**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 organization's network services were operating seamlessly until an abrupt halt occurred. The usual internal network access to network resources ceased entirely. In response, the incident management team was summoned to address the issue. Their investigation revealed that this interruption was a consequence of an influx of ICMP Packets, indicative of a Distributed Denial of Service (DDoS) attack. Consequently, the organization endured a two-hour disruption to its internal network before resolving the issue.  Upon delving further into the incident, the investigative team uncovered that a malicious actor had initiated a barrage of ICMP pings into the company's network. The cybersecurity team promptly reacted by implementing measures to block incoming ICMP packets, effectively restoring critical network services to their normal operation. |
| Identify | The incident management team conducted a comprehensive audit of the systems, devices, and access policies implicated in the attack to pinpoint security vulnerabilities. During this examination, it was determined that the incident indeed stemmed from a Distributed Denial of Service (DDoS) attack, in which the attacker inundated the company's network with ICMP pings. This security breach occurred due to a misconfiguration of the firewall, which failed to properly limit the rate of incoming ICMP packets. |
| Protect | The security team has implemented the following security hardening improvements to protect the organization from further attacks:   * 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 * Network monitoring software to detect abnormal traffic patterns * An IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To proactively detect flooding attacks similar to the one experienced, the organization plans to implement a comprehensive security strategy. This strategy involves the deployment of Security Information and Event Management (SIEM) tools, which will continuously monitor network traffic. Additionally, an Intrusion Detection System (IDS) will be put in place to identify abnormal packets and promptly alert the relevant authorities. |
| Respond | The cybersecurity team took immediate action by blocking incoming ICMP packets and swiftly restoring critical network services. Simultaneously, they initiated communication with upper management to apprise them of the situation. As part of the incident response protocol, management will send notifications to our customers via email to inform them of the data breach incident. Moreover, they will ensure compliance with local laws and regulations by liaising with law enforcement agencies and relevant organizations as necessary. |
| Recover | Following the successful blocking of malicious traffic and the necessary port configuration, the network services swiftly returned to their usual, uninterrupted operation. In preparation for potential future security incidents, the cybersecurity team has implemented a proactive approach. They are prepared to isolate affected systems promptly to prevent any further disruptions to the network.  To maintain a culture of security awareness and ensure business continuity, employees have been informed not to panic when encountering unusual network activities like this. Instead, they are encouraged to promptly report any such incidents to the Incident Response Department. This proactive communication ensures that the organization can respond swiftly to potential threats and maintain smooth business operations. |

|  |
| --- |
|  |