**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 security incident took place where the multimedia company network services stopped responding. The cybersecurity team discovered the unresponsive service was due to an ICMP flood attack, where the attack overwhelms a network device with a substantial amount of ICMP pings. The team responded by blocking incoming ICMP packets and stopped the non-critical network services to restore their critical network services. | | |
| --- | --- | --- | --- |
| Identify | A malicious attacker targeted a company with an ICMP flood attack. The entire internal network was affected. | | |
| Protect | The cybersecurity team implemented a new firewall rule which is accountable for limiting the rate of incoming ICMP packets. The team also adopted an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | The cybersecurity team utilized source IP address verification to check for spoofed IP addresses on incoming ICMP packets and used a network monitoring software to detect abnormal traffic patterns. | | |
| Respond | The team can contain the cybersecurity incidents and affected devices by isolating the affecting systems to prevent any more disruptions to the software. Some procedures that can help us neutralize cybersecurity incidents is to restore any critical systems and services that were disrupted by this event. The team can analyze network logs to investigate any suspicious behavior. The recovery process can be improved by ensuring we report all incidents to upper management to prevent any more incidents. | | |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services  need to be restored to a normal functioning state. In the future, external ICMP  flood attacks can be blocked at the firewall. Then, all non-critical network  services should be stopped to reduce internal network traffic. Next, critical  network services should be restored first. Finally, once the flood of ICMP  packets have timed out, all non-critical network systems and services can be  brought back online. | | |

| Reflections/Notes: |
| --- |