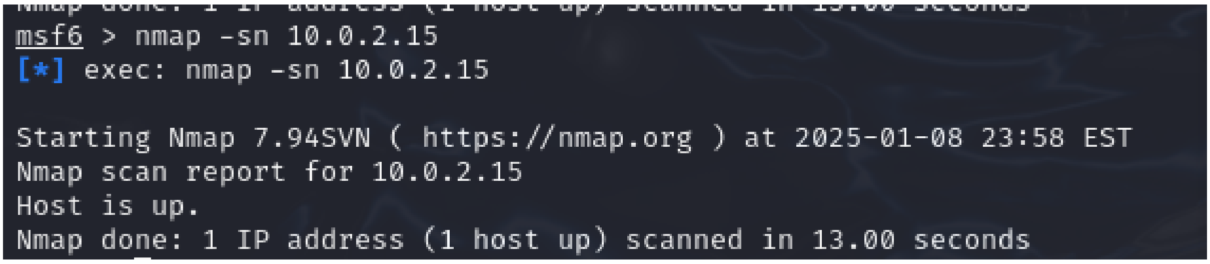
Assignment 4: Exploring nmap command

Karthikeyan G
Roll Number: CB.SC.P2CYS24008

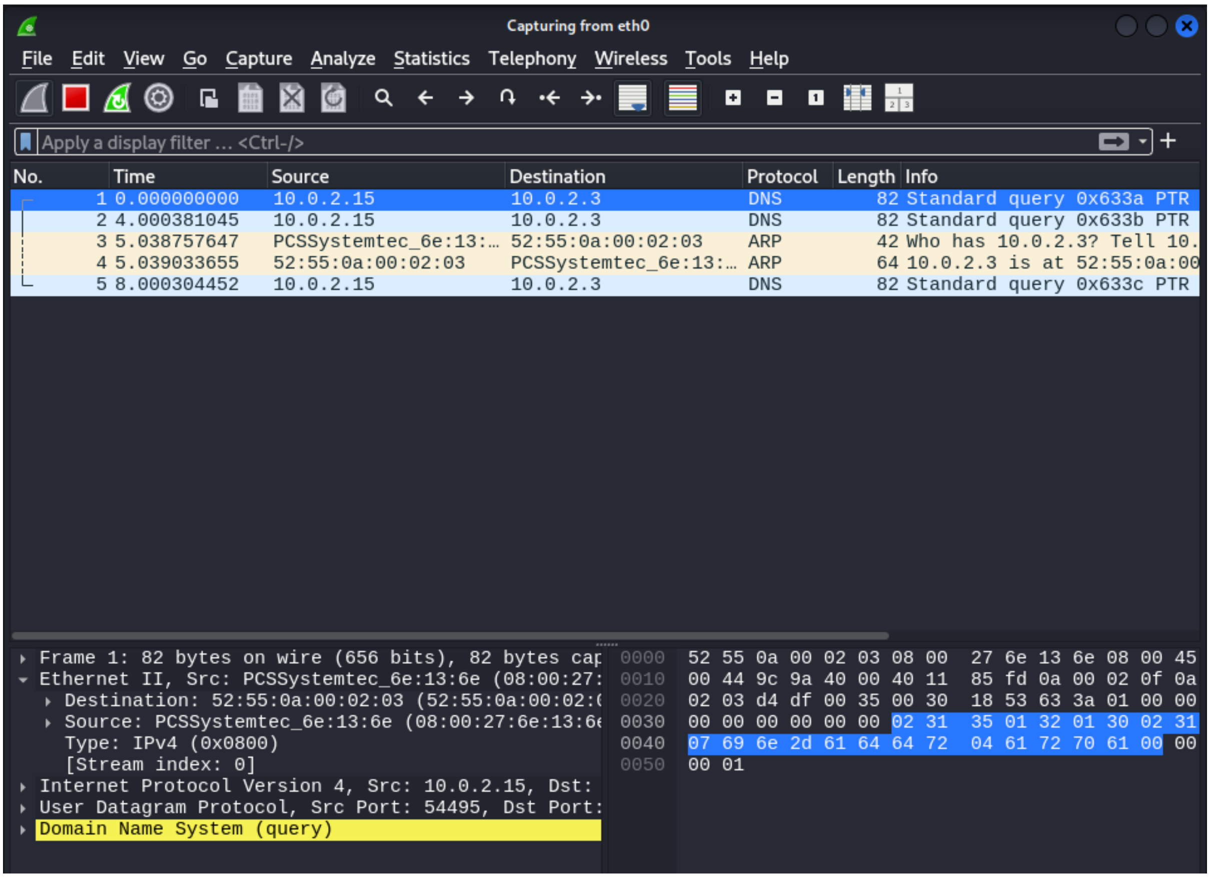
January 9, 2025

1. Scenario: You are tasked with verifying whether the victim Metasploit2 VM is active on the network and responding to any type of ping. What Nmap command would you use to check its availability?



```
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
msf6 > nmap -sn 10.0.2.15
[*] exec: nmap -sn 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 23:58 EST
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```

Figure 1: Nmap command: `nmap -sn 10.0.2.15`
Explanation: This command performs a ping scan to check if the victim Metasploit2 VM at IP 10.0.2.15 is active and responding to ping requests.



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

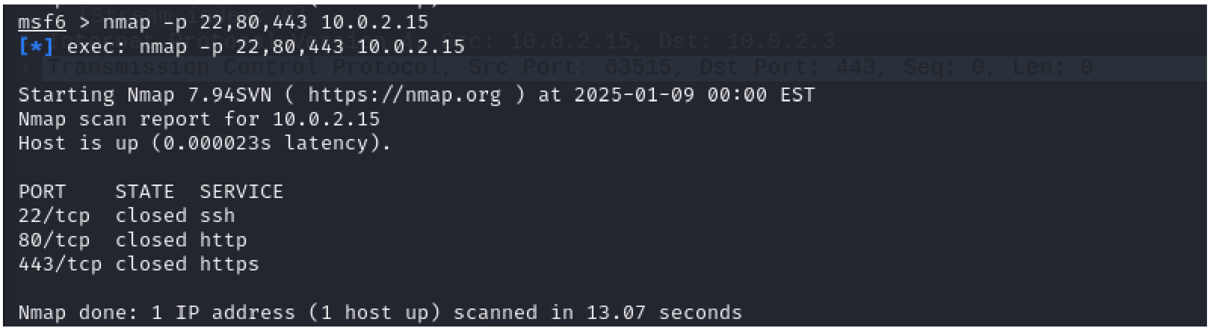
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.3	DNS	82	Standard query 0x633a PTR
2	4.000381045	10.0.2.15	10.0.2.3	DNS	82	Standard query 0x633b PTR
3	5.038757647	PCSSystemtec_6e:13:…	52:55:0a:00:02:03	ARP	42	Who has 10.0.2.3? Tell 10.
4	5.039033655	52:55:0a:00:02:03	PCSSystemtec_6e:13:…	ARP	64	10.0.2.3 is at 52:55:0a:00
5	8.000304452	10.0.2.15	10.0.2.3	DNS	82	Standard query 0x633c PTR

```
▸ Frame 1: 82 bytes on wire (656 bits), 82 bytes cap
▾ Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:
  ▸ Destination: 52:55:0a:00:02:03 (52:55:0a:00:02:(
  ▸ Source: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst:
▸ User Datagram Protocol, Src Port: 54495, Dst Port:
▸ Domain Name System (query)
```

```
0000  52 55 0a 00 02 03 08 00  27 6e 13 6e 08 00 45
0010  00 44 9c 9a 40 00 40 11  85 fd 0a 00 02 0f 0a
0020  02 03 d4 df 00 35 00 30  18 53 63 3a 01 00 00
0030  00 00 00 00 00 00 02 31  35 01 32 01 30 02 31
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00
0050  00 01
```

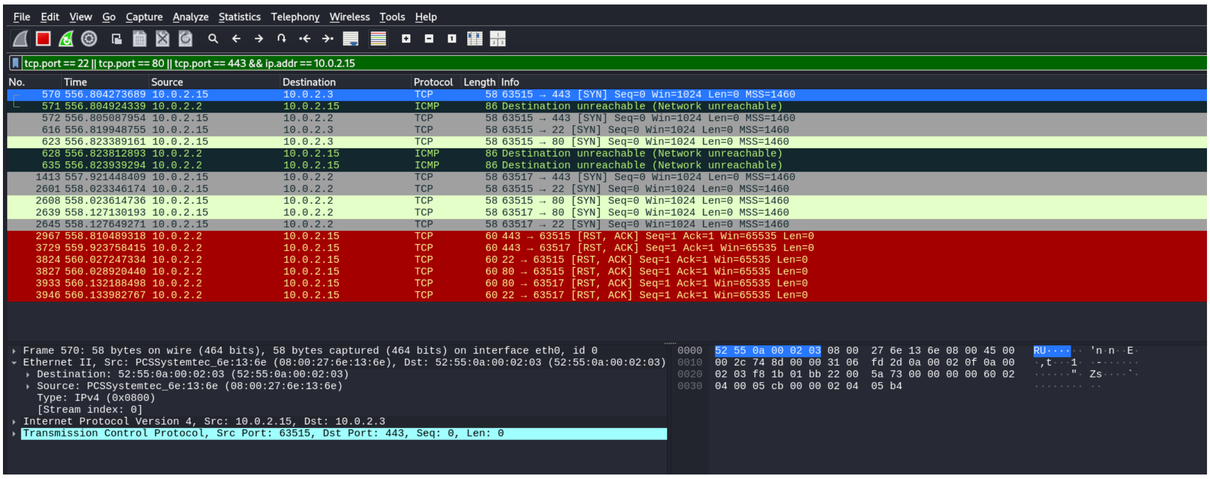
Figure 2: Wireshark filter: `icmp && ip.addr == 10.0.2.15`
Explanation: This filter captures ICMP packets to and from the victim Metasploit2 VM at IP 10.0.2.15.

2. Scenario: You want to check if common ports like SSH (22), HTTP (80), and HTTPS (443) are open on the victim Metasploit2 VM. How would you scan these specific ports?



```
msf6 > nmap -p 22,80,443 10.0.2.15
[*] exec: nmap -p 22,80,443 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:00 EST
Nmap scan report for 10.0.2.15
Host is up (0.000023s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
```

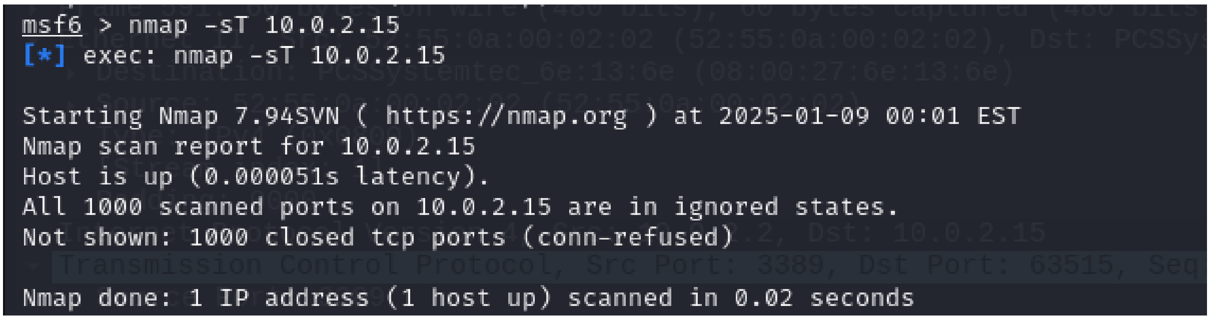
Figure 3: Nmap command: `nmap -p 22,80,443 10.0.2.15`
Explanation: This command scans specific ports (22, 80, 443) on the victim Metasploit2 VM at IP 10.0.2.15 to check if they are open.



```
tcp.port == 22 || tcp.port == 80 || tcp.port == 443 && ip.addr == 10.0.2.15

No.  Time           Source     Destination Protocol Length Info
 570 556.804273689 10.0.2.15  10.0.2.3    TCP      58 63515 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 571 556.804924339 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 572 556.805087954 10.0.2.15  10.0.2.2    TCP      58 63515 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 616 556.819948755 10.0.2.15  10.0.2.3    TCP      58 63515 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 623 556.823389161 10.0.2.15  10.0.2.3    TCP      58 63515 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 628 556.823812893 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 635 556.823939294 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
1413 557.921448409 10.0.2.15  10.0.2.2    TCP      58 63517 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2601 558.023346174 10.0.2.15  10.0.2.2    TCP      58 63515 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2608 558.023614736 10.0.2.15  10.0.2.2    TCP      58 63515 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2639 558.127130193 10.0.2.15  10.0.2.2    TCP      58 63517 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2645 558.127649271 10.0.2.15  10.0.2.2    TCP      58 63517 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2967 558.810489318 10.0.2.2   10.0.2.15   TCP      60 443 → 63515 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
3729 559.923758415 10.0.2.2   10.0.2.15   TCP      60 443 → 63517 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
3824 560.027247334 10.0.2.2   10.0.2.15   TCP      60 22 → 63515 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
3827 560.028920440 10.0.2.2   10.0.2.15   TCP      60 80 → 63515 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
3933 560.132188498 10.0.2.2   10.0.2.15   TCP      60 80 → 63517 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
3946 560.133982767 10.0.2.2   10.0.2.15   TCP      60 22 → 63517 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

› Frame 570: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
⌄ Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
  › Destination: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
  › Source: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
    Type: IPv4 (0x0800)
    [Stream index: 0]
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
› Transmission Control Protocol, Src Port: 63515, Dst Port: 443, Seq: 0, Len: 0

0000  52 55 0a 00 02 03 08 00  27 6e 13 6e 08 00 45 00   RU······'n·n··E·
0010  00 2c 74 8d 00 00 31 06  fd 2d 0a 00 02 0f 0a 00   ·,t···1··-······
0020  02 03 f8 1b 01 bb 22 00  5a 73 00 00 00 00 60 02   ······"·Zs····`·
0030  04 00 05 cb 00 00 02 04  05 b4                     ··········
```

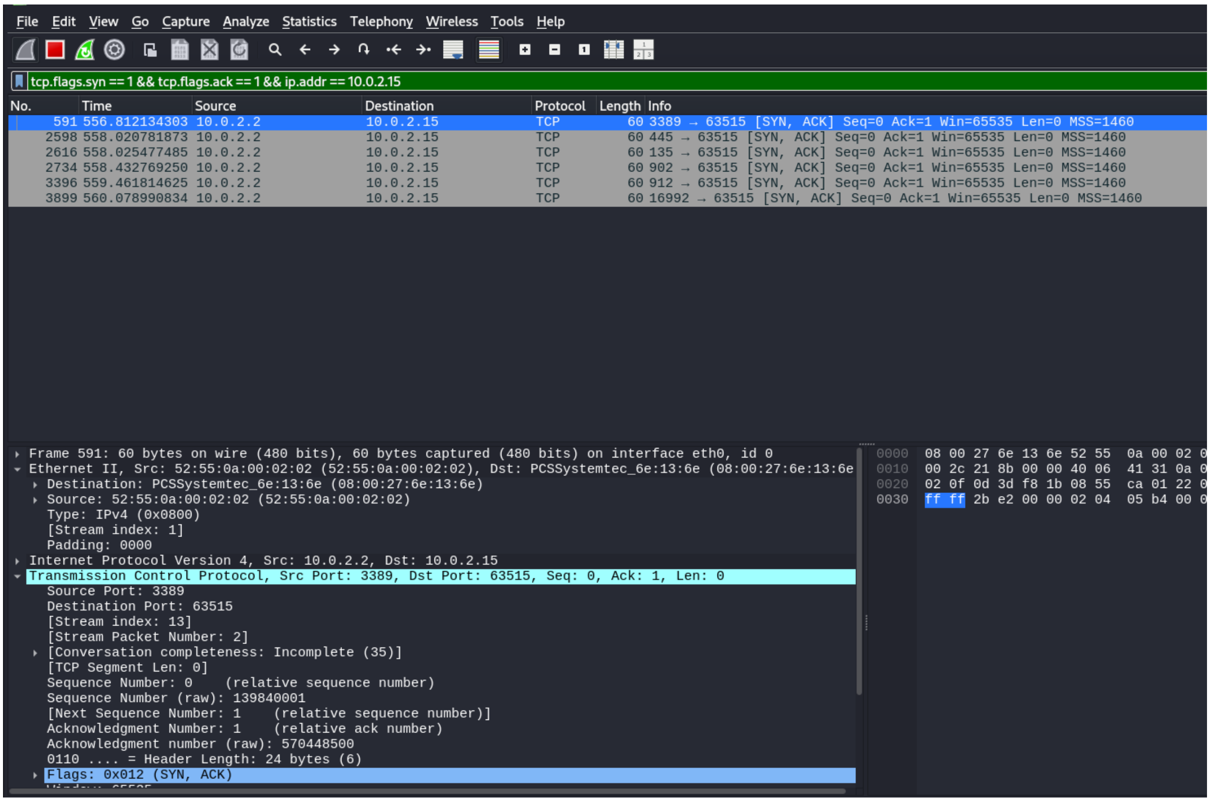
Figure 4: Wireshark filter: `(tcp.port == 22 || tcp.port == 80 || tcp.port == 443) && ip.addr == 10.0.2.15`
Explanation: This filter captures TCP packets on ports 22, 80, and 443 for the victim Metasploit2 VM at IP 10.0.2.15.

3. Scenario: You need to perform a full TCP connection scan on the victim Metasploit2 VM to see which ports are open. What would be your approach?



```
msf6 > nmap -sT 10.0.2.15
[*] exec: nmap -sT 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:01 EST
Nmap scan report for 10.0.2.15
Host is up (0.000051s 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 0.02 seconds
```

Figure 5: Nmap command: `nmap -sT 10.0.2.15`
Explanation: This command performs a full TCP connection scan on the victim Metasploit2 VM at IP 10.0.2.15 to identify open ports.



```
tcp.flags.syn == 1 && tcp.flags.ack == 1 && ip.addr == 10.0.2.15
```

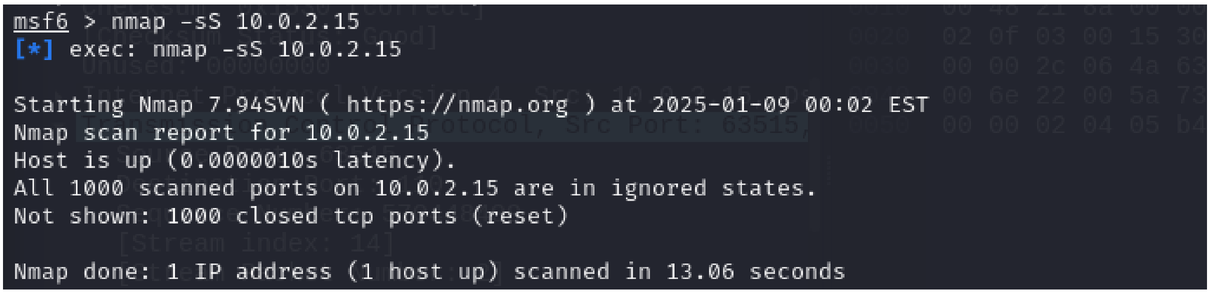
```
No.   Time           Source     Destination  Protocol Length Info
  591 556.812134303 10.0.2.2   10.0.2.15    TCP        60 3389 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 2598 558.020781873 10.0.2.2   10.0.2.15    TCP        60 445 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 2616 558.025477485 10.0.2.2   10.0.2.15    TCP        60 135 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 2734 558.432769250 10.0.2.2   10.0.2.15    TCP        60 902 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 3396 559.461814625 10.0.2.2   10.0.2.15    TCP        60 912 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 3899 560.078990834 10.0.2.2   10.0.2.15    TCP        60 16992 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
```

```
› Frame 591: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
⌄ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e
  › Destination: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
  › Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
    Type: IPv4 (0x0800)
    [Stream index: 1]
    Padding: 0000
› Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
⌄ Transmission Control Protocol, Src Port: 3389, Dst Port: 63515, Seq: 0, Ack: 1, Len: 0
    Source Port: 3389
    Destination Port: 63515
    [Stream index: 13]
    [Stream Packet Number: 2]
  › [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 139840001
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 570448500
    0110 .... = Header Length: 24 bytes (6)
  › Flags: 0x012 (SYN, ACK)
```

```
0000  08 00 27 6e 13 6e 52 55  0a 00 02 0
0010  00 2c 21 8b 00 00 40 06  41 31 0a 0
0020  02 0f 0d 3d f8 1b 08 55  ca 01 22 0
0030  ff ff 2b e2 00 00 02 04  05 b4 00 0
```

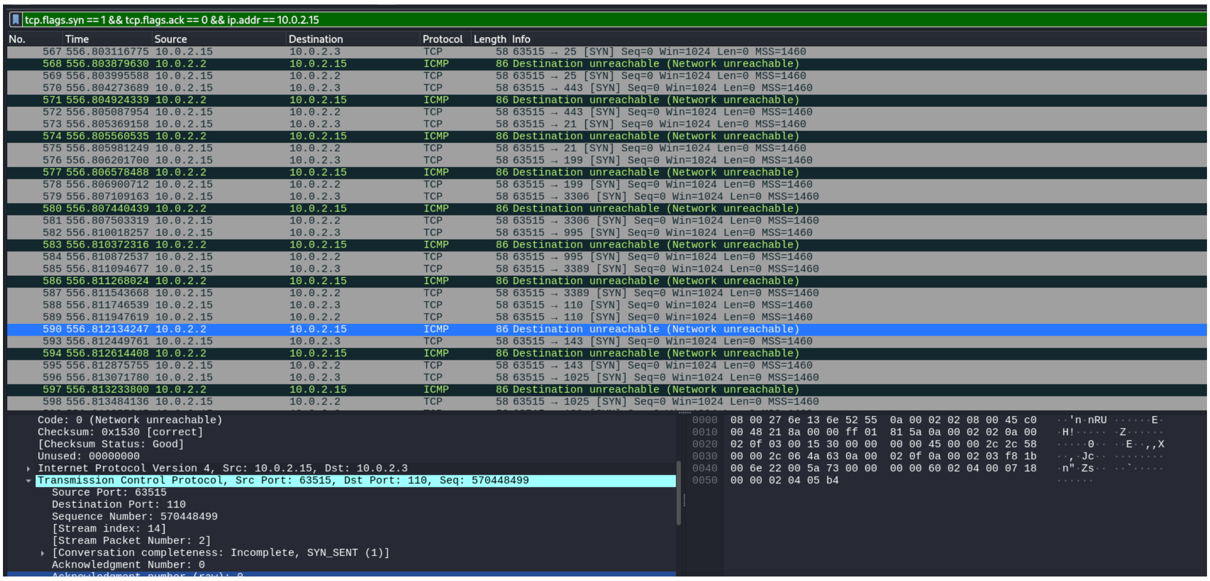
Figure 6: Wireshark filter: `tcp.flags.syn == 1 && tcp.flags.ack == 1 && ip.addr == 10.0.2.15`
Explanation: This filter captures TCP packets with SYN and ACK flags set for the victim Metasploit2 VM at IP 10.0.2.15.

4. Scenario: You want to conduct a stealthy scan on the victim Metasploit2 VM, trying to avoid detection by completing only part of the TCP handshake. Which Nmap command should you use for this scan?



```
msf6 > nmap -sS 10.0.2.15
[*] exec: nmap -sS 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:02 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```

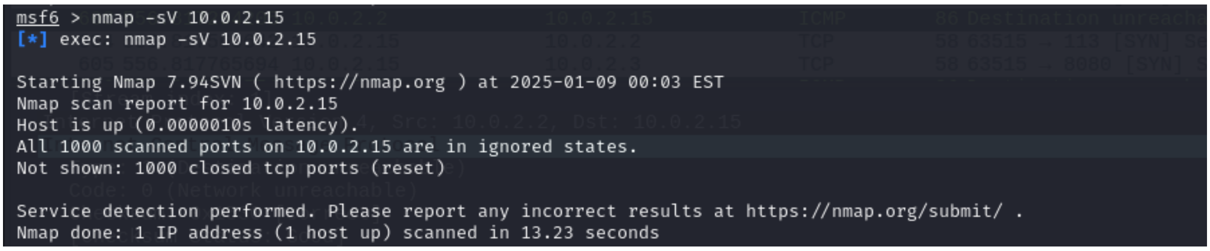
Figure 7: Nmap command: `nmap -sS 10.0.2.15`
Explanation: This command performs a SYN scan on the victim Metasploit2 VM at IP 10.0.2.15, which is stealthier as it does not complete the TCP handshake.



```
tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.addr == 10.0.2.15

No.     Time          Source      Destination  Protocol Length Info
    567 556.803116775 10.0.2.15   10.0.2.3     TCP      58 63515 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    568 556.803879630 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    569 556.803995588 10.0.2.15   10.0.2.2     TCP      58 63515 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    570 556.804273689 10.0.2.15   10.0.2.3     TCP      58 63515 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    571 556.804924339 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    572 556.805087954 10.0.2.15   10.0.2.2     TCP      58 63515 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    573 556.805369158 10.0.2.15   10.0.2.3     TCP      58 63515 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    574 556.805560535 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    575 556.805981249 10.0.2.15   10.0.2.2     TCP      58 63515 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    576 556.806201700 10.0.2.15   10.0.2.3     TCP      58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    577 556.806578488 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    578 556.806900712 10.0.2.15   10.0.2.2     TCP      58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    579 556.807109163 10.0.2.15   10.0.2.3     TCP      58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    580 556.807440439 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    581 556.807503319 10.0.2.15   10.0.2.2     TCP      58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    582 556.810018257 10.0.2.15   10.0.2.3     TCP      58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    583 556.810372316 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    584 556.810872537 10.0.2.15   10.0.2.2     TCP      58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    585 556.811094677 10.0.2.15   10.0.2.3     TCP      58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    586 556.811268024 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    587 556.811543668 10.0.2.15   10.0.2.2     TCP      58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    588 556.811746539 10.0.2.15   10.0.2.3     TCP      58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    589 556.811947619 10.0.2.15   10.0.2.2     TCP      58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    590 556.812134247 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    593 556.812449761 10.0.2.15   10.0.2.3     TCP      58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    594 556.812614408 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    595 556.812875755 10.0.2.15   10.0.2.2     TCP      58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    596 556.813071780 10.0.2.15   10.0.2.3     TCP      58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    597 556.813233800 10.0.2.2    10.0.2.15    ICMP     86 Destination unreachable (Network unreachable)
    598 556.813484136 10.0.2.15   10.0.2.2     TCP      58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

    Code: 0 (Network unreachable)
    Checksum: 0x1530 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  › Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
  ⌄ Transmission Control Protocol, Src Port: 63515, Dst Port: 110, Seq: 570448499
      Source Port: 63515
      Destination Port: 110
      Sequence Number: 570448499
      [Stream index: 14]
      [Stream Packet Number: 2]
    › [Conversation completeness: Incomplete, SYN_SENT (1)]
      Acknowledgment Number: 0

0000  08 00 27 6e 13 6e 52 55  0a 00 02 02 08 00 45 c0   ··'n·nRU ······E·
0010  00 48 21 8a 00 00 ff 01  81 5a 0a 00 02 02 0a 00   ·H!····· ·Z······
0020  02 0f 03 00 15 30 00 00  00 00 45 00 00 2c 2c 58   ·····0·· ··E··,,X
0030  00 00 2c 06 4a 63 0a 00  02 0f 0a 00 02 03 f8 1b   ··,·Jc·· ········
0040  00 6e 22 00 5a 73 00 00  00 00 60 02 04 00 07 18   ·n"·Zs·· ··`·····
0050  00 00 02 04 05 b4                                  ······
```

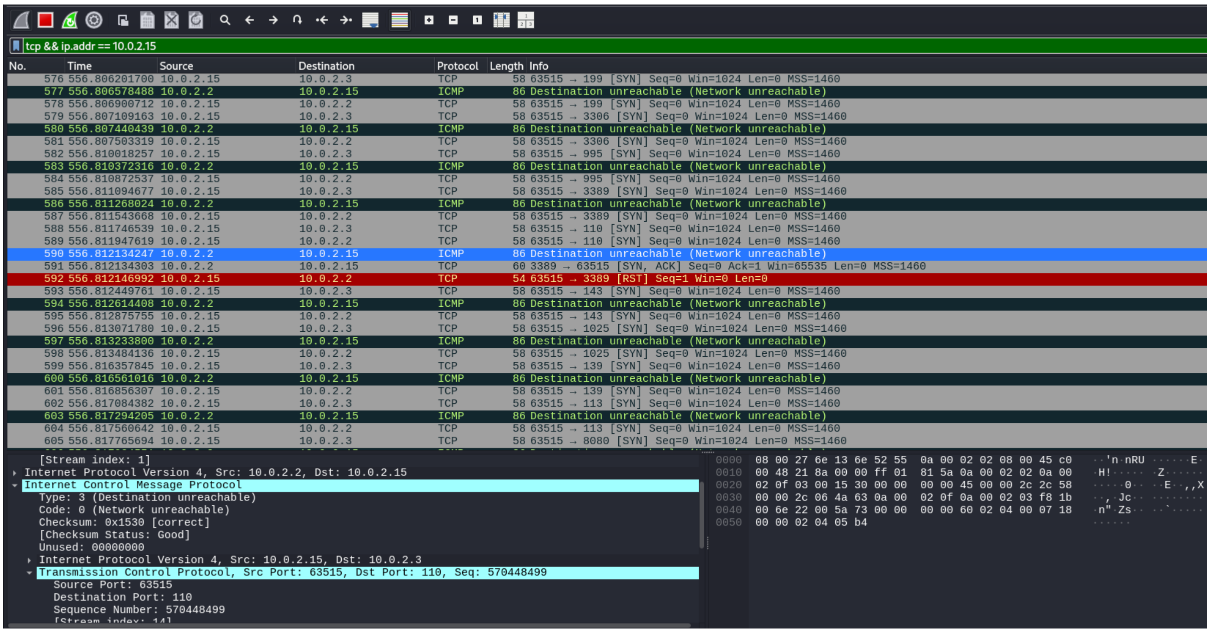
Figure 8: Wireshark filter: `tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.addr == 10.0.2.15`
Explanation: This filter captures TCP packets with only the SYN flag set for the victim Metasploit2 VM at IP 10.0.2.15.

5. Scenario: You want to determine the versions of the services running on the open ports of the victim Metasploit2 VM. How would you do this using Nmap?



```
msf6 > nmap -sV 10.0.2.15
[*] exec: nmap -sV 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:03 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Figure 9: Nmap command: `nmap -sV 10.0.2.15`
Explanation: This command performs a service version detection scan on the victim Metasploit2 VM at IP 10.0.2.15 to identify the versions of services running on open ports.



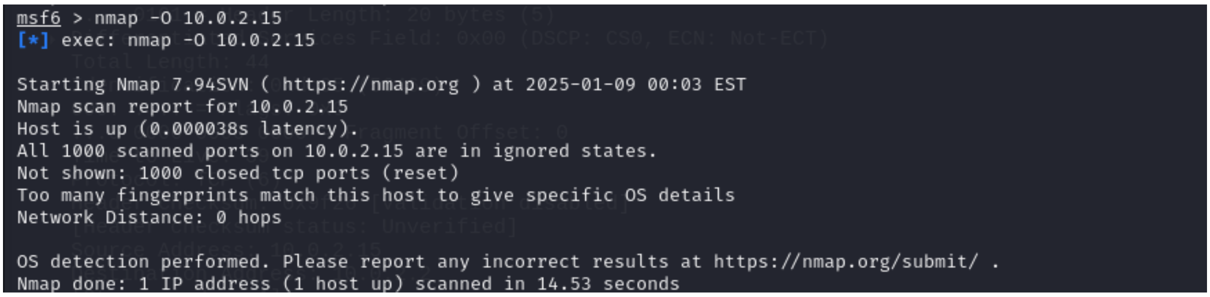
```
tcp && ip.addr == 10.0.2.15
No.  Time          Source     Destination Protocol Length Info
 576 556.806201700 10.0.2.15  10.0.2.3    TCP      58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 577 556.806578488 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 578 556.806900712 10.0.2.15  10.0.2.2    TCP      58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 579 556.807109163 10.0.2.15  10.0.2.3    TCP      58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 580 556.807440439 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 581 556.807503319 10.0.2.15  10.0.2.2    TCP      58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 582 556.810018257 10.0.2.15  10.0.2.3    TCP      58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 583 556.810372316 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 584 556.810872537 10.0.2.15  10.0.2.2    TCP      58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 585 556.811094677 10.0.2.15  10.0.2.3    TCP      58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 586 556.811268024 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 587 556.811543668 10.0.2.15  10.0.2.2    TCP      58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 588 556.811746539 10.0.2.15  10.0.2.3    TCP      58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 589 556.811947619 10.0.2.15  10.0.2.2    TCP      58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 590 556.812134247 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 591 556.812134303 10.0.2.2   10.0.2.15   TCP      60 3389 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 592 556.812146992 10.0.2.15  10.0.2.2    TCP      54 63515 → 3389 [RST] Seq=1 Win=0 Len=0
 593 556.812449761 10.0.2.15  10.0.2.3    TCP      58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 594 556.812614408 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 595 556.812875755 10.0.2.15  10.0.2.2    TCP      58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 596 556.813071780 10.0.2.15  10.0.2.3    TCP      58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 597 556.813233800 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 598 556.813484136 10.0.2.15  10.0.2.2    TCP      58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 599 556.816357845 10.0.2.15  10.0.2.3    TCP      58 63515 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 600 556.816561016 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 601 556.816856307 10.0.2.15  10.0.2.2    TCP      58 63515 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 602 556.817084382 10.0.2.15  10.0.2.3    TCP      58 63515 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 603 556.817294205 10.0.2.2   10.0.2.15   ICMP     86 Destination unreachable (Network unreachable)
 604 556.817560642 10.0.2.15  10.0.2.2    TCP      58 63515 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 605 556.817765694 10.0.2.15  10.0.2.3    TCP      58 63515 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
    [Stream index: 1]
  Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
  Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 0 (Network unreachable)
    Checksum: 0x1530 [correct]
    [Checksum Status: Good]
    Unused: 00000000
    Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
    Transmission Control Protocol, Src Port: 63515, Dst Port: 110, Seq: 570448499
      Source Port: 63515
      Destination Port: 110
      Sequence Number: 570448499
```

```
0000  08 00 27 6e 13 6e 52 55  0a 00 02 02 08 00 45 c0   ··'n·nRU ······E·
0010  00 48 21 8a 00 00 ff 01  81 5a 0a 00 02 02 0a 00   ·H!····· ·Z······
0020  02 0f 03 00 15 30 00 00  00 00 45 00 00 2c 2c 58   ·····0·· ··E··,,X
0030  00 00 2c 06 4a 63 0a 00  02 0f 0a 00 02 03 f8 1b   ··,·Jc·· ········
0040  00 6e 22 00 5a 73 00 00  00 00 60 02 04 00 07 18   ·n"·Zs·· ··`·····
0050  00 00 02 04 05 b4                                  ······
```

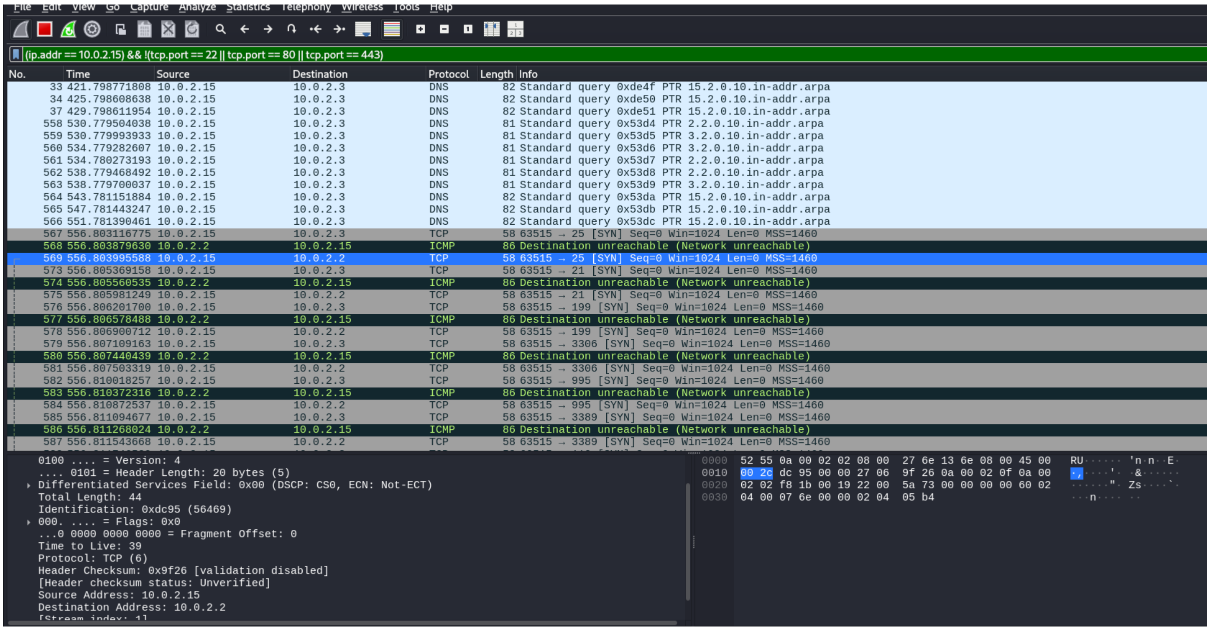
Figure 10: Wireshark filter: `tcp && ip.addr == 10.0.2.15`
Explanation: This filter captures all TCP packets to and from the victim Metasploit2 VM at IP 10.0.2.15.

6. Scenario: You need to find out the operating system running on the victim Metasploit2 VM. What Nmap command will help you gather this information?



```
msf6 > nmap -O 10.0.2.15
[*] exec: nmap -O 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:03 EST
Nmap scan report for 10.0.2.15
Host is up (0.000038s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```

Figure 11: Nmap command: `nmap -O 10.0.2.15`
Explanation: This command performs an OS detection scan on the victim Metasploit2 VM at IP 10.0.2.15 to determine the operating system.



```
(ip.addr == 10.0.2.15) && !(tcp.port == 22 || tcp.port == 80 || tcp.port == 443)
```

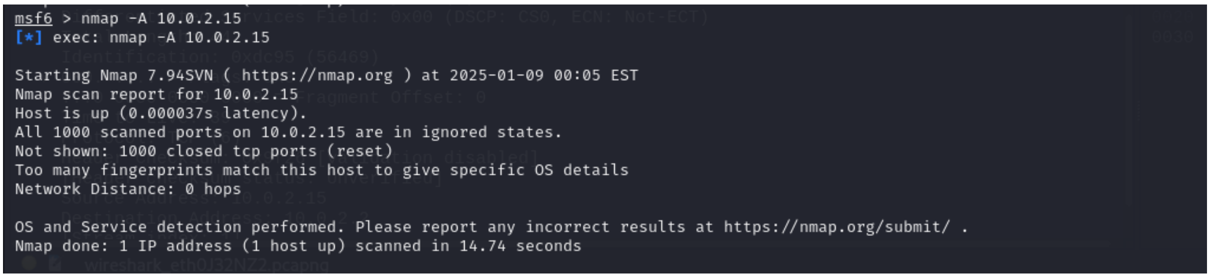
```
No.      Time          Source       Destination   Protocol Length Info
     33 421.798771808 10.0.2.15    10.0.2.3      DNS        82 Standard query 0xde4f PTR 15.2.0.10.in-addr.arpa
     34 425.798608638 10.0.2.15    10.0.2.3      DNS        82 Standard query 0xde50 PTR 15.2.0.10.in-addr.arpa
     37 429.798611954 10.0.2.15    10.0.2.3      DNS        82 Standard query 0xde51 PTR 15.2.0.10.in-addr.arpa
    558 530.779504038 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d4 PTR 2.2.0.10.in-addr.arpa
    559 530.779993933 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d5 PTR 3.2.0.10.in-addr.arpa
    560 534.779282607 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d6 PTR 3.2.0.10.in-addr.arpa
    561 534.780273193 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d7 PTR 2.2.0.10.in-addr.arpa
    562 538.779468492 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d8 PTR 2.2.0.10.in-addr.arpa
    563 538.779700037 10.0.2.15    10.0.2.3      DNS        81 Standard query 0x53d9 PTR 3.2.0.10.in-addr.arpa
    564 543.781151884 10.0.2.15    10.0.2.3      DNS        82 Standard query 0x53da PTR 15.2.0.10.in-addr.arpa
    565 547.781443247 10.0.2.15    10.0.2.3      DNS        82 Standard query 0x53db PTR 15.2.0.10.in-addr.arpa
    566 551.781390461 10.0.2.15    10.0.2.3      DNS        82 Standard query 0x53dc PTR 15.2.0.10.in-addr.arpa
    567 556.803116775 10.0.2.15    10.0.2.3      TCP        58 63515 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    568 556.803879630 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    569 556.803995588 10.0.2.15    10.0.2.2      TCP        58 63515 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    573 556.805369158 10.0.2.15    10.0.2.3      TCP        58 63515 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    574 556.805560535 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    575 556.805981249 10.0.2.15    10.0.2.2      TCP        58 63515 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    576 556.806201700 10.0.2.15    10.0.2.3      TCP        58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    577 556.806578488 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    578 556.806900712 10.0.2.15    10.0.2.2      TCP        58 63515 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    579 556.807109163 10.0.2.15    10.0.2.3      TCP        58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    580 556.807440439 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    581 556.807503319 10.0.2.15    10.0.2.2      TCP        58 63515 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    582 556.810018257 10.0.2.15    10.0.2.3      TCP        58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    583 556.810372316 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    584 556.810872537 10.0.2.15    10.0.2.2      TCP        58 63515 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    585 556.811094677 10.0.2.15    10.0.2.3      TCP        58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    586 556.811268024 10.0.2.2     10.0.2.15     ICMP       86 Destination unreachable (Network unreachable)
    587 556.811543668 10.0.2.15    10.0.2.2      TCP        58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xdc95 (56469)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 39
    Protocol: TCP (6)
    Header Checksum: 0x9f26 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 10.0.2.2
    [Stream index: 1]
```

```
0000  52 55 0a 00 02 02 08 00  27 6e 13 6e 08 00 45 00   RU······'n·n··E·
0010  00 2c dc 95 00 00 27 06  9f 26 0a 00 02 0f 0a 00   ·,····'··&······
0020  02 02 f8 1b 00 19 22 00  5a 73 00 00 00 00 60 02   ······"·Zs····`·
0030  04 00 07 6e 00 00 02 04  05 b4                     ···n······
```

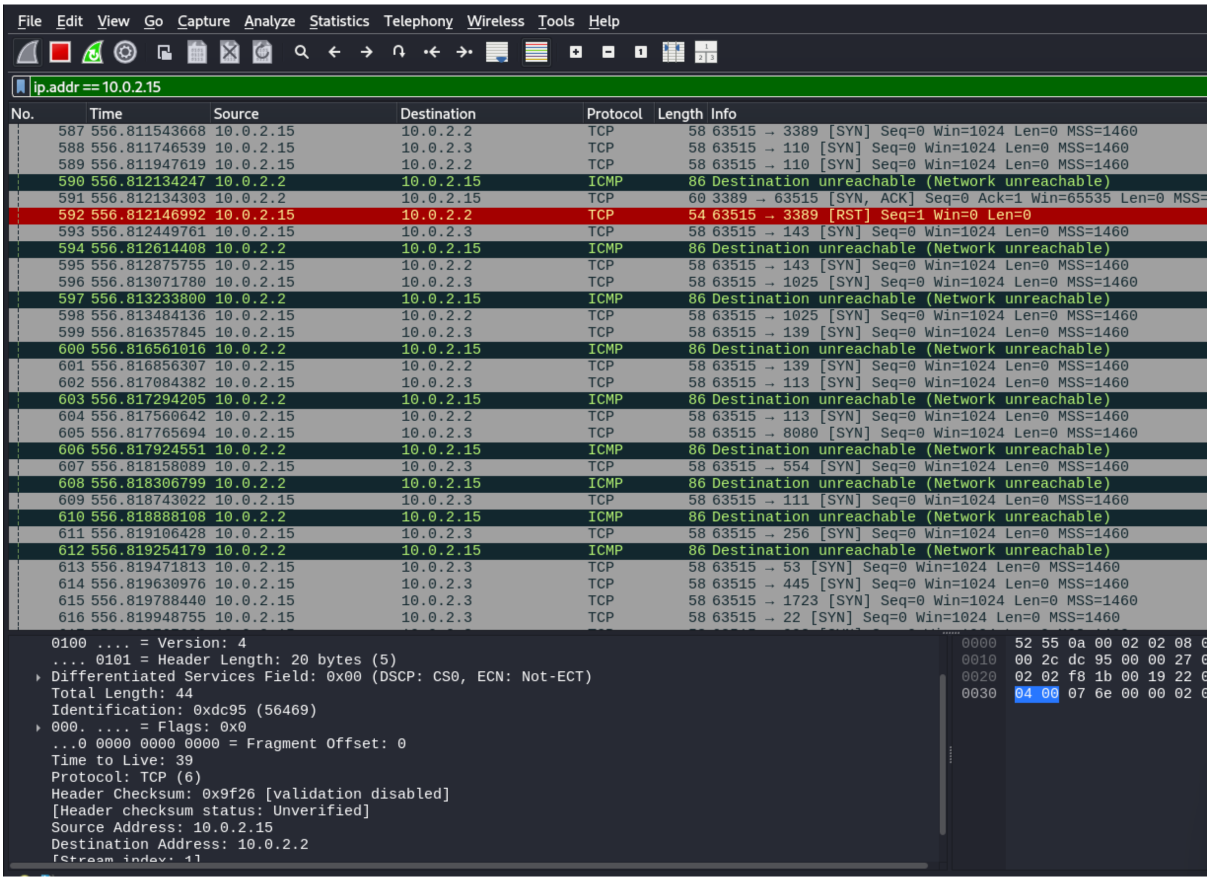
Figure 12: Wireshark filter: `(ip.addr == 10.0.2.15) && (tcp || icmp) && frame.len <= 128`
Explanation: This filter captures TCP and ICMP packets with a frame length of 128 bytes or less for the victim Metasploit2 VM at IP 10.0.2.15.

7. Scenario: You're performing a comprehensive scan of the victim Metasploit2 VM to gather information about open ports, services, operating system, and possible vulnerabilities. What Nmap command should you use?



```
msf6 > nmap -A 10.0.2.15
[*] exec: nmap -A 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:05 EST
Nmap scan report for 10.0.2.15
Host is up (0.000037s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.74 seconds
```

Figure 13: Nmap command: `nmap -A 10.0.2.15`
Explanation: This command performs a comprehensive scan on the victim Metasploit2 VM at IP 10.0.2.15, including OS detection, version detection, script scanning, and traceroute.



ip.addr == 10.0.2.15

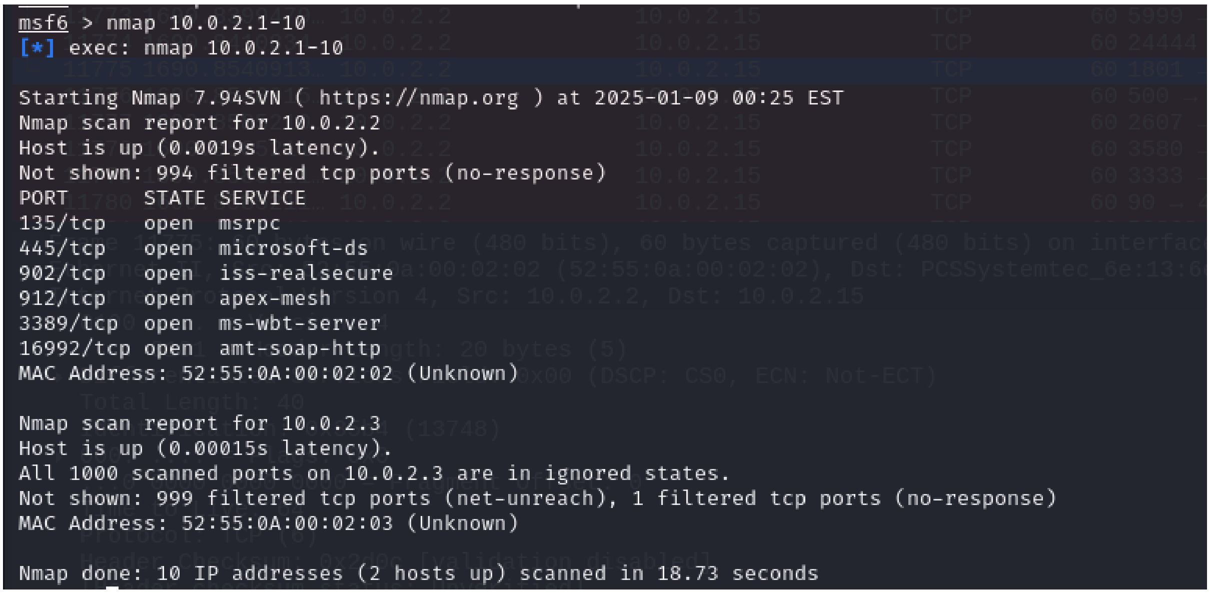
```
No.     Time            Source          Destination     Protocol  Length Info
    587 556.811543668 10.0.2.15       10.0.2.2        TCP       58 63515 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    588 556.811746539 10.0.2.15       10.0.2.3        TCP       58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    589 556.811947619 10.0.2.15       10.0.2.2        TCP       58 63515 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    590 556.812134247 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    591 556.812134303 10.0.2.2        10.0.2.15       TCP       60 3389 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
    592 556.812146992 10.0.2.15       10.0.2.2        TCP       54 63515 → 3389 [RST] Seq=1 Win=0 Len=0
    593 556.812449761 10.0.2.15       10.0.2.3        TCP       58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    594 556.812614408 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    595 556.812875755 10.0.2.15       10.0.2.2        TCP       58 63515 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    596 556.813071780 10.0.2.15       10.0.2.3        TCP       58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    597 556.813233800 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    598 556.813484136 10.0.2.15       10.0.2.2        TCP       58 63515 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    599 556.816357845 10.0.2.15       10.0.2.3        TCP       58 63515 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    600 556.816561016 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    601 556.816856307 10.0.2.15       10.0.2.2        TCP       58 63515 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    602 556.817084382 10.0.2.15       10.0.2.3        TCP       58 63515 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    603 556.817294205 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    604 556.817560642 10.0.2.15       10.0.2.2        TCP       58 63515 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    605 556.817765694 10.0.2.15       10.0.2.3        TCP       58 63515 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    606 556.817924551 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    607 556.818158089 10.0.2.15       10.0.2.3        TCP       58 63515 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    608 556.818306799 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    609 556.818743022 10.0.2.15       10.0.2.3        TCP       58 63515 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    610 556.818888108 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    611 556.819106428 10.0.2.15       10.0.2.3        TCP       58 63515 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    612 556.819254179 10.0.2.2        10.0.2.15       ICMP      86 Destination unreachable (Network unreachable)
    613 556.819471813 10.0.2.15       10.0.2.3        TCP       58 63515 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    614 556.819630976 10.0.2.15       10.0.2.3        TCP       58 63515 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    615 556.819788440 10.0.2.15       10.0.2.3        TCP       58 63515 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    616 556.819948755 10.0.2.15       10.0.2.3        TCP       58 63515 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xdc95 (56469)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 39
    Protocol: TCP (6)
    Header Checksum: 0x9f26 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 10.0.2.2
```

```
0000  52 55 0a 00 02 02 08
0010  00 2c dc 95 00 00 27
0020  02 02 f8 1b 00 19 22
0030  04 00 07 6e 00 00 02
```

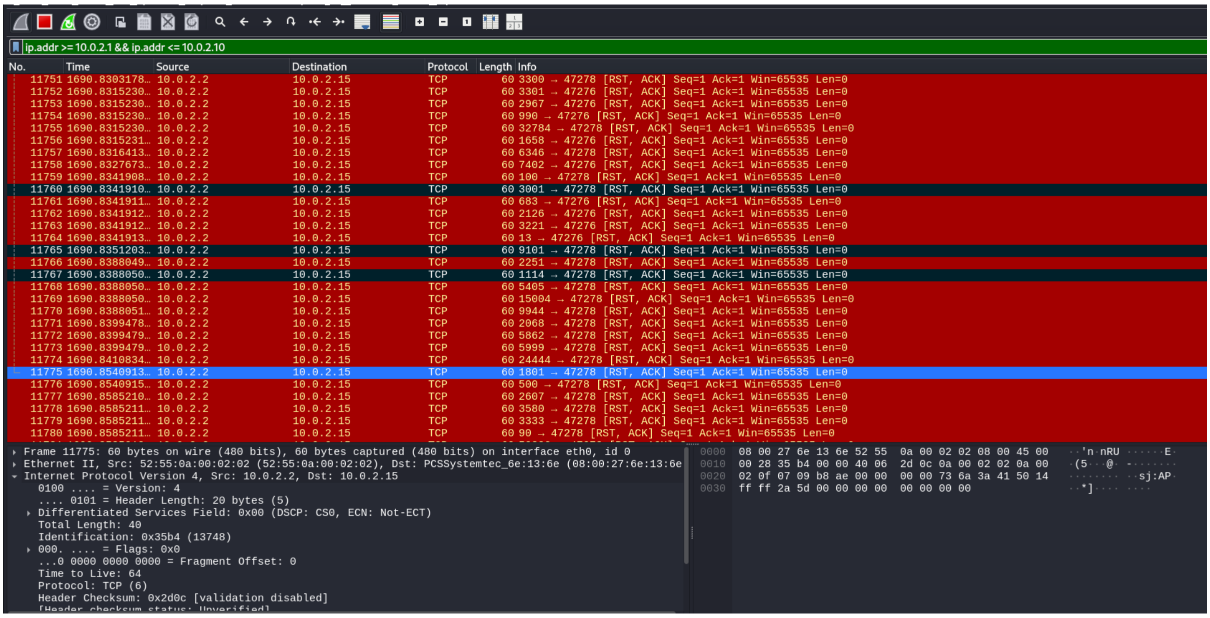
Figure 14: Wireshark filter: `ip.addr == 10.0.2.15`
Explanation: This filter captures all packets to and from the victim Metasploit2 VM at IP 10.0.2.15.

8. Scenario: You are assigned to scan a range of victim VMs within a network, specifically from the first to the tenth IP address in the subnet. Which Nmap command will help you scan this IP range to see which machines are alive or have open ports?



```
msf6 > nmap 10.0.2.1-10
[*] exec: nmap 10.0.2.1-10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:25 EST
Nmap scan report for 10.0.2.2
Host is up (0.0019s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3389/tcp  open  ms-wbt-server
16992/tcp open  amt-soap-http
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00015s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap done: 10 IP addresses (2 hosts up) scanned in 18.73 seconds
```

Figure 15: Nmap command: `nmap 10.0.2.1-10`
Explanation: This command scans the IP range from 10.0.2.1 to 10.0.2.10 to check which machines are alive or have open ports.



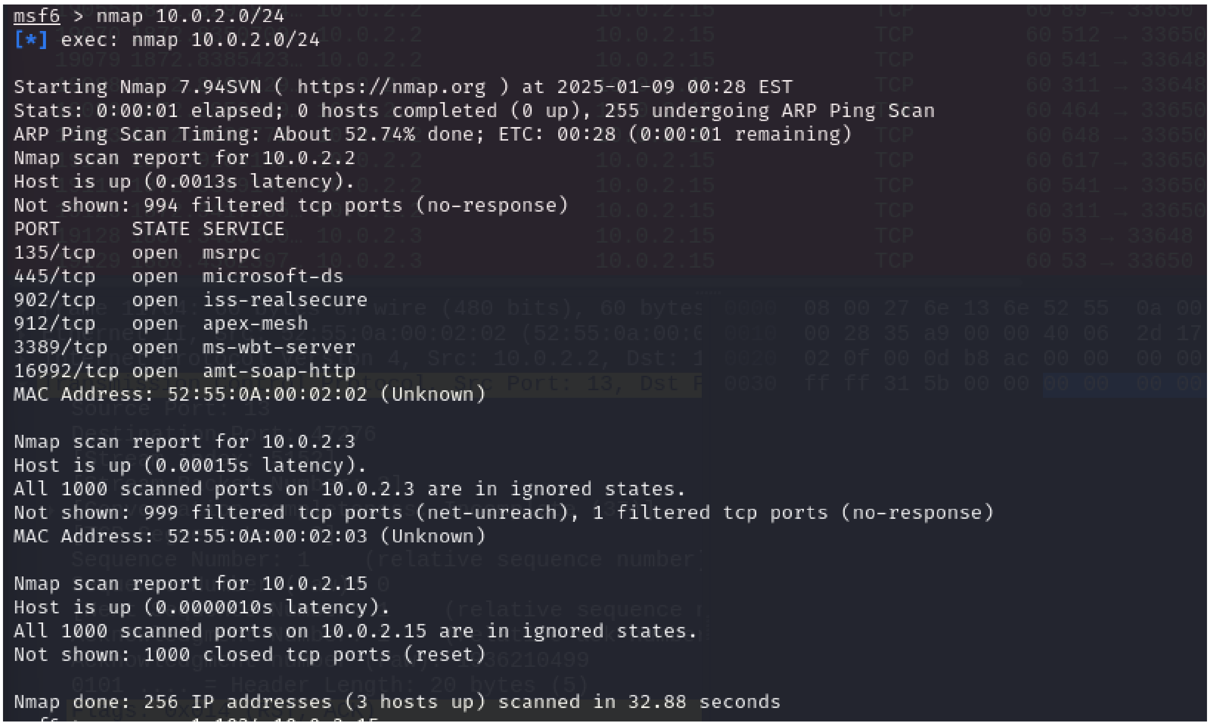
```
ip.addr >= 10.0.2.1 && ip.addr <= 10.0.2.10

No.   Time             Source    Destination  Protocol Length Info
11751 1690.8303178… 10.0.2.2  10.0.2.15    TCP      60 3300 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11752 1690.8315230… 10.0.2.2  10.0.2.15    TCP      60 3301 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11753 1690.8315230… 10.0.2.2  10.0.2.15    TCP      60 2967 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11754 1690.8315230… 10.0.2.2  10.0.2.15    TCP      60 990 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11755 1690.8315230… 10.0.2.2  10.0.2.15    TCP      60 32784 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11756 1690.8315231… 10.0.2.2  10.0.2.15    TCP      60 1658 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11757 1690.8316413… 10.0.2.2  10.0.2.15    TCP      60 6346 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11758 1690.8327673… 10.0.2.2  10.0.2.15    TCP      60 7402 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11759 1690.8341908… 10.0.2.2  10.0.2.15    TCP      60 100 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11760 1690.8341910… 10.0.2.2  10.0.2.15    TCP      60 3001 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11761 1690.8341911… 10.0.2.2  10.0.2.15    TCP      60 683 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11762 1690.8341912… 10.0.2.2  10.0.2.15    TCP      60 2126 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11763 1690.8341912… 10.0.2.2  10.0.2.15    TCP      60 3221 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11764 1690.8341913… 10.0.2.2  10.0.2.15    TCP      60 13 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11765 1690.8351203… 10.0.2.2  10.0.2.15    TCP      60 9101 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11766 1690.8388049… 10.0.2.2  10.0.2.15    TCP      60 2251 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11767 1690.8388050… 10.0.2.2  10.0.2.15    TCP      60 1114 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11768 1690.8388050… 10.0.2.2  10.0.2.15    TCP      60 5405 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11769 1690.8388050… 10.0.2.2  10.0.2.15    TCP      60 15004 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11770 1690.8388051… 10.0.2.2  10.0.2.15    TCP      60 9944 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11771 1690.8399478… 10.0.2.2  10.0.2.15    TCP      60 2068 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11772 1690.8399479… 10.0.2.2  10.0.2.15    TCP      60 5862 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11773 1690.8399479… 10.0.2.2  10.0.2.15    TCP      60 5999 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11774 1690.8410834… 10.0.2.2  10.0.2.15    TCP      60 24444 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11775 1690.8540913… 10.0.2.2  10.0.2.15    TCP      60 1801 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11776 1690.8540915… 10.0.2.2  10.0.2.15    TCP      60 500 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11777 1690.8585210… 10.0.2.2  10.0.2.15    TCP      60 2607 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11778 1690.8585211… 10.0.2.2  10.0.2.15    TCP      60 3580 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11779 1690.8585211… 10.0.2.2  10.0.2.15    TCP      60 3333 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
11780 1690.8585211… 10.0.2.2  10.0.2.15    TCP      60 90 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
▸ Frame 11775: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e
▾ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x35b4 (13748)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x2d0c [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  08 00 27 6e 13 6e 52 55  0a 00 02 02 08 00 45 00   ··'n·nRU ······E·
0010  00 28 35 b4 00 00 40 06  2d 0c 0a 00 02 02 0a 00   ·(5···@· -·······
0020  02 0f 07 09 b8 ae 00 00  00 00 73 6a 3a 41 50 14   ········ ··sj:AP·
0030  ff ff 2a 5d 00 00 00 00  00 00 00 00               ··*]···· ····
```

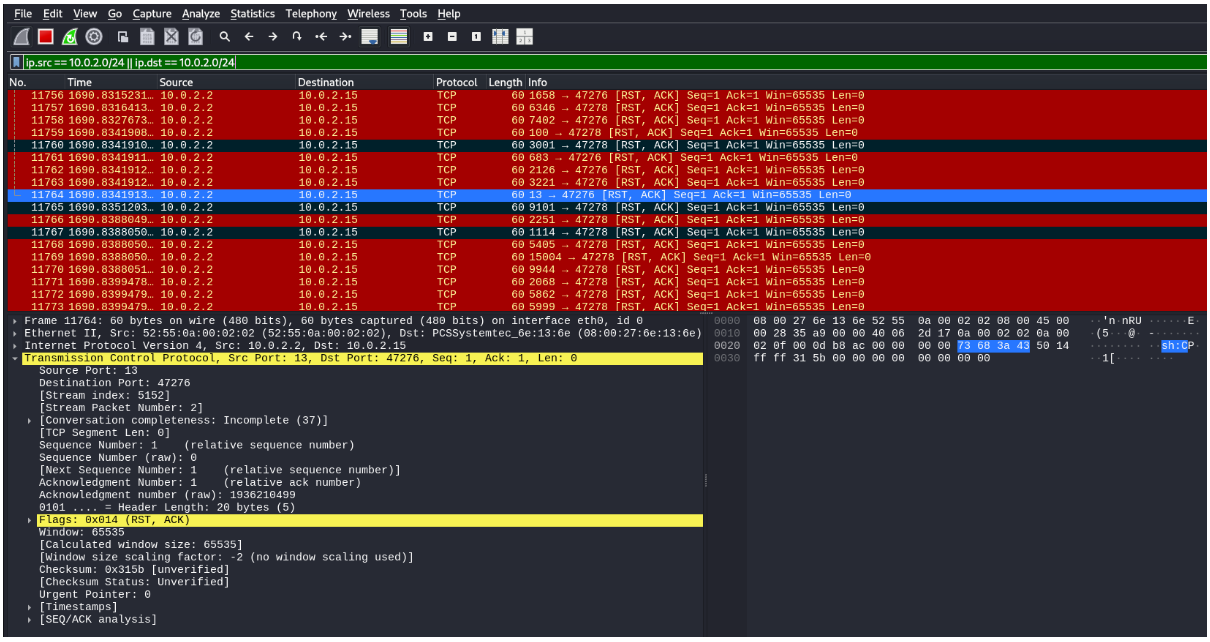
Figure 16: Wireshark filter: `ip.addr >= 10.0.2.1 && ip.addr <= 10.0.2.10`
Explanation: This filter captures all packets to and from the IP range 10.0.2.1 to 10.0.2.10.

9. Scenario: You want to scan all victim machines in the 192.168.x.x subnet, including the Metasploit2 VM, to find which ones are alive and open ports. What is the best approach for scanning an entire subnet?



```
msf6 > nmap 10.0.2.0/24
[*] exec: nmap 10.0.2.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:28 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 52.74% done; ETC: 00:28 (0:00:01 remaining)
Nmap scan report for 10.0.2.2
Host is up (0.0013s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3389/tcp  open  ms-wbt-server
16992/tcp open  amt-soap-http
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00015s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 32.88 seconds
```

Figure 17: Nmap command: `nmap 10.0.2.0/24`
Explanation: This command scans the entire 10.0.2.0/24 subnet to find which machines are alive and have open ports.



ip.src == 10.0.2.0/24 || ip.dst == 10.0.2.0/24

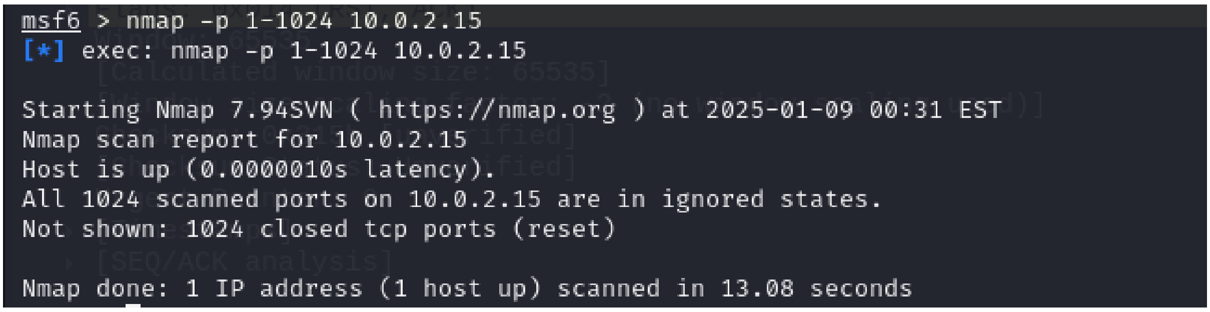
```
No.    Time          Source      Destination  Protocol  Length Info
 11756 1690.8315231… 10.0.2.2    10.0.2.15    TCP       60 1658 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11757 1690.8316413… 10.0.2.2    10.0.2.15    TCP       60 6346 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11758 1690.8327673… 10.0.2.2    10.0.2.15    TCP       60 7402 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11759 1690.8341908… 10.0.2.2    10.0.2.15    TCP       60 100 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11760 1690.8341910… 10.0.2.2    10.0.2.15    TCP       60 3001 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11761 1690.8341911… 10.0.2.2    10.0.2.15    TCP       60 683 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11762 1690.8341912… 10.0.2.2    10.0.2.15    TCP       60 2126 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11763 1690.8341912… 10.0.2.2    10.0.2.15    TCP       60 3221 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11764 1690.8341913… 10.0.2.2    10.0.2.15    TCP       60 13 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11765 1690.8351203… 10.0.2.2    10.0.2.15    TCP       60 9101 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11766 1690.8388049… 10.0.2.2    10.0.2.15    TCP       60 2251 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11767 1690.8388050… 10.0.2.2    10.0.2.15    TCP       60 1114 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11768 1690.8388050… 10.0.2.2    10.0.2.15    TCP       60 5405 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11769 1690.8388050… 10.0.2.2    10.0.2.15    TCP       60 15004 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11770 1690.8388051… 10.0.2.2    10.0.2.15    TCP       60 9944 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11771 1690.8399478… 10.0.2.2    10.0.2.15    TCP       60 2068 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11772 1690.8399479… 10.0.2.2    10.0.2.15    TCP       60 5862 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
 11773 1690.8399479… 10.0.2.2    10.0.2.15    TCP       60 5999 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
▸ Frame 11764: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
▸ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 13, Dst Port: 47276, Seq: 1, Ack: 1, Len: 0
    Source Port: 13
    Destination Port: 47276
    [Stream index: 5152]
    [Stream Packet Number: 2]
  ▸ [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): 1936210499
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x315b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

```
0000  08 00 27 6e 13 6e 52 55  0a 00 02 02 08 00 45 00   ··'n·nRU ······E·
0010  00 28 35 a9 00 00 40 06  2d 17 0a 00 02 02 0a 00   ·(5···@· -·······
0020  02 0f 00 0d b8 ac 00 00  00 00 73 68 3a 43 50 14   ········ ··sh:CP·
0030  ff ff 31 5b 00 00 00 00  00 00 00 00               ··1[···· ····
```

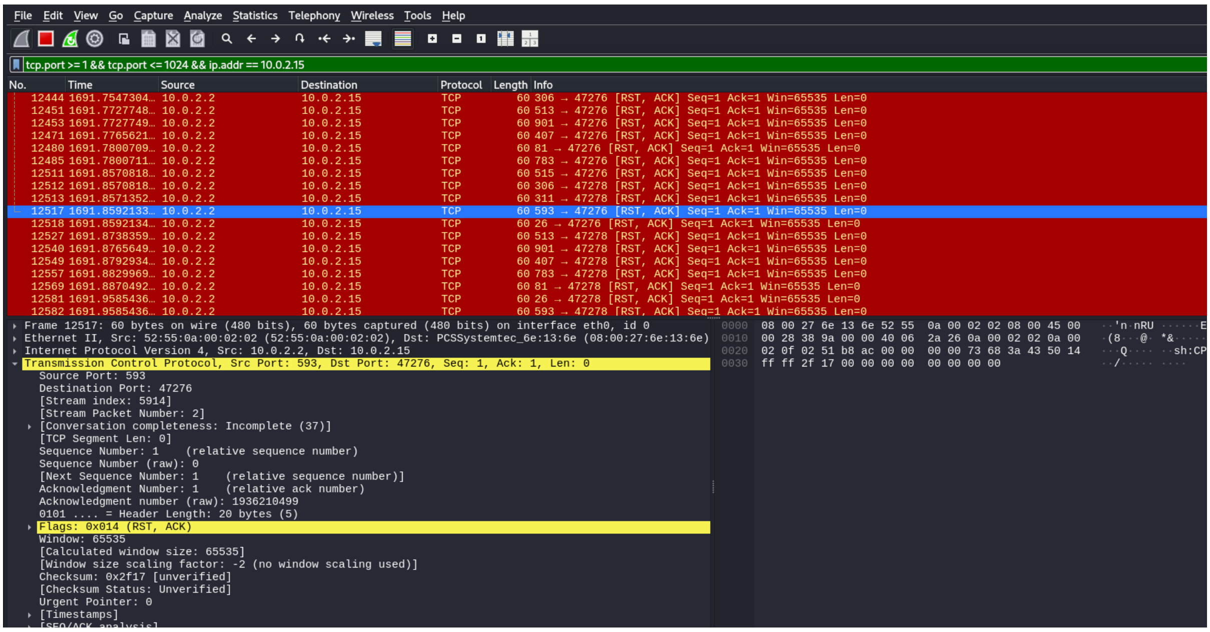
Figure 18: Wireshark filter: `ip.src == 10.0.2.0/24 || ip.dst == 10.0.2.0/24`
Explanation: This filter captures all packets to and from the 10.0.2.0/24 subnet.

10. Scenario: You want to focus your scan on checking common ports (from 1 to 1024) on the victim Metasploit2 VM to detect popular services like FTP, SSH, HTTP, etc. What Nmap command would you use to scan this range of ports?



```
msf6 > nmap -p 1-1024 10.0.2.15
[*] exec: nmap -p 1-1024 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 00:31 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1024 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1024 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

Figure 19: Nmap command: `nmap -p 1-1024 10.0.2.15`
Explanation: This command scans the port range from 1 to 1024 on the victim Metasploit2 VM at IP 10.0.2.15 to detect popular services.



```
tcp.port >= 1 && tcp.port <= 1024 && ip.addr == 10.0.2.15
```

```
No.   Time            Source     Destination  Protocol  Length Info
12444 1691.7547304… 10.0.2.2   10.0.2.15    TCP       60 306 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12451 1691.7727748… 10.0.2.2   10.0.2.15    TCP       60 513 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12453 1691.7727749… 10.0.2.2   10.0.2.15    TCP       60 901 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12471 1691.7765621… 10.0.2.2   10.0.2.15    TCP       60 407 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12480 1691.7800709… 10.0.2.2   10.0.2.15    TCP       60 81 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12485 1691.7800711… 10.0.2.2   10.0.2.15    TCP       60 783 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12511 1691.8570818… 10.0.2.2   10.0.2.15    TCP       60 515 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12512 1691.8570818… 10.0.2.2   10.0.2.15    TCP       60 306 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12513 1691.8571352… 10.0.2.2   10.0.2.15    TCP       60 311 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12517 1691.8592133… 10.0.2.2   10.0.2.15    TCP       60 593 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12518 1691.8592134… 10.0.2.2   10.0.2.15    TCP       60 26 → 47276 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12527 1691.8738359… 10.0.2.2   10.0.2.15    TCP       60 513 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12540 1691.8765649… 10.0.2.2   10.0.2.15    TCP       60 901 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12549 1691.8792934… 10.0.2.2   10.0.2.15    TCP       60 407 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12557 1691.8829969… 10.0.2.2   10.0.2.15    TCP       60 783 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12569 1691.8870492… 10.0.2.2   10.0.2.15    TCP       60 81 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12581 1691.9585436… 10.0.2.2   10.0.2.15    TCP       60 26 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
12582 1691.9585436… 10.0.2.2   10.0.2.15    TCP       60 593 → 47278 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
▸ Frame 12517: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
▸ Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 593, Dst Port: 47276, Seq: 1, Ack: 1, Len: 0
    Source Port: 593
    Destination Port: 47276
    [Stream index: 5914]
    [Stream Packet Number: 2]
  ▸ [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): 1936210499
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x2f17 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

```
0000  08 00 27 6e 13 6e 52 55  0a 00 02 02 08 00 45 00   ··'n·nRU ······E·
0010  00 28 38 9a 00 00 40 06  2a 26 0a 00 02 02 0a 00   ·(8···@· *&······
0020  02 0f 02 51 b8 ac 00 00  00 00 73 68 3a 43 50 14   ···Q···· ··sh:CP·
0030  ff ff 2f 17 00 00 00 00  00 00 00 00               ··/····· ····
```

Figure 20: Wireshark filter: `tcp.port >= 1 && tcp.port <= 1024 && ip.addr == 10.0.2.15`

Explanation: This filter captures TCP packets on ports 1 to 1024 for the victim Metasploit2 VM at IP 10.0.2.15.