**Incident report analysis**

| **Summary** | The company experienced a recent DDoS attack, where all network services suddenly stopped responding which compromised the internal network of the organization. It took about 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 management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company’s cybersecurity team then investigated the security event. It was found that a malicious actor had sent a flood of ICMP pings into the company’s network. | | |
| --- | --- | --- | --- |
| 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 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 | To address this security event, the network security team implemented:   * 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 cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. | | |
| Respond | Thet team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. For future security events, the cybersecurity team will isolate the affected system so that the attack surface is reduced, then will monitor the network log to detect any malicious or abnormal activity. The team then informed 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. | | |