**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.  During the attack, the 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 | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets |
| Detect | The network security team implemented a Network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Respond | The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Recover | The team will ensure that affected systems are recovered to normal operation as quickly as possible. This may involve restoring from backups or applying system patches to address vulnerabilities exploited during the attack. Then they will conduct a lessons-learned session with your incident response team to identify areas for improvement in your security processes. |

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