**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 the organization’s network services suddenly stopped working due to an incoming flood of ICMP packets. After examination it was determined that the disruption was caused by a Distributed Denial of Service Attack (DDoS attack). The team responded blocking the incoming ICMP packets and stopping all non-critical network services offline, allowing critical network services to be restored.** |
| Identify | **The Security Team was able to find that a Malicious Threat Actor had sent a flood of ICMP pings into the company’s network through an Unconfigured Firewall, which allowed for the malicious attacker to overwhelm the company’s network through a DDoS attack.** |
| Protect | **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 was installed.** |
| Detect | **Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implementation of Network monitoring software to detect abnormal traffic patterns.** |
| Respond | **For future security events, the cyber security teams are going ot isolate the affected systems to minimize the damage that can be done while the team works to fix the problems.** |
| Recover | **To recover from the 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 have timed out, all non-critical network systems and services can be brought back online.** |

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