Activity Overview

In this activity, you will create an incident report using 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). 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 demonstrate a proactive approach to security, improving communication and transparency with stakeholders, and improve security practices within your organization. You can also add the incident report you create to your cybersecurity portfolio when you complete it.

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.

Be sure to complete this activity before moving on. In the next course item, you will be able to self-assess your response. After that, there will be a completed exemplar to compare to your own work. It will also provide an opportunity for you to answer rubric questions that allow you to reflect on key elements of your professional statement.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

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 event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them 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

Earlier in this program you learned about the uses and benefits of the National Institute Standards and Technology (NIST) Cybersecurity Framework (CSF). There are five co functions of the NIST CSF framework: identify, protect, detect, respond, and recover.

Incident report analysis

Instructions

As you continue through this course, 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	
Identify	
Protect	
Detect	
Respond	
Recover	

Reflections/Notes:

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:

- Identify: Manage security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect: Develop a strategy to protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect: Scan for potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detectio
- Respond: Ensure that the proper procedures are used to contain, neutralize and analyze security incidents and implement improvements to the security process.
- Recover: Return affected systems back to normal operation and restore system data and assets that have been affected by an inciden

Incident Report with the NIST CSF framework

I*ncident Report: DDoS Attack on Internal Network*

NIST CSF

1. **Identify**
   a. **Risk Assesment:** The organization's firewall was not configured to limit ICMP traffic, allowing an attacker to exercute A DDoS attack by flooding the network with ICMP packets.
   b. **Vulnerability Identified**: Lack of Firewall ruels for ICMP(Internet Control Message Protocol) traffic, absence of rate limiting, and missing souce IP verification mechanisms.
   c. **Imapct**: The internal network was unaveilable for two hours, causing disruption to business operations.
2. **Protect**
   a. **Firewall Configuration**: A new firewall rule was implemented to limit the rate of incomming ICMP packets.
   b. **Source IP verification**: Firewall now checks for spoofed IP addresses to prevent attackeer from faking legimate network requests.
   c. **Security Policies & procedures:**
      i. Regular firewall audit and updates.
      ii. Implemention of acces control measures for network traffic.
      iii. Employee training on network security best practices.
3. **Detect**
   a. **Network Monitoring**: Implemented real-time monitoring software to detect unusual spikes in ICMP traffic.
   b. **Intrusion Detection/Prevention System(IDPS)**
      i. IDS detects anomalies in ICMP requests.
      ii. IPS automaticallu filters out malicious traffic based on defined security rules.
   c. I**ncident Response Plan (IRP)**: Enhanced protocols for early detection and immediate response to suspicious network activities.
4. **Respond**
   a. **Immediate Mitigation Steps Taken**:
      i. Blocked all incoming ICMP packets temporarily.
      ii. Shut down non-critical network services to reduce load.
      iii. Restored critical network services in a controlled manner.
   b. **Analysis & Documentation:**
      i. Security team conducted post-incident analysis to identify attack vectors.
      ii. Documentation of attack patterns for future reference.
   c. **Comunication**:
      i. Noitified stakeholders about the incident and resolution.
      ii. Implemented an internal alerting system for future threats.

Incident Report with the NIST CSF framework
I*ncident Report: DDoS Attack on Internal Network*
NIST CSF
5.Recover

- **Restoration of Services:** Network services were gradually restored after firewall rules and monitoring sysems were in place.
- **Data integrity checks:** Conducted Verification to ensure no data corruption or loss.
- **Post-Incident review:**
  - Assessed response effectiveness and identified areas for improvement.
  - Scheduled regular network security reviews to prevent similar incidents.

Conclusion: By following the NIST Cybersecurity Framework (CSF), the organization significantly improved its resilience agains DDoS attacks. The implemention of firewall rules, network monitoring, IDPS, and security policies ensure better prevention, detection, and response to future threats.