Activity: Use the NIST Cybersecurity Framework to respond to a security incident

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:

Summary	A media company that provides web design, graphic design and social media marketing services to small businesses was recently hit by a distributed denial of service (DDoS) attack. During the attack, the internal network was compromised for two hours, resulting in disruption of network services. The attack involved a flood of Internet Control Message Protocol (ICMP) packets that overwhelmed the network. The incident management team responded by blocking incoming ICMP packets, taking non-critical services offline and restoring critical network services.
Identify	Responding to a recent DDoS attack that compromised the internal network for two hours, the media company's cybersecurity team discovered a critical issue. The attack vector involves a large number of ICMP packets that take over the network. This vulnerability exploits a vulnerability created by an unconfigured firewall, allowing an attack to bypass network defenses. The

	impact of this incident is relatively large, resulting in disruption of normal network services and unavailability of network resources. The attack was orchestrated by malicious actors who exploited unconfigured firewall vulnerabilities, highlighting the need for proactive security measures and configuration management.
Protect	Cyber security teams have taken several proactive steps to prevent future incidents. These measures include implementing new firewall rules designed to limit the number of incoming ICMP packets and thus prevent excessive traffic. In addition, source IP address inspection is enabled in the firewall to detect and block spoofed IP addresses in incoming ICMP packets, greatly improving security. To improve threat detection capabilities, network monitoring software is implemented to identify unusual traffic patterns, thereby facilitating early detection of threats. In addition, an Intrusion Detection/Intrusion Prevention System (IDS/IPS) is implemented to filter specific ICMP traffic that has suspicious characteristics, adding an additional layer of protection. These comprehensive efforts are aligned with the core "defense" function of NIST's cybersecurity framework, which aims to protect systems, assets, and data from potential threats and vulnerabilities**.**
Detect	In response to a recent DDoS attack that compromised its internal network, the company's cybersecurity team focused on strengthening detection capabilities: **Network Monitoring Software:** Network monitoring software is implemented to proactively detect unusual traffic patterns. The software continuously analyzes network traffic and provides real-time alerts on any deviations from established baselines. This approach aligns with the "discovery" function of NIST's cybersecurity framework, enabling early identification of potential

	threats and anomalies. **IDS/IPS Systems:** Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) filter specific ICMP traffic based on suspicious characteristics. The system proactively monitors network activity and applies predefined rules to identify and respond to potentially malicious traffic. Doing so improves the network's ability to quickly detect and mitigate threats. Together, these measures improve an organization's ability to detect security incidents, such as DDoS attacks, and meet the NIST Cybersecurity Framework's core "detection" function, which emphasizes the importance of timely threat identification and response.
Respond	The company's cybersecurity team initiated a multi-pronged approach within the NIST Cybersecurity Framework's core "Response" function. First, they effectively mitigate attack vectors by immediately blocking incoming ICMP packets, preventing further damage. To ensure minimal disruption to core operations, non-critical network services were temporarily shut down while critical services were carefully restored. A comprehensive incident investigation followed, focusing on determining the cause and scope of the attack, in line with the system's emphasis on robust incident analysis and management. Proactive remediation was performed to address potential vulnerabilities. These include implementing new firewall rules to limit the rate of incoming ICMP packets and enabling source IP address verification in the firewall to detect and block spoofed IP addresses in incoming ICMP packets. In addition, the organization improves its security posture by implementing an intrusion detection system/intrusion prevention system (IDS/IPS) that effectively filters specific ICMP traffic with suspicious characteristics, allowing for timely threat mitigation. Together, these response actions demonstrate a comprehensive, proactive approach to addressing DDoS attacks, with an

	emphasis on rapid incident containment, recovery, and ongoing measures to prevent future incidents.
Recover	The organization's cybersecurity team executed a well-coordinated recovery effort aligned with the "Recover" core function of the NIST Cybersecurity Framework. Their actions encompassed multiple key aspects: First, the incident management team swiftly restored critical network services after blocking incoming ICMP packets to minimize disruption to essential business operations. Second, a thorough investigation was conducted to uncover the root cause and extent of the DDoS attack, aligning with the "Recover" function's emphasis on incident analysis and informing future recovery strategies. Proactive vulnerability remediation efforts were enacted, which included implementing new firewall rules and enabling source IP address verification to enhance security and prevent similar incidents. The deployment of an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) bolstered response capabilities and contributed to a more resilient network. Finally, the organization utilized lessons learned from the incident to refine its continuity planning, ensuring a robust response to potential future security incidents. These actions collectively underscore a comprehensive, well-prepared approach within the "Recover" core function, emphasizing rapid service restoration, vulnerability mitigation, and readiness to effectively respond to future incidents.

Reflections/Notes:

NIST Cybersecurity Framework: The NIST Cybersecurity Framework is an important reference point for organizations to effectively structure their cybersecurity efforts. It provides a clear framework for identifying, protecting against, detecting, responding to, and recovering from security incidents. The scenarios presented make it clear that each core function plays a critical role in addressing cybersecurity threats and incidents.

DDoS Mitigation: These scenarios highlight the importance of distributed denial of service (DDoS) attacks as a common threat. An effective DDoS mitigation strategy includes proactive protection (such as firewall rules and rate limiting) and rapid response (blocking malicious traffic and restoring service). The "defense" and "response" features of the NIST framework are particularly important for dealing with DDoS incidents. Incident Response: The importance of a clear incident response plan is obvious. Timely detection, containment and recovery are critical components of emergency response. The "detect" and "respond" functions within NIST emphasize the need for proactive monitoring and effective incident management.

Continuous improvement: Continuous improvement and learning from incidents are important capabilities. Organizations in the scenario recognize the value of improving their security posture based on experience. This is consistent with the NIST framework's emphasis on continuous evaluation and improvement. Multiple layers of defense: Implementing multiple layers of defense is critical to today's cyber security. This includes measures such as firewall rules, intrusion detection systems and access control. Together, these layers improve an organization's ability to protect, detect, and respond to threats.

Security Awareness: Effective security measures require not only technical solutions, but also employee awareness and training. Organizations should invest in educating employees about security best practices to mitigate social engineering and other man-made threats.

Logging: It is important to properly document incidents and responses. It helps to understand the impact of an attack, determine the effectiveness of countermeasures, and make informed decisions about future security policies.

Proactive measures: These scenarios emphasize the importance of proactive security measures, such as properly configuring firewalls, restricting traffic, and monitoring network patterns. These measures can significantly reduce the attack surface and potential impact of a security incident.

Collectively, these scenarios illustrate the importance of well-structured cybersecurity systems, proactive measures, and a comprehensive approach to incident response and recovery. They also emphasize that organizations must adapt and continuously improve their cybersecurity strategies to stay ahead of evolving threats.