Incident handler's journal

Date: 15/09/23	**Entry:** #1
Description	Documenting an Incident involving a ransomware attack on a healthcare clinic. This incident occurred in the two phases: 1. **Detection and Analysis:** The scenario 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 scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance.
Tool(s) used	None
The 5 W's	• **Who:** The incident was caused by a group of unethical hackers who target healthcare and transport organizations. • **What:** The clinics systems were infected with ransomware, resulting in the systems data and files being encrypted and held ransom • **Where:** The incident happened at the healthcare clinic • **When:** The incident occurred at approximately 9:00 am on a Tuesday • **Why**: The ransomware was able to be deployed due to a phishing attack that targeted employees of the clinic, which resulted in a malicious file being downloaded and a ransomware attack being successfully launched, this resulted in critical files being encrypted. The motive for

	the attack seems to be financial gain as the attackers requested a large sum of money.
Additional notes	1. Staff should receive training to better prepare themselves to detect fraudulent and malicious emails. 2. What was the subject of the email posing as to cause the employee to download the malicious file? 3. Should they pay the ransom fee to receive the decryption key and retrieve their critical files back?

Date: 19/09/2023	**Entry:** #2
Description	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. For this activity, I used VirusTotal to analyze a file hash, which 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
Tool(s) used	VirusTotal

The 5 W's	• **Who:** Incident was caused by an unknown malicious actor • **What:** Employee received an email which contained a malicious file with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where:** Incident happened at the office of a financial services company • **When:** Incident occurred at 1:13pm, an alert was sent after the IDS detected the file. • **Why:** Threat actor launched a phishing attack to cause an employee to execute a malicious file which would collect information and execute commands on the targets machine
Additional notes	VirusTotal results showed that more than 50 different security vendors flagged the files hash value as malicious. Results from the investigation concluded that the malicious file was malware, the type of malware was a flagpro trojan. To prevent issues like this in the future, employees should receive training to improve awareness.

Date: 21/09/23	**Entry:** #3
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface (GUI). Wireshark is a widely used tool in the cybersecurity industry and the value of Wireshark 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**: N/A • **What**: N/A • **Where**: N/A

	• **When**: N/A • **Why**: N/A
Additional notes	I was excited to begin this exercise to gain a better understanding of Wireshark and to analyze a packet capture file. The interface can be a lot to take in but after some further use the benefits of using it are easily seen. I can see why it's such a powerful tool for understanding network traffic.

Date: 23/09/2023	**Entry:** #4
Description	Capturing a data packet, filtering for specific types of traffic and saving captured packets to a file using tcpdump and Linux.
Tool(s) used	Linux CLI & tcpdump were used to capture and analyze network traffic
The 5 W's	• **Who**: I am performing the data packet analysis • **What**: I am using linux and tcpdump to capture data packets for inspection • **When:** My personal computer using linux CLI • **Where:** I performed this packet capturing on 27/09/2023 • **Why:** Performed this exercise to further my understanding on packet capturing, using tcpdump and the Linux CLI
Additional notes	Using the CLI to capture and filter network traffic was a fun challenge I thoroughly enjoyed, to achieve this I performed the following steps: I started by using the sudo `ifconfig` command to identify available instances, I then filtered live network packet data from the `eth0` interface with the command `sudo tcpdump -i eth0 -v -c5.` To break this down: `-i eth0`

	captures the data specifically from the `eth0` interface, `-v` displays detailed packet data and `-c5` instructs the command to capture 5 packets of data. Next I captured the packet data into a file called capture.pcap by executing the command: `sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &`. This command uses `-nn` to not attempt to resolve IP address or ports to names, which is best practice as the lookup data may not be valid and also prevents malicious actors from being alerted to an investigation; it then filters for only port 80 traffic which is the default HTTP port and saves the captured data to the file capture.pcap, this runs in the background. After capturing some packet data I filtered the data using the command: `sudo tcpdump -nn -r capture.pcap -X`.

Date: 25/09/2023	**Entry:** #5
Description	Using a playbook to respond to a phishing incident. This occurred in the **detection and analysis phase** of the NIST incident response lifecycle due to the need to analyze the incident using a companies response playbook to conclude if the incident ticket needs to be escalated further or can be marked as completed.
Tool(s) used	VirusTotal, Phishing incident playbook

The 5 W's	• **Who:** Incident was caused by an employee • **What:** Employee opened a malicious file attachment from a phishing email received from an unknown source • **When:** Incident occurred on Wednesday, July 20 at approximately 9:30am • **Where:** Incident happened in the company office • **Why:** The incident happened due to the employees inability to identify potential phishing emails, also due to opening a file from a unknown and untrusted source
Additional notes	Hash value for the file received in the email cross referenced on VirusTotal shows that over 50 vendors have flagged this hash value as malicious. Multiple grammatical errors and inconsistencies in the email can be seen in the subject line, email body as well as the senders 'name' not matching the email address. Ticket was escalated to a level 2 SOC analyst. Training should be provided to employees to better prepare them to spot and handle potential phishing scams.

Date: 26/09/2023	**Entry:** #6
Description	Reviewing a final report for a major security incident that occurred at a retail company. This is part of the **post-incident activity phase** of the NIST incident response lifecycle as Containment, Eradication & Recovery has been completed, therefore this activity is to better understand the incident's life cycle, identify any improvements that can be made and conclude the thorough

	investigation.
Tool(s) used	N/A
The 5 W's	• **Who:** Incident was caused by an external threat actor • **What:** Threat actor gained unauthorized access to customer personal identifiable information (PII) and financial information • **Where:** The incident occurred on December 28th, 2022 at 7:20pm • **When:** Incident occurred on the companies e-commerce web application • **Why:** The threat actor was able to conduct the attack due to a vulnerability in the e-commerce web application, using a forced browsing attack
Additional notes	Approximately 50,000 customer records were affected by the breach. Financial impact of the incident is estimated to be around $100,000 in direct costs and loss of revenue. The attacker accessed private data by modifying the order number included in the URL string of the purchase confirmation page, allowing the attacker to access thousands of customer purchase confirmation pages which exposed customer sensitive personal information. New measures should be put in place to prevent future recurrences: 1. Perform routine vulnerability scans and conduct penetration testing. 2. 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: 27/09/2023	**Entry:** #7
Description	Performing a query with Google Chronicle to investigate phishing attempts and identify which machines were affected and what data may have been leaked.
Tool(s) used	Google Chronicle
The 5 W's	• **Who:** Incident was caused by an external threat launching a phishing attack with a link to website signin.office365x24.com, additional domain name signin.accounts-gooqle.com found that resolved to the same IP address: 40.100.174.34. • **What:** 7 employees visited the suspicious site and made HTTP requests with their machines. • **Where:** Logs show the first connection was made on 31-01-2023, with the first connection to the site being made at 14:40:40 pm, with the last connection being made on 09-07-2023 at 05:06:49 am. • **When:** Phishing email was sent to employees' work emails. • **Why:** Phishing attack was launched to bait employees to enter login credentials on a malicious website.
Additional notes	Logs show multiple employees' computers making HTTP GET & POST requests with the site, further investigation showed 1 vendor had flagged this site as malicious. 7 machines listed as having made connections with the site: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc & warren-morris-pc. 2 POST requests were made from different machines, submitting login credentials to the website. 09-07-2023: - ashton-davidson-pc at 05:02:44, - emil-palmer-pc at 05:04:44

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

   I feel each activity and tool learnt had their own challenges, such as being able to communicate clearly using incident response forms to both technical and non technical people while ensuring summaries were kept clear and concise. Learning and understanding the different syntax and commands for tools such as the Linux CLI, tcpdump, Splunk and Chronicle was also a fun challenge.

2. **Has your understanding of incident detection and response changed after taking this course?**

   I feel my understanding of incident detection and response has greatly evolved after working through the different challenges and activities. I believe my mindset and how I think and approach such challenges has changed for the better and I understand the importance of plans, processes and the people in the industry and also the importance of gaining the skills to effectively use the tools widely used in the cybersecurity industry.

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

   I really enjoyed learning and improving on using the Linux CLI to manage permissions and inspect data packets using tcpdump, the skill of inspecting network traffic and analyzing data packets in real time is something that I think is important and can only be a great asset to continue to try to master these skills and tools.