Incident report analysis

Summary	A multimedia company experienced a network-wide outage when all services became unresponsive. Incident investigation revealed that the disruption was caused by a Distributed Denial of Service (DDoS) attack leveraging high volumes of ICMP packets. The cybersecurity team mitigated the attack by implementing traffic filtering to block the malicious ICMP requests, suspending non-critical services, and prioritizing the restoration of critical operations to resume normal business functionality.
Identify	It is unknown who the malicious actor is, yet the malicious actor or actors sent an ICMP flood attack. The internal network was completely stopped. All network services have to be blocked then restored.
Protect	The cybersecurity team deployed advanced firewall rule sets, including Unicast Reverse Path Forwarding (uRPF) to mitigate spoofed traffic, along with ingress and egress filtering to control malicious packet flow at the network boundary. Additionally, they integrated intrusion detection system (IDS) monitoring, enforced VPN tunneling for secure remote access, and applied critical system and security updates. These combined measures strengthened the network's defensive posture and improved detection, prevention, and response capabilities against future DDoS attempts.
Detect	The cybersecurity team enforced IP address validation on the firewall by leveraging stateful packet inspection (SPI) to ensure legitimacy of session traffic. Ingress and egress filtering was applied to regulate both inbound and outbound packets, mitigating the risk of spoofed or unauthorized traffic. Furthermore, network monitoring was enhanced through the deployment of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), enabling proactive detection and real-time mitigation of malicious activity.
Respond	For future incidents, the cybersecurity team will initiate rapid containment by isolating compromised hosts and network segments to prevent lateral movement and further disruption. Priority will be given to restoring mission-critical systems and services through established disaster recovery procedures. Post-containment, network and system logs will be thoroughly analyzed to identify indicators of compromise (IoCs), abnormal traffic patterns, and potential persistence mechanisms. All incidents

	will be formally documented and escalated to executive leadership, with notifications to regulatory bodies and legal authorities as required by organizational policy and compliance frameworks.
Recover	To mitigate the ICMP flood, the team will prioritize restoring normal packet flow by implementing firewall rules that filter malicious traffic and enforce rate limiting against DoS/DDoS vectors. Stateful packet inspection, source IP verification, and continuous intrusion detection monitoring will support both prevention and recovery efforts. Non-essential services will be suspended to reallocate bandwidth and processing resources toward mission-critical systems. Once traffic levels stabilize and malicious packets are no longer saturating the network, critical services will be restored first, followed by gradual reactivation of non-critical functions.

Reflections/Notes:**Bandwidth prioritization worked effectively** — by shutting down non-essential services, critical systems maintained functionality and were restored quickly.

- **Firewall hardening is essential** — packet filtering and rate limiting proved to be critical in reducing the impact of ICMP floods.
- **Layered defenses matter** — combining stateful inspection, IP verification, and IDS/IPS monitoring reduced the risk of blind spots.
- **Incident timing is critical** — early detection and immediate containment measures minimized downtime.
- **Communication gaps** — ensuring upper management and affected teams receive timely updates could be improved.

Notes for Future Incidents

- Pre-configure firewall rules and rate limits for ICMP to shorten response time.

- Automate service prioritization (critical vs. non-critical) during overload scenarios.

- Improve alerting thresholds in IDS/IPS to identify ICMP anomalies faster.

- Maintain a clear runbook for restoring services in priority order.

- Document and rehearse escalation procedures for faster coordination with ISPs if traffic exceeds local capacity.