Incident report analysis

Summary	The company encountered a significant security event as all network services abruptly became unresponsive. Upon investigation, the cybersecurity team determined that this disruption stemmed from a deliberate DDoS attack, where an overwhelming influx of ICMP packets flooded the network. In response, the team swiftly acted to counter the attack, blocking it effectively and temporarily halting non-critical network services to prioritize the restoration of critical services.
Identify	The company fell victim to a deliberate ICMP flood attack executed by one or more malicious actors. This attack had a profound impact on the entire internal network, necessitating the immediate safeguarding and restoration of all critical network resources to ensure their functionality.
Protect	To fortify the network's defenses, the cybersecurity team proactively implemented a new firewall rule aimed at restricting the influx of incoming ICMP packets to a manageable rate. Additionally, they bolstered the protective measures by deploying an advanced IDS/IPS system capable of identifying and filtering out ICMP traffic exhibiting suspicious characteristics.
Detect	To enhance the organization's detection capabilities, the cybersecurity team implemented source IP address verification on the firewall, effectively scrutinizing incoming ICMP packets for any signs of spoofed IP addresses. Moreover, they deployed sophisticated network monitoring software to actively identify and alert on abnormal traffic patterns, enabling swift

	detection of potential security incidents.
Respond	To effectively respond to future security events, the cybersecurity team will adopt a proactive approach. They will promptly isolate affected systems to prevent any further disruptions to the network's integrity. Simultaneously, efforts will be made to restore any critical systems and services that experienced disruptions during the incident. Thorough analysis of network logs will be conducted to identify and investigate any signs of suspicious or abnormal activity. Additionally, the team will diligently report all incidents to upper management and, if necessary, appropriate legal authorities, ensuring transparency and adherence to regulatory requirements.
Recover	To successfully recover from a DDoS attack caused by ICMP flooding, it is imperative to restore network services to their normal functioning state. For future incidents, external ICMP flood attacks can be thwarted by implementing firewall measures. In the recovery process, it is advised to temporarily halt all non-critical network services to alleviate internal network traffic. Subsequently, the restoration efforts should prioritize critical network services to ensure their prompt availability. Finally, once the flood of ICMP packets has subsided, it is safe to bring back online all non-critical network systems and services, completing the recovery process.

Reflections/Notes:

- The incident serves as a reminder of the utmost importance of implementing proactive network security measures to both prevent and effectively mitigate DDoS attacks. Regular monitoring and analysis of network traffic play a critical role in detecting abnormal patterns early on, enabling swift incident response. It is vital to foster collaboration between the cybersecurity team and other departments, such as incident management and legal

authorities, to ensure a comprehensive and coordinated response to such incidents.

- Continuous improvement is a necessary aspect of network security, ensuring enhanced resilience and readiness in the face of future security incidents. By constantly refining and adapting security strategies, the organization can effectively stay one step ahead of potential threats.

- Documentation of incident response procedures and the lessons learned from this incident are invaluable in refining future incident response strategies. By meticulously documenting the incident response process and incorporating key takeaways, the organization can continuously learn from past experiences and bolster their ability to handle similar incidents in the future.