**Incident report analysis**

| **Summary** | This morning, Multimedia Design Co. was targeted by a Distributed Denial of Service (DDoS) attack involving a flood of ICMP packets. The attack overwhelmed the servers with fake traffic, preventing legitimate network requests from being processed. As a result, the company’s internal services were unavailable for approximately two hours, causing significant operational disruption, financial loss, and damage to client trust. The attacker exploited a misconfigured firewall that failed to block suspicious ICMP traffic. In response, the incident response team blocked incoming ICMP packets, shut down all non-essential network services, and restored critical systems to resume normal operations. | | |
| --- | --- | --- | --- |
| Identify | During the investigation, the incident response team identified a major vulnerability in the firewall configuration. The firewall was not properly configured to filter or limit incoming ICMP traffic, which allowed the attacker to exploit this weakness and flood the network. Additionally, there was no Intrusion Detection or Prevention System (IDS/IPS) in place to analyze or block suspicious ICMP traffic. The abnormal traffic flow was detected using `tcpdump`, which revealed a high volume of inbound ICMP packets targeting the internal network. | | |
| Protect | **A new firewall rule was implemented to limit the rate of incoming ICMP packets. Additionally, source IP verification was enabled on the firewall to detect and block spoofed IP addresses. Intrusion Prevention Systems (IPS) and Detection Systems (IDS) were also added to filter suspicious traffic patterns. These measures help reduce risks by enforcing restrictions on incoming and outgoing traffic, blocking unauthorized packets, and strengthening the overall network security posture.** | | |
| Detect | Similar incidents will be detected using network monitoring tools such as `tcpdump`, which allows the security team to observe large volumes of suspicious traffic with spoofed IP addresses. Upon detection, preventive measures can be applied immediately to stop the attack. Additionally, an Intrusion Detection System (IDS) monitors network traffic to identify potential attacks or suspicious activities and alerts the security team without taking direct action. Complementing IDS, an Intrusion Prevention System (IPS) not only detects such activities but also takes immediate action to block malicious traffic or disconnect the attacker, thus providing an active defense layer. | | |
| Respond | Upon detecting the attack, the incident response team immediately blocked incoming ICMP traffic at the firewall to prevent further flooding. Non-essential network services were temporarily shut down to reduce load and protect critical systems. The security team restored essential services only after verifying system integrity. The incident was documented in detail, and upper management was informed to coordinate any necessary communications or legal actions. | | |
| Recover | Data was successfully restored from backups to recover affected systems. Additionally, new measures were implemented to strengthen the network infrastructure and minimize future risks. Updated business continuity and disaster recovery plans were developed, incorporating these new technologies and procedures to ensure smoother recovery from potential future incidents. | | |

| Reflections/Notes: I have learned the critical importance of ensuring that firewalls are properly configured and not left vulnerable, as well as the necessity of implementing advanced technologies to mitigate the impact of cyberattacks. I realized that the first and most crucial step when facing a security breach is to respond swiftly to contain the attack, followed by a thorough analysis to understand the root cause, minimize losses, and strengthen the system against future incidents. This incident report has deepened my understanding of the value of preparedness and continuous vigilance in cybersecurity. I am committed to ongoing professional development and staying updated with the latest cybersecurity technologies and best practices to provide optimal protection for the organization I serve. |
| --- |