**Incident Report Analysis**

|  |  |
| --- | --- |
| **Summary** | Earlier this week, several employees reported a sudden outage in the organization’s network services. It was later determined that the disruption was caused by a surge of ICMP packets flooding the network. These requests came from multiple sources, indicating a Distributed Denial of Service (DDoS) attack that exploited an unconfigured firewall. As a result, the influx of ICMP requests overwhelmed the network, preventing normal internal traffic from accessing network resources. |
| Identify | The incident management team conducted an audit of the network devices, firewalls, and access policies linked to the attack to uncover security vulnerabilities. They discovered that one of the organization’s firewalls had been left unconfigured, lacking port blocking and IP rules. This led to a complete outage lasting two hours, during which no business operations or revenue-generating services were accessible. Additionally, all data stored in the network must be compared to backups to determine if any information was compromised or lost. |
| Protect | The team has introduced several security measures, including a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification for firewalls, and network monitoring software to detect abnormal traffic patterns. They’ve also implemented an Intrusion Detection/Prevention System (IDS/IPS) to filter suspicious network activity. Furthermore, the team will establish new baseline configurations for all firewalls to ensure they meet a consistent and secure standard. |
| Detect | To identify similar attacks and potential threats, the team will utilize firewall logging tools and an IDS to monitor all incoming traffic from external IP addresses. Additionally, they are considering upgrading to a Next Generation Firewall (NGFW) to take advantage of features like intrusion prevention, depending on the organization’s needs. |
| Respond | The team has updated firewall and security rules to detect ICMP floods and similar request-based attacks. The affected firewall has been strengthened to align with the baseline security configuration. All security staff have been briefed on the incident, including its cause, response, and outcome. Upper management has been informed and will collaborate with content teams to notify customers about the outage. Additionally, management will coordinate with law enforcement and other relevant organizations as required by local regulations. |
| Recover | The affected server has been restored to its baseline configuration and is now fully operational. All server-related data and assets have been verified against the most recent backups, which should date back to the previous night. To mitigate future attacks, external ICMP requests should be blocked at the firewall level once a flood is confirmed. Non-critical network services should then be halted to minimize internal traffic, while critical services are prioritized for restoration. After the attack is resolved, the security team can focus on bringing non-critical services back online, repairing any damaged systems, and updating organizational leadership. |

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