**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** | My organization recently received a DDoS attack, in which the malicious actor flooded the network with ICMP packets through an unconfigured firewall. Because of this, our network services suddenly stopped responding, and normal internal network traffic could not access any network resources. In response, the incident management team blocked all incoming ICMP packets and stopped all non-critical network services so that critical network services could be restored. |
| Identify | The malicious actor targeted the organization with an ICMP flood attack. The attack had large surface area, affecting the entire internal network. The critical network resources needed to be secured and restored. |
| Protect | The cybersecurity team set up a firewall rule to restrict the rate of ICMP packets, and they added an IDS/IPS system to filter out and alert suspicious ICMP traffic. |
| Detect | The cybersecurity team configured a source IP address verification on the firewall to reduce the possibility of IP spoofing on incoming ICMP packets and put in place network monitoring tools to detect suspicious traffic patterns. |
| Respond | The team will now focus on isolating the incident as it occurs, as to prevent the attack from causing further disruption to the network – and will focus on restoring any critical systems that were affected by the attack. After which, the team will report all incidents to their management and if necessary, the authorities. |
| Recover | To restore the network to a functioning state when presented with an ICMP flooding DDoS attack, the team will focus on restoration of critical services to the network, and then the rest of the network to a functioning state. The ICMP flood attacks should be stopped at the firewall if the earlier rules were implemented. Then, the team will ensure all non-critical network services should be stopped to reduce internal network traffic, so the team can then focus on restoring critical network services. Once the ICMP flood finishes, then the non-critical network services can be turned back on. |

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