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	A critical availability outage occurred due to an **ICMP Flood DoS attack**. An attacker exploited a permissive firewall configuration, saturating internal network bandwidth. The incident lasted two hours, halting all design and marketing operations until the malicious traffic was mitigated.
Identify	**Attack Type:** DoS (ICMP Flood). **Scope:** Total downtime of internal network and multimedia services for 120 minutes. **Affected Systems:** Perimeter firewall, internal network gateways, and all workstations relying on shared network resources. **Vulnerability:** Inadequate ingress rule configuration on the perimeter firewall.
Protect	**To reduce the attack surface and harden the perimeter:** ● **Implemented Rate Limiting to restrict the volume of ICMP packets accepted by the firewall.** ● **Enabled Source IP Verification (anti-spoofing) to validate packet legitimacy.** ● **Established a hardening policy to disable unnecessary protocols on external interfaces.**

Detect	To reduce the attack surface and harden the perimeter: ● Implemented **Rate Limiting** to restrict the volume of ICMP packets accepted by the firewall. ● Enabled **Source IP Verification (anti-spoofing)** to validate packet legitimacy. ● Established a hardening policy to disable unnecessary protocols on external interfaces
Respond	The response protocol for similar future incidents now includes: ● Immediate isolation of non-essential ICMP traffic. ● Prioritization of critical services via **QoS** to maintain business continuity. ● Neutralization of the attack source through dynamic firewall blocking.
Recover	To restore operations and ensure resilience: ● Phased service restoration, prioritizing core production assets. ● Performance of post-mitigation connectivity and latency tests to ensure network stability. ● Post-incident review to update security policies based on audit logs.

Reflections/Notes: This incident demonstrated the need for a more rigorous hardening policy. The default factory firewall configuration is not sufficient for production environments. I recommend implementing a firewall rule audit every 90 days to ensure that legacy or misconfigured permissions do not create new attack vectors.