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

|  |  |
| --- | --- |
| **Summary** | Multiple employees reported earlier this week that the organization's network services had suddenly ceased functioning. The network had been disturbed by a deluge of ICMP packets, it was revealed. The requests came from a variety of sources, culminating in a Distributed Denial of Service (DDoS) attack that generated an ICMP flood across an unconfigured firewall. Because the network was overloaded with ICMP requests, any normal internal network traffic was unable to reach any network resources. |
| Identify | The incident management team examined the network devices, firewalls, and access restrictions used in the attack to uncover security flaws. The team discovered that one of the organization's firewalls had been left unconfigured, with no port blocking or IP rules in place. The subsequent disruption left no business activities or revenue-generating services available for a total of two hours. against identify any damaged or stolen data, any data stored on the network must be compared against backups. |
| Protect | To limit the number of incoming ICMP packets, the team installed a new firewall rule, source IP address verification for firewalls, network monitoring software for aberrant traffic patterns, and an Intrusion Detection/Prevention System (IDS/IPS) system to filter suspicious network behavior. Furthermore, the team will develop new baseline configurations for all firewalls to verify that all firewalls are secure. |
| Detect | To detect similar attacks and anomalies that could lead to attacks, the team will monitor all incoming network traffic from IP addresses outside the internal network using firewall logging tools and an IDS. The team will also evaluate moving to a Next Generation Firewall (NGFW) based on how much the organization would benefit from capabilities like as intrusion protection. |
| Respond | The team modified the firewall and security rules to detect ICMP floods and similar request flood attacks. The targeted firewall has been reconfigured with robust security rules to match the baseline configuration. The reason, response, and outcomes of the incident have been communicated to all security personnel. We have notified senior management of this incident, and they will work with content teams to notify customers of the outage. Management must also notify law police and other entities as needed by local laws. |
| Recover | The impacted server has been restored to its original configuration and is fully operational. All data or assets associated with the server have been confirmed to have been restored to their most recent backups, which should have been taken the night before. External ICMP requests must be stopped at the firewall level after confirmation of an ongoing flood for future attacks like this. Then, to reduce internal network traffic, all non-critical network services should be disabled. Following that, priority should be given to restoring vital network services. Finally, once the attack has been addressed, members of the security team can begin restoring non-critical services, restoring damaged systems, and interacting with company leadership. |

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