Incident handler's journal

Date: Record the date of the journal entry.	**Entry:** Feb 14th, 2024
Description	Analyze Network Packet
Tool(s) used	**Wireshark**
The 5 W's	I am using Wireshark to capture packets related to a user connecting to an internet site. The goal of this project is to capture and identify the source and destination IP address, examine the protocols that are used when the user makes a connection to the website and analyze some of the data packets to identify the type of information sent and received. The protocol being used in the first packet is ICMP. I also learned to use filters to sort the traffic and searched for specific IP addresses and mac addresses.
Additional notes	**Objective**: The primary goal of the project was to capture and identify both the source and destination IP addresses involved in the communication process. **Protocol Analysis**: Identified ICMP (Internet Control Message Protocol) as the protocol used in the first packet of the captured traffic. **Packet Examination**: Analyzed data packets to gain insights into the type of information being sent and received during user connections. **Filtering Techniques**: Demonstrated proficiency in using Wireshark filters to effectively sort and analyze network traffic, enabling focused examination of specific IP addresses and MAC addresses. **Skills Developed**: Enhanced understanding of network protocols and traffic

	analysis techniques, crucial for incident handling and network security operations.

Date: Record the date of the journal entry.	**Entry:** Feb 28th, 2024
Description	Investigate a suspicious file hash
Tool(s) used	**Virustotal, Indicators of Compromise, Crowdsourcing**
The 5 W's	I received a SIEM alert about a suspicious file being downloaded on an employee computer. Upon further investigation I discovered the employee received an email with an attachment disguised as a spread sheet. When the employee opened the file, a malicious payload was delivered to their computer. I uploaded the SHA file hash to the virus total website and discovered the file hash has been reported as malicious by over 50 vendors and is known as malware Flagpro and is commonly used by the threat actor Blacktech.
Additional notes	**Alert Source**: Received a Security Information and Event Management (SIEM) alert indicating a suspicious file download on an employee's computer. **Incident Investigation**: Conducted a thorough investigation into the incident to ascertain the nature and origin of the suspicious file. **Phishing Vector**: Discovered that the employee received an email containing an attachment disguised as a spreadsheet.

	Payload Delivery: Upon opening the attachment, the employee inadvertently triggered the delivery of a malicious payload to their computer. **Malware Identification**: Uploaded the SHA file hash to VirusTotal, a reputable malware analysis platform, for further analysis. **Malicious Indicators**: Identified the file hash as associated with malware known as "Flagpro," reported as malicious by over 50 antivirus vendors. **Attribution**: Noted that the malware is commonly utilized by the threat actor group "Blacktech," providing insights into potential threat actor involvement. **Response**: Initiated appropriate response actions, including containment, remediation, and further investigation, to mitigate the impact and prevent further spread of the malware within the organization.

Date: Record the date of the journal entry.	**Entry:** **Mar 11th, 2024**
Description	Use playbook to respond to a phishing incident
Tool(s) used	Playbooks,
The 5 W's	As an SOC analyst I received an alert ticket about a potential phishing attempt that occurred via email. I went to the company playbook and followed the procedures under “Receive Phishing Alert”. The playbook brought me through the process of assigning an alert severity to the incident of medium since the employee who was targeted did not fall for the attempt. I gathered the receiver’s details, sender’s details, subject line, message body, attachments

	and links. I used Virustotal and found that attachments and links were malicious then updated the ticket and escalated it per the playbook process.
Additional notes	**Role**: Acted as a Security Operations Center (SOC) analyst responsible for handling security incidents. **Incident Description**: Received an alert ticket regarding a suspected phishing attempt through email. **Procedure Followed**: Consulted the company playbook and adhered to the prescribed procedures outlined under the "Receive Phishing Alert" section. **Alert Severity Assessment**: Assigned a medium severity to the incident since the targeted employee did not fall for the phishing attempt, indicating a lower level of impact. **Information Gathering**: Gathered comprehensive details related to the phishing email, including receiver's details, sender's details, subject line, message body, attachments, and links. **Analysis with Virustotal**: Utilized Virustotal, a popular online malware analysis tool, to examine attachments and links for malicious content. **Identification of Malicious Content**: Confirmed the presence of malicious content within the attachments and links, indicating a genuine phishing attempt. **Ticket Update and Escalation**: Updated the alert ticket with the findings and escalated the incident as per the playbook's escalation process, ensuring appropriate action and response.

Date: Record the date	**Entry:** March 21st, 2024

of the journal entry.	
Description	Signatures and Logs with Suricata
Tool(s) used	Suricata
The 5 W's	I used Suricata to monitor network traffic and configure alerts. I used a custom rule with configured action, header and rule options. The action in this rule was ALERT. The header of the rule included $HOME_NET any → $EXTERNAL_NET any which would mean that the alert will be triggered on any network traffic from the home network leaving to an external network. With the rule options for the custom parameters were set to trigger when Suricata observes the text GET as the http method in a http packet. I also used Suricata to observe fast.log and the eve.json output.
Additional notes	**Tool Utilization**: Leveraged Suricata, an open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), for monitoring network traffic and configuring alerts. **Custom Rule Configuration**: Developed a custom rule with specific actions, headers, and rule options tailored to the organization's network security requirements. **Action**: Configured the action in the rule as "ALERT," indicating that alerts are triggered upon detection of suspicious network activity. **Header Specification**: Defined the header of the rule with "$HOME_NET any -> $EXTERNAL_NET any," signifying that alerts are generated for any traffic originating from the internal network (HOME_NET) destined for external networks (EXTERNAL_NET). **Rule Options**: Customized rule options to specify parameters for triggering alerts based on specific criteria. Specifically, configured the rule to trigger alerts when Suricata detects the HTTP method "GET" in HTTP packets. **Monitoring Outputs**: Utilized Suricata to monitor both the fast.log and eve.json outputs, enabling comprehensive visibility into network traffic and security events.

	Enhanced Detection Capabilities: By configuring Suricata with custom rules and parameters, strengthened the organization's ability to detect and respond to potential security threats in real-time, thereby enhancing overall network security posture.