Incident report analysis

Summary	A multimedia company experienced a DDoS attack that disrupted its internal network for two hours by flooding it with ICMP packets. The attack exploited an unconfigured firewall, allowing the malicious traffic to overwhelm network resources. In response, the cybersecurity team blocked ICMP traffic, shut down non-critical services, and restored key operations. They later implemented firewall rules, source IP verification, monitoring tools, and an IDS/IPS system to prevent similar attacks in the future.
Identify	Conduct regular security audits of firewalls, access controls, and network configurations to ensure they are properly configured and aligned with current best practices. Review asset inventories and user privileges to detect unauthorized access points or overlooked vulnerabilities like the unconfigured firewall that allowed the ICMP flood.
Protect	Update firewall configurations to enforce strict traffic rules, such as limiting ICMP packet rates and enabling source IP verification. Implement comprehensive security policies, employee cybersecurity awareness training, and automatic patch management to reduce the chance of misconfigurations and human error.
Detect	Deploy and maintain robust network monitoring tools and intrusion detection/prevention systems (IDS/IPS) to analyze traffic patterns in real time and flag anomalies. Establish alerts for high volumes of ICMP traffic or known DDoS signatures to enable faster threat identification.
Respond	Develop and regularly test an incident response plan that outlines roles, containment strategies, and communication procedures. After the ICMP flood attack, analyze logs, assess root causes, and adjust firewall rules and detection

	rulesets accordingly to strengthen future response capability.
Recover	Restore any affected services to full functionality using tested backup and recovery procedures. Conduct a post-incident review to capture lessons learned, document changes made (e.g., new firewall rules), and update business continuity plans to reflect improved resilience against DDoS attacks.