Incident report analysis

Summary	A multimedia company network service suddenly stopped responding due to a distributed denial of service (DDoS) attack through a flood of incoming ICMP packets. The network management team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored. Fortunately, no data breach occurred; the attack solely blocked network access due to the overwhelming number of packets flooding the network.
Identify	The incident management team audited the network and found that the ICMP pings flooded the network through an unconfigured firewall, enabling malicious attackers to launch a (DDoS) attack. This vulnerability necessitated the securing and restoration of all critical resources to ensure network functionality.
Protect	To mitigate future attacks, the team introduced a new firewall rule to regulate the influx of incoming ICMP packets. Additionally, an IDS/IPS system was deployed to filter out ICMP traffic exhibiting suspicious characteristics, supporting the network's defenses.
Detect	Proactive measures were implemented to prevent DDoS attacks. Source IP address verification was integrated into the firewall to scrutinize incoming ICMP packets for spoofed IP addresses. Furthermore, the team employed network monitoring software to detect aberrant traffic patterns, enhancing the network's ability to identify and respond to potential threats.
Respond	In preparation for subsequent security events, the cybersecurity team outlined a proactive response plan. They will immediately isolate affected systems to reduce further network disruption and prioritize restoring critical systems and

	services. Subsequently, network logs will be meticulously analyzed to identify any suspicious activity. Additionally, all incidents will be immediately reported to upper management and relevant legal authorities to ensure transparency and compliance.
Recover	Efficient recovery from a DDoS attack entails restoring network services to normal functionality. In future instances, external ICMP flood attacks will be preemptively blocked at the firewall. Subsequently, all non-critical network services will be temporarily halted to alleviate internal network congestion, prioritizing the restoration of critical services. Once the flood of ICMP packets subsides, non-critical network systems and services can be gradually reinstated, ensuring minimal disruption to network operations.