**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** | A DDoS attack caused our company’s network services to suddenly stop working. Our cybersecurity team investigated the incident and found that the a malicious actor was flooding the network traffic with ICMP packets causing users to lose access to network resources. The ICMP packets were being sent through an unconfigured firewall. The attack surface was addressed and the network was hardened through firewall configurations, network monitoring, and IDS/IPS filtering. | | |
| --- | --- | --- | --- |
| Identify | The incident management team was alerted when there was a stoppage of all network services. Upon investigation they found it was a malicious actor sending a flood of ICMP pings through an unconfigured firewall to take down the network through a DDoS attack. | | |
| Protect | The team implemented a new firewall rule to limit the rate of incoming ICMP packets. Source IP verification was implemented to mitigate IP spoofs for incoming ICMP packets. | | |
| Detect | Network monitoring software was implemented to detect abnormal traffic. IDS/IPS systems were implemented to filter out suspicious ICMP traffic. | | |
| Respond | The attacker was able to make it through the firewall because it was unconfigured. Our incident response team has now implemented IP source verification on the firewall to prevent attackers entering through IP spoofing. There is also now a firewall rule to limit the rate of incoming ICMP packets. | | |
| Recover | The network is now back online and protected since the flood of ICMP traffic has been stopped and any new ways to enter the network has been mitigated. | | |

| Reflections/Notes: |
| --- |