Incident report analysis

Summary	A DDoS attack compromised the internal network for two hours this morning. The attack involved flooding the network with ICMP packets through an unconfigured firewall, causing all network services to become unavailable. The incident management team successfully contained the attack by blocking ICMP traffic and implementing new security measures, including firewall rules, monitoring software, and an IDS/IPS system.
Identify	The firewall was unconfigured, lacking a limit on incoming ICMP packets and source IP address verification, making the network vulnerable. An IDS/IPS was not working to block the attack.
Protect	All firewalls should be configured with ICMP rate limits before going live. The network admin could use some training on secure firewall configuration standards, and the configuration should be reviewed on a monthly basis.
Detect	To detect future DDoS attacks, the network security team implemented a network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter ICMP traffic based on suspicious characteristics
Respond	The incident management team responded by blocking incoming ICMP packets and stopping all non-critical network services offline. After investigation, the team identified the root cause: an unconfigured firewall that failed to prevent a malicious actor from flooding the network with ICMP packets. The team successfully restored the network after two hours.
Recover	To improve future recovery capabilities, the organisation should implement backup network infrastructure to maintain business continuity during similar attacks. Additionally, the security team strengthened the network's resilience

	by deploying new firewall rules, IP address verification, network monitoring software, and an IDS/IPS system to prevent future incidents and enable faster recovery.

Reflections/Notes:

This incident highlights the critical importance of proper firewall configuration as a first line of defence - even basic security measures like ICMP rate limiting could have prevented this two-hour outage. The lack of proactive monitoring and IDS/IPS functionality meant the attack went undetected until services were already compromised, emphasising the need for layered security approaches. Moving forward, implementing automated configuration audits and establishing baseline traffic patterns will help prevent similar oversights and enable faster threat detection.