(Mock) Incident Report Analysis

A computer screen with text on it

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/17/24

**Table of Contents:**

Activity Overview (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2-3**

Incident Report Analysis (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3-4**

Reflection Notes (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**4**

**Activity Overview**

In this activity, you will use the knowledge you’ve gained about networks throughout this course to analyze a network incident. You will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and create an incident report that you can include as part of your cybersecurity portfolio documentation. The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. For a refresher, please review this reading about NIST frameworks and the five functions of the NIST CSF framework. Creating a quality cybersecurity incident report and applying the CSF can help you build trust and improve security practices within your organization.

The CSF is scalable and can be applied in a wide variety of contexts. As you continue to learn more and refine your understanding of key cybersecurity skills, you can use the templates provided in this activity in other situations. Knowing how to identify which security measures to apply in response to business needs will help you determine which are the best available options when it comes to network security.

**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.

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.

**Incident Report Analysis**

**Incident Summary:**

The multimedia company experienced a Distributed Denial of Service (DDoS) attack, causing a two-hour disruption to its internal network. The attack flooded the network with ICMP packets, overwhelming network resources and rendering critical services inaccessible.

**Identify Phase:**

Earlier today, employees began noticing the internal network was slower than normal until it stopped working all together. After reviewing the network traffic logs, our team saw a flood of ICMP packets incoming from multiple IPs that was overwhelming the internal network. Based on the evidence, we decided we were most likely under siege by an DDoS ICMP Flood Attack and that our first move should be to stop the attack.

**Protect Phase:**

The first actions we took in response to the attack were to block incoming ICMP packets, take the non-critical network services temporarily offline, and restore critical network functions from a recent backup.

**Detect Phase:**

Next, once we had halted the attack for the time being, we focused on finding the vulnerability that the threat actor(s) had exploited. Sure enough, we found an unconfigured firewall allowed the attack to penetrate the network.

**Respond Phase:**

In response, we implemented a new firewall rule to limit the rate of incoming ICMP packets and introduced source IP address verification on the firewall to prevent IP address spoofing. We also checked the configuration for all the critical network systems we restored for errors and notified leadership about the incident.

**Recover Phase:**

Finally, we completely restored the rest of the non-critical systems that were affected from a recent backup and did a full system review to check for proper configurations and ensure business continuity. Then we deployed a new network monitoring software to detect abnormal traffic patterns and integrated an IDS/IPS system to filter out suspicious ICMP traffic based on predefined characteristics so we wouldn’t be vulnerable to a similar attack again. Stakeholders were notified about the incident and that any changes made after the last backup wouldn’t be saved.

**Reflection Notes**

In addition to the measures already taken in the respond phase, our team recommends that the company introduce annual penetration testing, regular configuration/patch checks, and a restricted zone to further protect business critical systems. While the team’s response was swift and ultimately prevented a major loss, the attack could have been prevented with proper configuration of a single firewall. Details matter so it is important to be constantly vigilant and I believe the proposed recommendations will put our company on a path to continuous security posture improvement.