Incident report analysis

Summary	Our company had a successful DDos attack on our systems which disabled them for 2 hours . This was achieved due to an ICMP flood in which our servers get bombarded by ICMP packets in order to fill up server queries and use up our resources. We had to block incoming ICMP packets, Stop all non-critical network services offline, and restore critical network services. We also implemented a firewall rule to limit the rate of the ICMP packets and another to check for spoofed IP addresses on incoming packets. To finish it up we added network monitoring software to detect abnormal traffic patterns and an IDS / IPS system to filter packet traffic based on suspicious characteristics.
Identify	We failed to configure the firewall and might suggest we have other assets that need their configuration and risk assessment practices checked as they may be inadequate or incomplete. We need to conduct regular security audits, maintain updates and configurations, perform risk assessments and prioritize the mitigation of risks
Protect	After identifying problems the team implemented several preventive measures to protect the network from future DDos incidents. We limited incoming ICMP packets with a new firewall rule and implemented network monitoring software as well as an ids / ips system We could further implement cybersecurity awareness training and regular audits and maintenance checks to our systems
Detect	We were able to detect an attack due to the system being flooded and unresponsive. Because we had no automated monitoring we had no way to respond to or delay the attack until after it was already in place. We should

	ensure these systems are regularly maintained and updated as well as configured for real time alerts so we can respond to threats quickly.
Respond	Once it was detected our team immediately took steps to reduce the attack's impact. Team blocked incoming ICMP packets to stop flooding and took down all non critical network services offline to reduce strain on the network while promptly restoring critical network services to resume essential operations as well as investigated incidents to identify the problems that allowed the attack to occur.
Recover	We need to build a recovery plan in case of incidents and backuos of critical assets as well as conduct interviews of team to get input on how to better the systems and make sure recovery aligns with business priorities

---

Reflections/Notes: DDos exposed a weakness in our system and helped us further implement safeties to keep our business safe.
Identify: Enhance risk management and asset identification processes
Protect: Bolster security and risk management with training and testing
Detect: Ensure continuous real time threat detection
Respond: Develop incident response procedures
Recover: Implement and test new recovery strategies
With this in mind we can implement these to any company we work with and our cybersecurity posture against future DDos attacks is strengthened