Incident report using the NIST CSF

|  |  |
| --- | --- |
| Summary | A security incident was experienced in the company whereby the network services suddenly stopped responding. The security team discovered that it was a distributed denial of service(DDoS) attack through a flood of ICMP packets. The team responded by blocking incoming ICMP packets,stopped all non-critical network services offline, and restored critical network services. |
| Identify | A malicious actor disrupted the internal network with ICMP flood pings through an unconfigured firewall which affected the entire internal network. The critical network services must be secured and restored to a functioning state. |
| Protect | A new firewall rule to limit the rate of incoming ICMP packets was implemented by the Cybersecurity team to protect the network and an IDS/IPS system was also used to filter out some ICMP traffic with suspicious characteristics. |
| Dectect | The Cybersecurity team configured a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was implemented to detect abnormal traffic patterns. |
| Respond | For coming security events,the affected system should be isolated first to prevent further disruptions to the network. Attempts should be made to restore any critical network affected. Thereafter,the network logs should be analyzed to dectect abnormal and suspicious patterns. The team should report the incident to the management. |
| Recover | To restore the network to normal functioning state, incoming ICMP packets must be blocked by the firewall and all non-critical networks should be stopped to reduce traffic. The critical networks should be restored first,after stabilizing non-critical network system can be restored. |