**Incident report analysis**

| **Summary** | Last night the organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The organization's network services 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 incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company’s cybersecurity team then investigated the security event.  A malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. | | |
| --- | --- | --- | --- |
| Identify | The type of attack that occurred was a distributed denial of service (DDoS) attack. The malicious actor flooded the network with ICMP pings, the system that was affected during the attack was the company’s internal network, because of the unconfigured firewall. | | |
| Protect | The system that needs to be updated and changed to further secure the organization’s assets are the unconfigured firewall. Rules to the firewall and port filtering should be implemented immediately. | | |
| Detect | The team can monitor and analyze network traffic through the use of a SIEM and a packet sniffing tool, such as wireshark, or tcpdump. | | |
| Respond | The team can contain incidents and affected devices by taking it off of the network immediately and isolating the affected system within a sandbox environment.  Servers can be contained within a DMZ and isolated so that if the particular system is compromised by a malicious actor, it can now be dealt with in this environment, decreasing the likelihood of the threat actor pivoting out of this environment and other systems becoming compromised.  Using tcpdump, or wireshark can allow us to analyze the data from the incident to better understand how the attack happened and where.  There is no SIEM environment. In the future the company can implement better security by adopting a SIEM application. | | |
| Recover | The recovery plan has consisted of:   * 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 | | |

| 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. |
| --- |