scenario I developed a project where I made an incident handler’s journal outline to record how a company organization detected a ransom ware incident. This journal goes into deep detail to show what steps were taken in the situation to prioritize the issues to be resolved in this case. I also, made statements about the skills and fundamentals I’ve learned through this course I completed for my Google cyber security certificate program.

**Cyber-threat Incident Scenario:**

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransom ware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

**Incident handler's journal: Kiernan Rodriguez**

|  |  |
| --- | --- |
| **Date:** July 23, 2024 | **Entry:**  #1 |
| Description | Documenting a cyber-security incident  This incident occurred in the two phases:   1. **Detection and Analysis**: The scenario shows how the organization first detected the ransom ware incident. For the analysis step, the organization contacted several organizations for technical assistance to resolve the issue. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. |
| 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 business * **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 to affect their security infrastructure. 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 in order to receive the critical files back. |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again?   **My solution would be installing strong firewall settings to secure all networks/file structure to protect personal information. I would install a 2 factor authentication system on the security framework to strengthen defenses. Also, I would suggest installing a strong intrusion detection system on top of an intrusion prevention system to prevent and deter against cyber threat hackers. I would also, include a authentication login verification process challenge security code to prevent any threats from gaining access to the company’s critical files or infrastructure**   1. **Should the company pay the ransom to retrieve the decryption key**?   No the company should never pay ransom to the hacking group in order to attain their files again. The unethical hackers will find a way to trick and manipulate the host to attempt to hack the company again. Also, they can fool the company by giving out a fake decryption key and continue to harm the business financial resources to never give them access to the files at all. The best way to combat this is to have law enforcement involved to track the hacker’s location and force deprivation models to counter measure attacks on them in order to gain the files and expose their location to reclaim control of the assets. The hackers won’t stop until they receive their demands. The best way is too deter them with coercive means to combat their plans to reduce risk and destruction of more data and infrastructure for the hospital company’s assets. |

|  |  |
| --- | --- |
| **Date:** July 25 2024 | **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 to discover data found in network data traffic. The value of Wireshark in cyber security is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity to detect threats faster in cyber threat investigation. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | From utilizing my previous skills with wireshark I was able to adapt to the skills needed to find the threats in the early phase of conducting research of this issue. The great benefits of wireshark provide massive detailed overview of a network packet information to filter out certain lines of log data to analyze potential threat activity. The software provides great assistance with tracking suspicious activity in a security framework of network data traffic to detect bad actors in the event of any cyber security investigation to deter against any threats in real time protection. |

|  |  |
| --- | --- |
| **Date:** July 25 2024 | **Entry:**  #3 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer tool that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic in the flow of data. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I'm still intermediate to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands in some cases. After carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. It naturally adapts with your knowledge the more you practice it. I was able to find certain packet log data records that showed threat activity intruding the security framework at the time of the event incident. |

|  |  |
| --- | --- |
| **Date:** July 27 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 threats. 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 | * **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?  There should be a implemented malicious file detection software installed on the user’s computer to inform the person that a malicious file is detected for a threat to infect their computer. The user should be heavily educated on the potential cyber threats that can harm them whether they use a computer or not in their free time. Also, there should be massive firewall rule principles installed on the user’s computer to prevent them from downloading any malcious file that’s not safe for company use to obtain. This way it prevents the means of risk for a person’s computer and personal information to be exposed for the matter of a threat incident. |

|  |
| --- |
| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve for me. 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. I eventually mastered it better to elevate my knowledge faster.   1. **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 definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved in certain phases. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and 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.   1. **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. It was my first time learning about network traffic analysis, so 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. 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. This helped my skills grow a lot and I’m proud I put a lot of practice into this. |