**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. The cybersecurity team found that a malicious actor had sent a flood of ICMP packets into the company’s network through an unconfigured firewall. This allowed the attacker to overwhelm the network through a DDoS attack. The team responded by blocking incoming ICMP packets, stopping non-critical services and restoring the critical ones. |
| **Identify** | The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The attacker was able to flood the network through an unconfigured firewall. The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| **Protect** | To prevent future attack, the network security team implemented the following: 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** | To detect future attacks, the team will use a network monitoring software to detect abnormal traffic patterns, IDS and IPS to monitor all incoming traffic from the internet. |
| **Respond** | The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| **Recover** | To recover from ICMP flooding all critical network services need to be restored. All non-critical services should be stopped to reduce network traffic. When the ICMP packets have timed out, all non-critical services can be restored. |