**Incident report analysis**

**Instructions**

As you continue 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 to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored. |
| Identify | The company’s cybersecurity team then investigated the security event and found out that the malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service attack. |
| Protect | The cybersecurity team implemented a new firewall rule to limit the rate of  incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic  based on suspicious characteristics. |
| Detect | The cybersecurity team configured source IP address verification on the  firewall to check for spoofed IP addresses on incoming ICMP packets and  implemented network monitoring software to detect abnormal traffic patterns. |
| Respond | For future security events, we will be subnetting to divide the network for specific departments so we can isolate certain parts of the network when an attack occurs so the whole organization is not affected. We have informed the upper management team about this incident so they can further escalate the data breach information to the relevant interested parties. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services  needs 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 has timed out, all non-critical network systems and services can be brought back online. |

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