**INCIDENT REPORT ANALYSIS**

|  |  |
| --- | --- |
| **SUMMARY** | The company experienced a security event when all network services suddenly  stopped responding. The Cybersecurity team found the disruption was caused  by a distributed denial of services (DDoS) attack through a flood of incoming  ICMP packets. The team responded by blocking the attack and stopping all  non-critical network services, so that critical network services could be  restored. |
| **IDENTIFY** | The company has assets to protect in order to keep daily business activities from interruption. Assets such as website pages, safety in the internet space, firewalls, public facing web server(s), internal servers as well as social media platforms.  We have identified possible threat to these assets which are web page login brute forcing, Denial of Service(DoS)/DDoS as well as account hijacking(social media) among various other threats. |
| **PROTECT** | The Cybersecurity team implemented firewall to limit incoming network traffics and an IDS/IPS system to filter out packets based on suspicious characteristics/signatures.  Rate limiting has also been configured to prevent brute forcing of user accounts and any other possible attack.  Threat awareness training for the company`s staff was organized to get them abreast of possible security threat and social engineering vises. |
| **DETECT** | The company’s Cybersecurity team then investigated the security even and found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall.  A malicious actor or actors targeted the company with an ICMP flood attack.  The web server is no longer accessible and clients are stranded as daily work flow has been interrupted.  The entire internal network was also affected. |
| **RESPOND** | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services.  A new firewall rule to limit the rate of incoming ICMP packets  An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics  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.  For future security events, the Cybersecurity team will isolate affected systems  to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. |
| **RECOVER** | To recover from a DDoS attack by ICMP flooding, access to network services  need to be restored to a normal functioning state. In the future, external ICMP  flood attacks can be blocked at the firewall. Then, all non-critical network  services should be stopped to reduce internal network traffic. Next, critical  network services should be restored first. Finally, once the flood of ICMP  packets have timed out, all non-critical network systems and services can be  brought back online. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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