IT3700 nmap scan assignment, Jeff Sly

Table of Contents

Nmap Scans

Null

Nmap –sN –p80 192.168.56.102

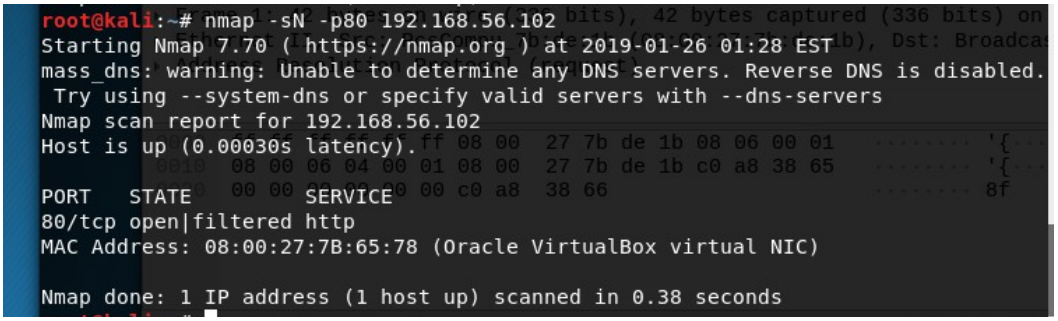
Flags set = None

Protocol = TCP

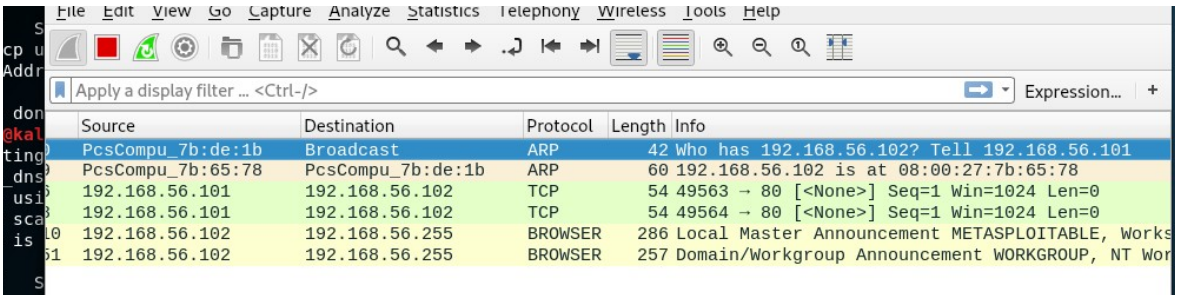
Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80



The header does not have any flags set, the response of the scan was open|filtered



Xmas

Nmap –sX –p80 192.168.56.102

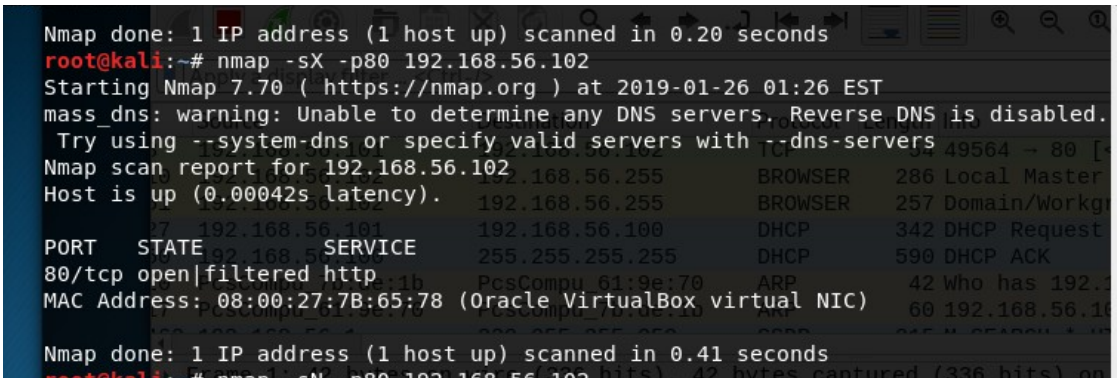
Flags set FIN PSH URG

Protocol = TCP

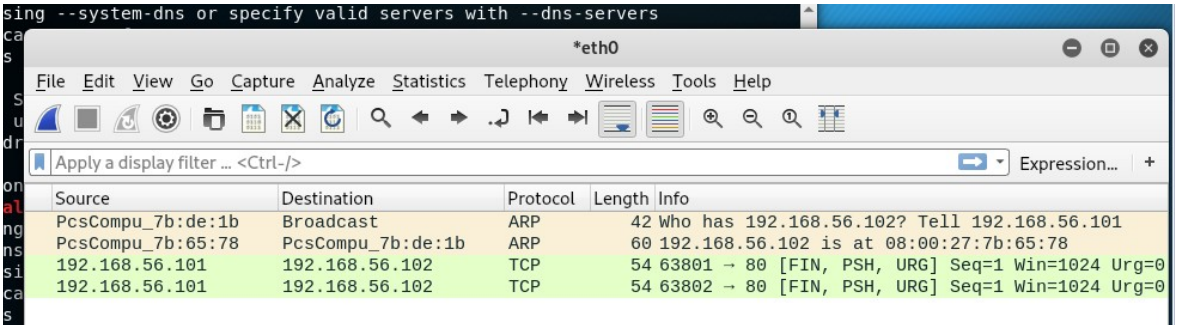
Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80



Got no response back so that means the port is open.



ACK

Nmap –sA –p80 192.168.56.102

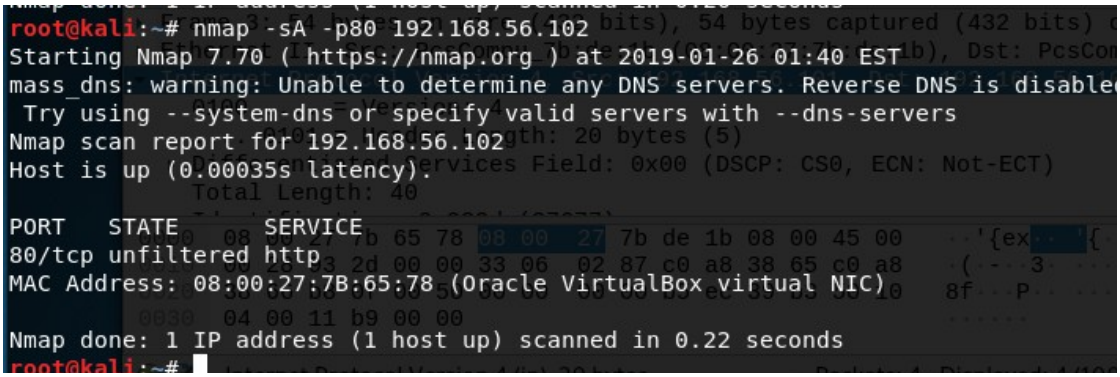
Flag set ACK

Protocol = TCP

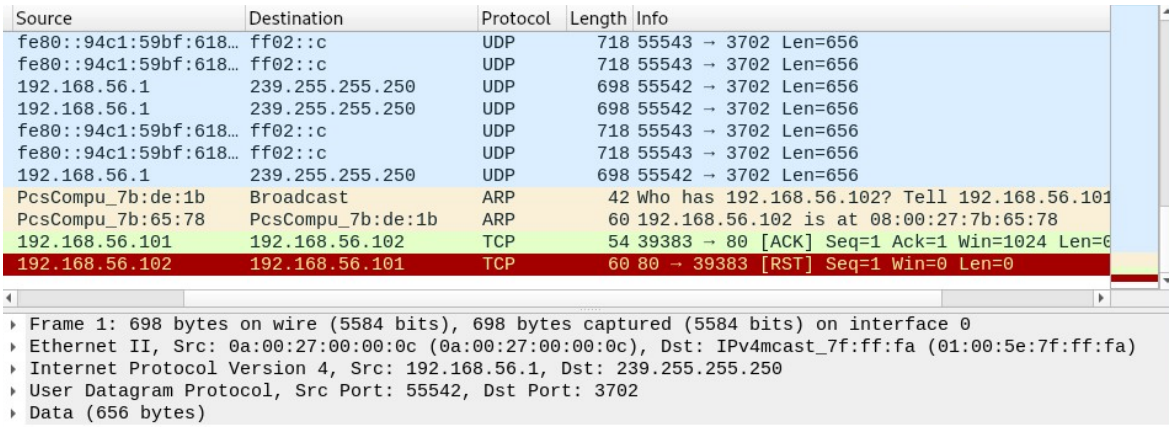
Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80



Got back a reset which means the port is not filtered by a firewall



Version Scan

nmap –sV –version-intensity 2 192.168.56.102

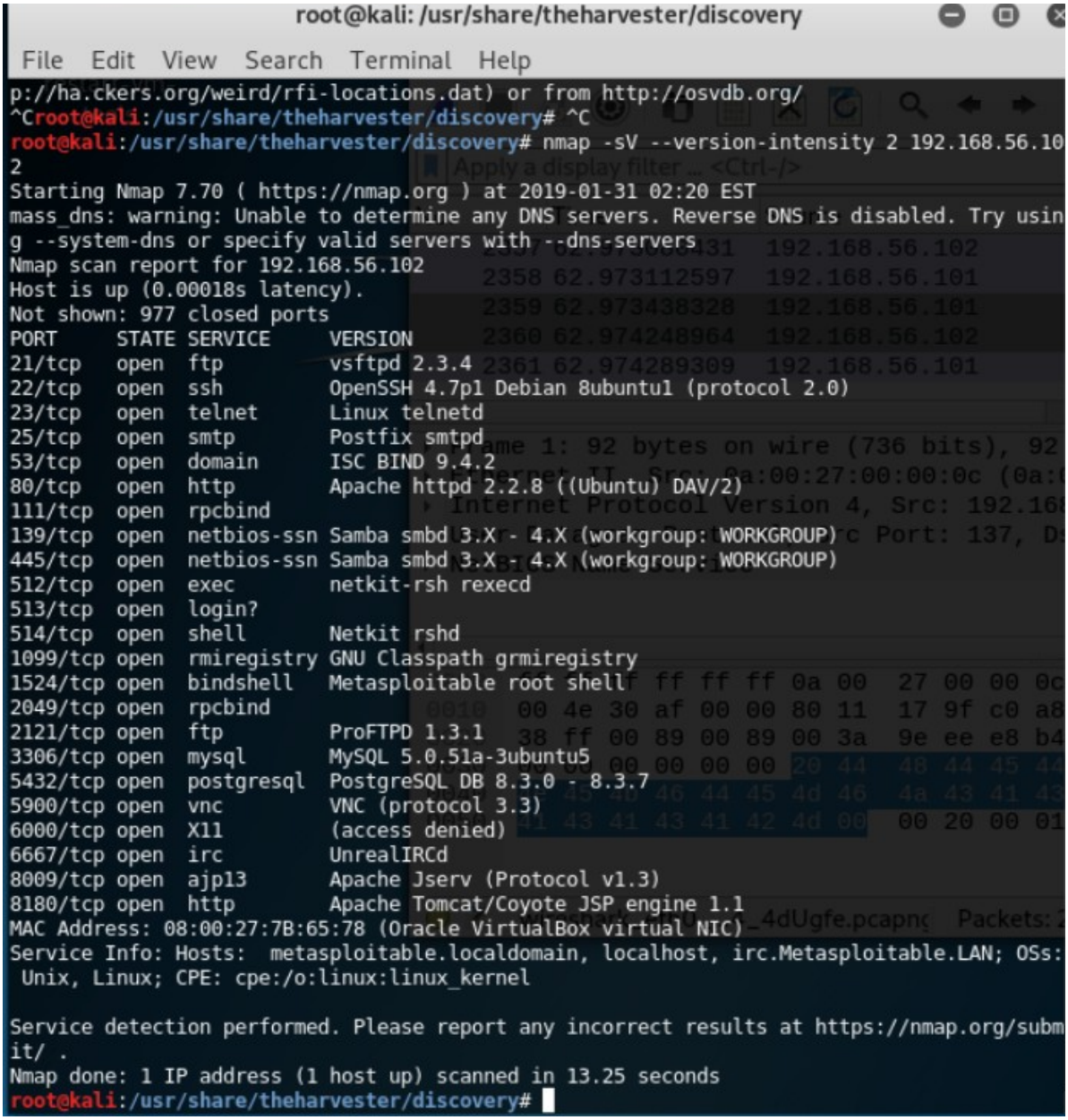
Flags set FIN ACK

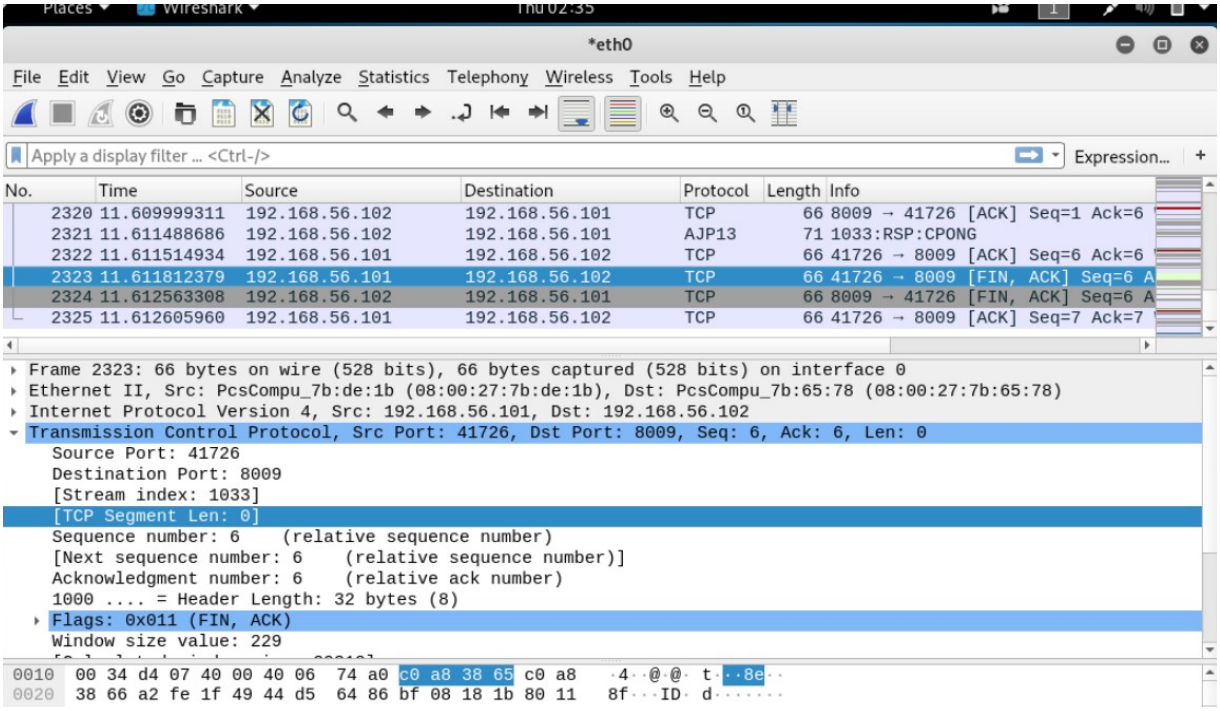
Protocol = TCP

Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Ports Open = 21 22 23 25 53 80 111 139 445 512 513 514 1099 1524 2049 2121 3306 5432 5900 6000 6667 8009 8180




Places
Wireshark
Thu 02:35
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
2320 11.609999311 192.168.56.102 192.168.56.101 TCP 66 8009 → 41726 [ACK] Seq=1 Ack=6
2321 11.611488686 192.168.56.102 192.168.56.101 AJP13 71 1033:RSP:CPONG
2322 11.611514934 192.168.56.101 192.168.56.102 TCP 66 41726 → 8009 [ACK] Seq=6 Ack=6
2323 11.611812379 192.168.56.101 192.168.56.102 TCP 66 41726 → 8009 [FIN, ACK] Seq=6 A
2324 11.612563308 192.168.56.102 192.168.56.101 TCP 66 8009 → 41726 [FIN, ACK] Seq=6 A
2325 11.612605960 192.168.56.101 192.168.56.102 TCP 66 41726 → 8009 [ACK] Seq=7 Ack=7
Frame 2323: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_7b:de:1b (08:00:27:7b:de:1b), Dst: PcsCompu_7b:65:78 (08:00:27:7b:65:78)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
Transmission Control Protocol, Src Port: 41726, Dst Port: 8009, Seq: 6, Ack: 6, Len: 0
Source Port: 41726
Destination Port: 8009
[Stream index: 1033]
[TCP Segment Len: 0]
Sequence number: 6 (relative sequence number)
[Next sequence number: 6 (relative sequence number)]
Acknowledgment number: 6 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x011 (FIN, ACK)
Window size value: 229
0010 00 34 d4 07 40 00 40 06 74 a0 c0 a8 38 65 c0 a8
0020 38 66 a2 fe 1f 49 44 d5 64 86 bf 08 18 1b 80 11

Extra Scan

SYN

Nmap –sS –p80 192.168.56.102