DDoS Incident Report Updated

Summary:

A multimedia company experienced a DDoS attack, halting all internal network access for two hours.
The incident involved an overwhelming number of ICMP packets..

Identify:

The attack was discovered through monitoring tools and confirmed by a sudden halt in internal traffic.
Analysis revealed the vulnerability was due to an unconfigured firewall..

Protect:

The team implemented firewall rules to limit ICMP packets, verified source IPs, and installed network monitoring to

Detect:

Anomalous traffic patterns were flagged, allowing the cybersecurity team to respond..

Respond:

The network was segmented, ICMP packets were blocked, and critical services were restored..

Recover:

Systems were monitored and reviewed.
Firewall configurations were updated, and a full security audit was initiated..

Reflections/Notes::

Highlighted the importance of baseline traffic behavior and prompt firewall configuration checks..