Scenario: Suspicious ICMP Traffic Detected

You're a SOC Tier 1 analyst on duty.
Your IDS (Intrusion Detection System) flagged unusually high ICMP traffic coming from multiple sources. You decide to use tcpdump to investigate.

Here's the log snippet you captured:

```
13:20:11.312315 IP 203.0.113.10 > 192.51.100.15: ICMP echo request, id 1024, seq 1, length 64
13:20:11.312427 IP 203.0.113.11 > 192.51.100.15: ICMP echo request, id 1025, seq 1, length 64
13:20:11.312532 IP 203.0.113.12 > 192.51.100.15: ICMP echo request, id 1026, seq 1, length 64
13:20:11.312641 IP 203.0.113.13 > 192.51.100.15: ICMP echo request, id 1027, seq 1, length 64
13:20:11.312748 IP 203.0.113.14 > 192.51.100.15: ICMP echo request, id 1028, seq 1, length 64
13:20:11.312861 IP 192.51.100.15 > 203.0.113.10: ICMP echo reply, id 1024, seq 1, length 64
13:20:11.312963 IP 192.51.100.15 > 203.0.113.11: ICMP echo reply, id 1025, seq 1, length 64
```

🕵️ Your task

Analyze this like a SOC analyst.

Write your short SOC report draft, including:

1. Incident Summary – what seems to be happening?
2. Indicators – what log evidence supports that?
3. Possible Causes – list *all possibilities* (malicious + non-malicious).
4. Next Steps / Recommendations – what should you do or suggest next?

SOC Incident Analysis Report

Incident Title:
Unusually High ICMP Traffic from Multiple Sources

---

1. Incident Summary
During network analysis using *tcpdump*, multiple ICMP echo requests from various external IP addresses were detected targeting the same internal host (192.51.100.15). The high frequency and volume of ICMP traffic indicate possible network probing or a Denial-of-Service (DoS) attempt.

---

2. Evidence / Observation
Log Findings:

- **Source IPs:** 203.0.113.10, 203.0.113.11, 203.0.113.12, 203.0.113.13, 203.0.113.14
- **Destination IP:** 192.51.100.15
- **Protocol:** ICMP (Echo Request and Echo Reply)
- **Behavior:** Multiple ICMP echo requests observed in a short time frame from different IPs, followed by echo replies from the target host.

---

3. Analysis
The repeated ICMP echo requests from multiple sources toward a single destination suggest potential flooding activity. This traffic pattern is consistent with a **possible ICMP flood (ping flood)**, a common form of **DoS/DDoS attack**.
However, further investigation is needed to confirm whether the traffic is malicious or part of legitimate network monitoring or testing.

---

4. Possible Causes

- Misconfigured network monitoring tools sending excessive ICMP requests.
- Firewall or IDS testing generating ICMP traffic.
- **DoS/DDoS attack** using ICMP flood from multiple sources.
- DNS or network service latency causing repeated requests.
- Network misconfiguration or routing issue.
- Temporary unavailability of DNS service leading to excessive retries.

---

5. Conclusion / Next Steps

- Verify DNS server and network connectivity using ping and nslookup.
- Check firewall and router configurations for unusual rules or blocked ports (especially UDP port 53).
- Review system and DNS logs for signs of overload or failed queries.
- Monitor network traffic volume to confirm if flooding continues.
- If DoS/DDoS activity is confirmed, implement **rate-limiting, firewall filtering, or upstream mitigation**.

---

6. Final Observation / Analyst Note
Based on the evidence, a **possible DoS/DDoS attack** or **network misconfiguration** cannot be ruled out. Further packet capture and correlation with firewall or IDS alerts are recommended to confirm the root cause.