Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 29 April 2024	**Entry:** #1
Description	Documenting a cybersecurity 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 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.
Tool(s) used	Nil
The 5 W's	• **Who** caused the incident: An organized group of unethical hackers • **What** happened: A ransomware incident • **When** did the incident occur: Tuesday, 9:00 a.m. • **Where** did the incident happen: At a small U.S. health care clinic • **Why** did the incident happen: The incident happened as unethical hackers were able to gain access to the company's systems by executing a successful phishing attack. After gaining access, the attackers encrypted critical files that they came across to launch a ransomware attack on the organization. The attackers left a ransom note demanding a large sum of money in exchange for the decryption key.
Additional notes	1. Are there alternative ways to respond to this issue other than paying the ransom money to the hackers? 2. How should the company further its defense system to prevent the reoccurrence of this attack in the future? 3. How can the company raise awareness to its customers regarding this issue?

Date: 29 April 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	Wireshark used to analyze a packet capture file.

The 5 W's	• **Who** caused the incident: NIL • **What** happened: NIL • **When** did the incident occur: NIL • **Where** did the incident happen: NIL • **Why** did the incident happen: NIL
Additional notes	Wireshark is a network protocol analyzer with a graphical user interface that allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.

Date: 29 April 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	Tcpdump used to capture and analyze network traffic.
The 5 W's	• **Who** caused the incident: NIL • **What** happened: NIL • **When** did the incident occur: NIL • **Where** did the incident happen: NIL • **Why** did the incident happen: NIL
Additional notes	Tcpdump is a network protocol analyzer that's accessed using the commandline interface. Similar to Wireshark, tcpdump allows security analysts to capture, filter, and analyze network traffic.

Date: 29 April 2024	**Entry:** #4

Description	Investigate a suspicious file hash: ## Scenario You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a **hash function** is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint. Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.
Tool(s) used	VirusTotal used—an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more—to analyze a file hash that 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** caused the incident: An unknown malicious actor • **What** happened: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab5 27f6b.

	• **When** did the incident occur: An alert was sent to the organization's SOC at 1:20 p.m. after the intrusion detection system detected the file. • **Where** did the incident happen: An employee's computer at a financial services company. • **Why** did the incident happen: An employee was able to download and execute a malicious file from an email attachment.
Additional notes	1. How can this incident be prevented in the future? 2. Should we consider improving security awareness training so that employees are careful with what they click on? 3. How can we better respond to the occurrence of such events in the future?

Date: 30 April 2024	**Entry:** #5
Description	Examine alerts, logs and rules
Tool(s) used	Suricata used to examine prewritten signature and log output.
The 5 W's	• **Who** caused the incident: NIL • **What** happened: NIL • **When** did the incident occur: NIL • **Where** did the incident happen: NIL • **Why** did the incident happen: NIL
Additional notes	Suricata is an open source intrusion detection system, intrusion prevention system and network analysis tool. It determines whether each packet should generate an alert and be dropped, rejected or allowed to pass through the interface it is monitoring.

Date: 30 April 2024	**Entry:** #6

Description	Perform a query: ## Scenario You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.
Tool(s) used	Splunk
The 5 W's	• **Who** caused the incident: NIL • **What** happened: NIL • **When** did the incident occur: NIL • **Where** did the incident happen: NIL • **Why** did the incident happen: NIL
Additional notes	Splunk is an SIEM system used to examine, monitor and search for machinegenerated big data through a browser-like interface. The data is analyzed to get operational insights into threats, vulnerabilities, security technologies and identity information.

Date: 30 April 2024	**Entry:** #7
Description	Perform a query: ## Scenario
	You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: **`signin.office365x24.com`**. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain.

Tool(s) used	Chronicle
The 5 W's	• **Who** caused the incident: NIL • **What** happened: An employee received a phishing email in their inbox. Suspicious domain name contained in email body. • **When** did the incident occur: NIL • **Where** did the incident happen: NIL • **Why** did the incident happen: NIL
Additional notes	Google Chronicle is a cloud based SIEM system. It uses big data analysis to help organizations detect, investigate, and respond to cyber threats.

- Sruthi Sathishkumar