**Incident report analysis**

|  |  |
| --- | --- |
| Summary | Our company, a multimedia firm offering web design, graphic design, and social media marketing services, experienced a Distributed Denial of Service (DDoS) attack. The attack lasted approximately two hours, during which internal network services stopped responding. The root cause was a flood of ICMP (Internet Control Message Protocol) packets sent from external sources that overwhelmed the network through an unconfigured firewall.  The incident response team mitigated the issue by:   1. Blocking incoming ICMP traffic 2. Shutting down non-critical services 3. Restoring access to essential services   Following the event, several security upgrades were implemented to prevent future attacks. |
| Identify | Type of attack: Distributed Denial of Service (DDoS) via ICMP flood  Systems impacted: Internal network of the organization  Vulnerability: Unconfigured firewall that allowed unrestricted ICMP traffic  Impact: Downtime of two hours, disruption of business operations, risk of losing user’s trust. |
| Protect | To better protect our assets from future DDoS incidents, we should:  Regularly audit firewall configurations to ensure all rules are enforced. Implement baseline security settings and check them weekly. Conduct staff training on identifying such threats. Limit ICMP traffic and apply rate limiting as a permanent rule. Use network segmentation to distribute the network into subnets so that even if one gets compromised others will be safe. |
| Detect | We can improve our ability to detect similar attacks by:   1. Using network monitoring tools to track real-time traffic flow 2. Setting up alerts for abnormal increases in ICMP or other packet types 3. Implementing Intrusion Detection/Prevention Systems (IDS/IPS) to detect spoofed IPs and suspicious packet behaviour 4. Running weekly log analysis to spot patterns or changes in traffic 5. Monitoring authentication attempts and resource usage on key devices |
| Respond | Our response plan for future incidents includes:  Isolate affected devices or segments of the network immediately. Block incoming traffic from the suspicious source using firewall and router rules. Use preconfigured playbooks for DDoS scenarios to speed up action. Collect data such as network logs, source IPs, and timestamps to analyse the attack. Conduct a post-incident review to update response plans and staff procedures. |
| Recover | To recover from a DDoS attack or similar incidents, we will:  Restore services using backups and configuration templates. Conduct system checks to ensure no data or configuration corruption occurred. Evaluate uptime metrics and monitor services for recurring issues. Inform affected clients or users, if needed, and share steps taken for resolution. Use insights from the incident to improve disaster recovery planning. |