**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The comapny recently experienced an ICMP Flood DDoS attack, which compromised the internal network for two hours until it was resolved. The incident management team responded to the attack by blocking all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | The cybersecurity team found an unconfigured firewall which was used by a malicious attacker to run a Distributed Denial of Service (DDoS) attack. |
| Protect | The team has implimented a new firewall rule to limit the rate of incoming Internet Control Message Protocol (ICMP) packets, added a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, added network monitoring software to detect abnormal traffic patterns, and added an Intrusion Prevention System (IPS) to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | To detect new unauthorized access in the future, the team will use an Intrusion Detection System (IDS) to monitor all incoming traffic from the internet. |
| Respond | The team responded to the attack by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. With the new security measures described above, the team will be able to respond to incidents like this in future by having a detection system to alert the team of suspicious activity and a prevention system to filter out suspicious traffic. |
| Recover | The team has recovered from the attack. The incident management team prioritized restoring critical network services. After that, the team brought back up all non-critical network services. |