Security Incident Analysis: ICMP Ping Flood 05-15-2024 #1

Globe Sistemas - Av. Libertador Jardin America

Report Overview

The situation will be analyzed using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The CSF is a voluntary framework consisting of standards, guidelines, and best practices for managing cybersecurity risk.

A quality cybersecurity incident report will be created and the CSF will be applied to demonstrate a proactive approach to security, improve communication and transparency with stakeholders, and enhance security practices within the organization. The CSF is scalable and can be applied in a wide variety of contexts.

It will identify which security measures should be implemented in response to business needs and determine what are the best options available with regards to network security.

Context

The context of the scenario is detailed below:

Conducted an incident analysis report as an external cybersecurity analyst for Globe Sistemas, a company that offers web design, app development, ecommerce, and social media marketing solutions to small businesses. The organization recently experienced a DDoS attack that compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly became unresponsive due to a flood of incoming ICMP packets. Normal internal network traffic was unable to access any network resources. The IT team responded by blocking incoming ICMP packets, taking all non-critical network services offline, and restoring critical network services.

As an analyst, I investigated the security event. I discovered that a malicious actor had sent a flood of ICMP pings to the company network through an unconfigured firewall. This vulnerability allowed the malicious attacker to invade the company network via a distributed denial of service (DDoS) attack.

To address this security event, as a network security measure I implemented:

* A new firewall rule to limit the rate of incoming ICMP packets
* Checking the source IP address on the firewall to check for spoofed IP addresses in incoming ICMP packets
* Network monitoring software to detect abnormal traffic patterns
* An IDS/IPS system to filter some ICMP traffic based on suspicious characteristics

As an analyst, I used this security event to create a plan to improve network security and create an overall security strategy for the company, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). I have divided the analysis into different parts:

* Identify security risks by periodically auditing internal networks, systems, devices, and access privileges to identify potential security breaches.
* Protect internal assets by implementing policies, procedures, training and tools that will help mitigate cybersecurity threats.
* Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
* Respond to contain, neutralize and analyze security incidents; implement improvements to the security process.
* Recover affected systems to normal operation and restore data and/or assets from systems that have been affected by an incident.

| **Summary** | The company experienced a security issue when all network services suddenly became unresponsive. The IT team discovered that the outage was caused by a distributed denial of service (DDoS) attack via a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. | | |
| --- | --- | --- | --- |
| **Identify** | One or more malicious actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be protected and restored to a functional state. | | |
| **Protect** | The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter 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 in incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. | | |
| **Reply** | For future security events, the cybersecurity team will isolate affected systems to prevent further network disruption. They will attempt to restore any critical systems and services that have been disrupted by the event. The team will then analyze network logs for suspicious and abnormal activity. The team will also report all incidents to senior management and appropriate legal authorities, if applicable. | | |
| **Recover** | To recover from an ICMP flood DDoS attack, access to network services must be restored to a normal working state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services must be stopped to reduce internal network traffic. Next, critical network services must be restored first. Finally, once the ICMP flood times out, all non-critical network systems and services can be brought back online. | | |