Incident handler's journal

This journal is used to record my findings after completing various activities on tool concepts and incident responses.

Date: 10/5/2023	**Entry:** **0001**
Description	Phishing attempt was successful on an employee resulting in ransomware affecting organizational data.
Tool(s) used	
The 5 W's	• **Who**: Threat actors • **What:** Ransomware infected database • **When:** Tuesday at 0900 hours • **Where**: At a healthcare company • **Why** A phishing campaign occurred resulting in malicious emails being sent to multiple company employees encouraging them to download a malicious file. An employee who was not trained to recognize the phishing email downloaded the malicious file allowing the malware to encrypt the organizational database from the workstation and demand a ransom be paid for decryption.
Additional notes	Employees should be involved in quarterly training to recognize phishing attempts and respond appropriately to quarantine them. Machine was removed from the network and the incident has been elevated to the incident response team.

Date: 10/6/2023	**Entry:** **0002**
Description	Phishing attempt was successful on an employee resulting in the opening of a malicious payload being executed on the workstation.
Tool(s) used	Sha256sum hashing of malicious file, VirusTotal
The 5 W's	• **Who**: Threat actors • **What:** Malware infected spreadsheet file • **When:** Friday, 1311 hours • **Where**: At a test company • **Why** A phishing attack with respect to a request to download a password protected spreadsheet. Employee opened the file and input the password triggering a download of a malicious file. AV software triggered an alert and the employee actions were logged. The downloaded file was hashed and checked against the VirusTotal database. Information observed is recorded as notes.
Additional notes	57/72 Vendor score, -64 User score, consistent assessment by multiple organizations describing the file as malicious as identified by file hash. Device disconnected from network and analyzed using antivirus software. Malicious files were located, quarantined and removed from the system.

Date: 10/7/2023	**Entry:** **0003**
Description	Utilize tcpdump to capture a network packet and save to a .pcap file.
Tool(s) used	Linux CLI
Operation	• Utilized tcpdump on Linux CLI to request information on available networks to capture network data from (sudo ifconfig) • Identified interface options to collect data from (sudo tcpdump -D) • Capture and display 5 packets of data from the desired network interface (-i eth0) (sudo tcpdump -i eth0 -v -c5), -v to set verbosity and -c5 to capture 5 packets. • Recognize that tcpdump attempts to automatically verify exchange IP with domain name • Open tcpdump to capture data in the background and make sample traffic to be captured. (sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &). (-nn telling tcpdump not to resolve IP to domain), (port 80 to filter only data operating on this port) (-w to write the captured data to a file named capture.pcap) (& being a shell command to run command in the background) • Finally, generate network data using curl, (curl opensource.google.com) which will be captured by our background process.
Additional notes	This was an example process where I utilized the tcpdump application to capture, review and save network data. There is far more depth to be understood utilizing the tcpdump application and the commands held within but this is a good baseline to form an expectation of use.

Date: 10/7/2023	**Entry:** **0004**
Description	Examine alerts, logs, and rules within Suricata
Tool(s) used	Linux CLI, Suricata

Operation	• Using a Qwiklab environment, I examine a prewritten Suricata rule and break down the process to better understand the SIEM tool operations.
	• A custom rule already exists in the environment: alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)
	• I break down the rule as follows:
	  ○ alert: Tells the action to take upon observation of the following
	  ○ http: Protocol to be observed
	  ○ $HOME_NET any ->: Sender address on any port
	  ○ $EXTERNAL_NET any: Destination address on any port
	  ○ msg:"GET on wire": Text to be provided on alert
	  ○ Flow:established, to_server: determines that packets from the client to the server should be matched (Syn to Syn:Ack)
	  ○ content:"GET": Search for http method GET
	  ○ sid:12345: Specific ID of the rule
	  ○ rev: Revision count of the rule
	• I run the rule with some test network data using (sudo suricata -r sample.pcap -S custom.rules -k none) where I run Suricata with elevated privileges, using the simulated file sample.pcap, and the rule set in custom.rules. -k none simply disables checksum checks.
	• Running this process creates a Suricata directory for multiple files, one being fast.log. Using (cat /var/log/suricata/fast.log) we can observe the alerts that were sent from running the test data through Suricata with our rule applied.
	• More information can be observed through JSON format using (cat /var/log/suricata/eve.json) and an appropriate JSON reader, like jq.

Additional notes	This was an example process where I utilized the SIEM tool Suricata to observe a written rule, and tested it against a sample of captured network traffic. Using Suricata, an open source SIEM tool, you can set up rules to provide alerts based on user designed rules or predesigned rules.

Reflections/Notes: My time spent working with CLI and utilizing tools like Chronicle, Splunk, Suricata, and tcpdump was very eye opening to the capabilities of packet capturing and network data analysis. I captured network packets utilizing the CLI and Linux built-in application tcpdump. I learned how to interpret both the packet information and a precursory amount of tcpdump commands and arguments.

I made simple queries using the Chronicle UDM search language, as well as Splunk's SPL to query data lake information with specific addresses and values. I reviewed various security incidents and broke down occurrences and responses.

To me, the most valuable information obtained was the experience of entry level use to SIEM tools utilized in cybersecurity operations. I will continue to familiarize myself with these tools with a plan to set up my own virtual network representative of a multi-workstation system set to a centralized network with rules set in an external firewall.