Incident report analysis

Summary	We experienced a DDoS attack which led to the organization's network services suddenly stopped responding for 2 hours due to an incoming flood of ICMP packets. We responded by blocking all incoming ICMP traffic and stopping all non-critical services. After investigation, we configured that the threat actor exploited an unconfigured firewall to send the ICMP flood through.
Identify	The incident analysis revealed that a Distributed Denial of Service (DDoS) attack using a flood of ICMP packets disrupted the organization's internal network. The root cause was traced to an unconfigured firewall, which allowed unfiltered traffic to pass through. The attacker exploited this vulnerability by spoofing IP addresses, overwhelming the network infrastructure, and preventing normal operations for approximately two hours. Critical systems were rendered unresponsive, highlighting a gap in perimeter defense, traffic validation, and overall network visibility.
Protect	To enhance protection against future incidents, the following actions are recommended: Firewall Configuration and Maintenance: Implement strict rate-limiting rules for ICMP packets and enable source IP validation to block spoofed traffic. Schedule regular firewall audits and configuration reviews to keep policies updated with the latest threat intelligence. Port Filtering and Least Privilege Principles: Disable or restrict unused ports and services to reduce the attack surface. Apply the principle of least privilege to service access. Network Segmentation: Isolate critical services and business units into separate VLANs or subnets. This limits the impact of future breaches to only affected segments, enabling better containment. User and Access Management: Enforce strong access controls and multi-factor authentication (MFA) to protect critical administrative functions and interfaces.
Detect	To proactively detect suspicious activity and potential threats: Intrusion Detection Systems (IDS):

	Deploy an IDS to identify malicious traffic patterns, particularly anomalies involving ICMP traffic and connection floods. Security Information and Event Management (SIEM): Utilize tools like Google Chronicle or Splunk to aggregate and analyze network logs for early indicators of compromise. Set alerts for traffic spikes, unauthorized access attempts, or ICMP surges.
Respond	In the event of future incidents, the organization should follow a structured response plan that includes isolating affected systems or network segments and disabling non-essential services to contain the spread. An updated incident response playbook should guide the team through containment, investigation, and recovery phases. Tools such as tcpdump and SIEM logs can assist in analyzing the nature of the attack, identifying indicators of compromise, and informing mitigation efforts.
Recover	After the incident, the first step is to bring back the most important systems and services so that the business can keep running. Once those are working, the rest of the non-essential systems can be turned back on carefully, making sure everything is safe and working correctly. It’s important to have up-to-date backups of important files and system settings to avoid losing data. After everything is restored, the team should review what happened, figure out what went wrong, and make improvements to prevent the same problem in the future.