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: January 17, 2026	**Entry:** #1
Description	Documenting a ransomware security incident at a primary-care health clinic.
Tool(s) used	**None.**
The 5 W's	• **Who:** An organized group of unethical hackers known for targeting the healthcare and transportation industries. • **What:** A ransomware attack that encrypted critical files and medical records, resulting in the total shutdown of business operations. • **When:** Tuesday morning at approximately 9:00 a.m. • **Where:** A small health care clinic specializing in primary-care services in the United States. • **Why:** The incident occurred because hackers used targeted phishing emails to trick employees into downloading a malicious attachment, which then deployed ransomware to encrypt files for financial gain.

Additional notes	1. What protocols are in place for data backups, and can the systems be restored without paying the ransom? 2. How can the clinic improve its email filtering and employee security awareness training to prevent future phishing attempts?

Date: January 18, 2025	**Entry:** #2
Description	Analyzing a packet capture file.
Tool(s) used	**Wireshark:** A network protocol analyzer (GUI) utilized for deep packet inspection (DPI). It allows for the capture and examination of data traffic to identify protocol anomalies, unencrypted sensitive information, and potential security breaches.
The 5 W's	• **Who:** N/A. • **What:** N/A. • **When:** N/A. • **Where:** N/A. • **Why:** N/A.
Additional notes	Mastering display filters is critical when analyzing packet captures because it allows an analyst to isolate specific suspicious protocols, such as DNS or HTTP, from thousands of unrelated packets.

Date: January 18, 2025.	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	**tcpdump:** A lightweight, command-line interface (CLI) network protocol analyzer used for real-time packet interception. Similar to Wireshark, it allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who:** N/A. • **What:** N/A. • **When:** N/A. • **Where:** N/A. • **Why:** N/A.
Additional notes	**CLI vs. GUI Utility:** Identified that **`tcpdump`** is often faster for initial data collection than GUI tools like Wireshark.

Date: January 18, 2025.	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	**VirusTotal:** A cloud-based threat intelligence platform used to aggregate data from multiple antivirus engines and URL scanners. Leveraged the tool to perform a static analysis of a file hash, cross-referencing it against global databases to identify Indicators of Compromise (IoCs) and confirm malicious intent.

The 5 W's	• **Who:** An unidentified external threat actor. • **What:** Phishing attack involving the delivery and execution of a malicious file attachment with the **SHA-256 Hash** `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`. • **When:** Alert generated at 1:20 p.m. following an Intrusion Detection System (IDS) trigger. • **Where:** An endpoint (employee workstation) within a financial services organization. • **Why:** The incident was made possible by the manual download and execution of an unsolicited email attachment by a user.
Additional notes	How quickly can the affected endpoint be isolated to prevent lateral movement within the financial network?

Date: January 19, 2025	**Entry:** #5
Description	Investigation of a phishing alert.
Tool(s) used	**Phishing Incident Response Playbook:** A standardized framework used to evaluate, investigate, and triage phishing alerts in a systematic order. **VirusTotal:** Utilized to perform a reputation check on the SHA-256 file hash to confirm the malicious nature of the attachment.

The 5 W's	• **Who:** An unidentified threat actor using the alias "Clyde West" and the sender name "Def Communications." • **What:** A phishing attempt delivering a password-protected malicious file named `bfsvc.exe` disguised as a resume. • **When:** Wednesday, July 20, 2022, at 09:30:14 AM. • **Where:** Targeted at the HR department (`hr@inergy.com`) of the organization. • **Why:** To deceive employees into bypassing security filters by providing a password for a malicious attachment to initiate a malware infection.
Additional notes	The email contained multiple red flags, including grammatical errors and a mismatch between the sender's display name and the sender's email address (`76tguy6hh6tgftrt7tg.su`).

Date: January 19, 2025	**Entry:** #6
Description	Analysis of the final report for the December 2022 data breach
Tool(s) used	**Web Application Access Log Analysis:** Utilized to identify the attacker's pattern of accessing thousands of purchase confirmation pages sequentially. **Web Server Logs:** Analyzed to pinpoint the single source of high-volume, sequential order requests.

The 5 W's	• **Who:** An unidentified external attacker who attempted to extort the company for cryptocurrency. • **What:** A data breach affecting approximately 50,000 customer records, including Personally Identifiable Information (PII) and financial data. • **When:** The breach was discovered on December 28, 2022, following an initial ransom email received on December 22, 2022. • **Where:** The vulnerability existed within the e-commerce web application's purchase confirmation pages. • **Why:** The attacker exploited a forced browsing vulnerability by modifying order numbers in the URL string to access and exfiltrate customer transaction data.
Additional notes	A critical delay occurred because an employee initially dismissed the ransom email as spam on December 22, delaying the security team's response by six days.

Date: January 19, 2025	**Entry:** #7
Description	Configuring Suricata to monitor network traffic and analyze generated alert logs.
Tool(s) used	**Suricata:** A high-performance Network IDS/IPS used for monitoring traffic and triggering security alerts. **jq:** A command-line JSON processor used to format and filter

	complex telemetry data from the `eve.json` log file.
The 5 W's	• **Who:** Security Analyst. • **What:** Simulation of network monitoring by running custom rules against a packet capture (`sample.pcap`). • **When:** Activity conducted on January 19, 2026, using logs timestamped from November 2022. • **Where:** Localized environment using the 172.21.224.0/20 subnet as the `$HOME_NET`. • **Why:** To develop practical skills in signature-based detection, log analysis, and network telemetry correlation.
Additional notes	Explored the three core components of a Suricata signature: **Action** (alert), **Header** (protocol and IP/port data), and **Rule Options** (metadata like `msg`, `sid`, and `rev`).

Reflections/Notes:

Were there any specific activities that were challenging for you? Why or why not? The most challenging activities involved mastering the syntax for Suricata custom rules and complex **`jq`** filters to parse telemetry data.

Has your understanding of incident detection and response changed since taking this course? My understanding has evolved from viewing security as a series of isolated events to recognizing it as a structured lifecycle of detection, analysis, and remediation. I now see how standardized playbooks and rigorous documentation in a journal are vital for maintaining consistency during a high-pressure security breach.

Was there a specific tool or concept that you enjoyed the most? Why? I particularly enjoyed working with **Wireshark** and **`tcpdump`** because they provided a look at how data travels across a network