Incident Report Analysis

Summary	Today, our organization's network services suddenly stopped responding. Regular internal network traffic could not access any network resources. The incident management team discovered an incoming flood of ICMP packets, causing the disruption. The IM team then blocked all incoming ICMP packets, stopped all non-critical network services offline, and began restoring critical network services. These ICMP packets were from multiple sources, signifying a suspected DDoS attack. The response and recovery of network services took two hours, therefore causing a potential impact of two business hours lost.
Identify	The cybersecurity team audited the systems, devices, and network policies involved in the attack to identify the security gaps. The team found an unconfigured firewall that allowed a malicious attacker to send a flood of ICMP pings into the company's network. This flood overwhelmed the company's network through a Distributed Denial of Service (DDoS) attack.
Protect	To better protect from future attacks, the network security 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 network security team added new detection features, such as source IP Address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.
Respond	The incident management team blocked all incoming ICMP packets and stopped all non-critical network services offline. In future events, the team will

	isolate affected systems to prevent further disruption to the network. They will attempt to restore any disrupted critical systems and services and then analyze network logs for suspicious and abnormal activity. If applicable, the team will also report all incidents to upper management and appropriate legal authorities.
Recover	The incident management team restored critical network services after the attack. To recover from ICMP flooding DDoS attacks, access to network services must be restored to a normal functioning state. In the future, the firewall can block external ICMP flood attacks. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored. Finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can be returned online.

Reflections/Notes: