Incident report analysis (NIST FRAMEWORK)

Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- 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

- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

Summary	The company experienced a significant network disruption when all services unexpectedly became unresponsive. After investigating, the cybersecurity team determined that the cause was a **Distributed Denial of Service (DDoS) attack** leveraging an overwhelming flood of **ICMP packets**. To mitigate the issue, the team blocked the attack, temporarily halted non-essential network services, and prioritized the restoration of critical systems.
Identify	A **malicious attacker** exploited a **firewall misconfiguration** to launch a **DDoS ICMP flood attack** against the company's network. The attack rendered internal services inaccessible, requiring an immediate response. To prevent further disruptions, all critical resources needed to be secured and restored to operational status.
Protect	To prevent similar attacks in the future, the cybersecurity team implemented the following protective measures: ● Configured **firewall rules** to restrict excessive incoming **ICMP traffic**. ● Deployed an **Intrusion Detection and Prevention System (IDS/IPS)** to identify and block suspicious network activity.
Detect	To enhance detection capabilities and improve early warning systems for future threats, the cybersecurity team: ● Enabled **source IP verification** on the firewall to prevent **IP spoofing** from malicious actors. ● Implemented **network traffic monitoring software** to identify unusual

	patterns and mitigate threats before they escalate.
Respond	For future incidents, the cybersecurity team will follow a structured response plan: ● **Isolate compromised systems** to prevent further network-wide disruptions. ● **Restore essential services** as a priority while analyzing affected areas. ● **Review and analyze network logs** to identify suspicious activity and determine the attack's origin. ● **Report security incidents** to upper management and relevant legal authorities when necessary.
Recover	To successfully recover from a **DDoS ICMP flood attack**, the following steps should be followed: 1. **Restore network services** in a phased approach, prioritizing critical infrastructure. 2. **Block external ICMP flood attacks** at the firewall to minimize future risks. 3. **Reduce non-essential network traffic** by temporarily halting non-critical services. 4. **Gradually bring non-essential services back online** once the attack subsides and network stability is confirmed.

Reflections/Notes:

By implementing these **preventative, detection, response, and recovery measures**, the company strengthens its **resilience against future cyber threats** and enhances overall network security.