**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | At 11:30 am, the IT department promptly notified the security team of a disruption in network services. The security team swiftly initiated an investigation, which revealed that the outage was triggered by a DDoS attack inundating the network with ICMP packets. Recognizing the severity of the situation, the team immediately took action by blocking all incoming ICMP packets. This decisive response allowed them to restore the network services by 13:30 pm.  Further examination during the investigation uncovered that the malevolent actor exploited an unconfigured firewall to launch the flood of ICMP pings.  With the incident successfully addressed, the security team proactively implemented a series of robust measures to rectify vulnerabilities and fortify the network against potential future attacks. These actions aim to bolster security and safeguard the network's integrity in the long run. |
| Identify | Malicious actor/s made an ICMP flood attack to the company network and stop the network services. |
| Protect | Security team implemented new firewall rules to limit incoming ICMP packets and an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics. |
| Detect | Security implemented source IP address verification on the firewall to check spoofed IP addresses on incoming ICMP packets. |
| Respond | In the future, the team will promptly isolate the affected systems and initiate restoration procedures. Following that, a thorough investigation will be conducted by the security team to identify the root cause of the attack. Based on the findings, they will then proceed to enhance the security measures with the goal of preventing similar incidents from occurring in the future. This proactive approach will enable the team to bolster the network's defenses and ensure a more secure environment going forward. |
| Recover | To recover from a DDoS attack, the first step is to promptly contain the attack by isolating the affected systems. Once the threat has been neutralized and the attack's impact minimized, the next crucial phase involves restoring the affected systems to normal operations. This process entails diligently verifying and ensuring the integrity of each system, followed by meticulous monitoring to guarantee a complete return to a stable and secure state. By following these steps, the organization can effectively recover from the DDoS attack and resume normal business operations with minimal disruption.Principio del formularioFinal del formulario |

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