**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | Network traffic suddenly stopped during normal operations and no network services could be accessed. The incident management team uncovered a flood of ICMP packets congesting the network. They concluded a DDoS attack prevented the network from responding to any other request halting all network traffic and that this was possible because the firewall was unconfigured. The team blocked the incoming packets and any services that were not crucial to normal operations so that critical network services could be restored. |
| Identify | When the network services stopped responding, the security team analyzed the network logs and observed a flood of ICMP packets congesting the network. This DDOS prevented the network from responding to any other request halting the network. |
| Protect | The team will first block or limit the incoming packets and or the Ip’s associated with the transmissions, update and configure the firewall, block any ports unnecessary for operations, and restore the company’s network so it is operational for business. |
| Detect | The team implemented an IPS or IDS alongside regular monitoring via SIEM tools to regulate traffic and prevent similar threat occurrence. |
| Respond | In the future similar attacks will be mitigated by implementing:   * Isolating affected systems. * 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(or alert to) some ICMP traffic based on suspicious characteristics. * Restoration of critical services/systems. * Report all incidents to the appropriate stakeholders and legal authorities when necessary. |
| Recover | To recover from a DDoS, the intruding packets need to be identified and blocked via firewall, and critical network services need to be restored for necessary operations. Following these actions, firewall rules and monitoring need to be created and enforced, as well as the education and instruction of involved parties on the new operations and procedures with an update to the company’s playbook. |

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