**Incident report analysis**

| **Summary** | This morning our organization, a multimedia company, experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, our organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. | | |
| --- | --- | --- | --- |
| Identify | After investigating the security event we found that a malicious actor sent a flood of ICMP pings into the company’s network through an unconfigured firewall, known as an ICMP flood attack. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack | | |
| Protect | The network security team has implemented new policies to prevent future attacks: A new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | To detect new attacks in the future, the team will regularly configure the firewall and use an intrusion detection system to monitor all incoming traffic from the internet. | | |
| Respond | In future events, security team will contain and neutralize affected systems to prevent full network disruption. The team will check for any suspicious activity and restore any systems that were critically affected during the attack. The team will also inform upper management and contact the appropriate authorities on this matter. | | |
| Recover | In order to recover from the DDos attack, systems will need to be converted back to their normal state. ICMP flood attacks will be blocked by the firewall in the future. Non-critical network services will be stopped to reduce internal network traffic. Next, critical network services will be restored first. Once they are restored, non-critical network services will be brought back online. | | |

| Reflections/Notes: |
| --- |