Incident report analysis

Problem Statement

You have been tasked with analyzing a security incident involving a DDoS (Distributed Denial of Service) attack that disrupted your organization's network. Your goal is to apply the **NIST Cyber security Framework** to document the entire incident lifecycle from initial detection and analysis to the final recovery and recommendations for preventing future attacks. The report must identify the root cause of the incident and detail the actions taken at each stage of the response.

Summary	A DDoS attack was launched against the company's network, resulting in a 2 hour disruption of network services. The attack was caused by an unconfigured firewall that allowed for a flood of ICMP packets to overwhelm the network. Several employees reported being unable to access critical network services, and the incident response team responded by blocking incoming ICMP packets and restoring critical network services.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that the firewall was not properly configured, allowing the malicious traffic to flood the network. The systems impacted were the company's internal network and critical network services. The attack was caused by an unconfigured firewall that allowed malicious traffic to flood the network.
Protect	The team has implemented new security measures to prevent future attacks: 1. Firewall configuration: Update firewall rules to limit incoming ICMP packets and implement source IP address verification.

	2. Network monitoring: Implement network monitoring software to detect abnormal traffic patterns. 3. Employee training: Provide employee training on cybersecurity best practices and incident response procedures. 4. IDS/IPS system: Implement an IDS/IPS system to detect and prevent similar attacks in the future.
Detect	To detect new unauthorized access attacks in the future, the team will use: 1. Firewall logging tool: Monitor firewall logs for suspicious activity. 2. Intrusion detection system (IDS): Implement an IDS to detect potential security threats.
Respond	The team responded to the incident by: 1. Blocking incoming ICMP packets to prevent further damage. 2. Restoring critical network services to ensure normal business operations. 3. Informing upper management of the incident and its status. 4. Analyzing the incident to identify root causes and areas for improvement.
Recover	The team will recover from the incident by: 1. Restoring network services to ensure normal business operations. 2. Verifying that systems and data have been restored correctly. 3. Closely monitoring systems and networks for signs of further malicious activity.

Reflections/Notes:

This incident highlights the importance of proper firewall configuration and regular security audits. The team will continue to monitor and improve its security posture to prevent similar incidents in the future.