Incident report analysis

Summary	Our multimedia company faced a disruptive DDoS attack, causing a two-hour compromise of the internal network. The attack flooded the system with ICMP packets, disrupting normal internal traffic. The incident management team swiftly responded, blocking incoming ICMP packets, temporarily halting non-critical services, and promptly restoring essential ones. Post-incident investigation revealed a malicious actor exploiting an unconfigured firewall, leading to the DDoS attack.
Identify	Conducted regular audits to identify potential security gaps in internal networks, systems, devices, and access privileges. Investigated the incident thoroughly to determine the root cause and exploited vulnerabilities.
Protect	Implemented new authentication policies, including multi-factor authentication (MFA) and limited login attempts. Provided training on safeguarding login credentials and strengthened protective measures with a new firewall configuration and intrusion prevention system (IPS).
Detect	Enhanced monitoring capabilities using a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic. Focused on detecting abnormal traffic patterns and potential unauthorized access.
Respond	Swiftly responded to the incident by blocking incoming ICMP packets, halting non-critical services, and restoring essential network services. Disabled compromised accounts, provided training to employees, and informed upper management. Communicated the incident to customers, law enforcement, and other relevant organizations as required by local laws.
Recover	Restored deleted data by recovering the database from the last night's full backup. Communicated to staff about the need to re-enter information changed during the incident once the database is restored.

Reflections/Notes:
This incident underscores the critical importance of a proactive cybersecurity strategy. The rapid response and integrated approach aligned with the NIST CSF not only mitigated the immediate threat but also paved the way for continuous improvement, ensuring enhanced resilience against future cyber threats.