**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | A security event was reported when all network services suddenly stopped responding. The disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. I responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. |
| **Identify** | A malicious actor(s) targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state. |
| **Protect** | I implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| **Detect** | Firewall source IP address verification was configured to check for spoofed IP addresses on incoming ICMP packets and network monitoring software was implemented to detect abnormal traffic patterns. |
| **Respond** | The affected systems were isolated to prevent further disruption to the network. Then, critical systems were restored. Network logs were analyzed to check for suspicious and abnormal activity and all incidents/findings were reported to management. |
| **Recover** | Access to network systems and services were restored to a normal functioning state. Moving forward, any external ICMP flood attacks will be blocked at the firewall. |