**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | On July 31, 2025, a distributed ICMP-flood DDoS attack against our unconfigured perimeter firewall rendered all web design, graphic design, and social-media marketing services—and internal collaboration tools—unavailable for two hours. Normal internal traffic could not reach any network resources until the flood subsided. | | |
| --- | --- | --- | --- |
| Identify | Post-incident analysis revealed that our external firewall lacked any rate-limiting rule for ICMP traffic and did not perform source-IP validation. We also identified an absence of regular firewall configuration audits and no baseline for normal volumetric traffic. | | |
| Protect | To harden our environment, we have:   * Added a firewall rule to rate-limit ICMP echo requests. * Enabled source-IP verification (reverse-path filtering) on the firewall. * Updated change-management policies to require periodic firewall-rule reviews. * Scheduled staff training on recognizing and escalating early DDoS indicators. | | |
| Detect | We augmented our monitoring capabilities by:   * Deploying network-wide traffic-flow baselining tools with ICMP-flood alert thresholds. * Integrating an IDS/IPS to flag and drop suspicious ICMP patterns. * Configuring real-time dashboards and multi-channel alerts for volumetric anomalies. | | |
| Respond | Our refined response playbook now directs the team to:   1. Immediately block all ICMP at the firewall perimeter. 2. Take non-critical services offline to conserve bandwidth. 3. Prioritize restoration of VPN, customer portals, and e-mail. 4. Communicate status updates to stakeholders and capture packet-trace logs for forensics. | | |
| Recover | After restoration, we:   * Verified the integrity of routers, switches, and application servers before re-enabling full services. * Confirmed no data loss or corruption occurred during the outage. * Conducted a lessons-learned review to update our DDoS playbook, adjust SLAs, and schedule semi-annual penetration tests for continual improvement. | | |

| Reflections/Notes:**Importance of Configuration Management:**  Regular audits of firewall and network device configurations are critical. An unconfigured or misconfigured firewall can turn into a single point of failure.  **Layered Defenses Work Best:**  Relying solely on perimeter blocking is insufficient. Combining rate-limiting, source-verification, IDS/IPS, and anomaly detection provides multiple hurdles for an attacker.  **Proactive Monitoring Pays Off:**  Establishing traffic baselines and alert thresholds ahead of an incident enables faster detection and reduces “time to detect.”  **Clear Response Playbooks Save Time:**  Having predefined, tested procedures for containment, communication, and restoration accelerates response and minimizes downtime.  **Continuous Improvement Cycle:**  Post-mortem reviews, lessons-learned meetings, and regular penetration tests ensure that each incident strengthens, rather than merely tests, the organization’s security posture. |
| --- |