GUÍA TÉCNICA PRÁCTICAS INSTRUCTOR

MÓDULO 5. TALLER 1

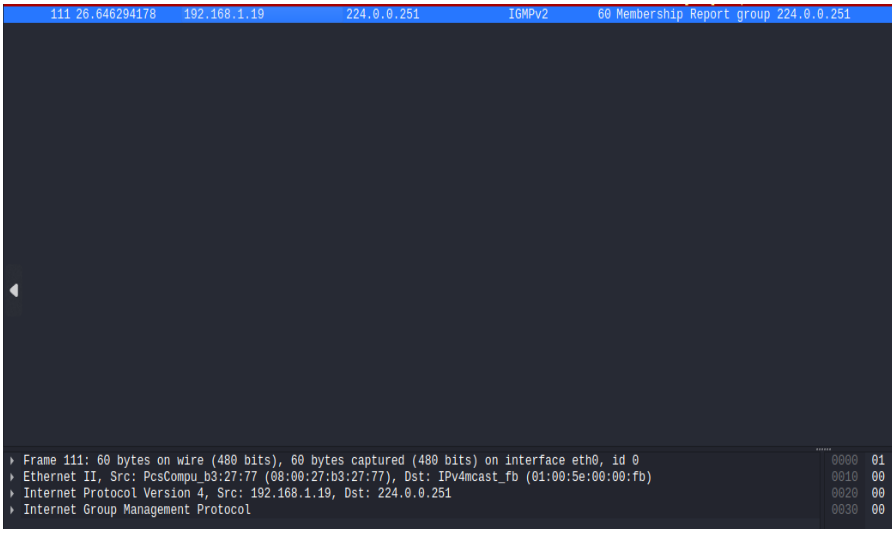
TALLER 1: ESCANEOS HPING3 Y NMAP

Hacer escaneos con HPING3 comparar resultados con Nmap, documentar los resultados y diferencias. Requiere Wireshark en la máquina con Kali Linux.

HPING3.

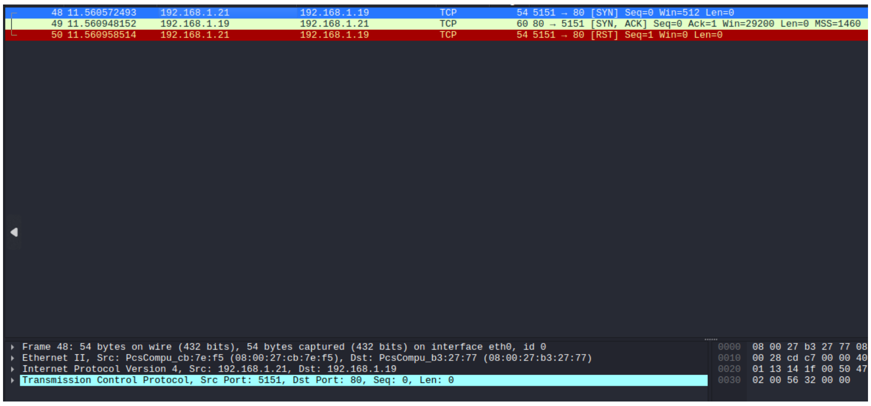
Usando el comando **sudo hping3 -S -c 1 -s 5151 -p 80 192.168.1.19** me saltan estos resultados en el WireShark:

TCP, source port 5151, port 80.



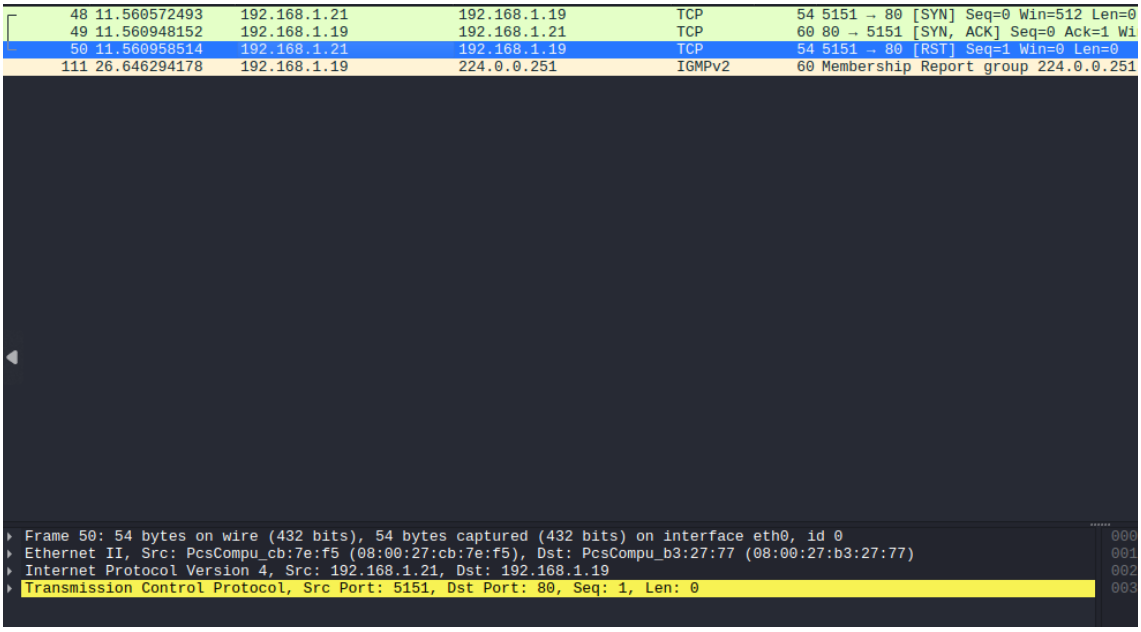
```
111 26.646294178    192.168.1.19          224.0.0.251          IGMPv2      60 Membership Report group 224.0.0.251
```

```
Frame 111: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0      0000  01
Ethernet II, Src: PcsCompu_b3:27:77 (08:00:27:b3:27:77), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)    0010  00
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 224.0.0.251                                  0020  00
Internet Group Management Protocol                                                                0030  00
```



```
48 11.560572493   192.168.1.21     192.168.1.19     TCP     54 5151 → 80 [SYN] Seq=0 Win=512 Len=0
49 11.560948152   192.168.1.19     192.168.1.21     TCP     60 80 → 5151 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
50 11.560958514   192.168.1.21     192.168.1.19     TCP     54 5151 → 80 [RST] Seq=1 Win=0 Len=0
```

```
Frame 48: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0        0000  08 00 27 b3 27 77 08
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_b3:27:77 (08:00:27:b3:27:77)  0010  00 28 cd c7 00 00 40
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.19                                  0020  01 13 14 1f 00 50 47
Transmission Control Protocol, Src Port: 5151, Dst Port: 80, Seq: 0, Len: 0                        0030  02 00 56 32 00 00
```



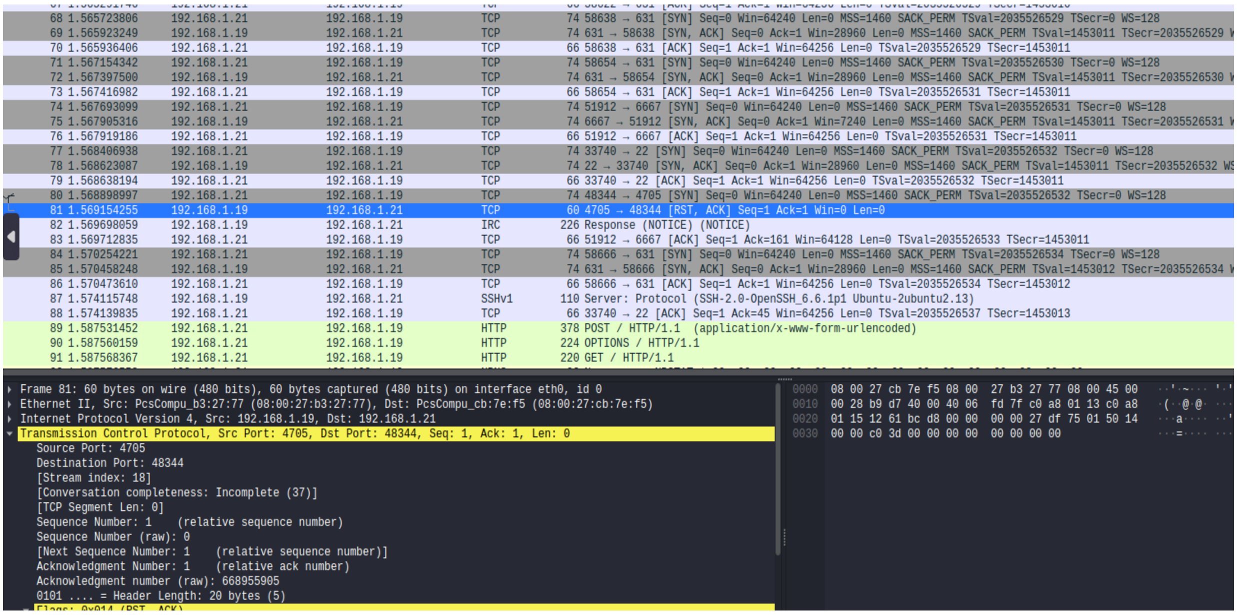
```
 48 11.560572493   192.168.1.21     192.168.1.19     TCP      54 5151 → 80 [SYN] Seq=0 Win=512 Len=0
 49 11.560948152   192.168.1.19     192.168.1.21     TCP      60 80 → 5151 [SYN, ACK] Seq=0 Ack=1 Wi
 50 11.560958514   192.168.1.21     192.168.1.19     TCP      54 5151 → 80 [RST] Seq=1 Win=0 Len=0
111 26.646294178   192.168.1.19     224.0.0.251      IGMPv2   60 Membership Report group 224.0.0.251

Frame 50: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_b3:27:77 (08:00:27:b3:27:77)
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.19
Transmission Control Protocol, Src Port: 5151, Dst Port: 80, Seq: 1, Len: 0
```

NMAP.

Usando el comando **nmap -A -T4 192.168.1.19**, obtenemos la siguiente información en WireShark:

Protocolos, puertos, tipos de paquetes, etc.



```
68 1.565723806   192.168.1.21   192.168.1.19   TCP      74 58638 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526529 TSecr=0 WS=128
69 1.565923249   192.168.1.19   192.168.1.21   TCP      74 631 → 58638 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1453011 TSecr=2035526529 W
70 1.565936406   192.168.1.21   192.168.1.19   TCP      66 58638 → 631 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2035526529 TSecr=1453011
71 1.567154342   192.168.1.21   192.168.1.19   TCP      74 58654 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526530 TSecr=0 WS=128
72 1.567397500   192.168.1.19   192.168.1.21   TCP      74 631 → 58654 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1453011 TSecr=2035526530 W
73 1.567416982   192.168.1.21   192.168.1.19   TCP      66 58654 → 631 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2035526531 TSecr=1453011
74 1.567693099   192.168.1.21   192.168.1.19   TCP      74 51912 → 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526531 TSecr=0 WS=128
75 1.567905316   192.168.1.19   192.168.1.21   TCP      74 6667 → 51912 [SYN, ACK] Seq=0 Ack=1 Win=7240 Len=0 MSS=1460 SACK_PERM TSval=1453011 TSecr=2035526531 W
76 1.567919186   192.168.1.21   192.168.1.19   TCP      66 51912 → 6667 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2035526531 TSecr=1453011
77 1.568406938   192.168.1.21   192.168.1.19   TCP      74 33740 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526532 TSecr=0 WS=128
78 1.568623087   192.168.1.19   192.168.1.21   TCP      74 22 → 33740 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1453011 TSecr=2035526532 WS
79 1.568638194   192.168.1.21   192.168.1.19   TCP      66 33740 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2035526532 TSecr=1453011
80 1.568898997   192.168.1.21   192.168.1.19   TCP      74 48344 → 4705 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526532 TSecr=0 WS=128
81 1.569154255   192.168.1.19   192.168.1.21   TCP      60 4705 → 48344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82 1.569698059   192.168.1.19   192.168.1.21   IRC     226 Response (NOTICE) (NOTICE)
83 1.569712835   192.168.1.21   192.168.1.19   TCP      66 51912 → 6667 [ACK] Seq=1 Ack=161 Win=64128 Len=0 TSval=2035526533 TSecr=1453011
84 1.570254221   192.168.1.21   192.168.1.19   TCP      74 58666 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2035526534 TSecr=0 WS=128
85 1.570458248   192.168.1.19   192.168.1.21   TCP      74 631 → 58666 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1453012 TSecr=2035526534 W
86 1.570473610   192.168.1.21   192.168.1.19   TCP      66 58666 → 631 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2035526534 TSecr=1453012
87 1.574115748   192.168.1.19   192.168.1.21   SSHv1   110 Server: Protocol (SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13)
88 1.574139835   192.168.1.21   192.168.1.19   TCP      66 33740 → 22 [ACK] Seq=1 Ack=45 Win=64256 Len=0 TSval=2035526537 TSecr=1453013
89 1.587531452   192.168.1.21   192.168.1.19   HTTP    378 POST / HTTP/1.1  (application/x-www-form-urlencoded)
90 1.587560159   192.168.1.21   192.168.1.19   HTTP    224 OPTIONS / HTTP/1.1
91 1.587568367   192.168.1.21   192.168.1.19   HTTP    220 GET / HTTP/1.1
```

```
Frame 81: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_b3:27:77 (08:00:27:b3:27:77), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 192.168.1.21
Transmission Control Protocol, Src Port: 4705, Dst Port: 48344, Seq: 1, Ack: 1, Len: 0
    Source Port: 4705
    Destination Port: 48344
    [Stream index: 18]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 668955905
    0101 .... = Header Length: 20 bytes (5)
```

```
0000  08 00 27 cb 7e f5 08 00  27 b3 27 77 08 00 45 00
0010  00 28 b9 d7 40 00 40 06  fd 7f c0 a8 01 13 c0 a8
0020  01 15 12 61 bc d8 00 00  00 00 27 df 75 01 50 14
0030  00 00 c0 3d 00 00 00 00  00 00 00 00
```