**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 company experienced a security incident when all network services abruptly stopped responding. The cybersecurity team identified the disruption as a distributed denial of service (DDoS) attack, characterized by a flood of incoming ICMP packets. In response, the team successfully blocked the attack and temporarily halted all non-critical network services to prioritize the restoration of critical network services. |
| Identify | Malicious actors targeted the company with ICMP flood attack. All critical network resources needed to be secured and restored to a functioning state |
| Protect | **The cybersecurity team set a firewall rule to limit incoming ICMP packets and used an IDS/IPS system to filter suspicious ICMP traffic.** |
| Detect | The cybersecurity team configured the firewall to verify source IP addresses on incoming ICMP packets to check for spoofing and implemented network monitoring software to detect abnormal traffic patterns. |
| Respond | The team will isolate systems to prevent further disruption, restore critical systems and services, analyze network logs for suspicious activity, and report all incidents to upper management and legal authorities if needed. |
| Recover | To recover from an ICMP flood DDoS attack, restore normal network functioning. Block future attacks at the firewall. Stop non-critical services to reduce internal traffic. Restore critical services first. Once the attack subsides, bring back non-critical services gradually. |

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