Incident report analysis

// Mathias Petry Peixoto

Summary	The company experienced a DDoS attack that disrupted the internal network for two hours. The attack used ICMP flood traffic, overwhelming the infrastructure and making it impossible for users to access internal resources. The incident response team quickly blocked incoming ICMP packets and restored critical services while starting a broader investigation.
Identify	The security team identified that the ICMP flood originated from spoofed IP addresses, exploiting a misconfigured firewall that lacked proper traffic filtering. All internal services were impacted. The team concluded that critical systems lacked proper segmentation and were exposed to the attack surface.
Protect	To improve protection, the team implemented firewall rules to limit ICMP traffic and detect spoofed IPs. They also began restructuring the network by segmenting sensitive systems into isolated subnets with stricter access controls. Ongoing staff training and secure configuration practices were also introduced.

Detect	Network monitoring tools were deployed to identify abnormal traffic patterns in real time. The firewall was configured to flag suspicious ICMP behavior, and an IDS/IPS system was added to detect and block potential threats. Log analysis procedures were established to proactively identify anomalies.
Respond	In case of future incidents, the team will isolate affected systems, prioritize critical service restoration, and notify leadership. Incident reports will be generated, and relevant logs reviewed to support deeper forensic analysis. If required, authorities will be informed in compliance with applicable laws.
Recover	Recovery procedures include restoring services from backups and validating system integrity. ICMP traffic will remain restricted until the threat has passed. After critical systems are online, non-critical services will be restored progressively, following a structured recovery checklist.

Reflections/Notes: The incident revealed gaps in firewall configuration and network segmentation. Strengthening detection capabilities, isolating systems, and adopting a more proactive security posture are key steps toward long-term resilience.