**Incident report analysis**

| **Summary** | The multimedia company, which provides web design, graphic design, and social media marketing solutions, recently experienced a Distributed Denial of Service (DDoS) attack. During the attack, network services were overwhelmed by a flood of ICMP packets, rendering the internal network inaccessible for two hours. The incident management team responded by blocking incoming ICMP packets, disabling non-critical network services, and restoring critical operations. The cybersecurity team identified an unconfigured firewall as the root cause, which allowed the malicious traffic to penetrate the network. | | |
| --- | --- | --- | --- |
| Identify | The incident management team audited the network and discovered that the DDoS attack was caused by an unconfigured firewall that allowed malicious ICMP traffic to overwhelm the network. The vulnerability highlighted a lack of proper firewall configuration and inadequate protection against volumetric attacks. | | |
| Protect | To mitigate future risks, the team implemented a new firewall rule to limit incoming ICMP traffic, enforced source IP address verification to prevent spoofing, and deployed an IDS/IPS system to filter suspicious ICMP packets. Employee training on network security best practices was also prioritized. | | |
| Detect | The organization deployed network monitoring software to identify abnormal traffic patterns and enhanced its detection capabilities with an intrusion detection system (IDS) to monitor for potential threats, ensuring faster and more accurate detection of future incidents. | | |
| Respond | During the attack, the team blocked incoming ICMP traffic, disabled non-critical network services to reduce system load, and restored critical operations. Additionally, the incident response plan was updated to include specific actions for mitigating DDoS attacks. | | |
| Recover | Critical systems were brought back online after reconfiguring the firewall, and data integrity was verified across all network resources. The team confirmed normal operations and established a plan for continuous improvement of the company’s incident recovery processes. | | |

| Reflections/Notes: |
| --- |