Incident report analysis

Summary	The organization experienced a Distributed Denial of Service (DDoS) attack, specifically a flood of ICMP packets that overwhelmed the internal network. This attack caused network services to become unresponsive for approximately two hours. The cybersecurity team discovered that an unconfigured firewall allowed malicious actors to exploit this vulnerability. The response included blocking ICMP packets, shutting down non-critical network services, and restoring critical services.
Identify	• **Type of Attack:** ICMP Flood DDoS Attack • **Affected Systems:** Internal network infrastructure, firewall, and critical business applications relying on network connectivity. • **Attack Source:** External malicious actors leveraging unconfigured firewall vulnerabilities. • **Impact:** Network downtime, disruption of business services, and potential financial loss.
Protect	To prevent future attacks, the organization should implement the following protective measures: • **Firewall Configuration:** Ensure the firewall is properly configured to limit the rate of incoming ICMP requests. • **Source IP Address Verification:** Deploy IP address verification to filter out spoofed addresses. • **Access Control Policies:** Implement strict access controls and segmentation to minimize exposure. • **Regular Security Audits:** Conduct periodic security reviews of

	firewalls, network configurations, and software patches. • **Security Awareness Training:** Educate employees on network security best practices and incident response procedures.
Detect	To enhance detection capabilities: • **Implement Network Monitoring Tools:** Deploy intrusion detection and prevention systems (IDS/IPS) to flag unusual ICMP traffic. • **Log Analysis:** Set up automated log analysis tools to track incoming and outgoing network traffic. • **Anomaly Detection Algorithms:** Utilize AI-driven analytics to detect irregular traffic patterns in real-time. • **User Behavior Monitoring:** Track access logs for anomalies and potential insider threats.
Respond	A well-defined incident response plan should include: • **Containment Strategies:** Isolate affected network segments to prevent further spread. • **Incident Classification:** Quickly categorize the threat level and engage appropriate teams. • **Mitigation Procedures:** Implement emergency firewall rules to block malicious traffic. • **Forensic Analysis:** Gather attack data for root cause analysis and future mitigation. • **Communication Protocols:** Establish internal and external communication strategies for incident updates.
Recover	To ensure smooth recovery and minimize downtime: • **Backup and Restore Protocols:** Maintain regular, secure backups to restore affected systems. • **Disaster Recovery Plan:** Define clear recovery steps and responsible teams. • **System Patch and Update Strategy:** Regularly update security policies

	and apply software patches. • **Post-Incident Review:** Conduct a retrospective analysis to document lessons learned and improve resilience. • **Testing and Simulation:** Perform regular incident response drills to ensure preparedness.

Reflections/Notes: By following this structured approach, the organization can significantly improve its ability to detect, respond to, and recover from future cybersecurity incidents while strengthening overall network security.