Incident report analysis

Summary	The company suffered a major disruption when network services stopped responding. After investigating, the cybersecurity team determined it was a distributed denial-of-service (DDoS) attack caused by an overload of ICMP packets. To get operations back online, the team blocked the attack traffic and shut down non-essential services so that critical systems could be restored quickly.
Identify	The attack was an ICMP flood launched by outside threat actors. It impacted the entire internal network, leaving all systems inaccessible. The immediate task was to secure and bring back the organization's most critical resources.
Protect	To reduce the chance of this happening again, the team updated the firewall with new rules that limit ICMP traffic. They also rolled out an IDS/IPS to filter packets that showed unusual or malicious patterns.
Detect	Additional safeguards were put in place to catch problems sooner. The firewall was configured to check source IP addresses for spoofing, and network monitoring tools were added to flag suspicious spikes or traffic flows.
Respond	For future incidents, the response plan calls for isolating any affected systems right away, restoring critical services as quickly as possible, and reviewing log files to find the root cause. The team will also make sure management is informed and involve legal authorities if needed.
Recover	To fully recover from the attack, normal network services had to be restored in stages. Going forward, ICMP floods will be blocked at the firewall before they reach the internal network. The recovery steps are to shut down non-essential services first, restore the most critical ones, and then bring everything else back online once the attack has run its course.

Reflections/Notes: This event underlined a few important lessons:

- Monitoring tools are just as important as firewalls. If unusual traffic patterns had been caught earlier, downtime might have been shorter.
- Firewalls must be regularly reviewed and configured properly. The attack worked in part because the firewall wasn’t set up to block ICMP floods.
- Clear procedures make response efforts faster. Having a written plan helps teams act with confidence instead of scrambling in the moment.
- Defense in depth is key. No single solution is enough—layering controls like firewalls, IDS/IPS, and monitoring offers stronger protection.
- Recovery planning should be tested. Practicing recovery steps ensures everyone knows what to do when the pressure is on.