



Incident report analysis

Summary	<p>The company experienced a security event when all network services stopped working. The cybersecurity team found out that the disruption was caused by a distributed denial of service (DDoS) attack through flooding by ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so critical services can be restored.</p>
Identify	<p>A malicious actor or actors attacked the company with an ICMP flood attack. The entire internal network was affected. The critical network components needed to be secured and restored to function.</p>
Protect	<p>The cybersecurity team implemented a firewall rule to limit the rate of ICMP incoming packets and an IDS system to filter the suspicious ICMP traffic</p>
Detect	<p>The cybersecurity team configured the verification of source IP address on the firewall to avoid future spoofing of IP addresses on incoming ICMP packets</p>
Respond	<p>For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical system affected by the event.</p>
Recover	<p>In order to recover from DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks will be blocked by the firewall. Then, to reduce network traffic all non-critical services will be shutdown. Next, critical services should be restored. Finally, when ICMP packets have timed out, non-critical network systems can be brought back online.</p>

Reflections/Notes: