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: 03/07/2024	**Entry:** #1
Description	Documenting a cybersecurity incident The incident investigation occurred in: 1. **Detection and Analysis:** The entry outlines how the organization first detected the ransomware incident. For the analysis step the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery:** the entrey details some of the steps that the organization took to contain the incident. The organization shut down their computer systems and since they could not work to eradicate and recover from the security incident alone they contacted several other organizations for assistance.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who:** The security event was triggered by a group of unethical hackers. • **What:** The unethical hackers sent phishing emails to employees with an attachment containing ransomware which encrypted the organizations patient data.

	• **When:** The event occurred on a Tuesday at 9:00am. • **Where:** A small U.S health care clinic. • **Why:** The incident happened because a group of unethical hackers were able to gain access to the company's systems using a phishing attack. After gaining access the attackers launched their ransomware on the organizations systems, encrypting critical patient files. The attackers motivation seems to be financial due to the ransom note they left demanding 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? 2. Should the company pay the ransom to retrieve the decryption key? The company should implement continuous monitoring and threat detection mechanisms to detect and prevent future security incidents. Employees also need training or retraining on known phishing techniques.

Date: 03/07/2024	**Entry:** #2
Description	Documenting a cybersecurity incident
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who:** The security event was triggered by an unknown unethical hacker(s). • **What:** The group sent a phishing email to an employee. The email included an attachment with a malicious payload that was executed

	when the employee downloaded the file. The Malware included a keylogger. • **When:** The event occurred at 1:20pm. • **Where:** The event occurred at a financial service company's employee workstation. • **Why**: The unethical hacker's objective was to enable input capture into employee workstations so that they would be able to gain access to login credentials as well as financial record data stored in the financial service companies data servers.
Additional notes	The cybersecurity team should immediately conduct a thorough impact assessment to fully understand the extent of the unauthorized access and potential data breach. The incident management team should also be developing a communication plan to notify relevant upper management and any other authorized personnel about the security event to ensure compliance with data breach notification requirements. The team also needs to determine if the incident violates any regulatory requirements such as data protection laws or industry specific regulations in order to determine what steps need to be taken to report the incident to regulatory authorities and implement remediation measures to address any compliance deficiencies the company may have.

Date: 03/08/2024	**Entry:** #3
Description	Evaluating possible phishing email security alert.
Tool(s) used	Phishing incident response playbook

The 5 W's	Capture the 5 W's of an incident. • **Who:** The security event was initiated by an unethical hacker who impersonated Clyde West and sent a phishing email to the HR department at Inergy. The email originated from the email address <76tguyhh6tgftrt7tg.su> and the IP address 114.114.114.114. • **What:** The unethical hacker, posing as applicant Clyde West, sent a phishing email containing a malicious executable file named “bfsvc.exe” to the HR department at Inergy. • **When:** The email was received on Wednesday, July 20, 2022 09:30:14 AM. • **Where:** The email was delivered to the HR department’s email server. • **Why:** The unethical hacker's objective was to deceive the recipient into opening the malicious attachment named “bfsvc.exe” by pretending to be a job applicant named Clyde West. The attackers intention was to deliver a malware payload to compromise the recipient’s computer and potentially gain unauthorized access to Inergy’s company systems and sensitive information.
Additional notes	Should we consider improving security awareness training so that employees are careful with what they click on so they are less likely to fall for phishing attempts?

Date: 03/08/2024	**Entry:** #4
Description	Review of an incident final report.
Tool(s) used	none

The 5 W's	Capture the 5 W's of an incident. • **Who:** An unethical hacker sent an email to a company employee claiming they had successfully collected and exfiltrated customer data. • **What:** the unethical hacker exploited a vulnerability in the e-commerce web application. This method allowed access to customer transaction data by manipulating the order number within the URL string of a purchase confirmation page. • **When:** the initial email was received at approximately 3:13 pm on December 22nd, 2022. Despite being initially dismissed as spam and deleted, the same employee received a subsequent email from the same sender on December 28th, 2022. • **Where:** This incident occurred on the organization's e-commerce web application. • **Why** the unethical hacker's objective was to extort the organization by threatening to release customer data publicly unless a ransom of $50,000 was paid.
Additional notes	Communications protocols were established to notify potentially affected customers about the incident including guidance on safeguarding personal information, offering support services, and identity theft protection and credit monitoring to potential victims of the malicious actor.

Date: 03/08/2024	**Entry:** #5
Description	Performing a query with chronicle

Tool(s) used	For this activity I performed a query using chronicle. Using this tool I performed a domain investigation for the domain signin.office365x24.com.
The 5 W's	• **Who:** N/A • **What:** N/A • **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	The initial investigation was challenging due to this being my first attempt at using Chronicle. However after investigating this domain I came to the conclusion that it has been involved in phishing campaigns that might have affected multiple assets spanning back to as early as january 2023. Logs indicated that login information was submitted to the suspicious domain via POST requests. I have identified there is at least one additional domain by examining the resolved IP address.

Date: 03/07/2024	**Entry:** #6
Description	Analyzing a packet capture file
Tool(s) used	For this coursera activity, I utilized the security tool called Wireshark in order to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface (GUI). The value of Wireshark in cyber security is that it allows security analysts to capture and analyze network traffic. This can help analysts in detecting and investigating malicious activity.
The 5 W's	• **Who:** N/A • **What:** N/A

	• **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	This was my first experience with Wireshark. At first the interface was overwhelming however through trial and error I was able to successfully analyze a packet capture file, and I can understand why it is such a powerful and useful tool for understanding network traffic.

Date: 03/07/2024	**Entry:** #7
Description	Capturing my first packet
Tool(s) used	For this coursera activity, I utilized the security tool tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using a command-line interface. Similar to wireshark, the value of tcpdump in cyber security is that it allows cybersecurity analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who:** N/A • **What:** N/A • **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	I am still new to using the command-line interface using it to capture and filter network traffic was definitely a challenge. Through carefully following the

	instructions and rechecking the commands I was entering I was able to successfully get through this activity and capture network traffic.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

There were definitely challenging activities such as using tcpdump. I am a beginner at using a command-line interface and learning the syntax for tcpdump in order to be able to get the system to display the information I was looking for was a learning curve. It definitely had its frustrating moments but it was worth learning because the moment I typed in a command and the exact information I was looking for popped up it was like when you're playing a video game and having trouble beating a boss then when you succeed you are just so happy and excited.

2. **Was there a specific tool or concept that you enjoyed the most? Why?**

I really enjoyed learning and using command-line interfaces like creating SQL queries and using tcpdump. It's a side of computers I never utilized or thought about and it was really interesting and fun to learn how to make those systems work and utilize them to find and analyze data. I am definitely interested in learning more about the command-line interfaces and how they can be utilized to perform different cybersecurity tasks.