**Incident report analysis**

**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 chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | * While working at a company specializing in web design, graphic design and social media marketing, there was a DDoS attack that disrupted normal network operations for 2 hours. * The incident involved a flood of ICMP packets overwhelming the network, and rendering normal internal traffic inaccessible. |
| Identify | * The type of attack was a DDoS attack. * This attack used a flood of ICMP packets to overwhelm the web server. * This attack is known as a Ping Flood. * The attack was sent through an unconfigured firewall. |
| Protect | * The first measure to take is to block all incoming ICMP packets. This method is fast and reliable, but not permanent. * This will allow the cybersecurity team to investigate the incident and develop a permanent solution that removes the viability of this attack. * An intrusion prevention system (IPS) will prevent unwanted connections, as well as reconfiguring the firewall to close any unused ports. |
| Detect | * Using a logging tool will ensure the organization has easily accessible records of the events leading up to the attack. * Also implementing an intrusion detection system (IDS) will monitor all incoming traffic from the internet. |
| Respond | * A new firewall rule was made to limit the rate of incoming ICMP packets. * Source IP address verification on the firewall will also ensure that IP addresses aren’t being spoofed. * We will continue to monitor the network by deploying monitoring software to detect abnormal traffic patterns. * An IDS/IPS system was implemented to filter out some ICMP traffic based on suspicious characteristics. |
| Recover | * In order to recover immediately, we need to make sure that the attack has stopped, and basic measures are in place for this attack to not happen again. * We will implement the network monitoring software immediately and the other systems mentioned previously. * No customer PII was stolen, so there is no need to make a plan in that regard. * This will ensure the network is secure from attacks in the future. |

|  |
| --- |
| Reflections/Notes: |