Incident Report Analysis

Summary	A DDoS attack on the multimedia company compromised the internal network for two hours, preventing normal internal network traffic from accessing network resources. The attack was initiated through an unconfigured firewall, allowing a flood of ICMP packets to overwhelm the network. The incident management team responded by blocking incoming ICMP packets, shutting down non-critical network services, and restoring critical ones. The cybersecurity team subsequently implemented several measures to prevent future attacks.
Identify	The company's cybersecurity team then investigated the security event. We 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. This allowed the company's network services, including web design, graphic design, and social media marketing solutions, to be affected. The attack disrupted normal business operations by halting network services for two hours, impacting all employees and customers relying on these services.
Protect	To address this security event, the network security team implemented a firewall rule to limit the rate of incoming ICMP packets and verify source IP addresses to block spoofed addresses. Employees received training on the importance of configuring and maintaining security measures. The firewall configurations were updated for better security against similar attacks. New procedures for regular firewall configuration checks and updates were established, and regular maintenance and updates for firewall configurations were scheduled. Additionally, an IDS/IPS system was deployed to filter out

	suspicious ICMP traffic and detect abnormal traffic patterns.
Detect	The team utilized firewall logging tools and IDS to detect and alert IT security staff of unusual traffic patterns. Network monitoring software was implemented to analyze real-time traffic and identify potential threats. The IDS was configured to continuously monitor and detect incoming ICMP packets from non-trusted sources.
Respond	The team developed a comprehensive response plan to address and mitigate future DDoS attacks. Response procedures were communicated to all relevant stakeholders, including IT staff and affected employees. We conducted a detailed analysis of the DDoS attack to understand its impact and refine the response strategy. Measures were implemented to isolate affected resources and prevent further damage during an attack. Response procedures were enhanced and the incident response plan was updated based on lessons learned.
Recover	The team restored the network services by reconfiguring the firewall and applying new security measures. The recovery process was improved to ensure faster restoration of services in the event of future incidents. All employees and customers were informed about the restoration of network services and any steps they needed to take.

Reflections/Notes: Lessons learned highlighted the importance of proactive firewall management, regular security audits, and continuous monitoring to prevent and detect similar attacks. Future improvements include increasing training programs for employees, implementing more robust monitoring tools, and conducting regular security assessments to identify potential vulnerabilities.