**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | This week, the organization experienced a **DDoS attack** that caused the internal network to stop working for about **two hours**. The attack was caused by a flood of ICMP ping packets that overwhelmed the firewall. During the incident, employees could not access network resources and normal business operations were interrupted. The investigation showed that the firewall was not properly configured, which allowed the attacker to send a large amount of traffic into the system. |
| **Identify** | The incident management team reviewed systems and firewall settings to find the security gap. It was discovered that the firewall did not have rules in place to block or limit ICMP traffic. This allowed a malicious actor to flood the network with packets, making it unavailable. |
| **Protect** | The team implemented new firewall rules to limit the rate of ICMP packets and enabled **source IP verification** to block spoofed traffic. Network security policies will be updated, and employees will be trained to regularly check configurations. |
| Detect | To detect unusual activity in the future, the company installed **network monitoring software** and an **Intrusion Detection/Prevention System (IDS/IPS)**. These tools will alert the security team if there is abnormal traffic or another attempt at a DDoS attack. |
| **Respond** | During the incident, incoming ICMP traffic was blocked, and non-critical services were taken offline to reduce the load. Critical services were restored first so employees could continue work. The incident response team analyzed the attack and updated the security process to handle future events more effectively. |
| **Recover** | After two hours, the network was fully restored. Firewall rules were strengthened, monitoring tools were added, and the system is now more resilient. A recovery plan has also been developed to ensure faster response and communication in case of another attack. |