Incident report analysis: NIST Cybersecurity Framework (CF)

Summary	A Distributed Denial of Service (DDoS) attack occurred due to an unconfigured firewall, allowing an ICMP packet flood. This caused a 2-hour network outage, disrupting critical services. The response included blocking ICMP packets, deploying firewall rules, IP verification, network monitoring tools, and an IDS/IPS.
Identify	Attack Type: DDoS (ICMP flood). Affected Systems: Internal network resources, critical services (web/graphic design tools, marketing platforms). Root Cause: Unconfigured firewall allowing unchecked ICMP traffic.
Protect	- Enforce firewall configuration audits. - Implement rate-limiting for ICMP traffic. - Deploy anti-spoofing measures (e.g., BCP38). - Conduct cybersecurity training for staff. - Establish strict access controls and multi-factor authentication (MFA).
Detect	- Use network monitoring tools to flag abnormal traffic (e.g., spikes in ICMP). - Integrate SIEM for real-time log analysis. - Enable IDS/IPS to auto-block suspicious patterns. - Regularly audit traffic sources and destinations.
Respond	Containment: Isolate affected segments, block malicious IPs. Neutralization: Activate incident response team, deploy firewall rules. Analysis: Collect logs for forensic review, identify attack vectors. Communication: Notify stakeholders, update status via predefined channels.
Recover	- Restore services using validated backups. - Test systems for vulnerabilities post-recovery. - Update incident response plans with lessons learned. - Conduct a post-mortem review to improve resilience.

Reflections/Notes: The incident highlighted gaps in firewall configuration and real-time monitoring. Future improvements should focus on proactive threat hunting and automated response mechanisms. Regular penetration testing and collaboration with external cybersecurity experts could further strengthen defenses.