Incident report analysis

Instructions

Summary	The organization faced a DDoS attack that exploited an unconfigured firewall, overwhelming the network with ICMP packets and disrupting access to internal resources. Immediate actions included blocking ICMP traffic, shutting down non-critical services, and restoring critical operations. To prevent recurrence, the organization implemented firewall rules to limit ICMP traffic, enabled source IP verification, deployed network monitoring tools, and installed an IDS/IPS to detect and mitigate suspicious activity, strengthening overall network security.
Identify	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.
Protect	To address this security event, the network security team implemented: - A new firewall rule to limit the rate of incoming ICMP packets - Network monitoring software to detect abnormal traffic patterns
Detect	Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Respond	To address this security event, the network security team implemented: - An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Recover	restoring critical network services