**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | A multimedia company that offers web design, graphic design and social media marketing solutions to small businesses have experienced a DDoS attack, which compromised the internal network for 2 hours, until it was resolved. The organizations network service suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded. By blocking the incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services. After investigating the security incident, we found that a malicious actor had sent a flood of ICMP pings into the company’s network through and unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. 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. |
| Identify | The team audited the security incident and found that a malicious actor had sent a flood of ICMP pings into the company’s network through and unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | To safeguards the systems and 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 team configured the Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented Network monitoring software to detect abnormal traffic patterns. |
| Respond | To respond any future security events the incident management team will blockthe incoming ICMP packets, stopping all non-critical network services offline and the team will attempt to restore the critical systems and services first that were disrupted by the network services shutdown. The team will report this incident to all the stakeholders and FBI Internet Crime Complaint Center (IC3) and National Cybersecurity Communications and Integration Center (NCCIC) |
| Recover | To recover from such security incidents in future, check all the network logs for malicious activity, the firewall can be configured to limit the ICMP packets. shut down all the network services and try to attempt to recover critical system and network services only. After the ICMP packets have timed out, all the non-critical network systems and services can be brought back. |

|  |
| --- |
| Reflections/Notes: The NIST CSF and its five core functions provide a framework of planning proactive to applying reactive measures to cybersecurity threats. These functions are essential for  ensuring that an organization has effective security strategies in place. An organization  must have the ability to quickly recover from any damage caused by an incident to  minimize their level of risk.  ● Identify: Manage security risks through regular audits of internal networks,  systems, devices, and access privileges to identify potential gaps in security.  ● Protect: Develop a strategy to protect internal assets through the implementation  of policies, procedures, training and tools that help mitigate cybersecurity threats.  ● Detect: Scan for potential security incidents and improve monitoring capabilities to  increase the speed and efficiency of detections.  ● Respond: Ensure that the proper procedures are used to contain, neutralize and  analyze security incidents and implement improvements to the security process.  ● Recover: Return affected systems back to normal operation and restore systems  data and assets that have been affected by an incident. |