Incident report analysis

Instructions

Summary	The company experienced a Ping ICMP flood DDoS attack for 2 hours which compromised the internal network. ICMP flood attack is a type of DOS attack performed by an attacker repeatedly sending ICMP packets. The attacker sent a flood of ICMP pings through an unconfigured firewall. Eventually, all the bandwidth for incoming and outgoing traffic used up and the system crashed. Internet Control Message Protocol (ICMP) is used to send diagnostic messages, like pings, and error reports about network issues. The impact of this attack is network services could not respond to legitimate requests and network resources became unavailable.
Identify	The attack was an ICMP DDOS attack and the entire network was damaged. IThe gap in the security of the organization is an unconfigured firewall, because network services stopped due to flood of ICMP packets income through this firewall.
Protect	The team has implemented new policies to prevent future attacks: 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. Implementing IDS/IPS systems will provide additional security..
Detect	To detect new attacks in the future, the team will use network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	The team will block incoming ICMP packets, so the attack stops temporarily. With also stopping all non-critical network services offline preventing further damage while troubleshooting. They will restore any critical systems and services.
Recover	The team needs to restore network services. In the future, ICMP flood attacks will be blocked by firewalls. After all non-critical services stop, critical network services need to be restored. Finally, the flood of ICMP packets has timed out, and other services can be restored.

Reflections/Notes: