Incident handler's journal

Scenario

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Friday morning, at approximately 10:00 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 ransomware, 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.

Date: October 11th, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident.
Tool(s) used	Playbook.
The 5 W's	● **Who:** An organized group of unethical hackers. ● **What:** A ransomware security incident. ● **Where:** At a health care company.

	● **When:** Friday 10:00 a.m. October 11th 2024. ● **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. 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.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? a. By conducting regular phishing awareness training for all employees to educate them about recognizing and avoiding phishing attacks. b. Conducting regular security audits and vulnerability assessments to identify and address potential security weaknesses. 2. Should the company pay the ransom to retrieve the decryption key? a. While paying the ransom may seem like a tempting solution in the short term, it is often a risky and ineffective approach. b. There is no guarantee that paying the ransom will result in the decryption key being provided. c. Paying the ransom directly funds criminal organizations that may use the money to finance further attacks or other illegal activities.

Date: October 15th, 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this task, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	● **Who**: Security analyst. ● **What**: Investigate traffic to a website. ● **Where**: qwiklabs server. ● **When**: Tuesday 9:30 A.M. October 15th, 2024 ● **Why**: Identify the source and destination IP addresses involved in this web browsing session.
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. In this task, I opened saved packet capture files, viewed high-level packet data, and used filters to inspect detailed packet data.

Date: October 16th, 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 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.
The 5 W's	● **Who**: Network analyst ● **What**: Capture and analyze live network traffic from a Linux virtual machine. ● **Where**: qwiklabs server

	● **When**: Wednesday 10:30 A.M. October 15th, 2024 ● **Why**: Identify the network interfaces that can be used to capture network packet data.
Additional notes	I identified network interfaces, used the tcpdump command to capture network data for inspection, interpreted the information that tcpdump output regarding a packet, and saved and loaded packet data for later analysis.

Date: October 18th, 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this task, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. 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. This incident occurred in the **Detection and Analysis** phase. 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	1. How can this incident be prevented in the future? a. Warn employees about the risks of opening attachments from unknown senders or suspicious emails.

	b. Advise employees to avoid downloading and opening files from untrusted sources. 2. Should we consider improving security awareness training so that employees are careful with what they click on? a. Yes, by encouraging employees to report any suspicious activity or security concerns to the security team. b. Tailoring the training to the specific roles and responsibilities of different employees.