Incident report analysis

Summary	The organization's network services stopped responding because a flood of ICMP packets prevented normal internal network traffic from accessing network resources. The internal network was compromised for two hours until resolution.
Identify	The cybersecurity team's investigation found that a malicious actor sent a flood of ICMP pings through an unconfigured firewall in a distributed denial of service attack. A distributed denial of service attack occurred. The network was overwhelmed by an ICMP flood, causing network traffic to halt.
Protect	The security 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 ICMP traffic based on known suspicious characteristics.
Detect	IDS/IPS systems can be used to detect and stop suspicious activity and filter ICMP traffic in the future. Network monitoring software can be used to detect abnormal traffic patterns. SIEM tools can be used to review and analyze network information in real-time.
Respond	The incident management team blocked incoming ICMP packets, stopped all non-critical network services, and then restored critical network services. Tcpdump was used to analyze network logs and identify the source of attack. A similar series of steps can be used to respond to future incidents. Using dynamically scaled network operations could also help the organization better handle future incidents by enabling operations to continue even if a portion of the network is overwhelmed by a DoS attack. Server memory could be

	increased or processing capacity could be adjusted to prevent the network from being completely overwhelmed and minimize disruption to business operations. Reporting incidents to management and appropriate legal authorities if appropriate falls under response.
Recover	To recover, the security team needed information on the cause of the network traffic being obstructed so that steps could be taken to stop the DDoS attack. The process of blocking incoming ICMP packets and halting non-critical network services until critical services are restored is in place to help the organization recover. Users attempting to access the network during the period of disruption will need to be notified that their requested network services were not completed and can be reattempted.

Reflections/Notes: