Incident Handler's Journal

Date: June 8, 2023
Entry: #1
Description:
Cybersecurity Incident Documentation

This incident occurred in two phases: Detection and Analysis, and Containment, Eradication, and Recovery. During the detection and analysis phase, the organization identified a ransomware incident and sought technical assistance from multiple organizations. In the containment, eradication, and recovery phase, the company took steps such as shutting down computer systems and seeking external assistance to mitigate the incident.

Tool(s) used: None

The 5 W's:
Who: An organized group of unethical hackers
What: A ransomware security incident
Where: At a healthcare company
When: Tuesday, 9:00 a.m.
Why: The incident was caused by unethical hackers gaining access to the company's systems through a phishing attack. The attackers launched ransomware, encrypting critical files, with a financial motive indicated by the demand for a large sum of money in exchange for the decryption key.

Date: June 9, 2023
Entry: #2
Description:
Analysis of a Packet Capture File

Tool(s) used:
For this activity, I utilized Wireshark, a network protocol analyzer with a graphical user interface. Wireshark enables security analysts to capture and analyze network traffic, assisting in the detection and investigation of malicious activity.

The 5 W's:

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

Additional notes:
I was initially overwhelmed by the interface of Wireshark, but I quickly recognized its power in understanding network traffic. Analyzing a packet capture file was an exciting exercise, and I appreciate the capabilities provided by Wireshark.

Date: June 10, 2023
Entry: #3
Description:
Capturing My First Packet

Tool(s) used:
For this activity, I employed tcpdump, a command-line network protocol analyzer. Tcpdump allows security analysts to capture, filter, and analyze network traffic, similar to Wireshark.

The 5 W's:
Who: N/A
What: N/A
Where: N/A
When: N/A
Why: N/A

Additional notes:
Using the command-line interface for capturing and filtering network traffic with tcpdump proved to be a challenge. I faced difficulties due to my limited experience, but with careful attention to instructions and perseverance, I successfully completed the activity.

Date: June 11, 2023

Entry: #4

Description:

Investigating a Suspicious File Hash

Tool(s) used:

For this activity, I utilized VirusTotal, an investigative tool for analyzing files and URLs. VirusTotal aids in detecting malicious content such as viruses, worms, and trojans. In this instance, I used VirusTotal to analyze a reported malicious file hash.

This incident occurred during the Detection and Analysis phase, where I acted as a security analyst investigating a suspicious file hash. After the security systems detected the file, I performed in-depth analysis and investigation to determine the severity of the 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: The intrusion detection system triggered an alert at 1:20 p.m.

Why: An employee downloaded and executed a malicious file attachment via email.