**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company was the target of a DDoS attack that compromised our internal network for 2 hours before it was resolved. The attack method was a flood of ICMP packets that made it impossible for traffic to access resources on the network. Upon investigation it was discovered that the attack was possible due to an unconfigured firewall. |
| Identify | An attacker or attackers undertook a DDoS attack using ICMP packet flooding, exploited through an unconfigured firewall, which disrupted all normal traffic within the internal network. |
| Protect | The security team added a new firewall rule to limit the rate of incoming ICMP packets, stopped non-critical network services to restore critical services, and implemented an IDS/IPS system to filter traffic from these packets based on suspicious characteristics. |
| Detect | In the firewall, source IP address scanning has been configured to check for possible spoofed IP addresses in incoming packets, and monitoring software has been implemented to identify abnormal traffic patterns. |
| Respond | To avoid or mitigate future incidents, it is necessary to periodically check the monitoring software, IDS/IPS system and firewall rules, be aware of suspicious activity alerts issued through monitoring software and investigate any suspicious and abnormal activity as soon as possible. In the event of a successful attack, isolate the affected systems to prevent the spread of the attack and recover critical systems and services affected in the incident. The team also commits to reporting the incident to management and, if necessary, to law enforcement. |
| Recover | To recover from such an attack, normal traffic and access to network services must be returned to the functional state. All non-critical network services should be stopped and critical services should be restored as soon as possible. After packet flooding is controlled and terminated, non-critical services must be restored. |

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