Incident report analysis

Am using the NIST Cybersecurity Framework to improve the company network security.

Summary	I am a cybersecurity Analyst working for a multimedia company that offers web design services, graphic design and social media marketing solutions to small businesses. The organization just experienced a two hour network outage due to a DDOS attack involving a flood of ICMP Packets. The malicious attacker exploited an unconfigured firewall, which allowed the malicious traffic to overwhelm the internal system, making traffic resources inaccessible. The incident response team mitigated the issue by blocking ICMP traffic, shutting down non-essential service and restoring critical ones. A post-incident investigation confirmed the firewall vulnerability.
Identify	The internet network service and connected devices relied upon delivering client facing service. The malicious actor sends a flood of ICMP ping into the company's network through an unconfigured firewall, and this unconfigured firewall is the vulnerability that the malicious actor exploited.
Protect	The team implemented the network segmentation and categorised them into critical and non critical network service, then implement policies to prevent future attacks: A new firewall rule to limit the rate of incoming ICMP packets, Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, Using network monitoring software to detect abnormal traffic patterns and lastly an IDP/IPS system to filter out some ICMP traffic based on suspicious

	characteristics
Detect	The internal monitoring tools detected that network service stopped working, analysis also showed an abnormal flood of the ICMP packets originating from different sources and location, which is as a result of no anomaly-based detection in place for DDOS patterns.To detect new unauthorized access attacks in the future, the team will use Firewall, Intrusion Detection system (IDS) and Intrusion prevention system (IPS) to monitor all incoming traffic from the network.
Respond	The first thing the team did was to block incoming ICMP at the firewall level, shut down non-critical network service to reduce the network load. Prioritize the restoration of the critical network service. Realized that the DDOS attack was as a result of lack of ICMP packet control. The incident response team worked with other teams to contain and mitigate the attack.
Recover	The team was able to restore network service after filtering the malicious traffic, we then tested the new firewall and detection rules. and business continued after the network was restored. But for future purposes we plan to conduct regular penetration testing, and schedule firewall configuration review.

Reflections/Notes: This incident was a critical learning experience that highlighted the importance of proactive cybersecurity measures, even for small to mid-sized businesses like ours. The DDoS attack exposed a significant vulnerability in our infrastructure: an unconfigured firewall which allowed a flood of ICMP packets to disrupt internal operations. Although the issue was resolved within two hours, it caused a complete halt in our network

services, impacting productivity and potentially damaging client trust.

What stood out most was how a single misconfiguration could be exploited at scale. It reminded us that basic security hygiene, such as proper firewall configuration and traffic filtering, must never be overlooked. The incident also demonstrated the value of having an effective incident response plan, as our team was able to contain the attack relatively quickly and restore essential services.

Moving forward, this event has reinforced the need for continuous monitoring, regular vulnerability assessments, and layered defense strategies. The implementation of new firewall rules, IP verification, and IDS/IPS systems are steps in the right direction, but they must be accompanied by periodic audits, team training, and simulation exercises to remain effective. Ultimately, this attack served as a wake-up call and an opportunity to strengthen our cybersecurity posture before more serious damage could occur.