Incident report analysis

Instructions

Summary	Recently, our organization faced an attack where the internal network was down for nearly 2 hours. A malicious actor tried to attack the internal network with a DoS attack by flooding ICMP packets, which led to a shutdown of the internal network. The incident management team took immediate action by stopping the flood of ICMP packets and all critical activities stopped and the network was recovered. The team found that the malicious actor took advantage of an unconfigured firewall. Due to that vulnerability the malicious actor overwhelm the company's network through a DoS attack. The Security Team has fixed all the vulnerabilities and configured the firewall and improved the security.
Identify	The incident management team identified the attack when the company's network service stopped working; they found that an ICMP packet flooding had disrupted the service .
Protect	The security team then configured the firewall with new protection rules that blocks the ICMP packet flooding and also an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The security team also configured a source IP address verification on the firewall, so that IP addresses get checked of the ICMP packets.
Respond	The cybersecurity team implemented the changes that can be helpful for the future attacks. Furthermore, the team should also analyze network logs and have proper checks of all the network activities.
Recover	The network was fully restored after critical services were brought back online.

	In the event of a future DoS attack, the firewall is now configured to block ICMP floods, and non-critical services can be taken offline to preserve network stability.

Reflections/Notes: