**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** | multimedia company was hit with a DDOS attack which compromised the internal network for two hours until it was resolved. The incident management team responded by blocking incoming ICMP packets , stopping all non-critical network services offline, and restoring critical network services. |
| Identify | DDoS attack, ICMP pings directed against an unconfigured firewall |
| Protect | To address this security event, the network security team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets |
| Detect | Implement IDS monitor to detect abnormal traffic patterns |
| Respond | Implement IPS for suspicious traffic characteristics and block abnormal traffic that makes it past the firewall. |
| Recover | Restored critical network services and determine if any data or systems have been affected by the incident. |

|  |
| --- |
| Reflections/Notes:   1. Create documentation to follow for standing up new firewalls 2. Create Documentation\policy for firewall configuration. 3. Defense in depth with the firewall update, the new IDS and IPS systems will reduce the companies vulnerability to attacks from outside actors. |