Incident handler's journal

Instructions

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 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:	**Entry:**

November 5th, 2024	Entry #1
Description	A small U.S. health care clinic experienced a security incident that has severely disrupted their business operations. This appears to be a ransomware attack from an experienced group of unethical hackers as several employees have reported their files to be encrypted and new ransom notes appearing on their devices
Tool(s) used	• SEIM Tools • Email filters • Network protocol analyzers
The 5 W's	Capture the 5 W's of an incident. • **Who:** An organized group of unethical hackers • **What:** An ransomware incident • **When:** November 5th, 2024 at 9 am • **Where:** At a small U.S clinc • **Why:** The incident happened because bad hackers tricked the company with a phishing scam. Once they got in, they put ransomware on the company's systems, locking important files. It looks like the hackers just wanted money since they left a note asking for a big payout to unlock the files.
Additional notes	The phishing attacks were aimed at specific people, with messages made just for them. The organization might need to look at its rules about employees using social media for work stuff and update them.

Date: Record the date of the journal entry.	**Entry: #2**
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to look at a packet capture file. Wireshark is a tool that lets you see what's happening on a network using a simple screen. It's useful in cybersecurity because it helps security people check out network traffic. I used the SHA256 hash that was sent to the email to analyze if there's any malicious activity with it.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Unknown email sender • **What:** Employee opened email with attached password-protected spreadsheet file. • **When:** 1:11 p.m. • **Where:** On one employee's device. • **Why:** The organization's email filter failed to detect or block the malicious file, which could have been prevented by utilizing the file's SHA256 hash for detection.
Additional notes	The behavior the employee reported matches what's on VirusTotal. It includes things like making new processes, changing files, setting registry keys, and other harmful actions.

Date: Record the date of the journal entry.	**Entry: #3**
Description	Using a playbook to respond to a phishing incident
Tool(s) used	For this activity, I received an alert ticket about a phishing incident as a cybersecurity analyst. I had to evaluate the details of the ticket and had to give my reasoning if the phishing alert was legitimate.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Clyde West • **What:** An employee downloaded and opened a malicious file from a phishing email. • **When:** July 20, 2022 09:20:14 AM • **Where** Inergy • **Why** An employee downloaded and opened a malicious file from a phishing email.
Additional notes	N/A

Date: Record the date of the journal entry.	**Entry: #4**

Description	Reviewing a final report
Tool(s) used	For this activity, I was given a final report about a cybersecurity incident. I had to review the details and answer questions about the report.
The 5 W's	Capture the 5 W's of an incident. • **Who** malicious actor • **What** The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. • **When** December 22, 2022 at 3:13 PT and December 28, 2022 • **Where** An organization • **Why** The incident happened because of a security flaw in the e-commerce website. This flaw allowed the attacker to use a technique called "forced browsing." In simple terms, the attacker changed the order number in the web address (URL) of a purchase confirmation page. By doing this, they could view other customers' transaction details. The flaw let the attacker access many customer confirmation pages, which showed sensitive information. The attacker then gathered and stole this data. After discovering the vulnerability, the security team checked the website's access logs and saw that the attacker had looked at thousands of these purchase confirmation pages.
Additional notes	• Perform routine vulnerability scans and penetration testing. • Implement the following access control mechanisms: • Implement allowlisting to allow access to a specified set of URLs and • automatically block all requests outside of this URL range. • Ensure that only authenticated users are authorized access to content.

Date: Record the date of the journal entry.	**Entry: #5**
Description	Performing a query with Splunk
Tool(s) used	For this activity, I used Splunk to search through logs by typing in queries to find specific stuff in the data, like errors or alerts. Splunk made it easy because I could put in different search commands to narrow things down, like choosing certain time frames or types of events. When I ran a query, Splunk quickly showed the results in a neat way. It also had cool features like charts and graphs to help me understand the data better. This made finding patterns or problems a lot faster and easier to figure out.
The 5 W's	Capture the 5 W's of an incident. • **Who**: root account • **What**: There were many failed SSH login attempts on the mail server using the root account • **When**: Thu Mar 06 2023 01:39:51 • **Where**: Multiple different IPs: 194.8.74.23 port 3768, 89.106.20.218 port 1392, 193.33.170.23 port 1151 • **Why**: It appears to be an attacker trying multiple different IP addresses to login to the account.
Additional notes	The login attempts all happen around the same time, with many tries on each day the attacker was active. This might mean the attacker is using a brute-force method to guess the account's password.

Date: Record the date of the journal entry.	**Entry: #6**
Description	Performing with Chronicle
Tool(s) used	For this activity, I used Chronicle to search for specific information by typing in what I wanted to look for. I added filters to focus on things like certain times, events, or types of activities.
The 5 W's	Capture the 5 W's of an incident. • **Who:** warren-morris-pc, ashton-davidson-pc, emil-palmer-pc • **What:** An employee reported a suspicious email that seemed like a phishing attempt, with the domain signin.office365x24.com in the email body. • **When:** 2023-01-31 14:51:45 • **Where:** 40.100.174.34 • **Why:** The email filter didn't flag this domain as suspicious, probably because there isn't much proof it's bad. There are only a few VirusTotal reports about it and related domains, but it's marked as a dump site for stolen logins.
Additional notes	The domain signin.office365x24.com points to the IP 40.100.174.34, and the main domain is office365x24.com. Chronicle says these domains and IPs are "drop sites for stolen logins." The domain signin.office365x24.com shows 2 POST requests to http://signin.office365x24.com/login.php. The IP 40.100.174.34 also has a

	POST request to http://signin.accounts-google.com/login.php, which might mean stolen logins were used to access another account.

Reflections/Notes: Learning cybersecurity tools is fun because they help you understand how things work and how to keep them safe. It's like solving puzzles—these tools help you find problems, catch attacks, and look at network traffic. Each tool, like Wireshark, Splunk, Chronicle, and tcpdump, does something different, and using them shows you how to protect stuff online. Every time you find something or catch a problem, it feels like you're getting better at it.

Tcpdump was a little tricky because it uses the command line, which means you have to type in commands instead of clicking buttons. It doesn't have a pretty screen like some other tools, and it shows a lot of confusing data. You need to know what to look for and how to read it. It took practice to get the right commands and use the filters to find what I needed. There was a lot of information, but once I figured it out, tcpdump became a really useful tool to see what's going on in a network. It was hard at first, but it felt great when I got it working.