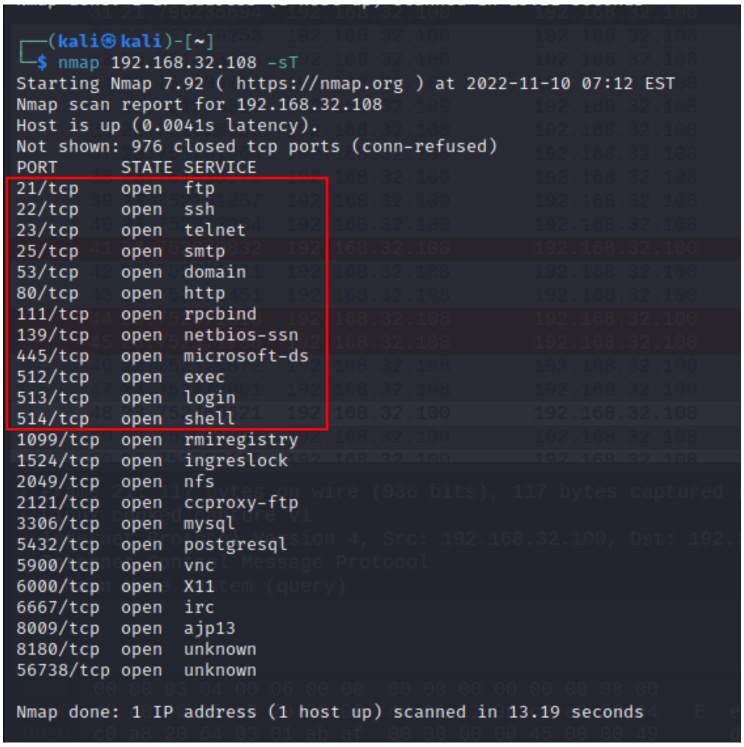
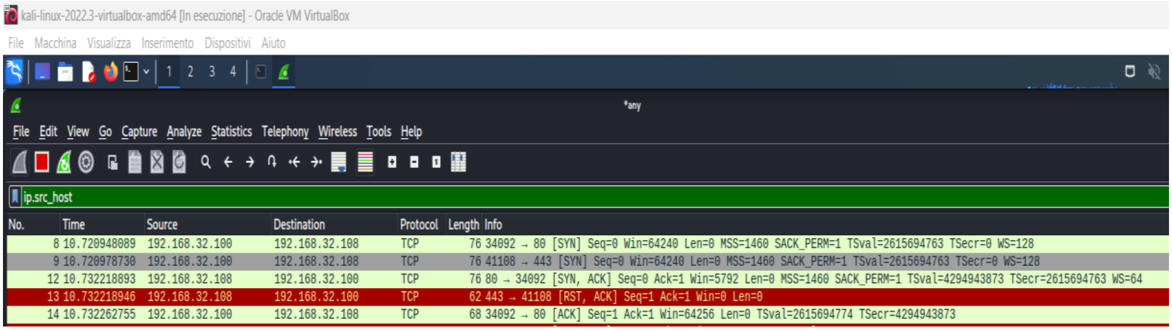
SCANSIONI CON NMAP

Lanciando su terminale kali il comando ‘nmap indirizzo ip –sT’, possiamo fare una scansione di tutti i servizi TCP sull’ host scelto; l’esercizio richiede solamente le porte well-known, quindi andiamo a vedere solamente le porte fino a 1023:



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.108 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 07:12 EST
Nmap scan report for 192.168.32.108
Host is up (0.0041s latency).
Not shown: 976 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
56738/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

Con questo tipo di scansione, nmap usa completamente il 3 way handshake per capire se una porta è aperta e per carpire informazioni; qui nell’immagine vediamo l’esempio con la porta 80:

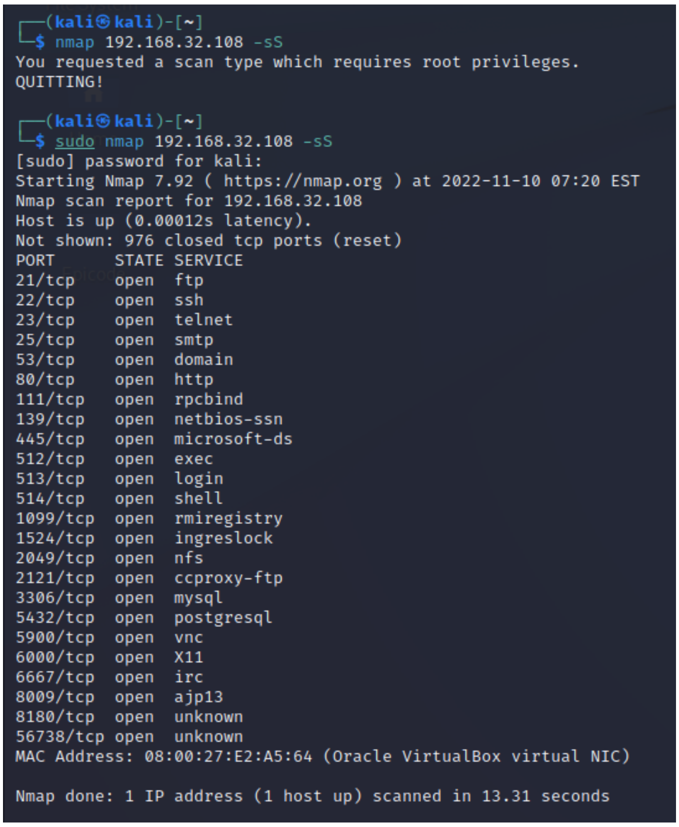


kali-linux-2022.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src_host

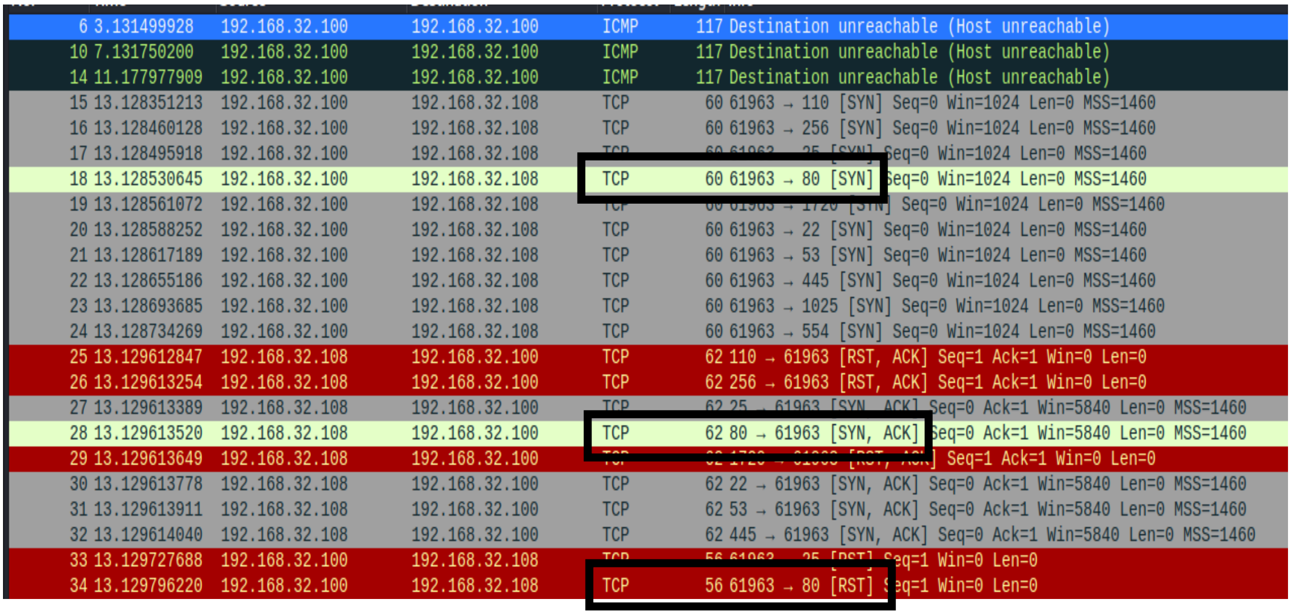
No.	Time	Source	Destination	Protocol	Length	Info
8	10.720948089	192.168.32.100	192.168.32.108	TCP	76	34092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2615694763 TSecr=0 WS=128
9	10.720978730	192.168.32.100	192.168.32.108	TCP	76	41108 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2615694763 TSecr=0 WS=128
12	10.732218893	192.168.32.108	192.168.32.100	TCP	76	80 → 34092 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294943873 TSecr=2615694763 WS=64
13	10.732218946	192.168.32.108	192.168.32.100	TCP	62	443 → 41108 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	10.732262755	192.168.32.100	192.168.32.108	TCP	68	34092 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2615694774 TSecr=4294943873

Lanciando su terminale kali il comando ‘nmap indirizzo ip –sS’, facciamo sempre una scansione di tutti i servizi TCP sull’ host scelto:



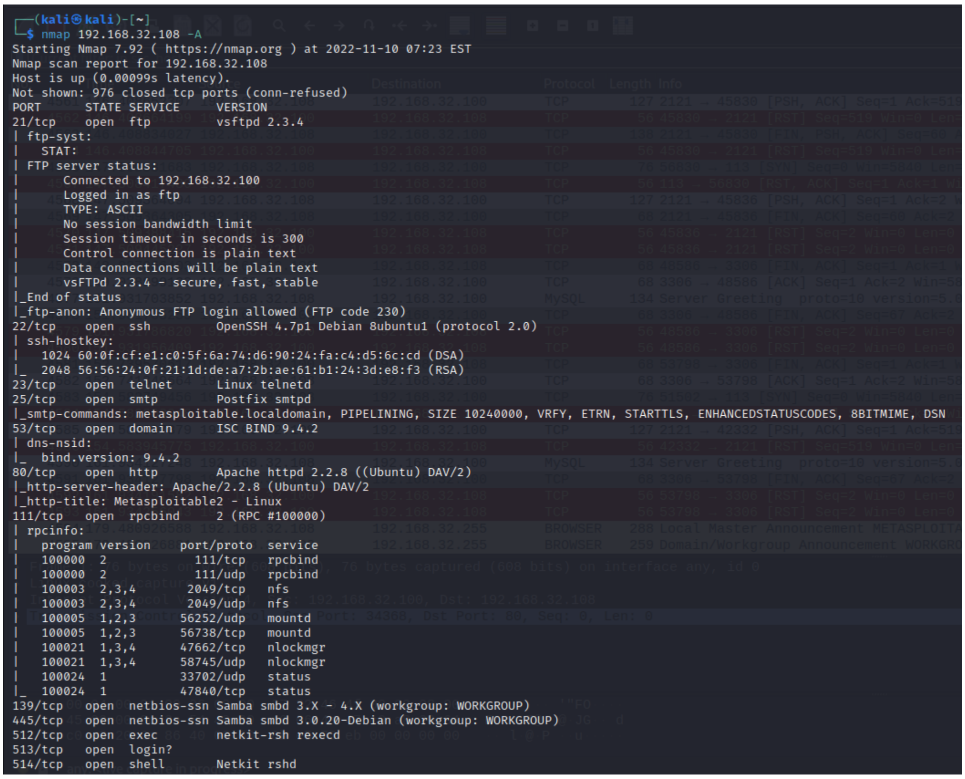
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.108 -sS
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.32.108 -sS
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 07:20 EST
Nmap scan report for 192.168.32.108
Host is up (0.00012s latency).
Not shown: 976 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
56738/tcp open  unknown
MAC Address: 08:00:27:E2:A5:64 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

IN questo caso però, la scansione è meno invasiva a livello networking in quanto non completa il 3 way handshake, ma una volta appurato che la porta è aperta, manda il RST (reset):

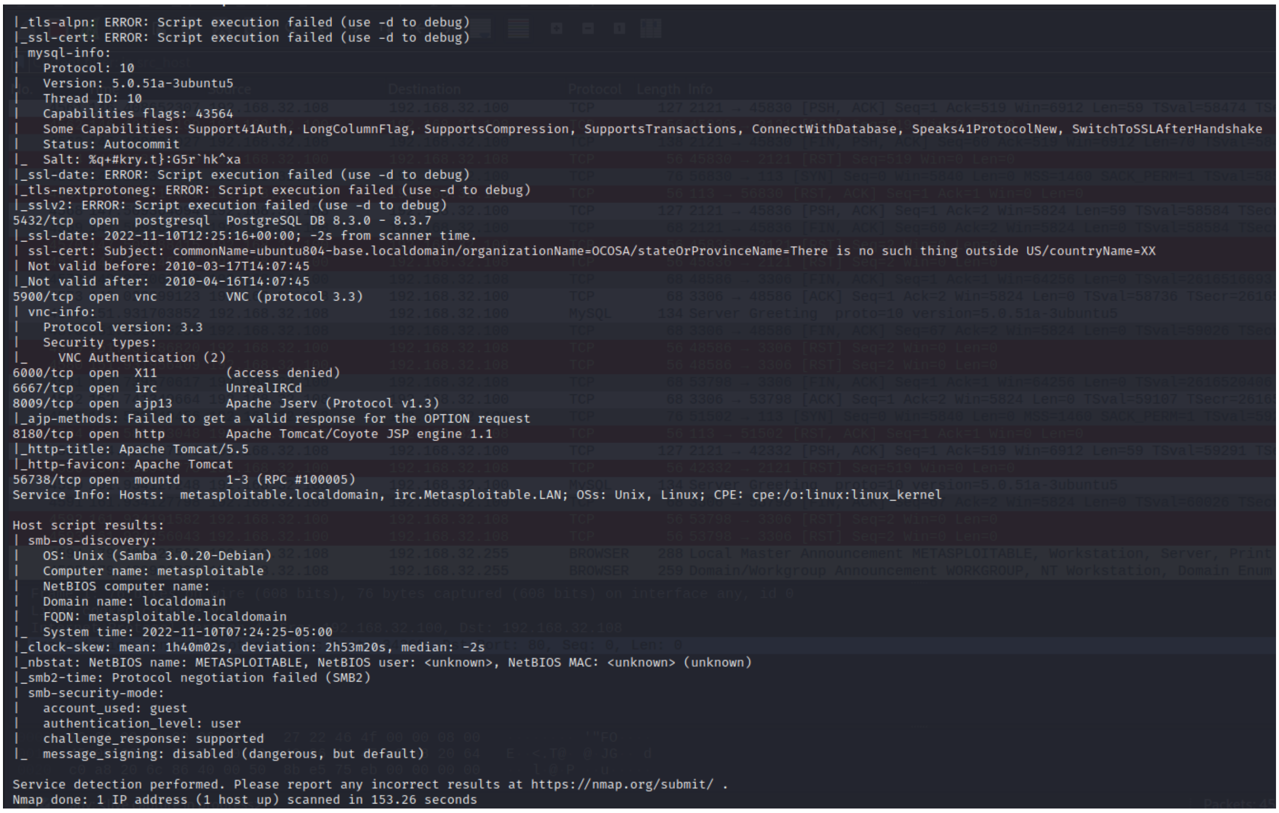


```
 6 3.131499928  192.168.32.100  192.168.32.100  ICMP  117 Destination unreachable (Host unreachable)
10 7.131750200  192.168.32.100  192.168.32.100  ICMP  117 Destination unreachable (Host unreachable)
14 11.177977909 192.168.32.100  192.168.32.100  ICMP  117 Destination unreachable (Host unreachable)
15 13.128351213 192.168.32.100  192.168.32.108  TCP    60 61963 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16 13.128460128 192.168.32.100  192.168.32.108  TCP    60 61963 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17 13.128495918 192.168.32.100  192.168.32.108  TCP    60 61963 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18 13.128530645 192.168.32.100  192.168.32.108  TCP    60 61963 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 13.128561072 192.168.32.100  192.168.32.108  TCP    60 61963 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 13.128588252 192.168.32.100  192.168.32.108  TCP    60 61963 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21 13.128617189 192.168.32.100  192.168.32.108  TCP    60 61963 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 13.128655186 192.168.32.100  192.168.32.108  TCP    60 61963 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23 13.128693685 192.168.32.100  192.168.32.108  TCP    60 61963 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24 13.128734269 192.168.32.100  192.168.32.108  TCP    60 61963 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25 13.129612847 192.168.32.108  192.168.32.100  TCP    62 110 → 61963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26 13.129613254 192.168.32.108  192.168.32.100  TCP    62 256 → 61963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 13.129613389 192.168.32.108  192.168.32.100  TCP    62 25 → 61963 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
28 13.129613520 192.168.32.108  192.168.32.100  TCP    62 80 → 61963 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29 13.129613649 192.168.32.108  192.168.32.100  TCP    62 1720 → 61963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30 13.129613778 192.168.32.108  192.168.32.100  TCP    62 22 → 61963 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
31 13.129613911 192.168.32.108  192.168.32.100  TCP    62 53 → 61963 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
32 13.129614040 192.168.32.108  192.168.32.100  TCP    62 445 → 61963 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33 13.129727688 192.168.32.100  192.168.32.108  TCP    56 61963 → 25 [RST] Seq=1 Win=0 Len=0
34 13.129796220 192.168.32.100  192.168.32.108  TCP    56 61963 → 80 [RST] Seq=1 Win=0 Len=0
```

Lanciando ‘nmap indirizzo ip –A’, si avrà lo scan aggressivo che comprende l’OS detection (-o), version scanning (-sV), script scanning (-sC) e traceroute (--traceroute):

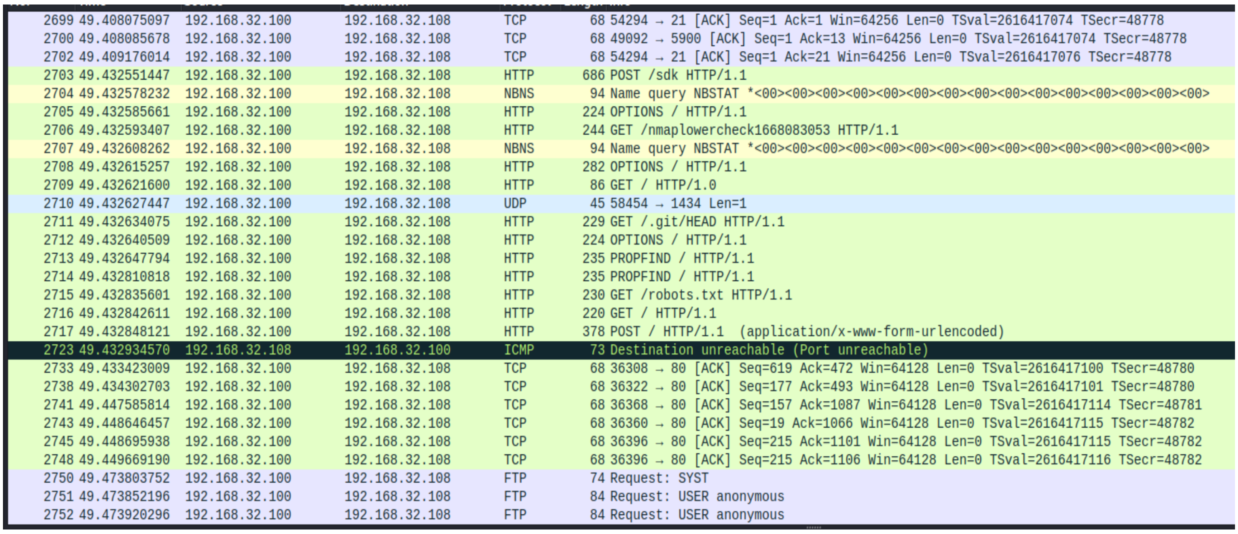


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.108 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 07:23 EST
Nmap scan report for 192.168.32.108
Host is up (0.00099s latency).
Not shown: 976 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| 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)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      56252/udp   mountd
|   100005  1,2,3      56738/tcp   mountd
|   100021  1,3,4      47662/tcp   nlockmgr
|   100021  1,3,4      58745/udp   nlockmgr
|   100024  1          33702/udp   status
|_  100024  1          47840/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
```



```
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsCompression, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: %q+#kry.t}:G5r`hk^xa
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-11-10T12:25:16+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
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-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
56738/tcp open  mountd      1-3 (RPC #100005)
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: 2022-11-10T07:24:25-05:00
|_clock-skew: mean: 1h40m02s, deviation: 2h53m20s, median: -2s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   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: 1 IP address (1 host up) scanned in 153.26 seconds
```

Qui su wireshark infatti possiamo vedere come ci siamo vari protocolli che lavorano una volta fatta questa richiesta ad nmap:



```
2699 49.408075097  192.168.32.100     192.168.32.108     TCP        68 54294 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2616417074 TSecr=48778
2700 49.408085678  192.168.32.100     192.168.32.108     TCP        68 49092 → 5900 [ACK] Seq=1 Ack=13 Win=64256 Len=0 TSval=2616417074 TSecr=48778
2702 49.409176014  192.168.32.100     192.168.32.108     TCP        68 54294 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=2616417076 TSecr=48778
2703 49.432551447  192.168.32.100     192.168.32.108     HTTP      686 POST /sdk HTTP/1.1
2704 49.432578232  192.168.32.100     192.168.32.108     NBNS       94 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
2705 49.432585661  192.168.32.100     192.168.32.108     HTTP      224 OPTIONS / HTTP/1.1
2706 49.432593407  192.168.32.100     192.168.32.108     HTTP      244 GET /nmaplowercheck1668083053 HTTP/1.1
2707 49.432608262  192.168.32.100     192.168.32.108     NBNS       94 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
2708 49.432615257  192.168.32.100     192.168.32.108     HTTP      282 OPTIONS / HTTP/1.1
2709 49.432621600  192.168.32.100     192.168.32.108     HTTP       86 GET / HTTP/1.0
2710 49.432627447  192.168.32.100     192.168.32.108     UDP        45 58454 → 1434 Len=1
2711 49.432634075  192.168.32.100     192.168.32.108     HTTP      229 GET /.git/HEAD HTTP/1.1
2712 49.432640509  192.168.32.100     192.168.32.108     HTTP      224 OPTIONS / HTTP/1.1
2713 49.432647794  192.168.32.100     192.168.32.108     HTTP      235 PROPFIND / HTTP/1.1
2714 49.432810818  192.168.32.100     192.168.32.108     HTTP      235 PROPFIND / HTTP/1.1
2715 49.432835601  192.168.32.100     192.168.32.108     HTTP      230 GET /robots.txt HTTP/1.1
2716 49.432842611  192.168.32.100     192.168.32.108     HTTP      220 GET / HTTP/1.1
2717 49.432848121  192.168.32.100     192.168.32.108     HTTP      378 POST / HTTP/1.1  (application/x-www-form-urlencoded)
2723 49.432934570  192.168.32.108     192.168.32.100     ICMP       73 Destination unreachable (Port unreachable)
2733 49.433423009  192.168.32.100     192.168.32.108     TCP        68 36308 → 80 [ACK] Seq=619 Ack=472 Win=64128 Len=0 TSval=2616417100 TSecr=48780
2738 49.434302703  192.168.32.100     192.168.32.108     TCP        68 36322 → 80 [ACK] Seq=177 Ack=493 Win=64128 Len=0 TSval=2616417101 TSecr=48780
2741 49.447585814  192.168.32.100     192.168.32.108     TCP        68 36368 → 80 [ACK] Seq=157 Ack=1087 Win=64128 Len=0 TSval=2616417114 TSecr=48781
2743 49.448646457  192.168.32.100     192.168.32.108     TCP        68 36360 → 80 [ACK] Seq=19 Ack=1066 Win=64128 Len=0 TSval=2616417115 TSecr=48782
2745 49.448695938  192.168.32.100     192.168.32.108     TCP        68 36396 → 80 [ACK] Seq=215 Ack=1101 Win=64128 Len=0 TSval=2616417115 TSecr=48782
2748 49.449669190  192.168.32.100     192.168.32.108     TCP        68 36396 → 80 [ACK] Seq=215 Ack=1106 Win=64128 Len=0 TSval=2616417116 TSecr=48782
2750 49.473803752  192.168.32.100     192.168.32.108     FTP        74 Request: SYST
2751 49.473852196  192.168.32.100     192.168.32.108     FTP        84 Request: USER anonymous
2752 49.473920296  192.168.32.100     192.168.32.108     FTP        84 Request: USER anonymous
```

FONTE SCAN	TARGET SCAN	TIPO DELLO SCAN	RISULTATO
192.168.32.100	192.168.32.108	scansione TCP (-sT)	23 servizi attivi, 12 servizi su porte well-known
192.168.32.100	192.168.32.108	scansione SYN (-sS)	23 servizi attivi, 12 servizi su porte well-known
192.168.32.100	192.168.32.108	scansione -A	oltre ai servizi attivi, ci sono altre informazioni come per esempio lo status di alcuni server, le versioni dei protocolli, il sistema operativo usato dal target,ecc..