# Incident report analysis

## Instructions

| | |
|---|---|
| **Summary** | This morning we experienced network services stoppage for about 2 hours during that time normal internal traffic was unable to access network resources. On further inspection through logs our team concluded that our network was flooded with ICMP packets from multiple sources. It is a DDoS attack and due to it our network services were down. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Investigation team 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. |
| Identify | The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that our firewall was not configured properly to deal with DDoS attacks. A malicious actor took advantage of it and flooded our network with ICMP packets from multiple sources and that resulted in our internal network unable to access network resources. |
| Protect | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets as well Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets to prevent future attacks. Additionally we will implement Network monitoring software to detect abnormal traffic patterns with an IPS system (intrusion prevention system) to filter out some ICMP traffic based on suspicious characteristics. |

| | |
|---|---|
| Detect | To detect future Dos or DDoS attacks we are implementing an IDS system (intrusion detection system) to detect abnormal traffic patterns. And we will create alerts for incoming ICMP packets coming from same source in a short span of time. |
| Respond | For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. 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: |