**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** | The organization recently experienced a DdoS attack, which compromised the internal network for two hours. The organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets through an unconfigured firewall. Normal internal network traffic could not access any network resources. The cybersecurity team found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. |
| Identify | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical networks services offline. The security team implemented source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| Protect | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets. |
| Detect | The network security team implemented networking monitoring software to detect abnormal traffic patterns. They also implemented and IDS / IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline. |
| Recover | After setting up a new firewall rule, implementing an IDS / IPS System and networking software, the network is restored by unblocking incoming ICMP packets. |

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