**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:**  Sept. 18, 2025 | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | A small U.S. health care clinic has been a victim of ransomware. At approximately 9AM, employees noticed they were unable to access files like medical records and the business operations were forced to shut down. A ransom note was found on their computers from a group of unethical hackers who demand a large sum of money in exchange for the decryption key for their data. They were able to gain access to the company’s network via phishing emails sent to employees which installed malware.  The NIST Incident Response Lifecycle phase this was apart of is: Detection and Analysis. | | |
| Tool(s) used | * Encryption * Ransomware | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   + An organized group of unethical hackers * **What** happened?   + Malware was installed by one of the employees through a malicious attachment via phishing emails.   + The malware encrypted all data and the attackers demand payment for the decryption key * **When** did the incident occur?   + 9AM on Tuesday * **Where** did the incident happen?   + Over email via phishing * **Why** did the incident happen?   + This group of hackers targets organizations in healthcare and transportation industries. We can assume the main motive is financial gain. | | |
| Additional notes | It seems not enough employee awareness is made around phishing, as this situation could have been avoided. | | |

| **Date:**  Sept. 22, 2025 | **Entry:**  #2 | | |
| --- | --- | --- | --- |
| Description | Activity: Analyze your first packet with Wireshark  In this lab we used Wireshark, a network protocol analyzer to analyze sample network packets. The incident was not malicious and only a result of regular internet browsing.  The NIST Incident Response Lifecycle phase this was a part of is: Detection and Analysis. | | |
| Tool(s) used | Wireshark, a network protocol analyzer | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   + A user on a system connecting to websites such as opensource.google.com * **What** happened?   + The user accessed websites which sent ICMP ping requests, TCP, connects, and DNS queries * **When** did the incident occur?   + There are different timestamps for each packet, but one of them was 2022/12/21 at 17:46:35.232748 * **Where** did the incident happen?   + On the user’s local system * **Why** did the incident happen?   + This incident was a result of normal browsing of the internet | | |
| Additional notes | The first request was an ICMP ping. The TCP packet port used was port 80. This was all normal browsing. | | |

| **Date:**  September 22, 2025 | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Activity: Investigate a suspicious file hash  Our employee was a victim of phishing via a suspicious attachment in a phishing email. We used SHA256 and VirusTotal to confirm our findings.  The NIST Incident Response Lifecycle phase this was a part of is: Detection and Analysis. | | |
| Tool(s) used | VirusTotal, an IDS tool, SHA-256 hash | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   + A threat actor used phishing on an employee at the company * **What** happened?   + Through a phishing email, the employee clicked an suspicious attachment which then downloaded a malicious malware file * **When** did the incident occur?   + The incident occurred between 1:11pm and 1:20pm, from the time the employee receives the email til when our IDS detected the .exe file * **Where** did the incident happen?   + The incident occurred on the employee’s computer (endpoint) * **Why** did the incident happen?   + The employee was not careful and aware of the attachment being malicious. Clicking on it immediately caused a download of the malware file. | | |
| Additional notes | After detecting the malware file, we used the SHA256 hash and searched the file hash on VirusTotal to confirm this was indeed a malware file. | | |

| **Date:**  September 22, 2025 | **Entry:**  #4 | | |
| --- | --- | --- | --- |
| Description | Activity: Explore signatures with Suricata  We used Suricata to examine sample packet captures. The results were not suspicious and were only a result of regular browsing.  The NIST Incident Response Lifecycle phase this was a part of is: Detection and Analysis. | | |
| Tool(s) used | Suricata, a IDS/IPS tool | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   + A user on our home network ($HOME\_NET) * **What** happened?   + We used Suricata to monitor network traffic with alerts for any http request going out. * **When** did the incident occur?   + When we used Suricata to scan sample.pcap with custom.rules * **Where** did the incident happen?   + On the home user’s computer, on our home network * **Why** did the incident happen?   + This was a regular http get request, i.e. regular internet browsing | | |
| Additional notes | The custom rule alert http $HOME\_NET any -> $EXTERNAL\_NET any (msg:"GET on wire"; flow:established,to\_server; content:"GET"; http\_method; sid:12345; rev:3;) was used. | | |

| Reflections/Notes:  Were there any specific activities that were challenging for you? Why or why not?   * The challenging activity was entry #2 which used Wireshark and entry #4 which used Suricata. These were unfamiliar tools and I was unsure how to interpret the results at first, i.e. if they were malicious or not.   Has your understanding of incident detection and response changed since taking this course?   * Yes, my understanding of incident detection and response has changed. By examining different logs, I see that we will have to use all our knowledge and be quick on our feet in a real life scenario to determine the results of our readings and the next best action.   Was there a specific tool or concept that you enjoyed the most? Why?   * I enjoyed using Wireshark as the GUI made our findings easier to parse and interpret. |
| --- |