**Incident report analysis of a multimedia company**

|  |  |
| --- | --- |
| **Summary** | The organization encountered a security incident marked by the abrupt cessation of all network services. Upon investigation, the cybersecurity team identified the root cause as a distributed denial of service (DDoS) attack, orchestrated through an overwhelming influx of ICMP packets. Swiftly, the team counteracted the threat by implementing measures to block the attack and temporarily halting non-essential network services. This strategic response facilitated the restoration of critical network services to normalcy. |
| Identify | A malicious actor or group aimed the company and flood it ICMP flood attack, resulting in the widespread impact on the entire internal network. The imperative task at hand involved safeguarding and reinstating all vital network resources to ensure their return to operational functionality. |
| Protect | Cybersecurity team have forged a formidable defense, weaving a tapestry of protection against potential cyber threats. A cutting-edge firewall incantation now weaves its magic, conjuring a shield that restricts the influx of ICMP packets, while an enchanted IDS/IPS system discerns and banishes suspicious ICMP entities with a keen eye for mystical anomalies. |
| Detect | The cybersecurity team set up the firewall to make sure incoming ICMP packets are legit by checking their source IP addresses. They also installed monitoring software to spot any weird traffic patterns on the network. |
| Respond | If there's a security issue in the future, the cybersecurity team will separate the affected systems to stop more problems in the network. They'll try to fix any important systems and services that got messed up. After that, they'll look at network logs to find anything strange. The team will also tell the higher-ups and legal authorities if needed. |
| Recover | To bounce back from DDos attack by ICMP flooding, we need to get our network services back to normal. In the future, we can stop outside ICMP flood attacks with the firewall. Then, we should pause less important network services to cut down on inside traffic. After that, we bring back the really important services first. Once the flood of ICMP packets has calmed down, we can turn on the rest of the network systems and services. |