Incident report analysis

Instructions

Summary	The organization recently experienced a DDoS attack, which compromised the internal network for two hours. During the attack, the company's network services suddenly stopped responding due to an incoming flood of ICMP packets and the normal internal network traffic could not access any network resources. The cyber team responded by blocking all incoming ICMP packets, stopping all non-critical network services so that non-critical network services,
Identify	The malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	The team has implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	The team has implemented network monitoring software to detect abnormal traffic patterns and IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Respond	For future security events, the team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.

Recover	To recover from a 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 can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: