Incident handler's journal

Date: Aug 28, 2023	**Entry:** #1
Description	Documenting the cybersecurity incident of a ransomware attack
Tool(s) used	None
The 5 W's	• **Who:** Organized group of unethical hackers • **What:** A ransomware attack • **Where:** At a small US health care clinic • **When:** Tuesday 9:00 a.m. • **Why:** The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. What backup and disaster recovery solutions are in place, and how can they be improved to minimize the impact of ransomware attacks? 2. What measures can the organization implement to enhance its cybersecurity posture and prevent future ransomware attacks? 3. What is the organization's policy or strategy regarding ransom payments in response to ransomware attacks?

Date: Sep 02, 2023	**Entry:** #2
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, the VirusTotal analyzes the file hash and reports it as malicious.
The 5 W's	• **Who:** An unknown malicious actor • **What:** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **When:** At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Where:** An employee's computer at a financial services company • **Why:** An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	1. How can this incident be prevented in the future? 2. Should the company consider improving security awareness training so that employees are careful with what they click on?

Date: Sep 04, 2023	**Entry:** #3
Description	Examine alerts, logs and rules with Suricata
Tool(s) used	For this activity I used Suricata, an open-source intrusion detection system, intrusion prevention system, and network analysis tool. The Suricata tool monitors network interfaces and applies rules to the packets that pass through the interface. Suricata determines whether each packet should generate an alert and be dropped, rejected, or allowed to pass through the interface. Source and destination networks must be specified in the Suricata configuration. Custom rules can be written to specify which traffic should be processed.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I created custom rules and ran them in Suricata, monitored traffic captured in a packet capture file and examined the fast.log and eve.json output. Now I understand the structure of the rules file, which has action, header and rule options.

Date: Sep 05, 2023	**Entry:** #4
Description	Capture and analyze live network traffic
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. It captures and displays network traffic in real-time, allowing users to inspect and analyze packets to diagnose network issues. This tool is valuable for debugging, security analysis, and network optimization.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I accomplished the following in this activity: • Use tcpdump to capture real-time network traffic, allowing for live monitoring and analysis of data packets. • Save network traffic to a packet capture file for later analysis and reference. • Filter packet capture data to focus on specific network events or information of interest, helping streamline analysis and troubleshoot network issues effectively

Date: Sep 07, 2023	**Entry:** #5
Description	To identify whether there are any possible security issues with the mail server by exploring any failed SSH logins for the root account.
Tool(s) used	For this activity, I used Splunk, a powerful data platform used for log management, real-time analytics, and monitoring of machine-generated data. It collects and indexes data from various sources, including servers, applications, and devices, making it accessible for searching and analysis. Splunk primarily uses its proprietary search and query language called "Splunk Search Processing Language" (SPL) for interacting with and analyzing data within the Splunk platform and it also supports various other query languages and data formats for data ingestion and integration.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: Buttercup Games e-commerce store • **When**: N/A • **Why**: N/A
Additional notes	I uploaded data into Splunk to analyze and extract valuable insights. With a basic search, I efficiently explored the data and evaluated crucial fields like host, source, and source type, gaining a better understanding of its origins and characteristics. To pinpoint potential security concerns, I narrowed down my search using wildcards to locate any instances of failed SSH logins specifically for the root account and found over 300 failed SSH logins for the root account on the mail server.

Date: Sep 13, 2023	**Entry:** #6
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	The following are done in this activity: • Identify the source and destination IP addresses and examine the protocols involved in the web browsing session. • Analyze some of the data packets to identify the type of information sent and received by the systems that connect to each other when the network data is captured.