**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:**  ??? | **Entry:**  User downloads file that is deemed to be malicious | | |
| --- | --- | --- | --- |
| Description | IDS detects a user downloading a file that is not trusted, the hash looked up is deemed by virustotal to be an executable malware/trojan/backdoor software deemed by almost every vendor. Deeming the file as malicious. | | |
| Tool(s) used | IDS software, Virustotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A random email from a random account * **What** happened? User saw suspicious email * **When** did the incident occur? ?? * **Where** did the incident happen? Company grounds * **Why** did the incident happen? Attacker was trying to phish users | | |
| Additional notes |  | | |

| **Date:**  ???. | **Entry:**  Random USB drive found | | |
| --- | --- | --- | --- |
| Description | Random usb drive was put in computer out of curiosity | | |
| Tool(s) used | No tools were used | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Random employee * **What** happened? Employee put USB drive into company computer * **When** did the incident occur? ??? * **Where** did the incident happen? Company grounds * **Why** did the incident happen? Curiosity | | |
| Additional notes | The USB drive could have contained malicious content | | |

| **Date:**  2:24pm??? | **Entry:**  UDP port containing unknown IP, sending a DoS attack | | |
| --- | --- | --- | --- |
| Description | Many requests going to port 53, sending packets too big for the network to handle | | |
| Tool(s) used |  | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Unknown IP * **What** happened? Description * Many requests going to port 53, sending packets too big for the network to handle * **When** did the incident occur? After noon * **Where** did the incident happen? Company network * **Why** did the incident happen? Lack of firewall | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:** | **Entry:**  Audit of MultiMedia company incident report | | |
| --- | --- | --- | --- |
| Description | DDoS attack to server | | |
| Tool(s) used |  | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Suspicious IP’s * **What** happened? ICMP flood attack to company servers * **When** did the incident occur? ?? * **Where** did the incident happen? Company servers * **Why** did the incident happen? Lack of DoS/DDoS protection | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  ??? | **Entry:**  Smurf Attack on server | | |
| --- | --- | --- | --- |
| Description | Dos/DDoS Attack on server, | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Unknown IP * **What** happened? Smurf Attack * **When** did the incident occur? ?? * **Where** did the incident happen? Company server * **Why** did the incident happen? Lack of DoS/DDoS protection | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

### 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: Record additional notes. |
| --- |