Incident report analysis

Summary	This incident involved a Distributed Denial of Service (DDoS) attack against the internal network of the organization. The attack occurred through an overwhelming volume of ICMP packets that disrupted normal network traffic, making it impossible for the internal network to access resources. The attack lasted for two hours until the incident management team responded by blocking incoming ICMP packets, taking non-critical services offline, and restoring critical network services. The investigation revealed that the attack exploited an unconfigured firewall, allowing the attacker to flood the network with ICMP traffic. The team has since implemented security measures to mitigate future risks, including new firewall rules, traffic monitoring tools, and an IDS/IPS system.
Identify	The incident management team performed an audit of the network systems, devices, and access privileges involved in the attack. They identified that the unconfigured firewall was a significant gap in security, as it allowed the attacker to send an avalanche of ICMP packets to the network. The attack targeted the availability of the network by overwhelming the system with ICMP pings. Additionally, there was a lack of monitoring and traffic filtering, which could have detected the attack earlier and minimized the impact.
Protect	To enhance the network's protection, the team implemented several measures: 1. A new firewall rule was applied to limit the rate of incoming ICMP packets. 2. IP source address verification was introduced to ensure that no spoofed IP addresses could be used in the incoming ICMP packets.

	3. Employees and network administrators were trained to configure and maintain firewalls correctly. 4. The organization also implemented software for network traffic monitoring to detect abnormal patterns and potential attacks. 5. An Intrusion Detection and Prevention System (IDS/IPS) was deployed to filter suspicious traffic based on known attack characteristics, especially ICMP-based anomalies.
Detect	The team enhanced their ability to detect future DDoS attacks by installing network monitoring software capable of detecting abnormal traffic patterns. The IDS/IPS system was configured to flag high volumes of ICMP traffic as potential DDoS activity. Additionally, the team implemented logging tools to monitor incoming traffic and track any unusual spikes in network activity, enabling faster detection and response to similar attacks in the future.
Respond	Once the attack was detected, the incident management team quickly took the following actions: 1. The incoming ICMP packets were blocked to stop the attack. 2. Non-critical services were taken offline to reduce the load on the network. 3. Critical network services were restored to resume business operations. 4. The team performed an analysis of the attack to understand the attack vector and how it was executed. 5. The organization communicated the incident to upper management, and the management informed clients about the disruption. 6. In compliance with local laws, the incident was reported to relevant authorities and law enforcement agencies.

Recover	To recover from the attack, the team performed the following steps: 1. The network services were restored to their normal functioning state. 2. No data was lost during the attack, as it was a network availability issue rather than a data breach or manipulation incident. 3. The network was fully restored, and services resumed operation after the attack was neutralized. 4. The team ensured that future DDoS attacks would be mitigated by implementing the newly deployed monitoring systems, firewall rules, and IDS/IPS systems.
Plan for Future Cybersecurity Incidents	Preventive Measures ● Regular firewall audits should be scheduled to identify any misconfigurations or gaps. ● Staff should receive ongoing training in recognizing and preventing DDoS attacks. ● Continuous evaluation and updating of network traffic monitoring tools to ensure they remain effective in detecting new attack patterns. Detection Methods ● Implementation of real-time traffic analysis tools to immediately detect unusual spikes in traffic or patterns indicative of DDoS attacks. ● Use of machine learning and anomaly detection tools to improve the identification of novel attack types. Response Plan ● Develop a detailed incident response playbook for DDoS and other common attack types.

	• The playbook should include specific actions, escalation procedures, and communication protocols to ensure quick and coordinated responses. Recovery Plan • Regularly test the recovery plan to ensure the network can be restored quickly in case of a DDoS attack or similar incident. • Implement automated traffic mitigation techniques, such as rate limiting and IP blocking, to reduce human intervention during recovery.

Reflections/Notes:
This incident highlighted the importance of proper firewall configuration and network traffic monitoring. In future, it is crucial to audit firewall rules regularly to ensure that security gaps, such as the unconfigured firewall, are closed. The implementation of rate-limiting for ICMP traffic, along with source address verification, has significantly improved the protection against DDoS attacks. Furthermore, the IDS/IPS system provides an added layer of security by proactively identifying suspicious activity. Training employees and network administrators on proper firewall configuration and response procedures is key to preventing similar incidents.