Incident handler's journal

Date: 03/04/2024	**Entry:** **Journal entry #1**
Description	Report of a security incident during the detection and analysis phase of the incident response lifecycle.
Tool(s) used	Phishing email campaign, malicious attachments and ransomware by way of encryption.
The 5 W's	Capture the 5 W's of an incident. • **An organized group of unethical hackers carried out the incident.** • **Access to company files and resources resulted in business disruptions after a successful phishing attack was carried out. The company was forced to shut down their computer systems until the situation was resolved.** • **The security incident occurred on Tuesday morning, at approximately 9:00 a.m.** • **A small U.S. health care clinic.** • **On Tuesday morning, at 9:00 a.m. A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident. It was the result of a malicious attachment in a phishing email campaign, which targeted several employees'. Once the attackers gained access, they deployed ransomware to encrypt critical files and demanded payment for the decryption key. The most likely cause is inadequate employee training on recognizing the signs of a social engineering or phishing attack.**
Additional notes	I think that the best approach for correcting this problem going forward, would be to implement social engineering training to familiarize all employees' on how

	to recognize these types of attacks. I would also like to gain a better understanding of ransomware and how it encrypts the target's files.

Date: 03/16/2024	**Entry:** **Journal entry #2**
Description	Report of a security incident during the detection and analysis phase of the incident response lifecycle.
Tool(s) used	SHA256 file hashing, VirusTotal and Alert Ticket
The 5 W's	Capture the 5 W's of an incident. ● **Attacker is unknown.** ● **An employee downloaded a file attachment in an email with a malicious payload.** ● **The security incident occurred between 1:11 p.m. and 1:20 p.m.** ● **A financial services company.** ● **An employee received an email with a file attachment that they downloaded onto their workstation. The file attachment contained a malicious payload that created multiple unauthorized executable files on the employees workstation. An intrusion detection system (IDS) detected the unauthorized executable files and alerted the SOC analyst who used SHA256 hashing to create a hash value for the malicious file to further investigate the incident using VirusTotal.**
Additional notes	Using VirusTotal I found that more than 50 security vendors flagged the file as malicious, suspicious or unsafe. As well as receiving a community score of -89. After further investigation, the file hash has been identified as the malware Flagpro.

Date: 03/19/2024	**Entry:** **Journal entry #3**
Description	Responding to a phishing alert during the detection and analysis phase of the incident response lifecycle.
Tool(s) used	**Phishing Playbook** Version 1.0 and Alert Ticket.
The 5 W's	Capture the 5 W's of an incident. ● **Clyde West/Def Communications.** ● **An email phishing attack.** ● **The security incident occurred between 1:11 p.m. and 1:20 p.m.** ● **A financial services company.** ● **Our HR department received an email inquiring about an open job position. The email contained an attachment that claimed to be a password protected resume file. Upon further investigation, the file was identified as the malicious malware Flagpro. I escalated the alert ticket to the level-two SOC analyst.**
Additional notes	I received an alert of a phishing attempt with a possible malicious file attachment, I proceeded to evaluate the alert and found multiple indications of it being a legitimate alert. There were inconsistencies between the sender's email address and the name signed at the end of the email, as well as the subject of the email containing multiple spelling and grammatical errors. The email contained an attachment that I investigated with VirusTotal using a file hash value and determined it as malicious. I'm escalating the ticket to the level-two SOC analyst.

Date: 03/20/2024	**Entry:** Journal entry #4
Description	Review of a final report during the post-incident activity phase of the incident response lifecycle.
Tool(s) used	Final report.
The 5 W's	Capture the 5 W's of an incident. ● **Malicious actors unknown.** ● **A forced browsing attack/data ex-filtration.** ● **December 28, 2022, at 7:20 p.m., PT. Incident response efforts lasted till December 31, 2022.** ● **A mid-sized retail company.** ● **The root cause of the incident was a vulnerability in the e-commerce web application. This allowed the attacker to perform a forced browsing attack allowing customer transaction data to be accessed and modified by altering the URL string of a purchase confirmation page, exposing customer data, which the attacker then collected and exfiltrated. This resulted in over 50,000 customers personal identifiable information (PII) and financial information being compromised.**
Additional notes	I think that they should also instruct employees' to treat any email similar to this as a serious issue that needs to be investigated by the security team until proven otherwise.

Date: 04/02/24	**Entry:** **Journal entry #5**

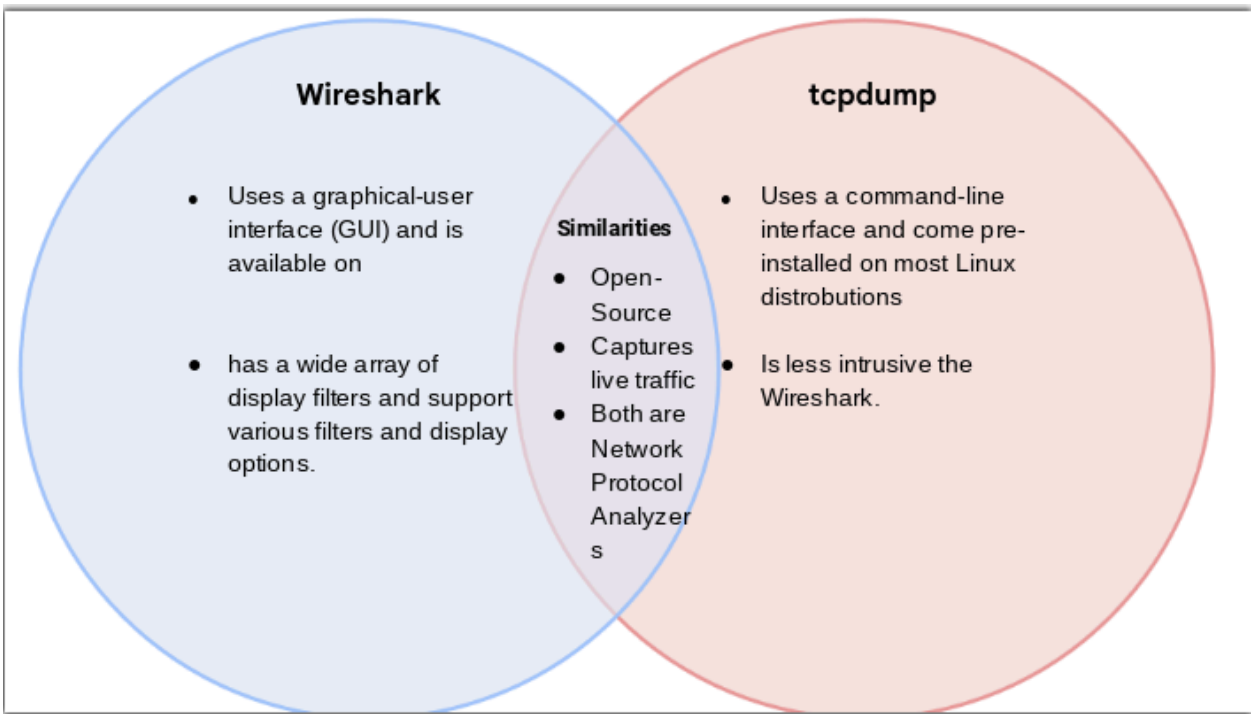
Description	Responding to a phishing alert during the detection and analysis phase of the incident response lifecycle.
Tool(s) used	**Google Chronicle**
The 5 W's	Capture the 5 W's of an incident. ● **A series of phishing emails that linked users to a malicious site signin.office365x24.com** ● **An employee received a phishing email in their inbox that triggered an alert.** ● **The first event occurred between 14:40:40 and 14:51:45 on 2023/01/31 while the second event occurred between 05:02:42 on 2023/07/08 and 05:06:49 on 2023/07/09.** ● **A financial services company.** ● **After receiving the alert, I searched the domain name that was linked in the phishing email through Chronicle and found that Ashton Davidson, Bruce Monroe, Coral Alvarze, Emil Palmer, Jude Reyes, and Robert Spence all visited the website on 2023/01/31 and then again on 2023/07/08 and 2023/07/09. While all the users mentioned have HTTP "GET" traffic on the above dates, both Ashton Davidson and Emil Palmer have both HTTP "GET" and "POST" traffic indicating possibly successful phishing email attacks. I then searched the IP address that was linked to the domain and found another event involving Warren Morris between 14:50:14 and 14:51:45 on 2023/01/31 with both HTTP "GET" and "POST" indicating another possibly successful phishing email attack.**
Additional notes	All of the HTTP "POST" traffic should be further investigated to ensure our system has remained uncompromised. Additional domains (signin.office365x24.com, signin.accounts-google.com) associated with the IP address were found during my investigation.

	Additionally, there were inconsistencies with the information I found on Chronicle and the information that the activity instructions told me would be found after taking the appropriate steps.

Reflections/Notes: Were there any specific activities that were challenging for you? Why or why not?
I found packet capture and sniffing to be challenging because of all the different locations you have to navigate through to find the data you need. But after taking my time with both the activity and the exemplar, I feel I developed a general understanding of the concept.

Was there a specific tool or concept that you enjoyed the most? Why?
I particularly enjoyed using the SEIM tool Splunk. It displays all the information in an easy to use interface and has a very readable format for the data that I was investigating.

Has your understanding of incident detection and response changed since taking this course?
I would say that my understanding of incident detection and response has improved greatly throughout this course. I feel I have a solid foundation with the command-line, as well as using SQL, tcpdump and Suricata within the command-line. I liked using the SIEM tools that we explored and would love the opportunity to expand on my abilities with them. I also enjoyed learning about the containment and eradication phase of the lifecycle and look forward to continuing my education of it.


Wireshark
Uses a graphical-user interface (GUI) and is available on
has a wide array of display filters and support various filters and display options.
Similarities
Open-Source
Captures live traffic
Both are Network Protocol Analyzers
tcpdump
Uses a command-line interface and come pre-installed on most Linux distrobutions
Is less intrusive the Wireshark.