Scenario

Unexpected Downtime Due to External ICMP Flood

Scenario Overview:
On a typical Wednesday afternoon at "NextWave Solutions GmbH", a mid-sized cloud services provider in Germany, the entire company's internal and client-facing services suddenly became unresponsive. Employees were unable to access email, cloud storage, internal tools, or even basic internet services. Clients began flooding customer support with reports of service outages.

Timeline & Discovery:

- **14:03**: Internal monitoring systems flagged an unusual spike in inbound network traffic.
- **14:07**: All users reported they lost access to the company's web-based systems.
- **14:10**: The incident response team began an investigation and noticed an overwhelming number of ICMP packets targeting all edge routers and internal servers.
- **14:15**: A full-scale Distributed Denial of Service (DDoS) attack using ICMP flood was confirmed.

Immediate Action Taken:

- Non-critical services were temporarily shut down to reduce internal load.
- A temporary rule was added to the firewall to drop excessive ICMP requests.
- An Intrusion Detection/Prevention System (IDS/IPS) was tuned to detect suspicious ICMP behavior.

Post-Attack Measures:

- The firewall was updated with rate-limiting rules for ICMP traffic.
- Source IP verification was enabled to prevent spoofing.
- Network traffic logs were analyzed to identify patterns and potential attacker IPs.
- A decision was made to report the event to upper management and, if needed, to law enforcement.

Lessons Learned & Future Mitigation:

- Additional training for IT staff on DDoS detection and mitigation.
- Scheduled simulations of DDoS response protocols.
- Review of contracts with internet providers for DDoS protection services.