EPICODE – ESERICIZO NMAP

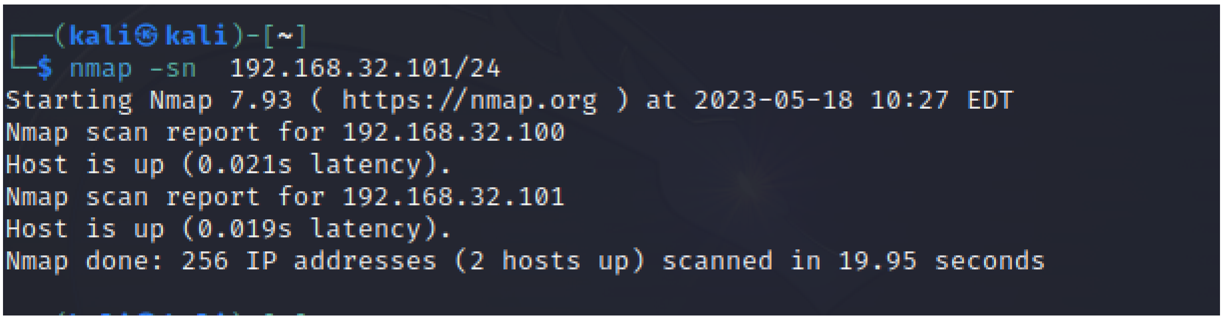
Report Nmap

Nell'esercizio di oggi pomeriggio vedremo da vicino NMAP e i suoi comandi. Sulla base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulle macchine metasploitable , come di seguito:

- Home descovery
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con Switch <- A> sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e quella SYN intercettando le richieste inviate dalla macchina sorgente con Wireshark.

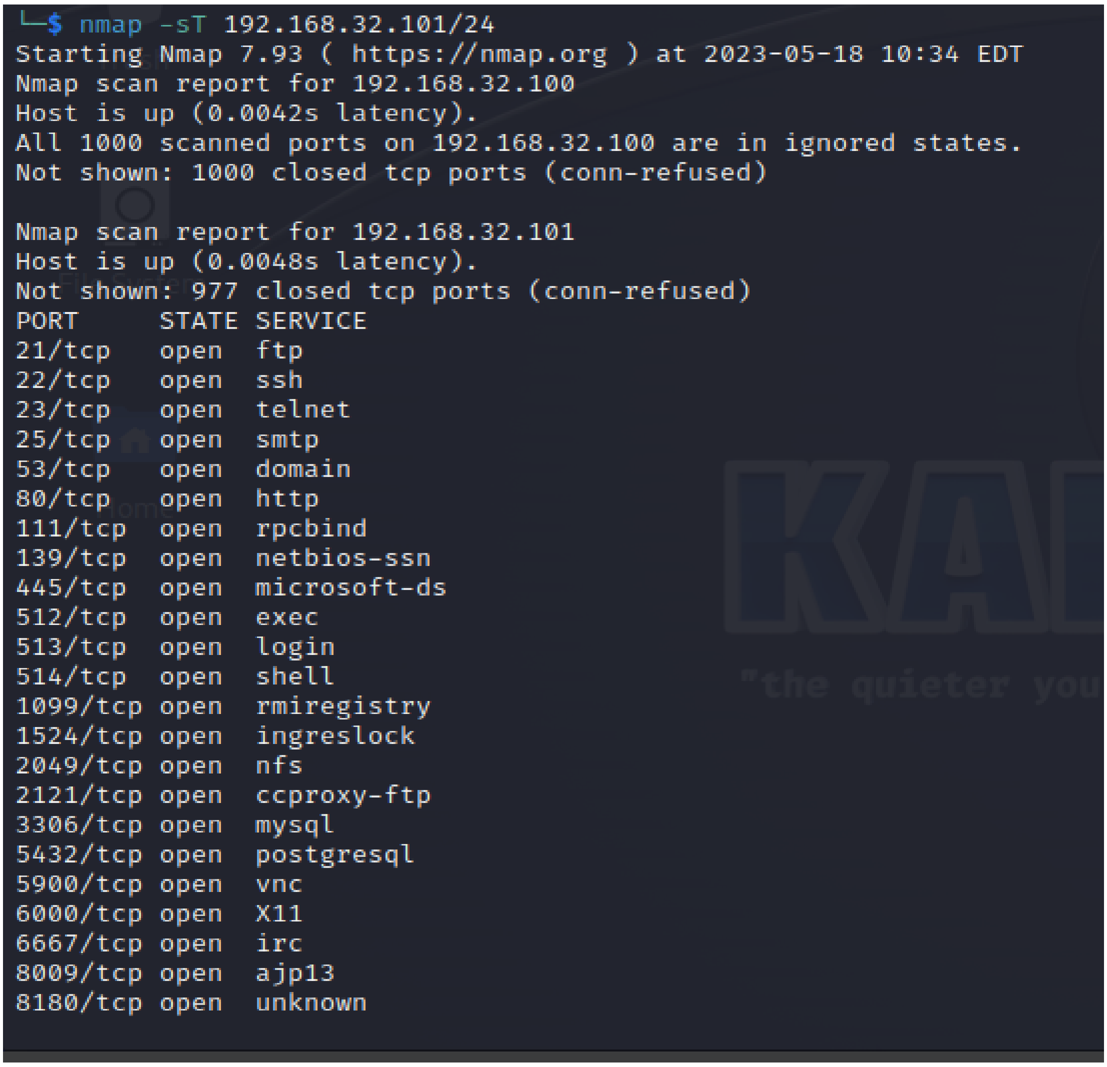
Home descovery



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn  192.168.32.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:27 EDT
Nmap scan report for 192.168.32.100
Host is up (0.021s latency).
Nmap scan report for 192.168.32.101
Host is up (0.019s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.95 seconds
```

Facciamo la scansione con comando **NMAP -SN e l'IP** della macchina per vedere se la macchina è attiva.

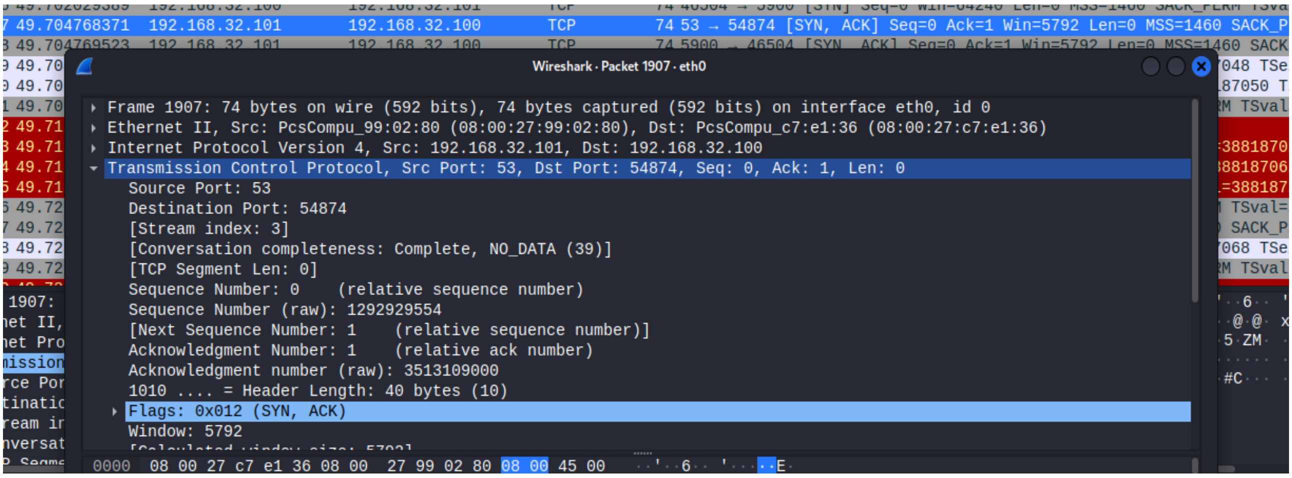
Scansione TCP sulle porte well-known



```
└─$ nmap -sT 192.168.32.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:34 EDT
Nmap scan report for 192.168.32.100
Host is up (0.0042s latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.32.101
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Con il comando NMAP -ST e L'IP scansioniamo tutte le porte well-known. Siamo riusciti a trovare 23 servizi aperti.

Wireshrk TCP

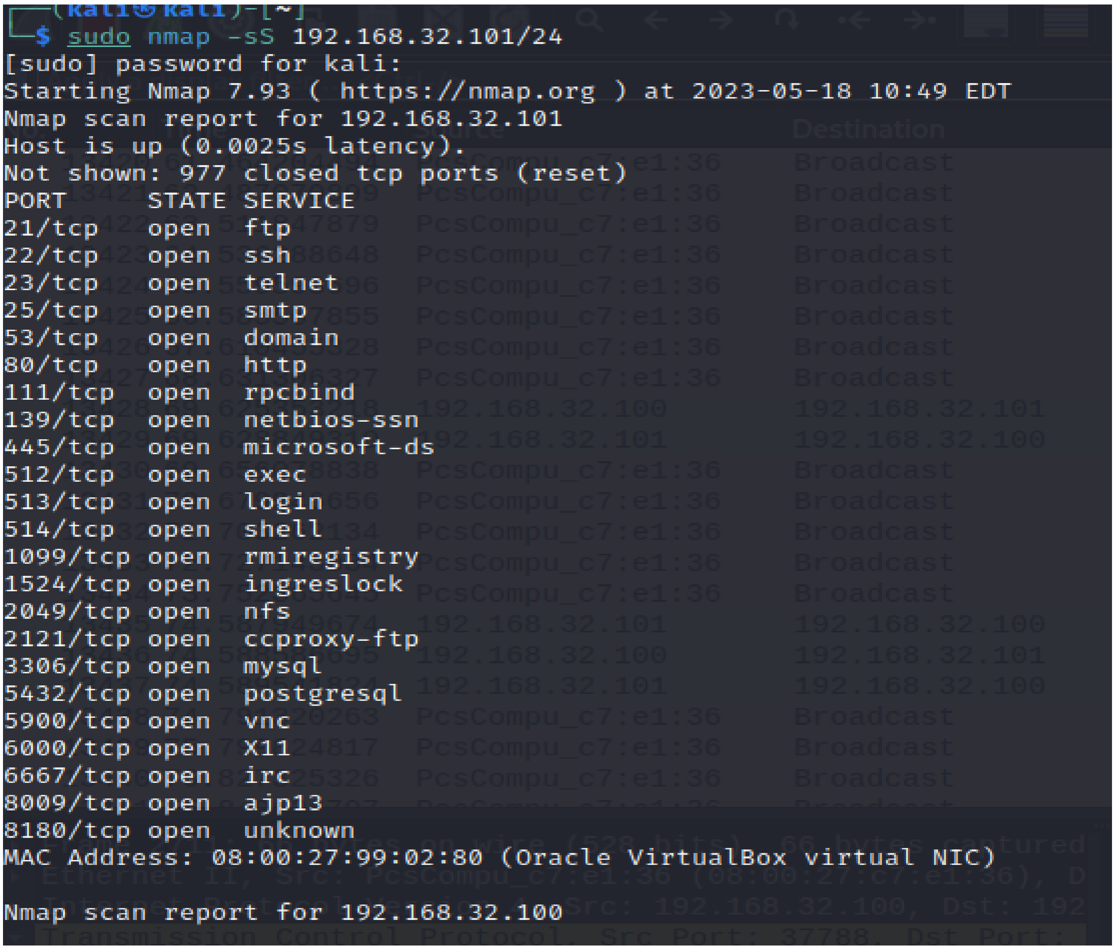


```
7 49.704768371  192.168.32.101    192.168.32.100    TCP    74 53 → 54874 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_P
```

```
▸ Frame 1907: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_99:02:80 (08:00:27:99:02:80), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▾ Transmission Control Protocol, Src Port: 53, Dst Port: 54874, Seq: 0, Ack: 1, Len: 0
    Source Port: 53
    Destination Port: 54874
    [Stream index: 3]
    [Conversation completeness: Complete, NO_DATA (39)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1292929554
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3513109000
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 5792

0000  08 00 27 c7 e1 36 08 00  27 99 02 80 08 00 45 00   ··'··6·· '·····E·
```

Siamo riusciti a intercettare le chiamate con wireshark e in figura si vede il pacchetto catturato TCP.

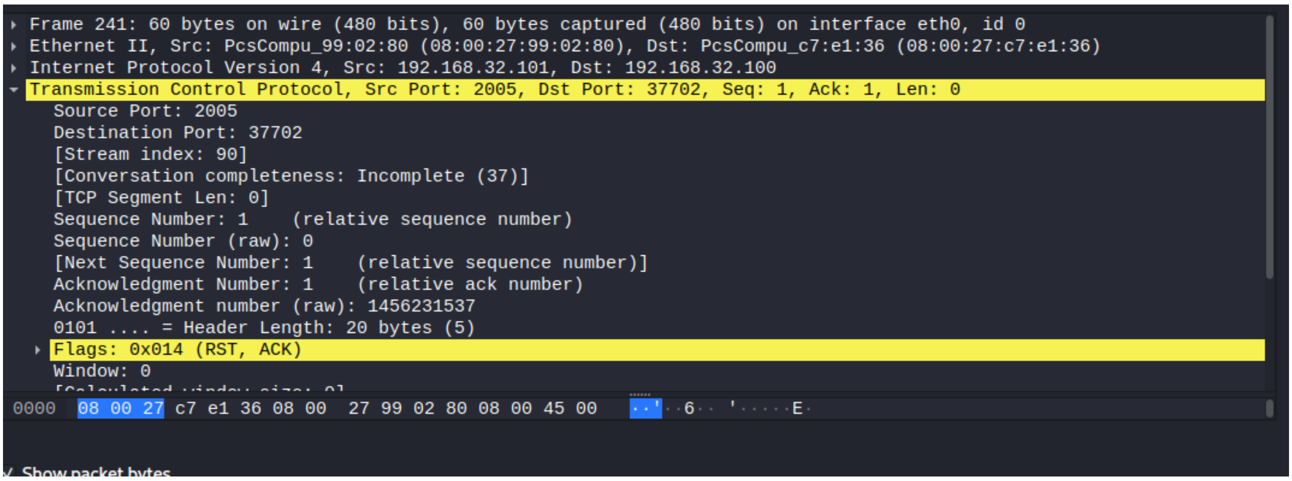
Scansione tipo SYN



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.101/24
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:49 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
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
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:99:02:80 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.32.100
```

Con il comando **SUDO NMAP -SS e L'IP** scansioniamo tutte le porte well-known. Siamo riusciti a trovare 23 servizi aperti più il MAC Address della macchina.

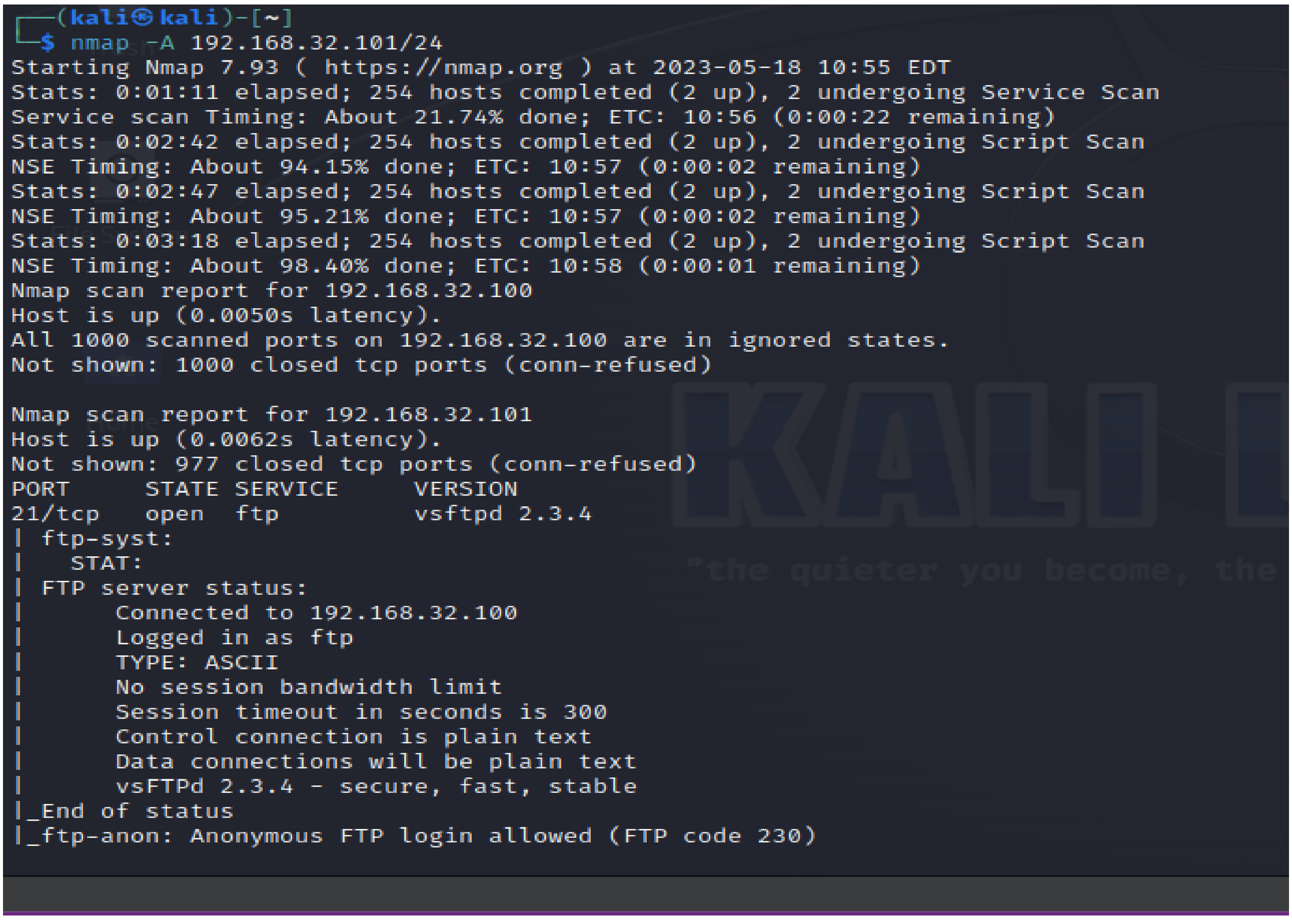
Wireshark SYN



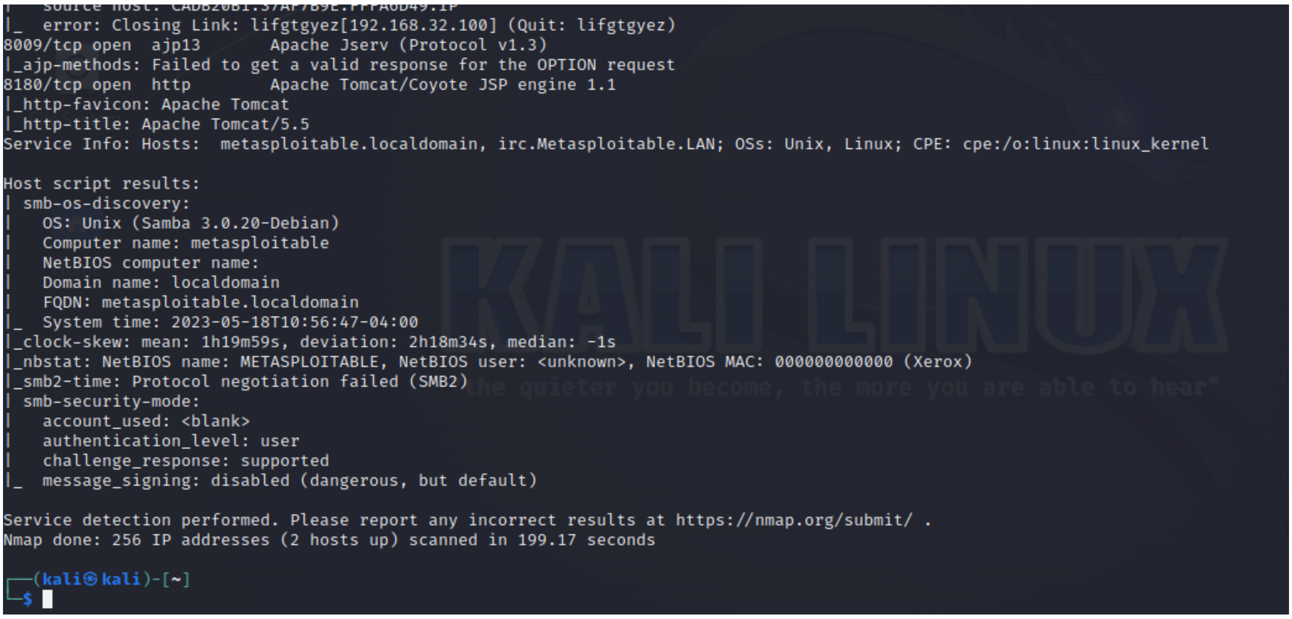
```
› Frame 241: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_99:02:80 (08:00:27:99:02:80), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
› Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
⌄ Transmission Control Protocol, Src Port: 2005, Dst Port: 37702, Seq: 1, Ack: 1, Len: 0
    Source Port: 2005
    Destination Port: 37702
    [Stream index: 90]
    [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): 1456231537
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
0000  08 00 27 c7 e1 36 08 00  27 99 02 80 08 00 45 00   ··'··6·· '·····E·
```

Siamo riusciti a intercettare le chiamate con wireshark e in figura si vede il pacchetto catturato (RST,ACK)

SCANSIONE SWITCH -A



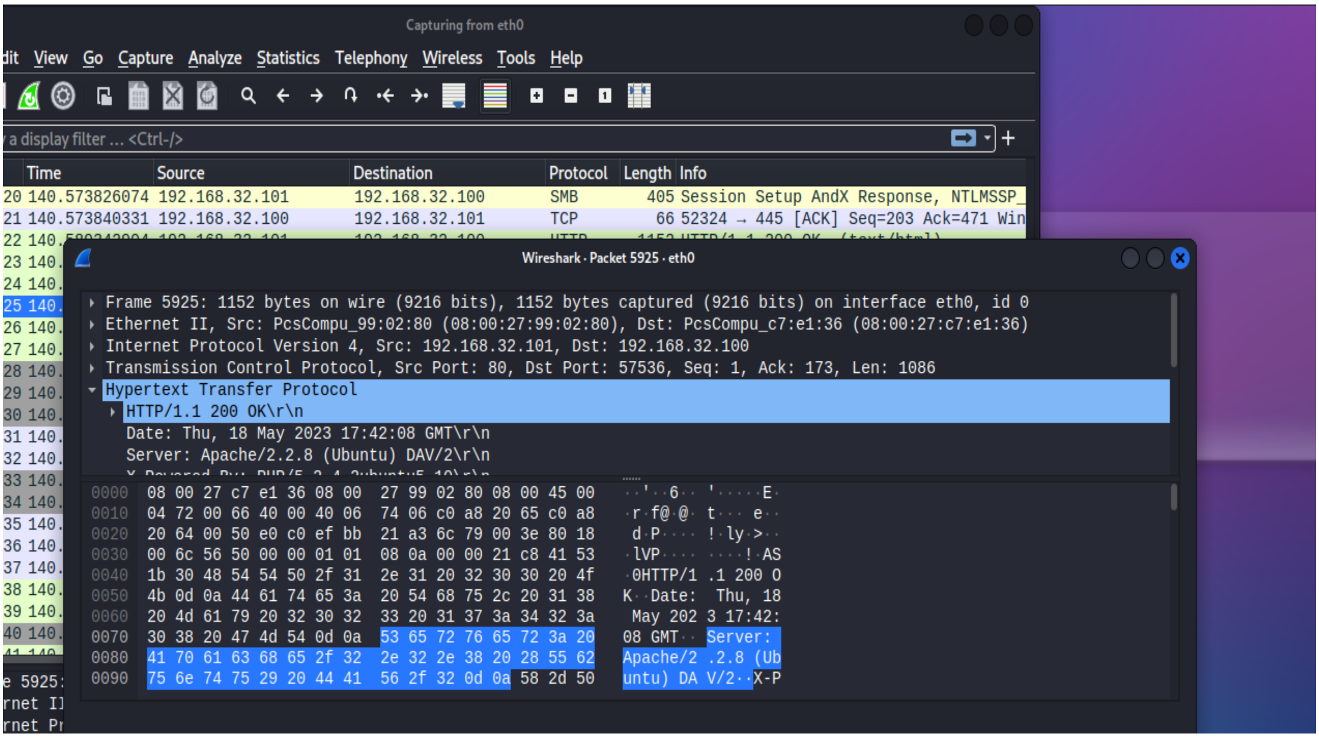
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.32.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:55 EDT
Stats: 0:01:11 elapsed; 254 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 21.74% done; ETC: 10:56 (0:00:22 remaining)
Stats: 0:02:42 elapsed; 254 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 94.15% done; ETC: 10:57 (0:00:02 remaining)
Stats: 0:02:47 elapsed; 254 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 95.21% done; ETC: 10:57 (0:00:02 remaining)
Stats: 0:03:18 elapsed; 254 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 98.40% done; ETC: 10:58 (0:00:01 remaining)
Nmap scan report for 192.168.32.100
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.32.101
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.32.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```



```
|   source host: CADB20B1.37AF7B9E.FFFA6D49.IP
|_  error: Closing Link: lifgtgyez[192.168.32.100] (Quit: lifgtgyez)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T10:56:47-04:00
|_clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: -1s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 199.17 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Con il comando NMAP -A e L'IP scansioniamo tutte le porte well-known. Siamo riusciti a trovare 23 servizi aperti con che descrive le caratteristiche più approfondite dell'utilizzo di ogni servizio trovato.

WIRESHARK CON -A



Capturing from eth0
dit View Go Capture Analyze Statistics Telephony Wireless Tools Help
a display filter … <Ctrl-/>
Wireshark · Packet 5925 · eth0

```
   Time          Source          Destination     Protocol Length Info
20 140.573826074 192.168.32.101  192.168.32.100  SMB       405 Session Setup AndX Response, NTLMSSP_
21 140.573840331 192.168.32.100  192.168.32.101  TCP        66 52324 → 445 [ACK] Seq=203 Ack=471 Win
22 140.580342004 192.168.32.101  192.168.32.100  HTTP     1152 HTTP/1.1 200 OK  (text/html)
23 140.
24 140.
25 140.
26 140.
27 140.
28 140.
29 140.
30 140.
31 140.
32 140.
33 140.
34 140.
35 140.
36 140.
37 140.
38 140.
39 140.
40 140.
```

```
▸ Frame 5925: 1152 bytes on wire (9216 bits), 1152 bytes captured (9216 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_99:02:80 (08:00:27:99:02:80), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 57536, Seq: 1, Ack: 173, Len: 1086
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Thu, 18 May 2023 17:42:08 GMT\r\n
    Server: Apache/2.2.8 (Ubuntu) DAV/2\r\n
    X-Powered-By: PHP/5.2.4-2ubuntu5.10\r\n
```

```
0000  08 00 27 c7 e1 36 08 00  27 99 02 80 08 00 45 00   ··'··6·· '·····E·
0010  04 72 00 66 40 00 40 06  74 06 c0 a8 20 65 c0 a8   ·r·f@·@· t··· e··
0020  20 64 00 50 e0 c0 ef bb  21 a3 6c 79 00 3e 80 18    d·P···· !·ly·>··
0030  00 6c 56 50 00 00 01 01  08 0a 00 00 21 c8 41 53   ·lVP···· ····!·AS
0040  1b 30 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ·0HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 68 75 2c 20 31 38   K··Date:  Thu, 18
0060  20 4d 61 79 20 32 30 32  33 20 31 37 3a 34 32 3a    May 202 3 17:42:
0070  30 38 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   08 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 32 2e 38 20 28 55 62   Apache/2 .2.8 (Ub
0090  75 6e 74 75 29 20 44 41  56 2f 32 0d 0a 58 2d 50   untu) DA V/2··X-P
```

Nell’immagine su abbiamo intercettato con wireshark la richiesta molto più approfondita delle informazione della macchina dell’IP e del pacchetto .

Conclusioni

Per quanto riguarda la differenza tra il la richiesta TCP e la richiesta SYN vediamo come nella richiesta TCP completa tutta la richiesta creando il canale con ACK mentre nella richiesta SYN chiude la comunicazione con RST.