**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. The company network was under DDOS attack. The company’s cybersecurity team found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall which was primary vulnerability that served as the basis of this DDOS attack. Normal internal network traffic could not access any network resources for 2 hours. The incident management team responded by configuring firewall, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | The company’s cybersecurity team investigated the security event. They 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 | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets and verification of source IP address to check for spoofed IP addresses on incoming ICMP packets. |
| Detect | To detect and prevent from future DDOS/DOS and other suspicious activities the network security team has installed Intrusion detection system/Intrusion prevention system and network monitoring software to detect abnormal traffic patterns. |
| Respond | For future security events, the cybersecurity team will isolate the affected system to prevent from further disruption. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. For future security purpose the team will keep record of logs and if they notice any suspicious activity the security team should report it to higher authorities. |
| Recover | As it was the DDOS attack the organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets that needed to be restored. In future such attacks can be avoided by the configured firewall which can limit the external ICMP packets. Further all the non-critical activities should be stopped to reduce network traffic and then the network services should be restored on priority bases and once the ICMP packet flood timed out then they can bring all non-critical systems back online. |

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