Incident report analysis

Summary	A DDoS attack targeted the company's internal network. The attack involved a flood of ICMP packets that caused network services to stop responding, affecting internal traffic for two hours. The security team responded by blocking incoming ICMP packets, shutting down non-critical services and restoring the services after mitigating the attack.
Identify	Through an internal audit, we discovered that the firewall lacked proper configuration, allowing unfiltered ICMP traffic. The vulnerability enabled the DDoS attack, highlighting the need for better firewall rules, rate-limiting, and security policies.
Protect	A new rule was implemented to the firewall to limit the rate of incoming ICMP packets and prevent packet flooding. Activate IP address verification to detect and block spoofed IPs.
Detect	Deploy network monitoring tools to identify abnormal traffic and installed IDS/IPS to filter suspicious ICMP packets, ensuring ongoing surveillance of user activities
Respond	For future security events, the cybersecurity team will isolate malicious traffic, block untrusted IP addresses, and use logs and monitoring data to investigate and refine security protocols. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.

Recover	To recover from an ICMP flooding DDoS attack, the priority is to restore network services to normal operation. Once normal operation is restored, review and assess the recovery process to ensure readiness for future incidents. To prevent ICMP flooding attacks in the future, all external ICMP requests should be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic.

Reflections/Notes:

- Implementing detection strategies through network monitoring tools and IDS/IPS systems highlighted the need for ongoing vigilance and anomaly tracking to detect potential threats early. Developing a well-structured incident response plan reinforced the importance of timely containment and neutralization of threats, ensuring that critical systems are quickly restored to minimize downtime.
- This report showcased the necessity of a comprehensive approach to cybersecurity, combining prevention, detection, response, and recovery to safeguard network infrastructure from evolving threats