Incident report analysis

Summary	A multimedia company that provides web design, graphic design, and social media marketing services experienced a **Distributed Denial of Service (DDoS) attack** that disrupted its internal network for **two hours**. The attack involved a **large flood of ICMP packets** that exploited an **unconfigured firewall**, overwhelming network resources and preventing normal internal traffic from accessing systems. This incident exposed vulnerabilities in the company's network defenses, including inadequate firewall configuration and limited traffic monitoring.
Identify	The company's internal network was disrupted by a **Distributed Denial of Service (DDoS) attack** that exploited an **unconfigured firewall**, allowing a flood of ICMP packets to overwhelm network resources. This caused a two-hour outage where normal traffic could not access critical services. Key security risks include **misconfigured firewall settings**, lack of **traffic filtering and rate limiting**, and **insufficient monitoring** to detect unusual network behavior early.
Protect	To prevent similar attacks, the company should strengthen its network defenses by **properly configuring the firewall** with strict access controls and ICMP rate limiting. Implementing **network segmentation** will isolate critical systems, reducing the impact of future disruptions. Regular **security audits and patching** will address vulnerabilities, while **staff training** will ensure employees understand security protocols. Additionally, deploying **intrusion prevention systems (IPS)** and **redundant network infrastructure** will help maintain service availability even during an attack.

Detect	To improve detection, the company should implement **real-time network monitoring** to quickly identify unusual traffic patterns, such as sudden ICMP floods. Deploying **intrusion detection systems (IDS)** will help flag suspicious activity, while **log analysis and automated alerts** can provide early warning of potential threats. Regular **penetration testing and vulnerability scanning** will also help uncover weaknesses before attackers can exploit them.
Respond	In the event of another attack, the company should have a **clear incident response plan** to quickly contain and neutralize threats. This includes **immediately blocking malicious traffic**, **isolating affected systems**, and **engaging the incident response team** to investigate. Communication protocols should be in place to **notify leadership, stakeholders, and service providers**, ensuring a coordinated effort to minimize downtime. A **post-incident review** should follow to identify lessons learned and strengthen security measures.
Recover	After the attack is contained, the company should focus on **restoring all systems and services** to full functionality and **verifying data integrity** to ensure nothing was lost or altered. Backups should be used to recover any impacted resources, and additional **resilience measures**, such as improved firewall settings, redundancy, and stronger monitoring, should be implemented. A formal **post-incident report** and updated security strategy will help the organization strengthen its defenses and reduce the risk of future disruptions.

Reflections/Notes:

The NIST Cybersecurity Framework (CSF) provided a clear structure for addressing this incident. Using the five core functions (Identify, Protect, Detect, Respond, and Recover) helped pinpoint vulnerabilities, strengthen defenses, and ensure a quick, organized response. This approach highlights the CSF's value in guiding smaller organizations toward better security practices and resilience.