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

|  |  |
| --- | --- |
| **Summary** | Earlier this week, several employees reported that the organization’s network services suddenly stopped working. It was found that the network had been hit by a large number of ICMP packets, which led to a Distributed Denial of Service (DDoS) attack. The ICMP flood came from multiple sources, and because the firewall wasn't properly set up, it couldn't stop the attack. As a result, normal network traffic couldn't access any resources, as the network was overwhelmed by the flood of ICMP requests. |
| Identify | The incident management team reviewed the network devices, firewalls, and access policies to find security weaknesses. They discovered that one of the organization's firewalls had not been configured, lacking any rules for blocking ports or controlling IP access. This led to a complete network outage, causing 2 hours of downtime where no business operations or revenue-generating services were available. The team now needs to compare stored data with backups to check for any data that might have been damaged or stolen during the attack. |
| Protect | The team has put in place a new firewall rule to control the rate of incoming ICMP packets and to verify the source IP addresses for firewalls. They are also using network monitoring software to detect unusual traffic patterns and have implemented an Intrusion Detection/Prevention System (IDS/IPS) to filter out suspicious activity on the network. Furthermore, the team will establish new baseline configurations for all firewalls to ensure that they all meet secure standards. |
| Detect | To identify similar attacks and any unusual activities that might lead to future attacks, the team will use firewall logging tools and an Intrusion Detection System (IDS) to monitor all incoming network traffic from IP addresses outside the internal network. They are also considering switching to a Next Generation Firewall (NGFW) to take advantage of its features, such as intrusion protection, if it would significantly benefit the organization. |
| Respond | The team has updated the firewall and security rules to identify ICMP floods and similar types of request flood attacks. The affected firewall has been strengthened with security rules that align with the established baseline configuration. All security staff have been informed about the cause of the attack, the response taken, and the outcomes. Upper management has also been notified about the incident, and they will collaborate with the content teams to inform customers about the outage. Additionally, management will need to notify law enforcement and other relevant organizations as required by local laws. |
| Recover | The affected server has been restored to its baseline configuration and is now fully operational. All data and assets related to the server have been verified and reverted to the most recent backups, which were made the previous night.  To prepare for future attacks like this, external ICMP requests should be blocked at the firewall level once a flood is confirmed. Then, non-critical network services should be halted to lessen internal traffic. After that, critical network services should be restored first. Once the attack is resolved, the security team can start restoring non-critical services, fixing any damaged systems, and communicating updates to the organization's leadership. |

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