Incident report analysis

Instructions

Summary	A distributed denial of service attack (DDoS) transpired through the use of ICMP packets flooding the business's network. The DDoS attack compromised internal servers for 2 hours, with the network traffic unable to access resources. Response by the incident management team was to block ICMP packets, pause all non-critical services, and restore the critical ones. Post-incident investigation found that the vulnerability was with an unconfigured firewall, allowing the packets to pass through with no detection or prevention in place.
Identify	Vulnerability identified to be an unconfigured firewall allowing all traffic to be transmitted with no intervention, affecting the internal network of the business, as direct communication is permitted.
Protect	With the vulnerability found, the security team implemented: updated firewall configured to limit the rate of incoming ICMP packets, verification on Source IP addresses to safeguard from spoofing attacks, monitoring services for suspicious traffic patterns, and IDS/IPS systems for detection of suspicious traffic
Detect	The addition of Network monitoring services, as well as an IDS and IPS, allows for sufficient detection of potential threats in the network traffic. Recurring patterns of suspicious behaviour will be identified through our monitoring services, and known attacks, such as an ICMP flooding attack that just took place, will be detected and prevented using the IPS.
Respond	The impact of this attack compromised the entire network for a prolonged period, which can lead to major financial loss as well as a worsened reputation.

	To lessen the impact, isolate any affected systems by splitting the network into subnets for specific departments and processes, creating security zones. Zones can isolate the attack while keeping business operations online to avoid loss. Respond by blocking the malicious packets, restoring the critical systems, and monitoring the network for anymore suspicious traffic. Once completed, report the incident to upper management when applicable
Recover	Recovery of critical systems of the business for normal operations will always be the priority. Pausing all non-critical operations to decrease the amount of traffic, then blocking the ICMP packet flooding till services are no longer overwhelmed. The blocking of ICMP packets will be done through the firewall in the future. Then, critical systems are recovered, and any lost data is recovered through backup in the database. Once completed, all non-critical systems are back online.