Incident report analysis

Instructions

Summary	Our multimedia company (which offers web design services, graphic design, and social media marketing solutions for small businesses) was experiencing a DDoS attack, which compromised the internal network for two hours until it was resolved. The services stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic was unable to access any resources. The incident management team blocked incoming ICMP packets which stopped all non-critical network services offline, restored critical network services. After investigation, it looked like an ICMP flood attack from a malicious actor sent through an unconfigured firewall. This vulnerability overwhelmed the network through the distributed denial of service attack.
Identify	The incident management team investigated the security event and noticed there was a malicious actor that sent a flood of ICMP pings into the company's network through an unconfigured firewall, a potential ICMP flood attack. This was the attack surface the actor used to conduct a distributed denial of service (DDoS) attack.
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and installed an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized attacks in the future, the team will use the network monitoring software to detect any abnormal traffic patterns and the IDS system to send alerts for any suspicious traffic.

Respond	The team disabled any incoming ICMP packets and stopped all non-critical network services offline. For future events, the cybersecurity team will isolate the affected systems to prevent further disruptions. They will attempt to restore any critical systems/services that were disrupted. Network logs will then be used to check for suspicious activity. The incident will be reported to upper management and if applicable, the appropriate legal authorities.
Recover	The team quickly recovered the information by restoring the critical network services. In the future, external ICMP flood attacks can be blocked at the firewall. All non-critical network services should be stopped to reduce internal network traffic. Critical network services should be restored first. Once the flood of ICMP packets have timed out, all other non-critical network systems and services can be brought back online.

Reflections/Notes: