**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** | Our multimedia company experienced a two-hour Distributed Denial of Service (DDoS) attack that exploited an unconfigured firewall, flooding our network with ICMP packets and disrupting services. Aligned with the NIST Cybersecurity Framework, our response encompassed five key functions to enhance network security: Identify, Protect, Detect, Respond, and Recover. | | |
| --- | --- | --- | --- |
| Identify | Through routine audits, we assessed internal networks, systems, devices, and access privileges, uncovering vulnerabilities that could be exploited. These insights enabled us to proactively address potential security gaps. | | |
| Protect | We implemented a new firewall rule limiting ICMP packets, enforced source IP address verification, and established policies, procedures, and training to ensure a secure environment. These measures safeguarded against future attacks. | | |
| Detect | Network monitoring software and an IDS/IPS system were deployed to swiftly identify anomalies and filter suspicious ICMP traffic, enhancing our ability to detect potential threats. | | |
| Respond | Our incident management team executed containment protocols to neutralize threats promptly. Thorough analysis of the incident informed improvements to our security process, enhancing our readiness for future incidents. | | |
| Recover | Following containment, we restored affected systems to normal operation, removed malicious code, and recovered data from secure backups. This phase emphasized efficient recovery and business continuity. | | |

| Reflections/Notes: |
| --- |