**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The organization recently 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. The incident was responded to and |
| Identify | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Protect | In the future the company plans to implement a new firewall rule to limit the rate of incoming ICMP packets and to do source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Also plans to invest in an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | To detect malicious traffic in the future the company’s cybersecurity team will use a network monitoring software to detect abnormal traffic patterns. |
| Respond | 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. |
| Recover | Since this was only a DDoS attack and no data was corrupted or stolen there is no need to restore anything from backups but rather to just implement the new firewall rules and monitor the network further for any more IoC’s (Indicators of comprimise). |

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