Incident Report Analysis

Name: Hridhima Karmakar

Summary:

A mid-sized e-commerce company experienced a major disruption when its website and internal systems became unresponsive during peak business hours. The incident was traced back to a DDoS attack using a flood of ICMP packets, overwhelming the network and preventing both customer access and internal operations. The IT security team took immediate steps to contain the attack and begin restoration efforts.

Identify:

The attack involved an ICMP flood targeting the company's external network perimeter. This traffic saturation disrupted inbound and outbound services across the network, affecting web servers, cloud-based inventory systems, and communication tools. The attack originated from multiple spoofed IPs and had a widespread impact across departments.

Protect:

In response, the security team configured rate-limiting rules on the perimeter firewall to throttle incoming ICMP packets. They also enabled intrusion prevention filters to automatically block abnormal ICMP traffic based on predefined patterns. Additional protective measures included disabling ICMP response from exposed endpoints and applying geo-restrictions for high-risk regions.

Detect:

The anomaly was first noticed through an alert from the network monitoring dashboard, which recorded a dramatic spike in ICMP traffic. The team verified the cause using log data from both firewall and cloud-based monitoring tools. They confirmed the source IPs were likely spoofed, commonly seen in denial-of-service scenarios.

Respond:

The IT team activated their incident response plan, which included:

- Blocking incoming traffic from flagged IP addresses
- Diverting traffic using a DDoS mitigation service
- Notifying cloud service providers to apply additional safeguards
- Communicating the issue to department heads and pausing non-essential online services to prioritize remediation

An internal incident report was drafted, and stakeholders were updated regularly throughout the response phase.

Recover:

Once malicious traffic subsided, the team prioritized recovery by:

1. Restoring web access and communication tools for customer support
2. Bringing cloud systems back online for order processing
3. Reviewing and updating network configurations
4. Implementing long-term DDoS prevention tools and a revised escalation plan for faster future recovery

---

Reflections/Notes:

This experience reinforced the need for layered protection and real-time visibility into network traffic. While firewalls and detection tools played a critical role in defense, proactive response coordination was just as essential. Going forward, scheduled DDoS drills and improved logging will be implemented to further reduce the organization’s exposure to similar threats.