Incident report analysis

Summary	The company experienced a significant security event when all internal network services stopped responding due to a Distributed Denial of Service (DDoS) attack. The attack involved a flood of incoming ICMP packets targeting the company's network. The cybersecurity team promptly responded by blocking the malicious traffic and shutting down non-critical services to prioritize restoring critical network operations.
Identify	The DDoS attack was carried out by a malicious actor using an ICMP flood to overwhelm the internal network infrastructure. The entire network was affected, disrupting all services. The primary objective was to secure and restore critical network resources while preventing further disruption. The cause of the breach was identified as an unconfigured firewall that allowed the attack to penetrate.
Protect	To protect against future attacks, the cybersecurity team implemented the following measures: • **Firewall Rules:** A new rule was added to limit incoming ICMP packet rates. • **IDS/IPS Implementation:** An Intrusion Detection and Prevention System (IDS/IPS) was deployed to filter out suspicious ICMP traffic. • **Source IP Verification:** The system now verifies the source of IP addresses to detect and block spoofed or malicious IPs attempting to initiate an attack.

Detect	To improve the detection of future attacks: • **Network Monitoring**: Network monitoring software was installed to continuously scan for unusual traffic patterns, particularly surges in ICMP packets. • **Firewall Configuration**: Source IP address verification on the firewall was activated to check for spoofed IP addresses in real-time. • **Anomaly Detection**: IDS/IPS systems now monitor for abnormal traffic volumes, immediately alerting the cybersecurity team to potential threats.
Respond	For current and future incidents, the following response plan was established: • **Immediate Action**: The team will isolate affected systems to contain the attack and minimize damage. • **Service Restoration**: The team will prioritize restoring critical services and infrastructure. • **Log Analysis**: Post-incident, the team will thoroughly analyze network logs to trace the attack and identify any suspicious activity. • **Incident Reporting**: All incidents will be reported to senior management and, if necessary, to legal authorities, in compliance with regulatory requirements.
Recover	The recovery plan focused on restoring full network functionality: • **Service Restoration**: Network services were restored to normal operation following the blocking of ICMP packets. • **Future Recovery Plan**: Non-critical network services will be stopped during similar attacks to reduce internal traffic. The cybersecurity team will focus on restoring critical services first. • **Post-Attack Recovery**: After the attack times out, all non-critical services will be restored, ensuring minimal downtime for business

	operations.

Reflections/Notes: This incident highlighted the importance of having a well-configured firewall and robust intrusion detection systems in place. The response plan and preventive measures will be updated regularly to strengthen the organization's defenses against similar attacks in the future.