Portfolio Project

Responding to a Security Incident

Google Cybersecurity Professional Certificate

Prepared by :

Aleck Kitenge

1 Activity Overview

In this activity, you will use the knowledge you've gained about networks throughout this course to analyse a network incident. You will analyse the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and create an incident report. The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

2 Activity Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your 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. They found 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.

2 Activity Scenario cont.

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
As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy:

·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.

3 Incident Report Analysis

Summary

The company's network services abruptly became unavailable, prompting the cybersecurity team to investigate the cause of the disruption. They identified the incident as a distributed denial-of-service (DDoS) attack, characterized by a surge of incoming ICMP packets designed to overwhelm the network's resources. In response, the team implemented measures to block the attack and halt all non-essential network services to prioritize the restoration of critical services.

Identify

A malicious actor or group launched an ICMP flood attack against the company, impacting the entirety of the internal network. The immediate focus was to secure and restore all critical network resources to a fully operational state.

Protect

To enhance network security and mitigate the risk of future DDoS attacks, the cybersecurity team implemented a comprehensive defense strategy. They introduced a new firewall rule to restrict the rate of incoming ICMP packets, effectively throttling the flood of malicious traffic. Additionally, they deployed an IDS/IPS system to scrutinize incoming ICMP traffic and filter out suspicious packets based on pre-defined signatures, further bolstering network defenses.

3

Incident Report Analysis cont.

Detect

To strengthen network defenses and identify potential attacks, the cybersecurity team implemented a multi-pronged approach. They enabled source IP address verification on the firewall to identify and block incoming ICMP packets with spoofed IP addresses, effectively preventing adversaries from masking their true identities. Additionally, they deployed network monitoring software to continuously analyze network traffic patterns and detect anomalies that could indicate malicious activity.

Respond

In the event of future security breaches, the cybersecurity team will implement a multi-stage response plan to mitigate damage and restore operations. They will swiftly isolate affected systems to prevent the spread of the attack and further disruption to the network. Next, they will prioritize the restoration of critical systems and services that were impacted by the event. Following the restoration process, the team will conduct a thorough analysis of network logs to identify any suspicious or anomalous activity that may indicate the cause or scope of the attack. Additionally, they will report all security incidents to upper management and, if applicable, relevant legal authorities to ensure compliance with regulatory requirements and to initiate any necessary legal proceedings.

Recover

To effectively recover from an ICMP flood-based DDoS attack, the primary objective is to restore network services to their normal operational state. As a preventive measure, future external ICMP flood attacks can be effectively mitigated by implementing firewall rules that block such traffic. In the event of an attack, non-critical network services should be temporarily halted to reduce internal network traffic and alleviate the load on critical services. Subsequently, critical network services should be prioritized and restored first to ensure the availability of essential operations. Once the flood of ICMP packets has subsided, non-critical network systems and services can be gradually brought back online, carefully monitoring their performance and ensuring they function properly.