**Multimedia Company DDoS Attack: Incident Report Analysis**

|  |  |
| --- | --- |
| **Summary** | Earlier this week, reports from multiple employees stated that the organization’s network services had suddenly stopped responding. It was then discovered that the network had been disrupted by a flood of ICMP packets. The requests were originating from multiple sources, resulting in a Distributed Denial of Service Attack (DDoS) that created an ICMP flood through an unconfigured firewall. All normal internal network traffic was unable to access any network resources due to the network being overwhelmed with ICMP requests. |
| Identify | The incident management team audited the network devices, firewalls, and access policies involved in the attack to identify vulnerabilities in security. The team found that the attacker targets the company with an ICMP flood attack. As a result, one of the organization’s firewalls was left unconfigured. The network was affected negatively and disrupted all operations while losing money as well. Any data stored within the network must be compared to backups to identify any damaged or stolen data. |
| Protect | The Incident Response team should always be one step ahead and be prepared when the threats arrive. The team should implement a new firewall system to limit the rate of incoming ICMP to filter the suspicious network activity. Additionally, the team should update the OS to make sure the latest updates are in place as well. |
| Detect | The cybersecurity team can verify source IP addresses on the firewall to block fake ones. They should use tools like Wireshark or TCPdump to inspect suspicious packets. SIEM software can also helps detect unusual traffic patterns. Firewall logs and an intrusion detection system (IDS) monitor incoming traffic, especially from unknown external IPs. The team may upgrade to a Next Generation Firewall (NGFW) for added features like intrusion prevention and deeper traffic control. |
| Respond | The cybersecurity team should have a plan to manage risks and respond to future security problems. This report can be used as a guide when threats happen. If an attack occurs, the team will quickly tell users what to do next and try to stop the attack from spreading by isolating the systems that were affected. They will work to bring back any important systems or services that were disrupted. Then, they will check network logs to look for anything suspicious. The team will also report the incident to managers and legal authorities, as required by law. |
| Recover | The team needs to stop the ICMP flood to keep network services running. A firewall can be used to block this kind of attack. The team should focus on keeping critical services online, while non-critical services can be turned off for. Once the flood of ICMP packets ends, the non-critical systems and services can be safely turned back on. |

|  |
| --- |
| Reflections/Notes: |