# Incident report analysis

| | |
|---|---|
| **Summary** | Two hours ago, the organization experienced a Distributed Denial-of-Service (DDoS) attack. During the incident, all internal network services stopped responding due to a flood of ICMP packets. The incident response team quickly intervened by blocking incoming ICMP traffic, stopping non-critical services, and restoring critical ones. A post-incident investigation revealed that the attack was made possible due to an **unconfigured firewall**, which allowed a malicious actor to overwhelm the company's infrastructure. The cybersecurity team has since implemented measures to mitigate the risk of future attacks. |
| Identify | The cybersecurity team audited the network and firewall configuration to determine the root cause of the incident. They found that the firewall lacked essential configurations and rules, allowing the attacker to send a flood of ICMP packets into the internal network. The team identified this misconfiguration as the primary vulnerability exploited during the attack. |
| Protect | To address this security event, the network security team implemented:<br>• A new firewall rule to limit the rate of incoming ICMP packets<br>• Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets<br>• Network monitoring software to detect abnormal traffic patterns<br>• An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristi**cs** |

| | |
|---|---|
| Detect | The team adopted advanced network monitoring tools such as Wireshark and Nagios to identify future threats. These tools will monitor:<br>• **Sudden spikes** in network traffic.<br>• **Unusual IP addresses** that may indicate spoofing or botnets.<br>• **Repeated requests** or anomalies that signal a potential DDoS attempt. |
| Respond | During the attack, the team quickly took the following response steps:<br>• **Blocked all incoming ICMP traffic**.<br>• **Shut down non-essential services** to conserve resources.<br>• **Restored critical systems** to ensure business continuity.<br>• **Logged the event** and initiated a forensic investigation to understand the attack in detail.<br>• **Updated the incident response plan** based on lessons learned. |
| Recover | The IT department ensured that all systems were fully operational post-incident. Non-critical services were brought back online after confirming network stability. The team also:<br>• **Patched the firewall** and other network devices.<br>• Conducted a **post-incident meeting** to document insights.<br>• Scheduled **regular firewall audits** and **configuration reviews** as part of recovery and continuous improvement. |

Reflections/Notes: