**ADELEKE ODUNAYO JOSEPH**

**Incident report analysis for an organization recently experienced a DDoS attack**

|  |  |
| --- | --- |
| **Summary** | The company experienced a distributed denial of service (DDoS) attack that disrupted network services for approximately two hours. The attack was initiated by a malicious actor who flooded the company's network with ICMP (Internet Control Message Protocol) packets, causing network services to become unresponsive. The incident management team responded promptly by blocking incoming ICMP traffic and temporarily taking non-critical network services offline to prioritize the restoration of critical services. |
| Identify | A malicious actor or actors flooded the company with an ICMP attack.  The entire internal network was affected. All critical network resources needed  to be secured and restored to a functioning state. |
| Protect | The cybersecurity team update firewall rules to include limiting the rate of incoming ICMP packets and implementing source IP address verification to prevent spoofing. |
| Detect | The cybersecurity team deploy network monitoring software capable of detecting abnormal traffic patterns, such as sudden increases in ICMP traffic or other anomalous behavior. |
| Respond | The cybersecurity team ensure that the incident response plan includes specific steps for addressing DDoS attacks, such as isolating affected systems and restoring critical network services.  Cybersecurity team also conduct regular tabletop exercises and simulations to test the effectiveness of the incident response plan and identify areas for improvement. |
| Recover | Establish backup and recovery procedures to quickly restore affected systems to normal operation in the event of a security incident.  External ICMP flood attacks can be blocked at the firewall in the future.  Document lessons learned from the DDoS attack incident and use them to update and improve network security policies, procedures, and controls. |

|  |
| --- |
| **Reflections/Notes:** By following this plan based on the NIST CSF, the organization can strengthen its network security posture, mitigate the risk of future DDoS attacks, and improve overall resilience to cybersecurity threats. |