Incident Report Analysis

Utilizing the NIST Cybersecurity Framework for Security Incident Response

Wendy Alayon
17/06/2024 **@syszern**

Incident report analysis

Scenario

A cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses recently encountered a Distributed Denial of Service (DDoS) attack, which compromised the internal network for two hours until it was resolved.

During the attack, 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, taking all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They discovered that 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.

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

The cybersecurity analyst is tasked with using this security event to create a plan to improve the company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The analyst will use the CSF to navigate through the different steps of analyzing the cybersecurity event and integrate the analysis into a general security strategy. The analysis has been broken down into different parts in the template below. These can be explored here:

- **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.

- **Protect** internal assets through the implementation of policies, procedures, training and tools that 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 systems data and/or assets that have been affected by an incident.

Applying the NIST CSF core functions

Summary	The organization experienced a DDoS attack that disrupted its internal network, causing network services to abruptly become unresponsive and preventing access to any network resources. Upon investigation, the cybersecurity team determined that a malicious actor had flooded the company's network with ICMP pings through an improperly configured firewall, allowing them to overwhelm the network. In response, the incident management team swiftly blocked incoming ICMP packets, temporarily took non-critical network services offline, and restored critical network operations.
Identify	A malicious actor flooded the company's network with incoming ICMP packets by exploiting an improperly configured firewall, resulting in network overload. It affected the entire internal network, as normal internal traffic couldn't access any network resources.
Protect	The network security team implemented several measures to enhance security: introducing a new firewall rule to restrict the rate of incoming ICMP packets and integrating an IDS/IPS system to filter suspicious ICMP traffic based on specific characteristics.
Detect	The network security team added source IP address verification on the firewall to detect spoofed IP addresses in incoming ICMP

	packets and deployed network monitoring software to identify unusual traffic patterns.
Respond	In preparation for future cybersecurity incidents such as an ICMP flood attack, the team’s approach includes network segmentation, strict firewall rules for ICMP traffic, and rate limiting to prevent network overload. Advanced monitoring tools and IDS/IPS are also essential for promptly containing incidents. When an incident occurs, affected devices are promptly isolated, and thorough forensic analysis is conducted using network logs, system logs, and packet captures. Network logs are utilized for ICMP traffic analysis, system logs for anomaly detection, and packet captures for event reconstruction. The team is committed to restoring all critical systems and services that were disrupted during the event.
Recover	To recover from a DDoS attack by ICMP flooding in the future, the first priority is restoring network services to their normal state after addressing disruptions from the flood of ICMP packets. Firewall rules to block external ICMP flood attacks are implemented to help prevent potential incidents. Priority is given to restoring critical network services promptly once the attack is contained. Meanwhile, non-critical networks must be temporarily halted during attacks, and they will be restored after the ICMP packet flood subsides.