Incident report analysis

Summary	The company recently experienced a Distributed Denial of Service (DDoS) attack that disrupted network operations for two hours. The attack exploited an unconfigured firewall, allowing a flood of ICMP packets to overwhelm network services. This resulted in internal network traffic being unable to access resources. The attack targeted critical infrastructure and was traced to a botnet-controlled source. The estimated impact included financial losses due to downtime and potential reputational damage. In response, the company implemented firewall rules to limit ICMP traffic, source IP address verification, real-time network monitoring, and an Intrusion Detection/Prevention System (IDS/IPS) to detect and mitigate future threats. Moving forward, additional security enhancements will be made to strengthen the network's resilience.
Identify	The recent security event was a Distributed Denial of Service (DDoS) attack, specifically an ICMP flood attack that targeted the company's internal network. The attack overwhelmed network resources by sending a large volume of ICMP packets through an unconfigured firewall, disrupting normal operations. The targeted systems included the company’s internal servers and critical network infrastructure, causing downtime and financial losses. The attack source was identified as a botnet, using spoofed IP addresses to evade detection. Regular security audits will be conducted to assess vulnerabilities in internal networks, firewalls, and access controls. Penetration testing will help identify exploitable weaknesses, and an updated inventory of network assets will ensure timely patching. Role-Based Access Control (RBAC) will limit access to necessary personnel, and third-party vendors will be evaluated for security

	compliance to prevent supply chain vulnerabilities.
Protect	Security measures will be strengthened by configuring firewalls to limit ICMP traffic, segmenting networks to isolate critical assets, and enforcing Multi-Factor Authentication (MFA) for all access points. Regular security updates and patches will be applied promptly to reduce vulnerabilities. Employee cybersecurity training will focus on recognizing phishing, social engineering, and DDoS attack tactics. Additionally, a robust DDoS mitigation plan will be implemented, incorporating cloud-based protection and traffic filtering services.
Detect	Real-time network monitoring software will be deployed to track incoming and outgoing traffic, identifying unusual patterns such as excessive ICMP packets from untrusted sources. The IDS/IPS system will be fine-tuned to detect and block suspicious activities, including potential DDoS attacks. Automated alerts will notify security teams of anomalies, while continuous log monitoring and behavioural analysis will help detect unauthorized access attempts and early signs of cyber threats. User activity tracking and access logs will be reviewed regularly to differentiate between authorized and unauthorized access.
Respond	An Incident Response Team (IRT) will be established with predefined roles and responsibilities to ensure a rapid and coordinated response. Standard Operating Procedures (SOPs) will be continuously updated to address emerging threats. Forensic analysis tools will be used to investigate attack origins, track malicious activity, and gather evidence for mitigation strategies. A structured communication plan will be put in place to notify stakeholders, employees, and customers while ensuring transparency. Additionally, incident containment measures, such as temporarily isolating affected systems and

	implementing emergency firewall rules, will be enforced to minimize impact.
Recover	To ensure business continuity, automated system backups will be maintained with periodic testing for quick data and system restoration. Post-incident reviews will evaluate response effectiveness and refine security strategies. Network redundancy and failover mechanisms will be enhanced to improve system resilience. Incident response documentation will be regularly updated with key lessons, and ongoing cybersecurity training will be expanded to include simulated attack scenarios for better preparedness.

Reflections/Notes: This incident highlights the need for proactive security. Addressing firewall misconfigurations earlier could have prevented the attack. Moving forward, real-time monitoring, automated alerts, and employee training will be key to improving detection and response. A structured cybersecurity framework will strengthen network security and support ongoing improvements.