Incident report analysis

Summary	• Security Event: Distributed Denial of Service (DDoS) attack targeting the company's network. • Cause: Malicious actor sent a flood of ICMP pings through an unconfigured firewall, overwhelming the network. • Impact: Network services stopped responding for two hours, disrupting internal operations and access to network resources. • Response: Incident management team blocked incoming ICMP packets, took non-critical network services offline, and restored critical network services.
Identify	• Type of Attack: Distributed Denial of Service (DDoS) attack using ICMP flood. • Affected Systems: Internal network services, including web design, graphic design, and social media marketing solutions.
Protect	• Implement Proper Firewall Configuration: Ensure all firewalls are properly configured to filter and block malicious traffic, including ICMP floods. • Regular Firewall Rule Review: Conduct regular reviews of firewall rules to identify and address potential vulnerabilities. • Employee Training: Provide training on recognizing and responding to suspicious network activity, emphasizing the importance of cybersecurity protocols.

Detect	• Network Traffic Monitoring: Deploy network monitoring software to detect abnormal traffic patterns, especially ICMP floods. • User Account Activity Monitoring: Utilize software applications to track authorized versus unauthorized users and detect unusual activity on user accounts. • Anomaly Detection: Implement intrusion detection and prevention systems (IDS/IPS) to detect and mitigate suspicious network activity.
Respond	• Containment: Immediately isolate affected systems to prevent further spread of the attack. • Neutralization: Utilize IDS/IPS to filter out malicious traffic and mitigate the impact of the attack. • Analysis: Collect and analyze data on the incident, including network traffic logs and firewall configurations, to identify the attack source and potential vulnerabilities. • Recovery Improvement: Develop and document procedures for faster recovery, including system backups and restoration processes.
Recover	• Immediate Recovery Needs: Restore critical network services and ensure all systems are functioning properly. • Recovery Processes: Follow documented procedures for system restoration, including data recovery and configuration resets. • Continual Improvement: Conduct post-incident analysis to identify areas for improvement in the recovery process, such as enhancing backup strategies and updating recovery documentation.

Reflections/Notes: