**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | Our organization recently experienced a DDOS attack, which compromised the Internal network for 2 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. |
| Identify | The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | **To address this security event, the network security team implemented:**   * **A new firewall rule to limit the rate of incoming ICMP packets** * **Network monitoring software to detect abnormal traffic patterns** * **An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics** * The network security team implemented a **Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets** |
| Detect | The network security team implemented a **Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets** |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. |

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