Incident report analysis

Applying the NIST Cybersecurity Framework

Summary	A multimedia company experienced a DDoS attack for two hours before it was resolved. The network stopped due to an ICMP packet that flooded the network.
Identify	Regular Audits of the internal network and system
Protect	**Implementation of policies, procedures, and training tools that help with cybersecurity. The use of security hardening to reduce vulnerabilities, update the installation, remove unusable apps and penetration testing**
Detect	Potential security incident and improve monitoring capacity. Detect future vulnerability attacks.
Respond	To contain, neutralize and analyze a security incident
Recover	Put the system back to normal operations and restore system data or assets that have been affected by an accident

---

Reflections/Notes:

2. The attack was a network attack, specifically a distributed denial-of-service attack, that compromised the network by sending multiple ICMP packets. Overwhelming ICMP pings have been sent to block the service through the configured firewall.