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 multimedia company offering web design, graphic design, and social media marketing services experienced a distributed denial of service (DDoS) attack that compromised the internal network for two hours. The attack occurred through a flood of ICMP packets sent by a malicious actor who exploited an unconfigured firewall vulnerability. The massive influx of ICMP pings overwhelmed the network infrastructure, preventing normal internal traffic from accessing network resources and disrupting all business operations. The incident management team responded by blocking incoming ICMP packets, shutting down non-critical services, and restoring critical network functions. The attack was successfully mitigated after implementing rate limiting rules, source IP verification, network monitoring tools, and an IDS/IPS system.
Identify	The incident involved a volumetric DDoS attack specifically targeting our network layer through ICMP flood. The affected systems included our main firewall infrastructure which lacked proper configuration, all internal network services, web servers hosting client websites, database servers containing client project data, and internal communication systems. The attack vector was identified as excessive ICMP echo requests exploiting the misconfigured firewall that allowed unlimited ICMP traffic to pass through without filtering or rate limiting. The business impact included complete network unavailability for

	two hours, inability to access client projects and files, disrupted communication between teams, and potential damage to client trust and company reputation.
Protect	To strengthen our security posture and prevent similar incidents, we will implement comprehensive firewall hardening including proper ACL configurations and geo-blocking of suspicious regions. All network devices will undergo security baseline configurations with unnecessary services disabled and default settings changed. We will establish a defense-in-depth strategy with multiple security layers including perimeter firewalls, internal segmentation, and endpoint protection. Employee training programs will be developed to increase awareness about DDoS attacks and proper incident response procedures. Additionally, we will implement automated backup systems for critical services and establish redundant network paths to maintain business continuity during attacks.
Detect	Our detection capabilities will be enhanced through implementation of real-time network traffic analysis using SIEM tools to identify abnormal traffic patterns and sudden spikes in ICMP packets. We will deploy NetFlow monitoring to track traffic flows and detect volumetric anomalies across all network segments. The IDS will be configured with custom rules to alert on excessive ICMP traffic from single sources or distributed sources. Automated alerting thresholds will be established for packet rates, bandwidth utilization, and connection attempts. Additionally, we will implement log aggregation and correlation to identify attack patterns across multiple network devices and establish a 24/7 monitoring schedule with escalation procedures.
Respond	Our incident response plan includes immediate activation of DDoS mitigation procedures when abnormal ICMP traffic is detected, with automated rate limiting rules triggering at predetermined thresholds. The response team will isolate affected network segments to prevent lateral spread while maintaining critical services through alternate routes. Communication protocols include

	immediate notification to management, IT staff, and affected clients through predetermined channels. We will conduct real-time traffic analysis to identify attack sources and patterns for blocking at the ISP level if necessary. Post-incident procedures include comprehensive logging of all actions taken, evidence preservation for potential legal action, and coordination with law enforcement and ISP for persistent attacks.
Recover	Recovery procedures focus on systematic restoration of services starting with critical business functions, followed by client-facing services, and finally internal tools. We will verify the integrity of all systems before bringing them back online to ensure no backdoors or persistent threats remain. Database synchronization will be performed to ensure data consistency across all replicated systems. Client communication will include transparent updates about service restoration timelines and any potential data impacts. Post-recovery validation includes stress testing of implemented controls, verification of monitoring tool functionality, and documentation updates reflecting new security measures. We will conduct a lessons-learned session within 48 hours to identify improvement areas and update our incident response playbooks accordingly.

Reflections/Notes: