Incident Report Analysis

This template comes from the Google Cybersecurity Certificate course. It is used to record findings after completing an activity, or to note what has been learned about a specific tool or concept. This chart is also a way to continue practicing applying the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) in different situations.

Summary	In the given scenario, a company encountered a security incident that disrupted all network services. The root cause of the problem was a distributed denial of service (DDoS) attack due to a ICMP packet flood. The cybersecurity team blocked the attack, and stopped non-critical network services to prioritise the restoration of critical network services.
Identify	Unknown malicious actor(s) flooded the company with ICMP packets that brought down the whole internal network. Critical network resources must be secured and restored.
Protect	The cybersecurity team created a new firewall rule that limited the rate of incoming ICMP packets. They also filtered out suspicious ICMP packets using an Intrusion Prevention System.
Detect	Source IP address verification was enabled on the firewall to attempt to filter out spoofed IP addresses, although the success of such measures may be limited [1]. Network monitoring software was also installed to attempt to detect abnormal traffic.
Respond	External ICMP floods can be blocked with a firewall. Affected internal systems will hopefully be specific systems that can be isolated to prevent whole network disruption. Critical network resources will be restored. Logs will be checked for abnormal activity. Suspicious activity will be reported to upper management, CSA and the police. If more manpower or resources is needed, the company may also work with CSA's SingCert [2] to respond to the event.
Recover	Non-critical network services are stopped to limit internal network traffic. Critical network services are prioritised for restoration. Non-critical network services are subsequently restored after the ICMP flood is either blocked externally or stopped internally.

Reflection/Notes
Reference [1] states that IPv6 includes encryption and authentication features that help to limit the occurrence of ICMP floods, whereas IPv4 lacks these features and makes it hard to determine if packets are legitimate or forged at the receiving network's end rather than the sending network's end.

IP address forgery occurs at layer 3 (network layer), as it applies to IP packets, in the Open Systems Intercommunication (OSI) network model.

References

1. Kaspersky (2023) IP spoofing: How it works and how to prevent it. https://usa.kaspersky.com/resource-center/threats/ip-spoofing.
2. CSA (2023) About SingCERT. https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert.