**Incident report analysis**

| **Summary** | Recently, a security event occurred when all network services suddenly  stopped responding. The cybersecurity team found the disruption was caused  by DDoS attack, which overwhelmed the internal network with ICMP flood, causing network services to fail. The incident management team responded by blocking ICMP packets, shutting down non-essential services, and restoring critical ones. | | |
| --- | --- | --- | --- |
| Identify | A malicious actor exploited an unconfigured firewall to flood the network with ICMP packets. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state. | | |
| Protect | In order to prevent future incidents, the network security team implemented new firewall configurations and an IDS/IPS system to filter out suspicious ICMP traffic. | | |
| Detect | To detect new unauthorized access attacks in the future, the team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and a network monitoring software, notably a firewall logging tool, to monitor all incoming traffic from the internet. | | |
| Respond | For future security events, the cybersecurity team will implement an enhanced incident response strategy, which will involve isolating affected systems to prevent further disruption to the network, restoring critical systems and services that were disrupted by the event, and analyzing network logs to monitor suspicious and abnormal activity. Additionally, the team will report all incidents to upper management and appropriate legal authorities, if applicable, to ensure transparency and compliance. | | |
| Recover | To remediate a DDoS attack via ICMP flooding, it's essential to restore network services to their normal state. For future protection, external ICMP flood attacks can be blocked at the firewall. A recommended approach is to initially stop all non-essential network services to decrease internal network traffic. Subsequently, prioritize the recovery of critical network services. Once the ICMP packet flood has expired, gradually reintroduce non-critical network systems and services. | | |

| Reflections/Notes: |
| --- |