**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The organization experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the services stopped due to an incoming flood of ICMP packets.  The attack was stopped by blocking the ICMP packets, stopping non-critical systems and restoring the critical systems. |
| Identify | The incident team audited firewalls and network traffic to identify the gap in security. The team found that the firewall was not configured for the vulnerability that allowed the malicious actor to flood the network with ICMP pings. Detected attack was a DDoS attack and compromised the internal network for two hours. |
| Protect | The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets. They updated their IDS/IPS system to filter the suspicious ICMP traffic. |
| Detect | The cybersecurity team also added a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. They also updated their network monitoring software to detect abnormal traffic patterns. |
| Respond | To prevent the spread of the attack and reduce the size of possible damage, the affected systems will be isolated. Then, critical systems and services will be restored. After that, logs will be checked for suspicious and abnormal activities. Finally, the team will report the incident to their managers and legal authorities if necessary. |
| Recover | To recover from a DDoS attack with ICMP flooding, network systems must be restored to functional state. Considering external ICMP flood attacks will be blocked at the firewall, first the non-critical networks should be stopped to reduce the traffic volume. Then, critical systems should be restored. Finally, if the ICMP flood was stopped successfully and the packets timed out, non-critical systems can be brought back online. |

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