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.

Summary	The company experienced a Distributed Denial of Service (DDoS) attack, specifically through a flood of ICMP packets. This resulted in network services becoming unresponsive, and internal network traffic was unable to access network resources. The attack was due to an unconfigured firewall vulnerability, which allowed the malicious traffic to overwhelm the network. The incident management team responded by blocking incoming ICMP packets, stopping non-critical services, and restoring critical services. After the event, the company implemented new firewall rules, IP address verification, network monitoring software, and an IDS/IPS system.
Identify	**Attack Type:** DDoS attack using ICMP flood. **Extent of the Incident:** The entire internal network was impacted due to the overwhelming flood of ICMP traffic, causing network services to become non-responsive. The firewall vulnerability was exploited to allow the malicious traffic to reach the internal network. **Devices/Systems Affected:** The internal network infrastructure, including routers, switches, and servers, were impacted. The attack led to the temporary unavailability of critical network resources for users. Systems relying on network connectivity, such as file servers, databases, and business-critical applications, would have been disrupted or rendered inaccessible.
Protect	**Protection Measures:** Implement rate-limiting on the firewall to restrict incoming ICMP packets, especially during high-volume traffic events. Configure source IP address verification to prevent spoofed IP addresses from flooding the network. Additionally, ensure the firewall is properly configured to filter malicious traffic and prevent unauthorized access to internal systems. Regular updates and patches should be applied to the firewall, routers, and network devices to prevent exploitation of vulnerabilities. Deploy access control measures to limit access to sensitive systems and data.
Detect	**Detection Measures:** The company implemented network monitoring software to detect abnormal traffic patterns, such as high volumes of ICMP traffic, which could indicate a DDoS attack. IDS/IPS systems were also deployed to detect and mitigate suspicious traffic in real time by analysing packets and identifying anomalies or signatures that match known DDoS attack behaviours. Alerts should be configured for traffic spikes or anomalies in network usage to detect similar attacks more quickly in the future.
Respond	**Response Actions:** When the attack was identified, the incident management team acted swiftly by blocking the incoming ICMP packets at the firewall level, effectively stopping the DDoS attack. Non-critical network services were temporarily shut down to preserve resources for critical services. The team investigated the incident and identified the unconfigured firewall as the root cause, which allowed the malicious actor to overwhelm the network. Communications were

	made to relevant stakeholders about the ongoing attack and actions taken to mitigate it.
Recover	**Recovery Steps:** After the DDoS attack was mitigated, the company restored critical network services and monitored the systems for any signs of residual malicious activity. The cybersecurity team performed a thorough review to ensure that no systems or data were compromised during the attack. They also updated and tested the disaster recovery plans to ensure the response would be quicker and more efficient in the future. The firewall configurations were corrected, and the IDS/IPS systems were updated to better detect and prevent future attacks. Regular audits and tests should be conducted to ensure ongoing resilience against similar incidents.