Incident report analysis

Summary

The organization experienced a Denial of Service (DoS) attack that disrupted internal network services for approximately two hours. The attack was caused by a malicious actor flooding the network with ICMP packets, overwhelming network resources and preventing legitimate internal traffic from accessing services. The attack entered the network through an unconfigured firewall, which lacked ICMP rate limiting and source verification. As a result, normal business operations were interrupted, and critical internal services became unavailable. The incident response team mitigated the attack by blocking ICMP traffic, disabling non-essential services, and restoring critical network functions.

Identify

The security event was identified as a Denial of Service (DoS) attack using an ICMP flood.

- Targeted systems: Internal network infrastructure, network services, and critical internal resources
- Attack source: External malicious actor using spoofed or unverified IP addresses
- Vulnerability identified: Firewall misconfiguration allowing unrestricted ICMP traffic
- Impact: Network outage lasting two hours, loss of service availability, and reduced employee productivity

The incident revealed gaps in firewall configuration, network monitoring, and traffic filtering policies, increasing the organization's exposure to availability-based attacks.

Protect

To better secure the organization's assets, the following systems and procedures need to be updated:

- Implement ICMP rate-limiting firewall rules
- Enable source IP address verification to prevent spoofed traffic

- Harden firewall configurations using secure baseline standards
- Limit exposure of non-critical network services
- Update network security policies and procedures
- Provide targeted training for IT and network staff on DoS mitigation techniques

These protective measures reduce the attack surface and strengthen defenses against future network-based attacks.

Detect

To improve detection of similar incidents in the future, the organization should:

- Deploy network monitoring tools to analyze traffic patterns in real time
- Implement an Intrusion Detection System (IDS) to flag abnormal ICMP traffic
- Use firewall logging to track allowed and blocked traffic
- Monitor authorized vs. unauthorized access attempts
- Establish alert thresholds for traffic spikes and anomalies

These tools allow faster identification of suspicious activity before it escalates into a full network outage.

Respond

For future cybersecurity incidents, the response plan should include:

- Rapid containment by blocking malicious traffic at the firewall
- Isolating affected network segments if necessary
- Temporarily disabling non-critical services
- Collecting and analyzing firewall logs, IDS alerts, and traffic data
- Documenting the incident and communicating findings to stakeholders
- Updating response procedures based on lessons learned

This structured response ensures incidents are contained quickly and analyzed effectively.

Recover

To recover from similar incidents, the organization should:

- Prioritize restoration of critical network services
- Validate system integrity before returning services to normal operation
- Use configuration backups to restore secure firewall settings
- Ensure network availability is fully restored
- Review and improve recovery documentation and communication processes

Improving recovery planning reduces downtime and strengthens organizational resilience.

Incident report analysis - Example

Summary	This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicate that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern indicated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. It appears that not only was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that an intern's login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database.
Protect	The team has implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, and training for all employees on how to protect login credentials. Additionally, we will implement a new protective firewall configuration and

	invest in an intrusion prevention system (IPS).
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.
Respond	The team disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup.