**Security Hardening using NIST CSF Incident report analysis**

| **Summary** | The organization recently experienced a Distributed Denial of Service (DDoS) attack that disrupted internal network operations for approximately two hours. The disruption was caused by a large volume of ICMP packets flooding the network, which led to service outages across multiple systems.  The incident response team acted quickly by blocking incoming ICMP traffic at the firewall, taking non-essential services offline to reduce network load, and restoring critical services to resume operations.  Following a joint investigation with the cybersecurity team, it was discovered that the attacker was able to exploit a misconfigured firewall, which had not been properly set to filter ICMP traffic. This oversight allowed the attacker to successfully launch an ICMP flood — a type of DDoS attack that overwhelms systems by sending excessive ICMP echo requests (pings), rendering network services temporarily unavailable. | | |
| --- | --- | --- | --- |
| Identify | Upon investigation, the company's cybersecurity team discovered that the attack originated from a malicious actor who exploited an unconfigured firewall to send a high volume of ICMP packets into the network. This misconfiguration created a vulnerability that allowed the attacker to launch a successful ICMP flood, overwhelming the internal network infrastructure. As a result, the organization’s core network resources were impacted, requiring immediate containment efforts and the restoration of critical systems to resume normal operations. | | |
| Protect | To address the issues with the attack the cybersecurity team has implemented a new firewall rule to limit the rate of incoming ICMP packets to the company’s network, Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, Implemented a network monitoring software to detect abnormal traffic patterns and Installed an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics | | |
| Detect | To detect and prevent new attacks like this. The cybersecurity team has configured the firewall to do a Source IP address verification to check for spoofed IP addresses on incoming ICMP packets, Installed a network monitoring software to detect abnormal traffic patterns as well as an IDS/IPS system to detect and report suspicious patterns. | | |
| Respond | In response to future security incidents, the cybersecurity team will take immediate steps to contain the threat by isolating any compromised systems. Priority will be given to restoring essential systems and services affected by the disruption. Once stability is ensured, the team will review network logs to identify any unusual or suspicious activity. All findings and incident details will be communicated to senior management and, if necessary, reported to legal or regulatory authorities. | | |
| Recover | To recover from an ICMP flood DDoS attack, the first priority is to bring network services back to normal operation. Moving forward, similar attacks can be mitigated by configuring the firewall to block external ICMP traffic. During recovery, it's important to temporarily shut down non-essential services to reduce internal load on the network. Restoration efforts should focus on bringing critical services back online first. Once the attack subsides and ICMP traffic returns to normal, non-critical systems can then be safely reactivated. | | |

| Reflections/Notes: |
| --- |