Incident report analysis

Instructions

Summary	Recently we experienced an attack that compromised our internal network for two hours until it was resolved. Normal internal network traffic could not access any network resources due to an incoming flood of ICMP packets, which was responded to by the incident management team blocking incoming ICMP packets. The cybersecurity team investigated the event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	The team has implemented a new firewall rule to limit the rate of incoming ICMP packets, and an IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized access attacks in the future, the team will do a firewall verification to verify the source IP to check for spoofed IP addresses on incoming ICMP packets.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical

	network services. 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 involving ICMP flooding, the first step is to restore network services to their normal operational state. Moving forward, blocking external ICMP flood attacks at the firewall will be necessary. After that, all non-essential network services should be shut down to minimize internal network traffic. Critical network services should be brought back online first. Finally, once the ICMP packet flood subsides, non-essential network systems and services can be reactivated.