By: caami.sec

Incident report analysis

Instructions

Summary	The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a DDoS attack. Due to the large amount of incoming ICMP packets, the network services became overwhelming and suddenly stopped responding. The internal network was compromised for 2 hours until it was fixed. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The cybersecurity team investigated the event and found that a malicious actor had flooded the network with ICMP packets due to an unconfigured firewall.
Identify	The cybersecurity team found that the event was caused by a malicious actor who had flooded the network with ICMP packets due to 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 implemented 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, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.

Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	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 systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity
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: