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	The organization experienced a Distributed Denial of Service (DDoS) attack caused by a flood of ICMP packets entering through an unconfigured firewall. This overwhelmed the internal network and disrupted all services for two hours. The incident was mitigated by blocking ICMP traffic, shutting down non-critical services, and restoring essential services. A post-incident review identified firewall misconfiguration as the main vulnerability.
Identify	Conducted a security audit and discovered that the firewall lacked proper configuration to block ICMP flood traffic. Identified affected systems: internal network services (web, email, file servers). Business impact: complete halt of network operations for two hours, affecting service delivery to clients. Access gaps: no verification of spoofed IP addresses, leaving network exposed to volumetric attacks.
Protect	Implemented new firewall rules to limit ICMP packet rates.

	Enabled source IP verification to block spoofed traffic. Enhanced employee awareness on DDoS risks and response procedures. Updated firewall configurations and documented standard operating procedures for network security. Added training for IT staff to review and maintain firewall and IDS/IPS configurations regularly.
Detect	Installed network monitoring tools to flag abnormal traffic patterns. Deployed IDS/IPS to analyze ICMP traffic and detect malicious activity. Established logging and alerting to notify IT teams in real time of unusual spikes in network traffic. Continuous monitoring of traffic baselines to quickly identify deviations.
Respond	Response plan included immediate blocking of ICMP packets. Disabled non-critical services to preserve essential operations. Communication of incident status shared with IT leadership and management. Conducted forensic analysis to confirm attacker methods (ICMP flood via firewall gap). Documented lessons learned and updated the incident response playbook for DDoS attacks.

Recover	● Restored network functionality within two hours of the attack. ● Verified restoration of critical services (email, web hosting, file servers). ● Improved recovery strategy: faster failover plans, redundant systems, and enhanced firewall policies. ● Planned periodic simulation exercises for DDoS scenarios to test recovery readiness.

Reflections/Notes: This incident emphasized the importance of proactive firewall management and layered defense. Implementing monitoring, IDS/IPS, and firewall hardening reduced the attack surface. Moving forward, recovery testing and ongoing audits will ensure the organization maintains resilience against similar threats.