Incident report analysis

Summary	Today, the organization experienced a two-hour outage of network services caused by a Distributed Denial of Service (DDoS) attack known as an ICMP flood. ICMP (Internet Control Message Protocol) is used to transmit network error messages. During the attack, the threat actor overwhelmed our network with a flood of ICMP ping requests. The investigation revealed that an unconfigured firewall allowed this malicious traffic to bypass security controls, resulting in the disruption of internal network services.
Identify	After investigation, the network security team determined that an unconfigured firewall allowed malicious ICMP traffic to enter the company's internal network. This vulnerability enabled the attacker to overwhelm the organization's servers with ICMP requests, saturating the LAN and resulting in a two-hour outage of internal network services. The audit confirmed that the disruption was limited to the internal network and caused all normal traffic to be unable to access network resources.
Protect	The team implemented new firewall configurations, including a rule to limit the rate of incoming ICMP packets and source IP address verification to detect and block spoofed addresses. In addition, new network monitoring software was deployed to identify abnormal traffic patterns, and an IDS/IPS (Intrusion Detection and Prevention System) was installed to filter ICMP traffic based on suspicious characteristics.

Detect	To detect future similar attacks, the team will implement a NGFW (Next Generation Firewall) which allows stronger security capabilities such as Deep Packet Inspection, Intrusion Protection and Threat Intelligence.
Respond	The Incident Management Team responded by blocking incoming ICMP packets, stopping all non-critical network services, and restoring critical ones. The Network Security Team also implemented new firewall rule configurations and deployed network monitoring software. Future response plans could include implementing stricter network segmentation and security zones to isolate critical resources, reducing the internal impact of similar attacks.
Recover	The team restored critical network services after identifying and mitigating the attack. After two hours, normal internal network operations were fully recovered. Following the restoration, IT staff were informed of the incident resolution and advised to monitor for any residual issues or abnormal network behavior. Recovering from an ICMP flood DDoS attack involves restoring access to network services to normal operational status. In the future, such attacks can be mitigated by blocking external ICMP traffic at the firewall. During the recovery process, non-critical network services should be temporarily halted to reduce internal traffic load. Priority should be given to restoring critical services first. Once the ICMP flood subsides, non-critical systems and services can then be safely brought back online.

Reflections/Notes: *This incident highlighted the importance of proper firewall configuration and proactive network monitoring to prevent DDoS attacks. I also learned how the NIST CSF provides a clear framework for analyzing incidents in stages, which helps separate immediate actions from long-term improvements. In future scenarios, I would consider additional measures such as stricter network segmentation and periodic response drills to reduce recovery time and impact.*