Incident report analysis

Completed By Carla Jacobsen August 13, 2025

Google Cybersecurity Cohort 2025

Summary	There was a DDOS attack using ICMP packets that took down the company's internal network.
Identify	The type of DDOS attack was an ICMP flood, which floods the server with ICMP error message packets. It affected the company's internal network. It got through because the firewall was unconfigured.
Protect	The firewall was unconfigured, so now it must be configured. The attacker's IP should also be blacklisted.
Detect	There needs to be an intrusion detection and prevention system in place to be able to detect malicious incoming traffic in the future. Use a SIEM/SOAR system to monitor traffic and look for suspicious activity. Log all IP addresses that try to communicate with the firewall.
Respond	Investigate the other machines for further signs of infection. Block the ICMP packets from the attacker and take offline any unnecessary equipment and restore any necessary equipment to full operation. The firewall was configured to block ICMP flooding.
Recover	The critical network services are back in full operation.

Reflections/Notes: