Incident report analysis

Summary	The multimedia company experienced a security event where all network services became unresponsive due to a distributed denial of service (DDoS) attack through a flood of incoming ICMP packets. The incident was mitigated by blocking the attack and temporarily stopping non-critical network services until critical services could be restored.
Identify	The security incident involved a targeted ICMP flood attack by malicious actors, affecting the entire internal network. The focus was on securing and restoring critical network resources.
Protect	To enhance network security, the cybersecurity team implemented a new firewall rule to restrict the rate of incoming ICMP packets and deployed an IDS/IPS system to filter suspicious ICMP traffic.
Detect	To improve detection capabilities, the team configured source IP address verification on the firewall to identify spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to identify abnormal traffic patterns.
Respond	For future incidents, the cybersecurity team will isolate affected systems, restore critical services, analyze network logs for suspicious activity, report incidents to management and legal authorities if necessary.
Recover	To recover from a DDoS attack involving ICMP flooding, the network services should be restored to normal operation. External ICMP flood attacks can be blocked at the firewall, non-critical network services temporarily stopped, critical services restored first, and non-critical systems brought back online after the flood subsides.

Reflections/Notes:

- The incident highlights the importance of proactive network security measures to prevent and mitigate DDoS attacks.
- Regular monitoring and analysis of network traffic can provide early detection of abnormal patterns, aiding in incident response.
- Collaboration between the cybersecurity team and other departments, such as incident management and legal authorities, is crucial for a comprehensive response.
- Continuous improvement is necessary to enhance network resilience and readiness against future security incidents.
- Documentation of incident response procedures and lessons learned can contribute to refining future incident response strategies.