Day 20

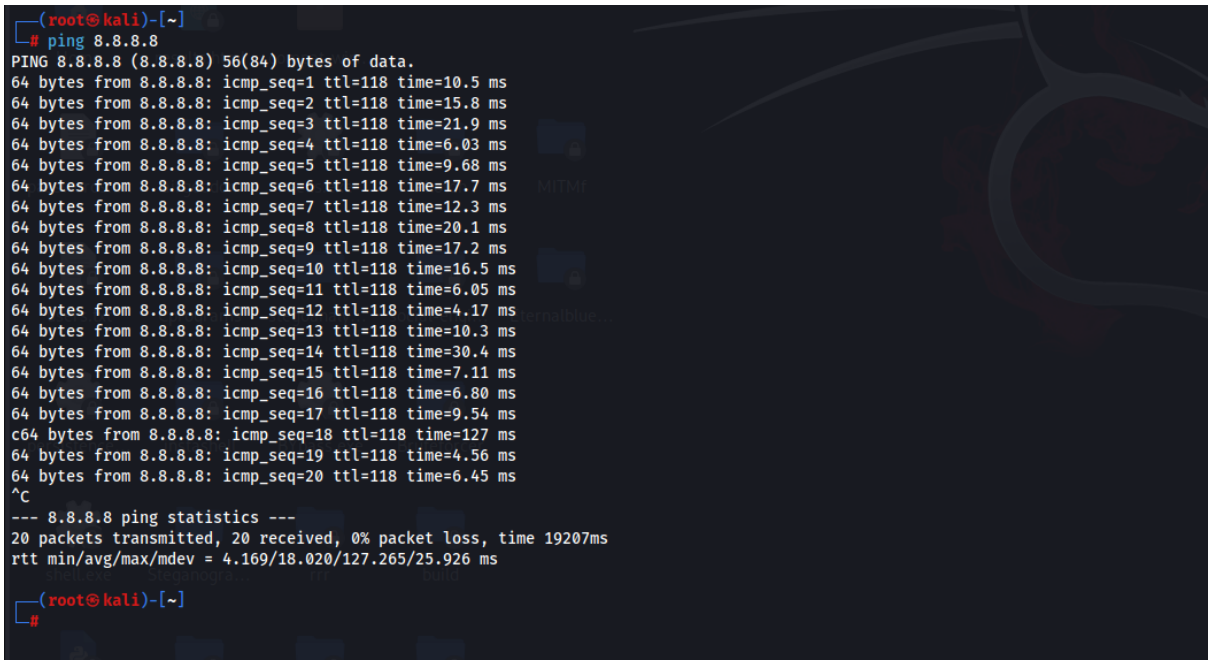
Exploitation Analyst

ICMP Protocol:

To see the presence of ICMP and verify if it's working on your network:

Method 1:

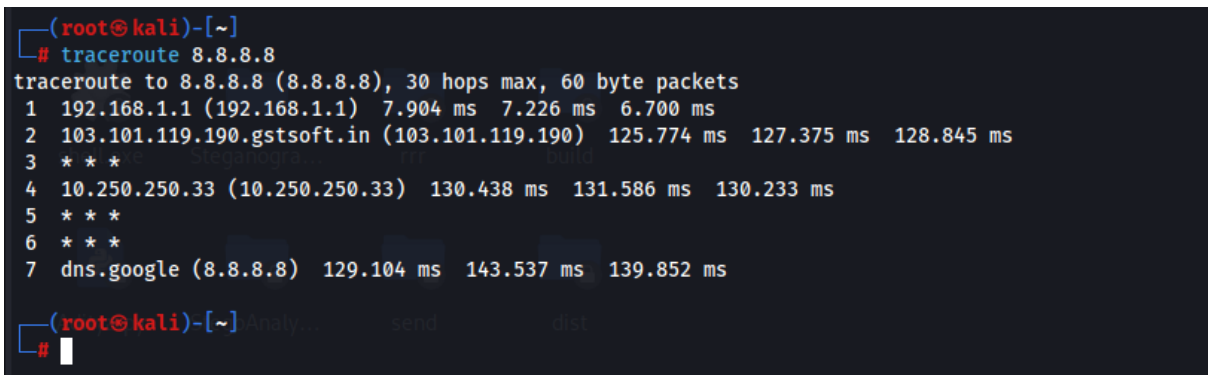
Using the ping command.



This command sends ICMP Echo Request packets to Google's DNS server (8.8.8.8) and expects ICMP Echo Reply in return. Each line of the output confirms a reply, showing that ICMP is functioning correctly between your host and the destination. The presence of fields like icmp_seq, ttl, and time proves successful ICMP communication.

Method 2:

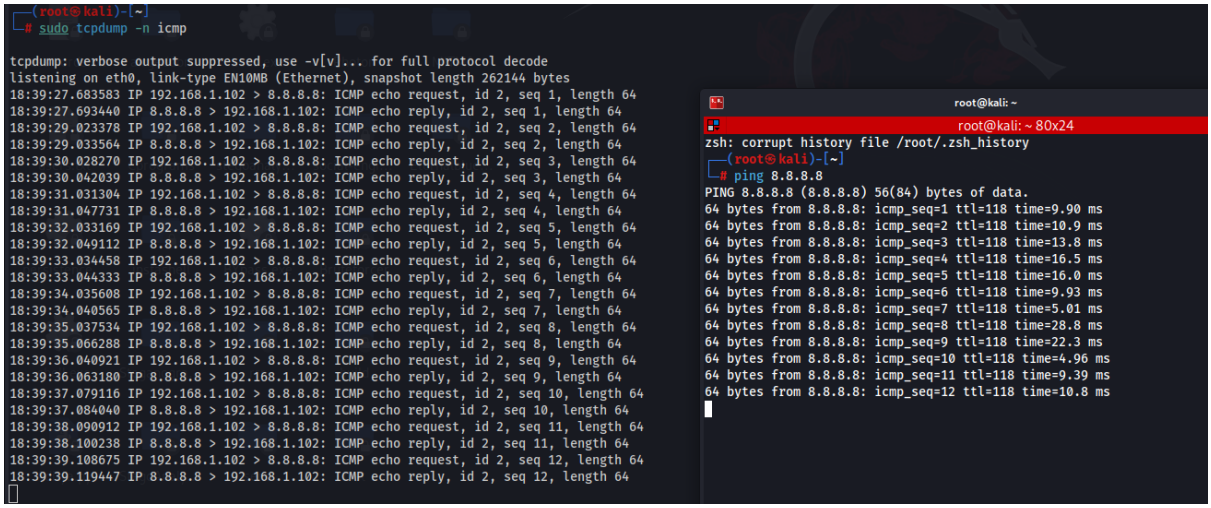
Using the traceroute command.



Traceroute helps identify each hop (router) between your system and 8.8.8.8. It works by sending packets with increasing TTL values, and each router that drops the packet (when TTL hits 0) sends back an ICMP Time Exceeded (Type 11) message. That's how the tool maps the path. Routers along the path are sending ICMP error messages (Time Exceeded), proving ICMP is supported for diagnostic purposes.

Method 3:

Using the command 'tcpdump -n icmp': and in another terminal pinging.



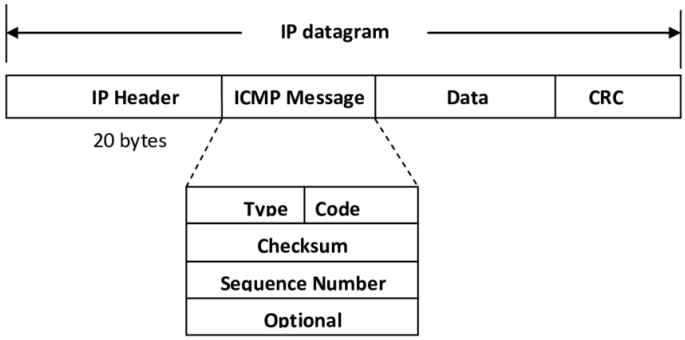
This command sniffs network traffic and filters only ICMP packets. When used during a ping or traceroute, it shows real-time ICMP Echo Requests and Replies, verifying that your machine is actively sending and receiving ICMP messages.

Types of ICMP Packets (ICMPv4)

ICMP messages are categorized by **Type** and **Code**. Here are the most common types:

Type	Name	Purpose
0	Echo Reply	Reply to an Echo Request (used by ping)
3	Destination Unreachable	Informs that a packet cannot reach its destination
5	Redirect Message	Suggest a better route to the sender
8	Echo Request	Ping request (used to test connectivity)
11	Time Exceeded	TTL expired (used in traceroute)
12	Parameter Problem	Header field error
13/14	Timestamp Request/Reply	Used to measure network delays

What is an IP Datagram?



An IP datagram is a packet at the Network Layer (Layer 3). It carries data from a source to a destination across IP-based networks.

Why is it sent?

- It's the basic unit of data transmission in IP networks.
- Sent whenever a higher-layer protocol (TCP, UDP, ICMP, etc.) needs to transmit data across the network.

Structure of an IP Datagram:

- **IP Header**:
  - Source IP
  - Destination IP
  - TTL (Time to Live)
  - Protocol (e.g., ICMP = 1, TCP = 6, UDP = 17)
  - Header length, checksum, etc.
- **Payload**:
  - This contains the actual data. For ICMP, this will be the ICMP message.

How ICMP Fits into an IP Datagram

When ICMP sends a message, it is encapsulated within the payload of an IP datagram:

- IP header:
  - Protocol = 1 (indicates payload is ICMP)
  - Source and destination IPs
- Payload:
  - ICMP Header:
    - Type (e.g., 3 for Destination Unreachable)
    - Code (finer reason like "Port Unreachable")
    - Checksum
  - ICMP Data:
    - Often includes part of the original packet that caused the error, especially first 8 bytes of the transport header (TCP/UDP) and original IP header.

--The End--