Incident handler's journal Portfolio Project

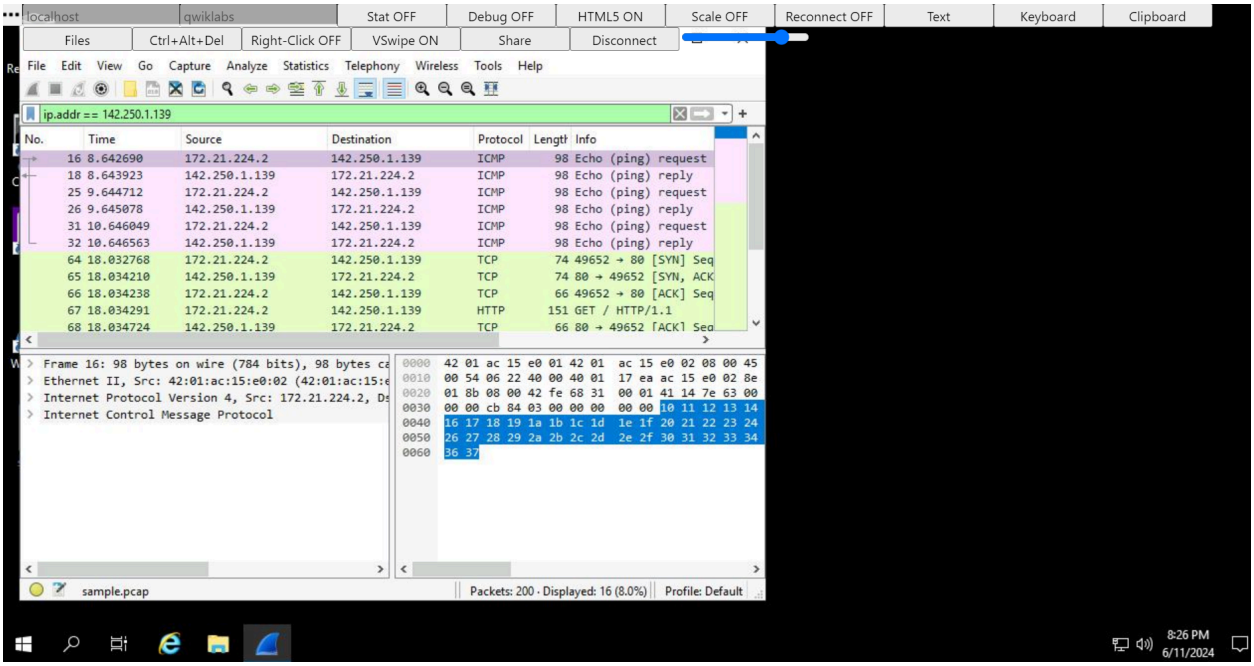
Within this journal is the use of Wireshark (Entry 3) and tcpdump (Entry 4)

Date: 6/6/2024 Record the date of the journal entry.	**Entry: 1**
Description	Cybersecurity incident involving a ransomware attack launched by using a Phishing email.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who**? Unethical Hackers • **What**? Hackers sent a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. • **When** ? Tuesday 6/4/24 at 9:00 am • **Where** ? Incident occurred at a U.S. health care clinic • **Why** ? The attack happened because unethical hackers gained access to the company's computer system. Hackers appear to have a financial motive due to a ransom note left demanding large amounts of money in exchange for the encryption key.
Additional notes	• How could the health care company prevent an incident like this from occurring again? • Should the company pay the ransom to retrieve the decryption key?

Date: Record the date of the journal entry.	**Entry: 2**
Description	Cybersecurity event involving a malicious email sent in a possible Phishing attempt.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who**? A possible threat actor under the name “Clyde West” • **What**? Email was sent to HR department containing a malicious file hash • **When**? This occurred July 20,2022 at 9:30 am • **Where**? This incident occurred within the HR department mail server • **Why** did the incident happen?
Additional notes	I do find the attachment malicious due to threat intelligence gathered from open sources. Within the email the sender name and address did not match, the body of the email also contained grammatical errors indicating a possible phishing attempt. have escalated the ticket.

Date: Record the date	**Entry: 3**

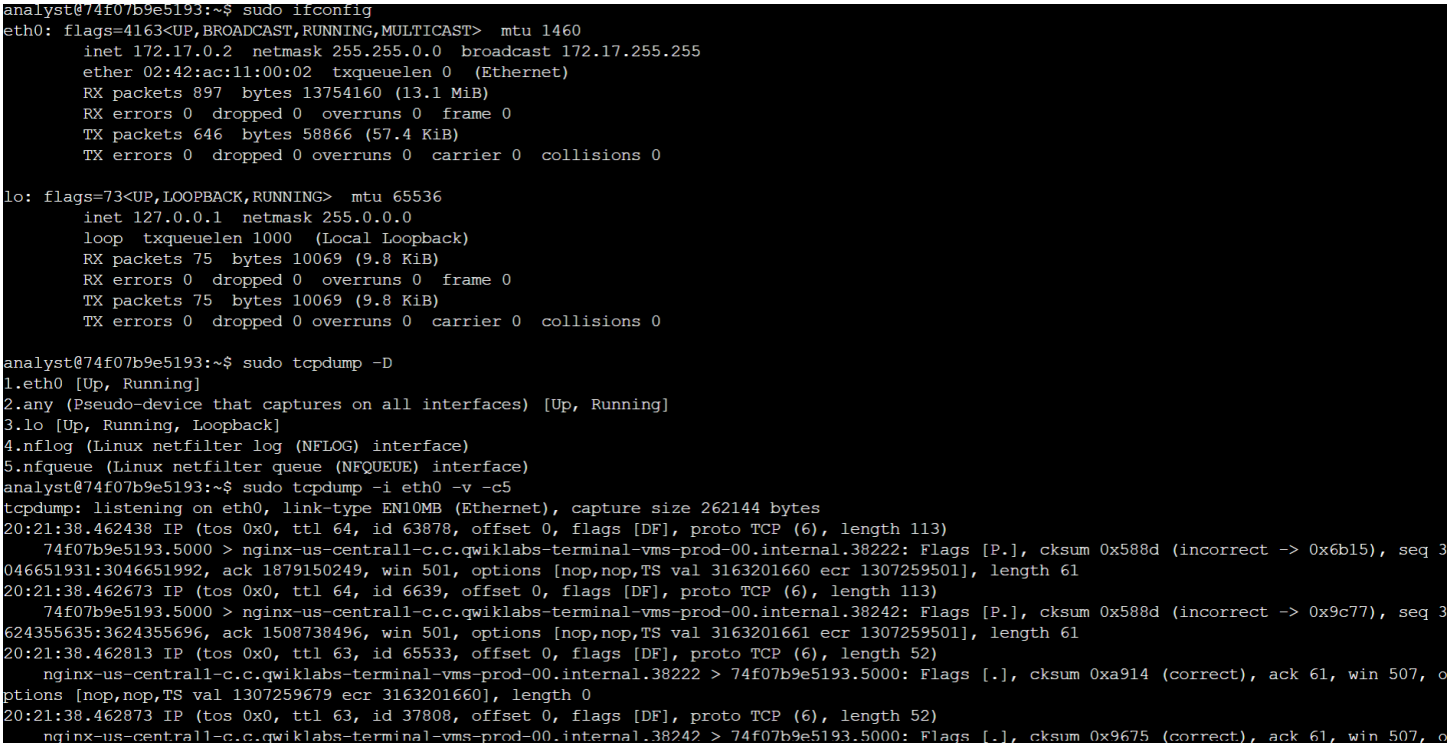
of the journal entry.	
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts 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've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.



Caption: Use of Wireshark to analyze packets

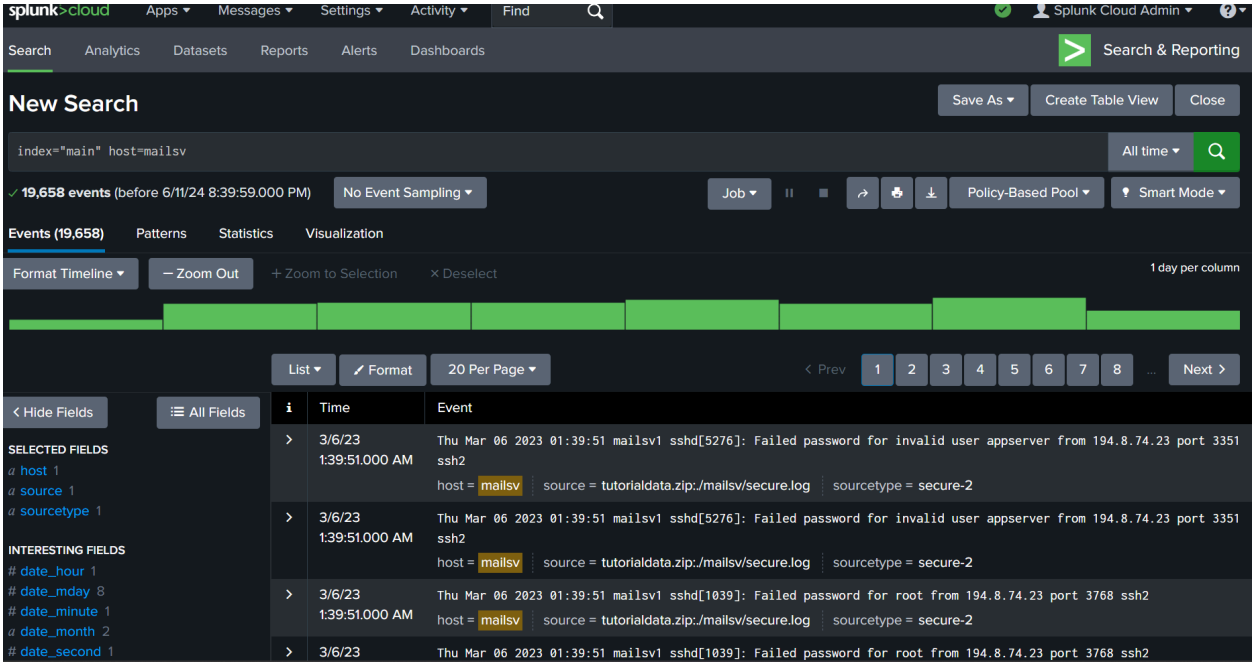
Date: Record the date of the journal entry.	**Entry: 4**
Description	Capturing Network packets
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.

The 5 W's	● Who: N/A ● What: N/A ● Where: N/A ● When: N/A ● Why: N/A
	I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic.



Caption: Use of tcpdump on Linux

Date: Record the date of the journal entry.	**Entry: 5**
Description	Using SIEM tools to search for data
Tool(s) used	Splunk and chronicle
The 5 W's	● Who: N/A ● What: N/A ● Where: N/A ● When: N/A ● Why: N/A
Notes	In this activity I used Splunk and Chronicle to carry out tasks given to me in the Google Cyber Security Course. Below is a screenshot I took using splunk to find events that occurred within a mail server.



Reflections/Notes: Record additional notes.

1. **Were there any specific activities that were challenging for you? Why or why not?**
I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process Slowly.

2. **Has your understanding of incident detection and response changed after taking this course?**
After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**
I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it really fascinating to be able to use tools to capture network traffic and analyze it in real time. I am definitely more interested in learning more about this topic, and I hope to one day become more proficient in using network protocol analyzer tools.