Incident report analysis

Summary	Our company faced a severe security issue when our internal network suddenly stopped working. This problem occurred due to an attack called Distributed Denial of Service (DDoS), which used a massive number of incoming ICMP (Internet Control Message Protocol) packets. This attack completely disrupted our network services, and we had to act quickly to fix the problem.
Identify	We discovered that someone intentionally targeted our company with an ICMP attack. This attack affected our entire internal network and made it impossible to access many important network resources.
Protect	In response to the attack, we put some protective measures in place to reduce the threat. We made changes to our network security system to limit the number of ICMP packets coming in, and we added a IDS and IPS to spot and block suspicious ICMP traffic.
Detect	To improve our network security, we made sure our network security system could tell if the incoming ICMP packets had fake sender information. We also installed software to quickly notice any unusual network activity.
Respond	For future security problems, we've planned to react more effectively. We'll quickly separate the affected systems to stop the issue from spreading. We'll work to bring back the important systems and services that were disrupted. Then, we'll closely check our network logs for anything strange. If needed, we'll report the incidents to the company's leaders and the right legal authorities.

Recover	To get back to normal after a DDoS attack with ICMP flooding, we'll block these attacks at the network's entrance. We'll stop some less important network services to reduce the internal traffic. We'll bring back the critical services first. After a while, when the flood of ICMP packets stops, we can bring back the less important network systems and services.

Reflections/Notes: This report explains what happened during the DDoS attack and how we dealt with it. We're making changes to be better prepared for future attacks, making our network more secure.