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

|  |  |
| --- | --- |
| **Summary** | Earlier this week the multimedia company had experienced a distributed denial of service attack that compromised their internal networks for two hours. It is believed that this is caused by a malicious actor which involved a flood of ICMP ping packets that overwhelmed the network preventing normal internal traffic from accessing network resources. |
| 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 unconfigured firewall allowing the excessive ICMP traffic which leaves it open to DDos attacks that can overwhelm network resources. |
| Protect | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification for firewalls, network monitoring software for abnormal traffic patterns, and an Intrusion Detection/Prevention System (IDS/IPS) system to filter suspicious network activity. |
| Detect | To detect similar attacks in the future, the team will use firewall logging tools and analyze logs and alerts from IDS/IPS for potential threats. In order to detect vulnerabilities in the future, penetration testing would be conducted periodically. |
| Respond | The team has reconfigured firewall and security rules to recognize ICMP floods and similar request flood attacks. The targeted firewall has been reconfigured with strong security rules to match that of the baseline configuration. All security employees have been notified of the cause, response, and results of the attack. We have informed upper management of this event and they will work with content teams to notify customers about the outage. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Recover | The affected server has been reset back to the baseline configuration and is fully functioning. All data or assets related to the server have been confirmed to be reverted to their most recent backups, which should be from the previous night. For future attacks like this, external ICMP requests need to be blocked at the firewall level after confirmation of an ongoing flood. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, when the attack has been resolved, security team members can begin restoring non-critical services, restoring damaged systems, and communicating to organization leadership. |

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