Incident report analysis

Summary	This morning, a manager sent a request through to the IT department that the network services had suddenly stopped responding and could no longer access the network. This could possibly indicate that a malicious actor could have found a vulnerability in the network and exploited it to initiate a Denial of Service (DoS) attack.
Govern	To build a digital presence, it is important to secure our own digital presence. To convey to stakeholders, both internal and external, the possible financial, legal, regulatory and contractual ramifications in which a Denial of Service may have in connection to the services we provide as well as the capabilities, objectives, and outcomes that would suffer due to a cybersecurity threat of that nature. “To help small businesses build their digital presence, we blend creative design with smart marketing strategies to form strong brands and captivate audiences.”
Identify	The incident response team audited the systems and devices connected to the network by use of a virtual machine called tcpdump to analyze the network traffic. The network’s logs revealed that there had been a flood of incoming ICMP pings from multiple source IP addresses which is a possible indication that a malicious actor had initiated a DdoS (Distributed Denial of Service) attack on the network. The malicious actor flooded the ICMP pings into the network through an unconfigured firewall on the network’s server which overwhelmed the network’s bandwidth.
Protect	The network security team has implemented a new firewall rule to limit the rate of incoming packets. Source IP verification on the firewall has been added to check for spoofed IP addresses on

	incoming ICMP packets., and an IPS (Intrusion Prevention System) has been deployed to filter out some ICMP traffic based on suspicious characteristics.
Detect	An IDS (Intrusion Detection System) which is network monitoring software has been deployed in order to detect abnormal traffic patterns.
Respond	The incident management team responded by blocking incoming ICMP packets, and stopping all non-critical network services offline.
Recover	The incident management team has restored critical network services. We have notified management of the restoration of the services.

Reflections/Notes: