Incident report analysis

Summary	The organization’s network services suddenly became unresponsive, preventing regular internal traffic from accessing any network-based resources. This disruption was caused by a surge of incoming ICMP packets. In response, the incident management team blocked ICMP traffic, temporarily disabled all non-essential network services, and worked to restore the critical ones. Following the event, the cybersecurity team launched an investigation and discovered that a threat actor had initiated a flood of ICMP pings through a firewall that was not properly configured. This security gap enabled the attacker to execute a Distributed Denial of Service (DDoS) attack, overwhelming the organization’s network infrastructure.
Identify	The type of attack that occurred was a DDoS attack using ICMP packets, which caused a two-hour network outage. The systems affected were internal network services, user access to shared resources, and the firewall itself.
Protect	To protect the company from future cyberattacks, the network security team implemented the following measures: a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics. The company should also consider conducting a penetration test to reveal hidden vulnerabilities. In addition to these technical controls, the organization should perform regular audits to ensure systems are running correctly and configured properly.

Detect	Alerts should be set up to warn the security team if there's unusual ICMP activity or sudden spikes in traffic trying to go through the firewall. The IDS/IPS is already in place to help detect suspicious traffic patterns that could point to an ICMP flood or other types of attacks, so when something is detected or blocked, it should be investigated right away. User accounts should be watched for unusual login times, strange locations, or anything else that might suggest someone is trying to break in.
Respond	If another cybersecurity incident happens, the organization should have a clear response plan in place, such as a playbook that explains the steps to take during an active attack. The first step should be to isolate any affected systems so the attack doesn't spread. Any suspicious or harmful traffic should be blocked at the firewall. The security team should check logs and monitoring tools to figure out where the attack came from and why it's happening.
Recover	To recover from a cybersecurity incident, the organization should focus on getting critical systems and services running again as quickly and safely as possible. Before reconnecting anything to the network, it's important to check that the systems haven't been compromised. Recovery procedures should also be updated based on what was learned from the incident. Keeping a list of the most important systems and data can help speed up recovery if something like this happens again.

Reflections/Notes: