**Incident report analysis**

Date: 09/12/2024

Nela\_officer

|  |  |
| --- | --- |
| **Summary** | The company experienced an attack, which compromised the internal network for two hours until it was resolved. The organization’s network services suddenly stopped responding and the normal internal network traffic could not access any network resources.  The incident management team responded by blocking incoming input in the network, stopping all non-critical network services offline, and restoring critical network services.  The company’s cybersecurity team found that a malicious actor had sent a flood of packets 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.  To address this security event, the network security team implemented:   * 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 some ICMP traffic based on suspicious characteristics   To mitigate the risk and protect against future attacks it was created a plan to improve the company’s network security describes as follow: |
| Identify | Implement regular security audits to identify vulnerabilities in the network |
| Protect | The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.  Implement an intrusion prevention system (IDS) for the firewalls and procedures and policies to keep updates the configuration of all the devices in the network. |
| Detect | Implement and regular use of an information and event management system (SIEM) tool to monitoring continuously the network |
| Respond | * 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. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. * Guarantee the implementation of this plan. |
| 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: - |