**Incident report analysis**

Applying the NIST CSF reactively to an incident analysis to prevent a repeat of such incident.

|  |  |
| --- | --- |
| **Summary** | Recently, the organization’s internal network was compromised by an attack for about two hours. During the attack, network services suddenly stopped responding due to a distributed denial of service (DDoS) attack. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company’s cybersecurity team investigated the event and found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall overwhelming the network. Thus, preventing legitimate users from accessing normal network resources. |
| Identify | Through their investigation and analysis of the security event artifacts, the cybersecurity team concludes that the malicious attacker overwhelmed the network through an ICMP flood attack. |
| Protect | To address this security event, the network security team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets. * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. * Network monitoring software to detect abnormal traffic patterns. * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Also, a SIEM tool will be incorporated to collect and analyze all network traffic with alert system configured for abnormalities. |
| Respond | For future security events, the cybersecurity team will follow the steps outlined below:   * Isolate affected systems to prevent further disruption to the network. * They will attempt to restore any critical systems and services that were disrupted by the event. * Then, the team will analyze network logs to check for suspicious and abnormal activity. * The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. |

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