Incident report analysis

Summary	The cybersecurity incident involving a DDoS attack on our organization's network has exposed critical gaps in our overall security posture. The incident, which lasted for two hours, was caused by a flood of ICMP packets exploiting a vulnerability in an unconfigured firewall. To address these shortcomings and enhance our network security, we have implemented a comprehensive and systematic approach aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This incident report analysis provides a detailed breakdown of the actions taken and proposed improvements across each phase of the CSF.
Identify	To proactively identify and mitigate potential threats, we have undertaken the following measures: • **Regular Audits:** We conduct regular audits of internal networks, systems, devices, and access privileges to identify and remediate vulnerabilities. This includes comprehensive reviews of firewall configurations and rules to prevent vulnerabilities like the one exploited in the recent DDoS attack. • **Risk Assessment:** We implement a robust risk assessment process to identify and prioritize potential threats, such as DDoS vulnerabilities, before they can be exploited. This assessment helps us allocate resources effectively and prioritize mitigation efforts.
Protect	To strengthen our network defences and prevent similar incidents, we have implemented the following measures: • **Firewall Rule Enhancement:** We have implemented a new firewall rule to limit the rate of incoming ICMP packets, effectively mitigating the risk of future DDoS attacks. This rule helps to ensure that our network can withstand even large-scale volumetric attacks. • **Source IP Address Verification:** We have enhanced firewall security by incorporating source IP address verification to detect and block packets with spoofed IP addresses. This measure helps to prevent attackers from disguising their origin and launching attacks from unsuspecting sources. • **Policy Development:** We have established and enforced policies that enhance cybersecurity resilience, including guidelines for configuring firewalls and handling network traffic. These policies ensure that our

	organization adheres to best practices and protects itself from common cyber threats.
Detect	To improve our ability to detect and respond to security incidents promptly, we have implemented the following measures: • **Network Monitoring:** We have implemented advanced network monitoring software to detect abnormal traffic patterns promptly. This software provides real-time visibility into our network activity and allows us to identify suspicious behaviour early, enabling us to take pre-emptive action. • **Intrusion Detection/Prevention System (IDS/IPS):** We have deployed an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics. This system helps us to identify and block malicious traffic before it can impact our network.
Respond	To ensure a swift and effective response to security incidents, we have refined and enhanced our incident response plan: • **Incident Response Plan:** We have enhanced the incident response plan to ensure a swift and coordinated response to DDoS attacks and other cybersecurity incidents. This plan outlines clear roles and responsibilities, communication protocols, and recovery procedures. • **Security Training:** We provide training to the incident management team and relevant staff on responding to DDoS attacks and other cybersecurity incidents effectively. This training ensures that our team is well-equipped to handle various security threats.
Recover	To minimize downtime and restore operations in the event of a security incident, we have established procedures for system restoration: • **System Restoration:** We have developed and implemented procedures to recover affected systems swiftly and restore any data or assets impacted during the incident. This ensures minimal disruption to our business operations. • **Continuous Improvement:** We have established a continuous improvement process for the incident response plan, incorporating lessons learned from the DDoS incident to enhance future responses. This process ensures that our incident response capabilities evolve with emerging threats and technologies.

Reflections/Notes:

In addition to the above-mentioned measures, we are exploring the following initiatives to further strengthen our cybersecurity posture:

- **Continuous Monitoring:** We are considering implementing continuous monitoring practices to ensure real-time visibility into network activities and potential threats. This will enable us to detect and respond to incidents even before they cause significant damage.
- **Collaboration:** We are encouraging collaboration between IT and cybersecurity teams to strengthen the overall security posture and response capabilities. This cross-functional collaboration ensures that everyone is working towards a common goal and leveraging their unique expertise.
- **Incident Simulation:** We are conducting periodic incident simulation exercises to test the effectiveness of the incident response plan and identify areas for improvement. This proactive approach helps us identify and address potential shortcomings before they manifest in real-world incidents.
- **Employee Awareness:** We are emphasizing the importance of employee awareness in recognizing and reporting security anomalies to strengthen the overall cybersecurity defence. This includes training on identifying and reporting suspicious activities, such as unusual emails or changes to network configurations.