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: 20-08-2024	**Entry:** #1
Description	Explore signatures and logs with Suricata
Tool(s) used	Suricata
The 5 W's	Capture the 5 W's of an incident. ● **Who**: A group of malicious actors ● **What**: DDoS attack ● **When:** Friday 11:00 a.m. ● **Where**: at a logistic company, Human Resources department ● **Why**: A misconfigured firewall was the cause of the DDoS attack. The firewall was not configured to limit the rate of ping requests, so the servers were overwhelmed. Therefore, it was an ICMP flood type of DDoS attack.
Additional notes	What determined the misconfiguration of the firewall?

Date: 21-08-2024	**Entry:** #2
Description	Performing queries with Splunk
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. ● **Who**: An insider ● **What:** unsuccessful authentication requests ● **When**: Tuesday 10:00 am ● **Where**: Finance department ● **Why**: the attacker tried to login with the root user, which has the highest level of privileges
Additional notes	What determined the insider to try to authenticate with the root user?

Date: 22-08-2024	**Entry:** #3
Description	Analyze packet with Wireshark
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. ● **Who**: a malicious actor ● **What**: a successful vishing attack ● **When**: Monday 16:00 ● **Where**: Logistics department

	● **Why**: an employee was tricked to disclose his credentials to someone claiming to be from external support. The intruder managed to connect on the network using the credentials and downloaded sensitive files.
Additional notes	Internal phishing awareness training shall be conducted.

Date: 23-08-2024	**Entry:** #4
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: Several accounts from the IT department were locked out. 2. **Containment, Eradication, and Recovery**: After it was determined which accounts were affected, they were locked. After that network segmentation was implemented to isolate the accounts.
Tool(s) used	Suricata, Splunk
The 5 W's	Capture the 5 W's of an incident. ● **Who** a malicious actor ● **What**: LLMNR poisonous attack ● **When**: Friday 16:30 ● **Where**: IT department ● **Why**: The attacker exploited the vulnerabilities of a misconfigured router and gained unauthorized access. The attacker set up a malicious machine to respond to LLMNR queries. By manipulating LLMNR traffic remotely, the attacker carried out an LLMNR poisonous attack.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: It was very interesting to act like a SOC analyst. This domain represents a great interest to me, due to the high level of analysis involved.