Incident report analysis

Instructions

Summary	The organization suffered a distributed denial-of-service (DDoS) attack based on an ICMP flood. The attack was made possible due to an improperly configured firewall, allowing a malicious actor to overwhelm the network. This resulted in two hours of downtime for both internal and critical external services. The impact included network service interruptions and temporary productivity loss. The attack was mitigated by taking non-critical services offline, blocking ICMP packets, and implementing new firewall rules.
Identify	**Type of attack**: Distributed Denial-of-Service (DDoS) attack (ICMP flood). **Affected systems**: The company's internal network, including critical and non-critical services. **Cause**: Improperly configured firewall allowing unrestricted ICMP packet entry. **Origin**: Malicious actor using spoofed IPs to send a massive number of ICMP packets. **Estimated impact**: Two hours of functionality loss, potential financial damage, and harm to the company's reputation.
Protect	● Update the firewall with more restrictive rules for incoming ICMP packets, including rate limiting and blocking spoofed IPs. ● Implement a training program for the team on security practices and incident response. ● Adopt network segmentation policies to isolate critical services from vulnerable systems. ● Keep software and firmware on network devices updated.

Detect	● Install and configure real-time network monitoring tools to identify anomalous traffic patterns. ● Implement IDS/IPS systems to analyze and automatically block suspicious packets. ● Conduct regular audits of firewall logs and critical systems. ● Continuously monitor user accounts to detect unauthorized access attempts.
Respond	● Create a response plan that includes: 1. **Contain**: Quickly identify and block the source of suspicious traffic. 2. **Neutralize**: Isolate affected devices and apply appropriate firewall rules. 3. **Analyze**: Review event logs to identify failures and attack patterns. ● Ensure the incident response team is trained to handle similar attacks. ● Improve communication processes between teams during incidents to ensure a coordinated response.
Recover	● Restore critical network services and verify data integrity. ● Reconfigure the firewall and network devices to prevent similar vulnerabilities. ● Document the incident and the actions taken as a reference for future events. ● Conduct a post-incident analysis to identify improvements in response and recovery processes. ● Ensure regular backups are maintained and tested for quick recovery.

Reflections/Notes: This incident highlights the importance of an effective approach to cybersecurity, including conducting regular audits, team training, and implementing robust monitoring tools. Additionally, it emphasizes the need for a well-documented and tested incident response plan