Incident report analysis

Summary	This afternoon, we experienced network outrange because the company's internal network was not accessible. To know the source of the cause, we investigate the incident by viewing the event logs. In the event log we notice many devices were attempting to access the company network at once causing it to be overwhelmed, this is a malicious actor attack flooding the company's network with ICMP pings. We could not know the actual attacker device so we blocked all incoming ICMP packets and stopped all-non critical network service. After two hours, the issue was resolved and all critical network services were restored. During the investigation we discovered that the malicious attacker was able to overwhelm the company network through a distributed denial of service due to an unconfigured firewall. The security team then implemented a new security policy to harden the company network. The following were 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 • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

Identify	The incident management team audited the systems, devices and access policy involved in the attack to identify the gaps in security. The team found out that the company was experiencing a Distributed Denial of Service from a malicious attack and the internal network has been compromised. During the investigation, it was discovered that the malicious actor was able to overwhelm the company network with ICMP pings due to an unconfigured firewall.

Protect	The team blocked all incoming ICMP packets and stopped all-non critical network service. The security team was told to reconfigure the firewall to meet the organization's security needs. A new firewall rule has been set to: ● limit the rate of incoming ICMP packets ● Verified the source of IP address to check for spoofed IP address ● A network software to prevent abnormal traffic in the internal network ● An IDS/IPS systems has been installed to filter out some ICMP traffic on suspicious characteristics

Detect	To prevent this kind of attack in the future, the team needs to install IDS/IPS tools such as Next Generation Intrusion Prevention System (NGIPS) and SIEM tools like Chronicle to analyze logs and alert security when there are suspicious activities.

Respond	The team blocked all incoming ICMP packets and stopped all-non critical network service. Our training was on how to configure firewalls to meet organization security needs and necessary tools to have to strengthen the security posture like SIEM tools, IDS/IPS tools etc.

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: