**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | On this day, the company was subjected to a DDoS attack using ICMP packets. The security team noticed a vulnerability that was exploited by the attacker. The vulnerability was a firewall device that was not configured to properly verify ICMP packet traffic. This allowed the attacker to disrupt the organization's internal network services for two hours. The security team then responded to the influx and temporarily blocked all ICMP packets. Non-critical network devices were also shut down for recovery, allowing traffic to continue on critical network devices. |
| Identify | The incident management team reviewed the systems, devices, and access policies involved in the attack to identify vulnerabilities. The team found that a malicious attacker exploited a configuration vulnerability in the firewall to prevent ICMP messages from being blocked, and then launched a denial-of-service attack against the organization using ICMP floods. Upon initial review, the company appears to have been down for two hours. |
| Protect | The network security team has 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 | To detect new ICMP flooding or any DDOS attacks in the future, the network security team will use a firewall logging tool and an intrusion detection system IDS\IPS to monitor all incoming traffic from the internet. |
| Respond | The team Blocked all the ICMP traffic temporary, and fixed the firewall gab that was discovered. We informed upper management of this event and they will contact our customers by mail to inform them about the temporary denial that happened to our services. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Recover | The company's cybersecurity team will prepare services for the return to operation after taking all necessary security measures and fixing the firewall vulnerability. We have informed employees to review their firewall rules weekly and monitor incoming internet traffic to respond quickly to any future incidents. |

|  |
| --- |
| Reflections/Notes: |