Incident report analysis

Benjamin Taylor – Google Cybersecurity

Instructions

Review the scenario below. Then complete the step-by-step instructions.
You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.
During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

Summary	The company experienced a DDoS attack that overwhelmed the internal network with ICMP packets, disrupting services for two hours. The attack took advantage of a misconfigured firewall, allowing the malicious traffic to flood into the network. In response, security measures were taken such as updating firewall rules, implementing source IP verification, network monitoring, and an IDS/IPS system. This incident highlights the need for stronger network hardening as well as security monitoring to prevent future events.
Identify	Regular audits of network infrastructure, firewall configurations, and access controls will be conducted to uncover vulnerabilities and make sure that security gaps are quickly addressed.
Protect	Firewall rules will be updated to limit ICMP traffic, enforce source IP verification, and create internal policies and training to prevent future misconfigurations.

Detect	Real-time network monitoring and IDS/IPS systems will be used to quickly identify abnormal traffic patterns that may indicate DDoS attacks.
Respond	Incident plans will be updated with clear steps to contain, analyze, and mitigate DDoS threats through predefined procedures/communication protocols.
Recover	Disaster recovery processes will prioritize restoring critical systems quickly, with routine testing of backups/restoration procedures to ensure operational continuity.

Reflections/Notes: This incident highlights how important proactive firewall configuration and regular audits are in preventing overlooked vulnerabilities. Implementing rate-limiting and ICMP filtering significantly reduced future DDoS risk.