Incident handler's journal

Note:

All incidents in this journal are from the Google Cybersecurity course, and are not reflective of real-life incidents. The goal of this journal is to learn the process of incident management, as well as become accustomed to the process of recording logs for incidents.

Date: Entry: Oct 17, 3PM (Practice Event: Tuesday, 9:00AM)	**Entry:** Entry #1: Health Care Ransomware
Description	Documentation of a ransomware attack on a U.S health care clinic
Tool(s) used	None.
The 5 W's	- **Who:** An organized group of hackers led a phishing attack on employees at the health care clinic. - **What:** Once they got the employee to download the malware, they deployed their ransomware, which encrypted critical files. - **Where:** This incident occurred on Tuesday at 9:00AM. - **When:** The incident occurred at a small U.S health care clinic which specializes in delivering primary-care services. - **Why:** This incident occurred as leverage to use against the health care clinic for money. The group's goal was to receive a large sum of money in exchange for the decryption key.
Additional notes	1. How complex is the encryption? Should the company pay the ransom

	to retrieve the decryption key? 2. How can the health care company mitigate incidents like this in the future?

Date: Entry: Oct 18, 4:30PM	**Entry:** Entry #2: Packet Analysis with Wireshark
Description	Documentation of the process and findings from a lab where I analyzed network packets using Wireshark, a network protocol analyzer.
Tool(s) used	Wireshark
The 5 W's	• **Who:** I conducted the analysis as part of my cybersecurity class assignment. • **What:** The task involved capturing and analyzing network traffic to identify patterns and potential security issues. • **When:** The lab was completed on October 28th at 4:30PM. • **Where:** The analysis was performed on a local network environment set up for educational purposes. • **Why:** The goal was to understand how to use Wireshark for packet analysis and to identify potential security threats within network traffic.
Additional notes	- During the analysis, I identified several common protocols, such as HTTP, TCP, and DNS within the captured packets. - Detected unusual traffic patterns that could indicate potential security

	threats - Was initially overwhelmed by the sheer amount of data, but learned to apply filters effectively to isolate relevant traffic

---

Date: Oct 20th, 3:30PM	**Entry:** Entry #3: Malware Analysis with VirusTotal
Description	Documentation of the analysis of a potentially malicious file using VirusTotal. The activity involved examining the file's hash and identifying various indicators of compromise (IoCs) associated with the file.
Tool(s) used	VirusTotal
The 5 W's	• **Who:** The analysis was conducted as part of a cybersecurity class project. • **What:** The task involved using VirusTotal to determine the malicious nature of a file and identify associated IoCs. • **When:** The lab was completed on October 20th at 3:30PM. • **Where:** The analysis was performed in a controlled educational environment. • **Why:** The goal was to understand how to use VirusTotal for threat intelligence and to identify potential security threats.
Additional notes	- Over fifty security vendors flagged the file as malicious, identifying it as Flagpro malware

	- The identified IoCs included: Domain Name: ‘org.misecure.com’ IP Address: `207.148.109.242` (though there were other IP addresses under the Relations tab) Hash Value: `287d612e29b71c90aa54947313810a25` - I observed HTTP requests made to the domain ‘org.misecure.com’ - Noted input capture as a tool used by threat actors in the Collection section. Command and control tactics were identified, indicating communication channels between infected systems and attackers.

Date: Oct 22, 4PM	**Entry:** Entry #4: Responding to a phishing incident
Description	Documentation of a phishing alert within a financial services company involving a suspicious email and attachment, following the organization's security procedures.
Tool(s) used	VirusTotal, Phishing Playbook
The 5 W's	• **Who:** The email was sent by "Def Communications" with the name "Clyde West," which is inconsistent and suspicious. • **What:** A phishing email was received, containing a malicious attachment identified by its hash. The attachment was named "bfsvc.exe" instead of the claimed PDF. • **When**: The incident occurred on Wednesday, July 20, 2022, at 09:30:14 AM. • **Where:** The email was sent to hr@inergy.com from IP address <114.114.114.114>.

	• **Why**: The phishing attempt aimed to deceive the recipient into opening a malicious file under the guise of a job application.

Additional notes	1. **Alert Evaluation:**
	  ○ **Severity:** Medium, indicating potential need for escalation.
	  ○ **Sender Details:** Mismatch between sender's name and email address suggests phishing.
	  ○ **Message Body:** Contains grammatical errors and misleading information about attachments.
	2. **Reasons for Escalation:**
	  ○ Known malicious file hash detected.
	  ○ Suspicious sender details and inconsistent attachment type.
	  ○ Grammatical errors in the email body further indicate phishing intent.
	3. **Action Taken:**
	  ○ Updated ticket status to "Escalated."
	  ○ Notified Tier 2 SOC analyst for further investigation.

Date: Oct 23, 4:00PM	**Entry:** Entry #5: Failed SSH Logins Investigation
Description	Documentation of the investigation of failed SSH login attempts for the root account on Buttercup Games' mail server using Splunk Cloud.
Tool(s) used	Splunk Cloud
The 5 W's	• **Who:** Unauthorized users attempting to access the root account. • **What:** Investigation of failed SSH login attempts on the mail server. • **When:** The investigation occured on October 23rd at 4PM.

	• **Where:** Buttercup Games' mail server, identified as `mailsv`. • **Why:** To identify potential security issues with unauthorized access attempts.
Additional notes	**Process Overview:** • Set up a Splunk Cloud account and uploaded log data. • Queried data using `index=main host=mailsv fail* root` to locate failed SSH login attempts. • Over 300 events were identified, indicating multiple unauthorized access attempts. **Key Findings:** • High frequency of failed login attempts suggests possible brute force attack. • Need for further investigation and potential strengthening of security measures.
