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: April 16, 2025	**Entry:** #1
Description	Exploring my home network with Wireshark For this exercise, I decided to analyze live traffic from my home Wi-Fi using Wireshark. I captured packets while browsing various websites and streaming a video. I was able to observe DNS requests, TCP handshakes, and various HTTP and HTTPS connections.
Tool(s) used	Wireshark
The 5 W's	● Who: Myself, conducting a personal network exploration ● What: Normal user-generated network traffic (DNS, HTTP/S, TCP) ● Where: My home network ● When: Wednesday Night ● Why: To gain a hands-on understanding of how everyday network traffic looks and how to identify different protocols
Additional notes	I found it interesting to filter the packets by protocol and follow TCP streams to see the back-and-forth communication between my machine and web servers.

Date: April 18, 2025	**Entry:** #2
Description	Spotted unexpected port forwarding on my home Wi-Fi While using tcpdump on my home Wi-Fi, I noticed unusual traffic pattern specifically, high volumes of outbound connections on a non-standard port (UDP/TCP 25565). After investigating further on my gateway’s settings, I realized a household member had set up port forwarding on the router to stream a game server, Minecraft specifically, from their PC to a handheld gaming device over the internet.
Tool(s) used	tcpdump
The 5 W's	● Who: A household member using a game streaming setup ● What: Port forwarding configured for outbound game streaming ● Where: My home network ● When: Friday afternoon ● Why: To enable remote access for game streaming purposes
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.

Date: April 20, 2025	**Entry:** #3
Description	Investigated the "Honey" coupon browser extension I decided to take a closer look at the popular "Honey" coupon extension, which I had installed out of curiosity. I noticed that it frequently displayed available coupons on websites that weren’t actually selling anything, including some personal blog pages and informational sites. This raised a red flag for me.

Tool(s) used	VirusTotal
The 5 W's	● Who: A commercial browser extension used by millions (Honey) ● What: Displaying misleading coupon offers on non-commerce sites ● Where: Firefox on my personal laptop ● When: Saturday evening ● Why: Likely part of aggressive user tracking or affiliate marketing strategy
Additional notes	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.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**
   Using tcpdump was probably the most challenging activity for me. Unlike graphical tools like Wireshark, tcpdump requires you to be familiar with command-line syntax and filters, which I'm still learning. At first, I kept using incorrect command options and couldn't interpret the output correctly. After re-reading the documentation and testing simple filters, I gained a better understanding. It was a great reminder that hands-on practice is essential when learning command-line tools.

2. **Has your understanding of incident detection and response changed after these activities?**
   Yes, definitely. Initially, I thought incident detection and response was mostly reactive — something you only do after a major breach. But through these activities, I've come to understand it's a continuous process that involves not only reacting but also proactively monitoring, analyzing, and documenting unusual behaviors. Even something like unexpected port forwarding or sketchy browser extensions can be part of a broader security conversation.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**
   I really enjoyed using Wireshark. Even though it was overwhelming at first, it was

fascinating to see how much information is transmitted across the network — from DNS queries to secure HTTPS traffic. It made the abstract concept of “network traffic” feel very real and tangible. Being able to follow individual TCP streams and analyze conversations between hosts was especially cool and gave me a deeper appreciation for how the internet works at a lower level.