**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company recently came under a DDoS attack, which compromised the internal network for about two hours untill it was resolved by the security team.  During the attack, the company’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 investigated the security breech. 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 incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.  The network security team implemented the following measures:   * 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 * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | 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. |
| Respond | The security team responded by configuring the firewall in order to limit the amount of ICMP packets coming in and going out of the internal network.  The staff were educated of the effects of ping flood as to the impacts it can have over the entire company’s services.  The management was adequately informed of the incident and steps taken in order to contain it. It was recommended that periodic internal network audit must be in the day-to-day policy of the organization. |
| Recover | The team will recover all services of the organization both critical and non-critical ones once the DDos attack had been contained. |

|  |
| --- |
| s |