⚔️ ICMP Flood (Ping Flood) Attack

📖 Description of the Attack

This practical demonstrates an ICMP Flood (Ping Flood) Denial of Service attack.
The attacker sends continuous ICMP Echo Request packets with a maximum packet size to the target system. This overwhelms the target's network bandwidth and CPU, leading to performance degradation or temporary unavailability.

⚠️ Ethical Disclaimer

This experiment was conducted **only in a controlled virtual lab environment** using private IP addresses for educational purposes.

⚔️ Type of Attack Performed

- **Attack Name:** ICMP Flood / Ping Flood
- **Category:** Denial of Service (DoS)
- **Protocol Used:** ICMP
- **OSI Layer:** Network Layer (Layer 3)

🧪 Step-by-Step Procedure (Continuation for Report)

Step 1: Start the Windows Target

- Power on the **Windows machine**
- Open **Task Manager**
- Go to **Performance → CPU, Memory, Network**

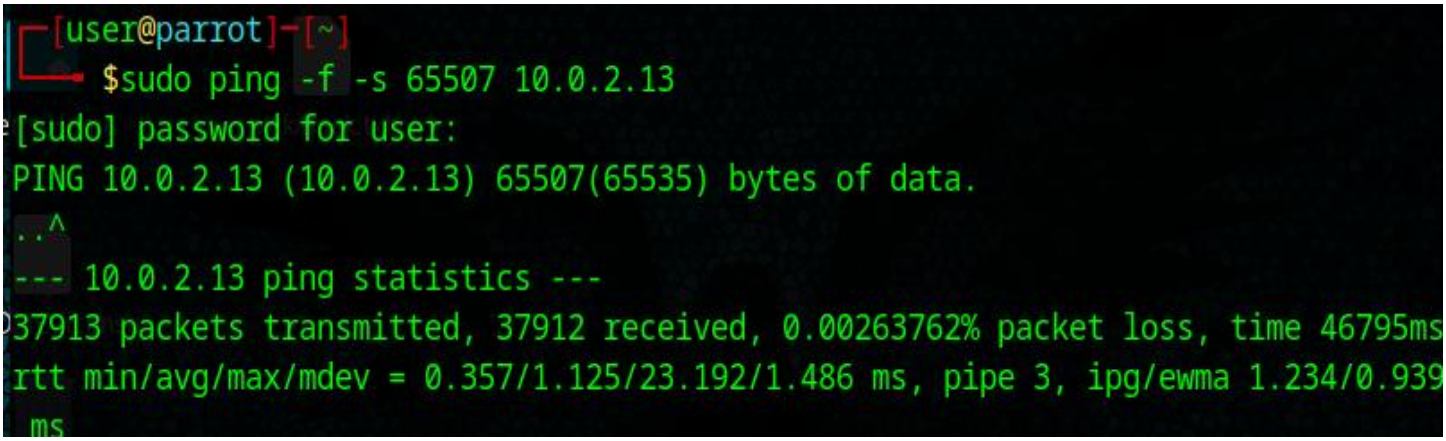
Step 2: Start the Attacker Machine

- Power on **Parrot Security OS**
- Open **Terminal**

Step 3: Execute ICMP Flood Command

Run:

sudo ping -f -s 65507 10.0.2.13

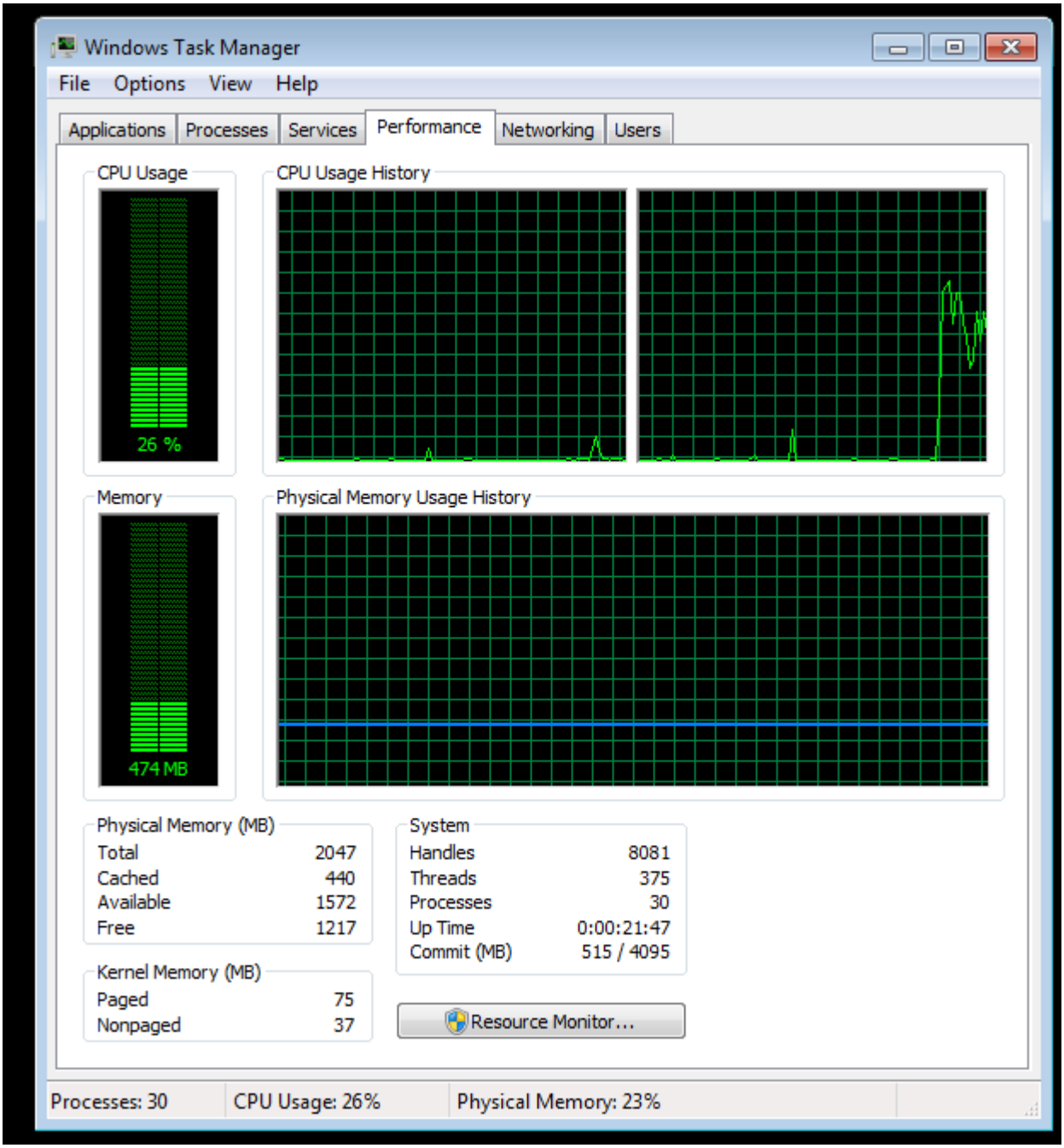


Option	Meaning
sudo	Required to send packets at high speed
ping	ICMP echo request utility
-f	Flood mode (sends packets as fast as possible)
-s 65507	Sets packet size to maximum allowed ICMP payload
10.0.2.13	Target Windows IP address

➡️ This combination makes the attack **more powerful**.

Step 4: Observe the Target System

- Network usage spikes rapidly
- CPU usage increases
- System becomes slow or unresponsive
- Packet drops may be observed



Result

The ICMP Flood attack was **successfully executed**, demonstrating how continuous large-sized ICMP packets can **exhaust network and system resources** of the target machine.