## Activity Overview

In this activity, we have to analyze a network incident. We will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and create an incident report that can include as part of cybersecurity portfolio documentation. The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Creating a quality cybersecurity incident report and applying the CSF can help build trust and improve security practices within organization.

The CSF is scalable and can be applied in a wide variety of contexts. Knowing how to identify which security measures to apply in response to business needs will help determine which are the best available options when it comes to network security.

## Scenario

Assume that 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 un-configured 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**

**Instructions**

You may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | Form of attack:- DDOS attack which means malicious actor flooded network with ICMP packets which are generally used to trouble shoot the network problems.  Root Cause:- Un-configured firewall is installed in the network  - As per the scenario given it is very clear that company network got attacked in the form of DDOS attack in which the malicious actor flooded ICMP packets to the internal network which lead to pause in the network functionality for 2 hours. All this was happened because of un-configured firewall in the network. |
| --- | --- |
| Identify | The Company's cyber security team found that a malicious actor had sent a flood of ICMP pings into the company’s network through an un-configured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. Because of this 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. |
| Protect | Present situation will not assure to protect the organization from future attacks. So we need to update the existing infrastructure in the view of security. Below are the changes required.  1. Configuring the firewall properly  2. Creating and implementing firewall rules to check each incoming data packet to examine whether the source IP address is genuine or spoofed IP address.  3. Implementing Intrusion Detection or Prevention Systems (IDS / IPS) to prevent the future attacks |
| Detect | From this experience we need to increase the network monitoring and need to take below actions and implement them as early as possible.  1. At firewall level examining each incoming data packet regarding the source and destination IP addresses, looking into the content of data packet to make sure it doesn't contain any malicious content which will harm the network and systems  2. Implementing Intrusion Detection System or Intrusion Prevention System  3. Keeping up to date with the Cyber Security Industry trends will help a lot to know about the latest trends in Attacks and Incident Response. |
| Respond | \* Proactively preparing action plan to respond to the cyber attacks saves lot of time  \* To address security events, 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   \* After recovering from the incident conveying the same to the company management in the form of Cyber Security Incidents Response Report. |
| Recover | \* By implementing firewall rules, verifying source IP address at incoming data packet, network monitoring, detecting abnormal traffic patterns, An IDS/IPS solutions organization recovered from the current DDOS attack |

| Reflections/Notes: |
| --- |

**Identify the type of attack and the systems affected:**

Determine what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet.

### Protect the assets in your organization from being compromised

Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

* What systems or procedures need to be updated or changed to further secure the organization’s assets?

Write your response in the incident report analysis template.

### Determine how to detect similar incidents in the future

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization’s network firewall.

For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet .

### Create a response plan for future cybersecurity incidents

After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

* How can you and your team contain cybersecurity incidents and affected devices?
* What procedures are in place to help you and your team neutralize cybersecurity incidents?
* What data or information can be used to analyze this incident?
* How can your organization’s recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template.

### Help your organization recover from the incident

Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.

Consider the following questions:

* What information do you need to be able to recover immediately?
* What processes are in place to help the organization recover from the incident?

Write your response in the “recover” portion of the worksheet.

**Applying the NIST CSF**

There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover.



*Image: 5 core functions of the NIST CSF*

These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Plans based on this framework should be continuously updated to stay ahead of the latest security threats. The core functions help ensure organizations are protected against potential threats, risks, and vulnerabilities. Each function can be used to improve an organization’s security:

Some questions to ask for each of the five core functions, include:

| Identify | Create an inventory of organizational systems, processes, assets, data, people, and capabilities that need to be secured:   * Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. * Process/Business environment: Which business processes were affected in the attack? * People: Who needs access to the affected systems? |
| --- | --- |
| Protect | Develop and implement safeguards to protect the identified items and ensure delivery of services:   * Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? * Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? * Data security: Is there any affected data that needs to be made more secure? * Information protection and procedures: Do any procedures need to be updated or added to protect data assets? * Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? * Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IDS), that should be implemented to protect against future attacks? |
| Detect | Design and implement a system with tools needed for detecting threats and attacks:   * Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? * Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? * Detection process: What tools are needed to detect security events, such as an IDS? |
| Respond | Design action plans for responding to threats and attacks:   * Response planning: What action plans need to be implemented to respond to similar attacks in the future? * Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? * Analysis: What analysis steps should be followed in response to a similar attack? * Mitigation: What responding steps could be used to mitigate the impact of an attack, such as off-lining or isolating affected resources? * Improvements: What improvements are needed to improve response procedures in the future? |
| Recover | Construct a plan and implement the framework for recovering and restoring affected systems and/or data:   * Recovery planning: How will resources be restored following an attack? * Improvements: Do any improvements need to be made to the current recovery systems or processes? * Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? |

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.