EPICODE

W9D1 - Pratica (2) PDF

Esercizio
Nmap scan

Traccia:

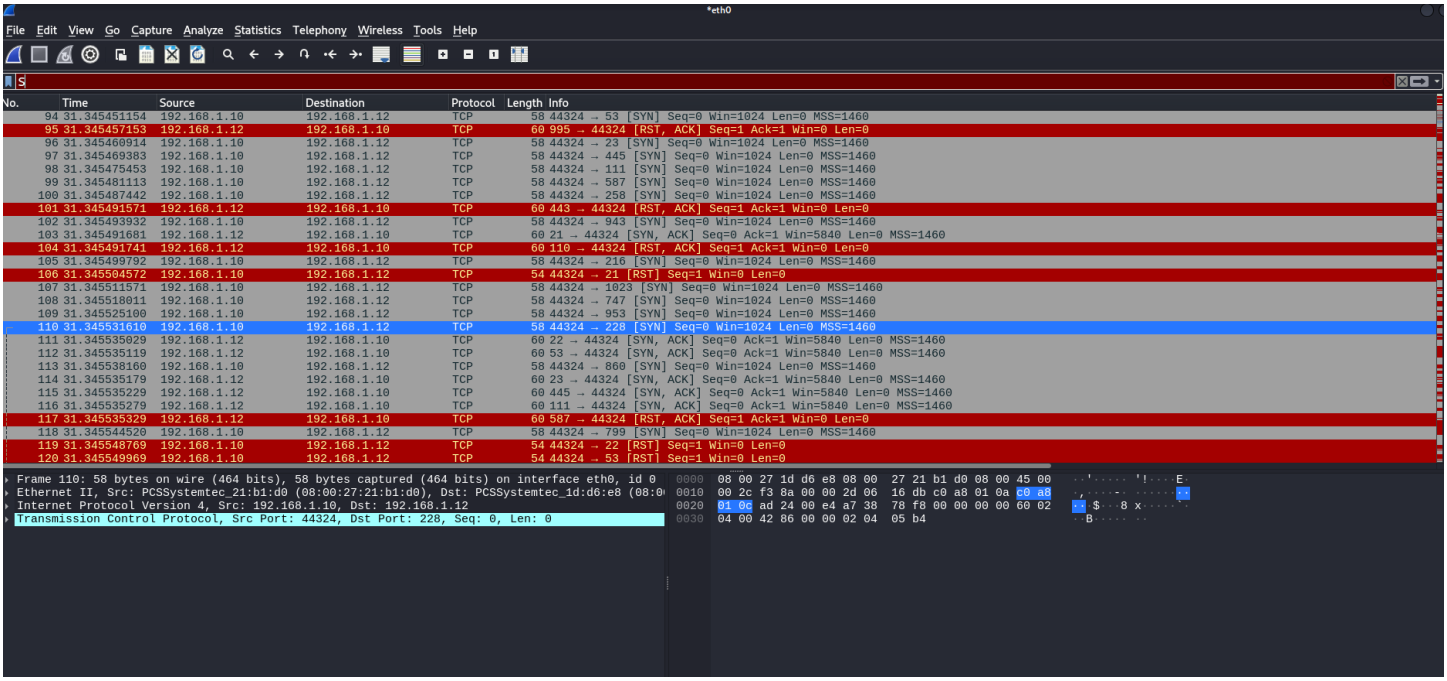
Vedremo da vicino nmap e i suoi comandi.
Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- 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 la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

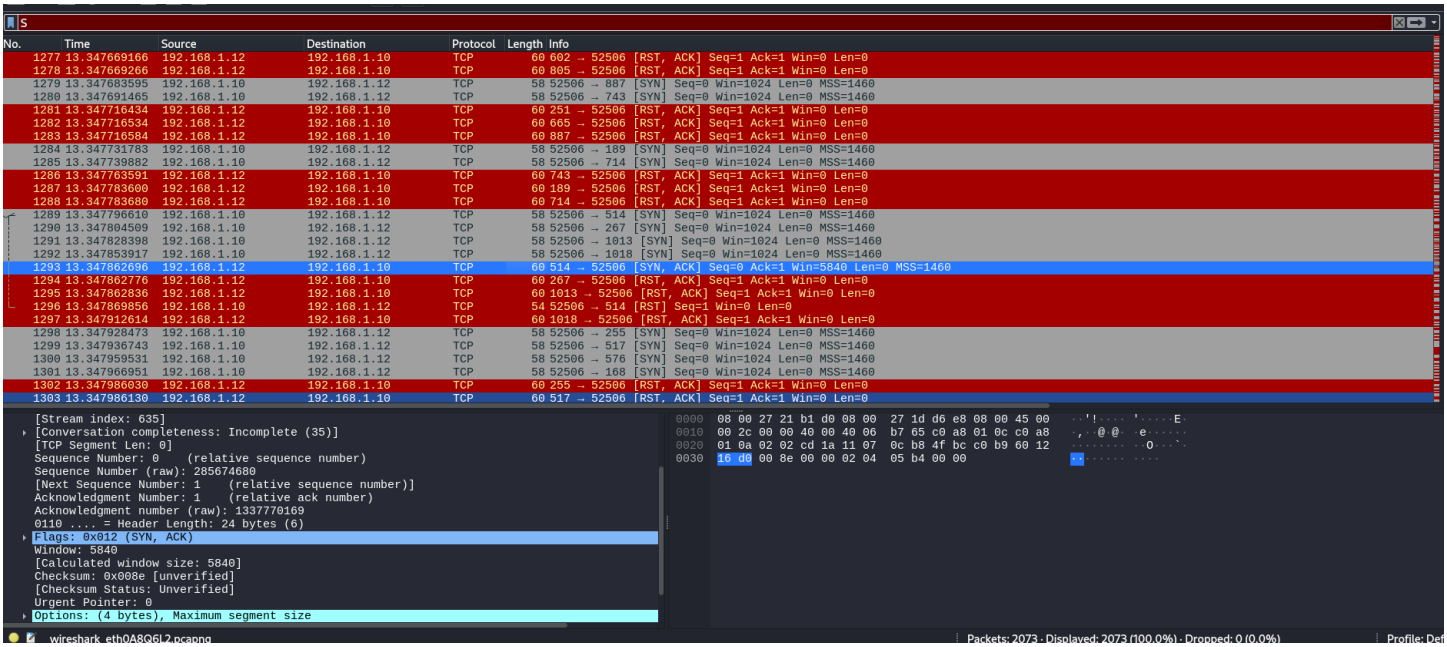
namp -p 1-1023 da Kali a Meta

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1-1023 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 16:51 EDT
Nmap scan report for PC192.168.1.12.homenet.telecomitalia.it (192.168.1.12)
Host is up (0.000074s latency).
Not shown: 1011 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
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```



namp -sS -p 1-1023 da Kali a Meta

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 0-1023 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 16:54 EDT
Nmap scan report for PC192.168.1.12.homenet.telecomitalia.it (192.168.1.12)
Host is up (0.000061s latency).
Not shown: 1012 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
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```



namp -A -p 1-1023 da Kali a Meta

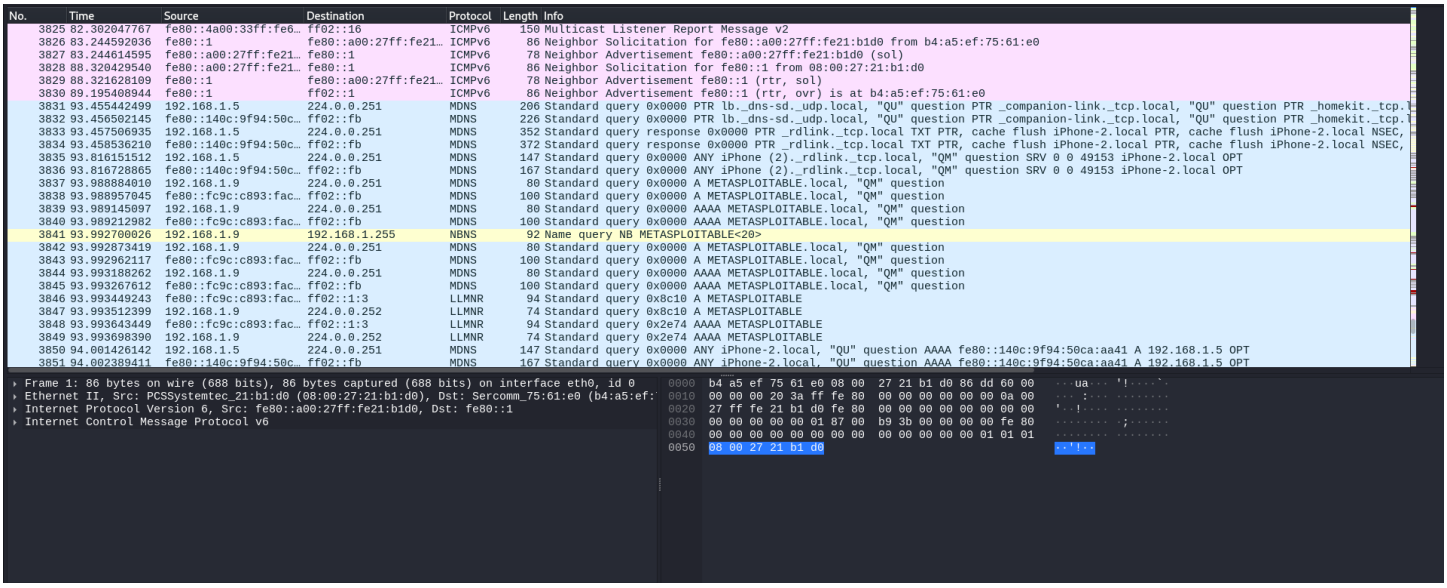
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -p 0-1023 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 16:57 EDT
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 16:58 (0:00:03 remaining)
Nmap scan report for PC192.168.1.12.homenet.telecomitalia.it (192.168.1.12)
Host is up (0.00011s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.10
|      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
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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| 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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-04-15T20:58:52+00:00; +1s from scanner time.
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
```

```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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      34734/tcp   mountd
|   100005  1,2,3      55541/udp   mountd
|   100021  1,3,4      36217/udp   nlockmgr
|   100021  1,3,4      55254/tcp   nlockmgr
|   100024  1          40847/udp   status
|_  100024  1          46397/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?
513/tcp open  login       OpenBSD or Solaris rlogind
514/tcp open  tcpwrapped
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; 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: 2024-04-15T16:58:44-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.11 ms PC192.168.1.12.homenet.telecomitalia.it (192.168.1.12)

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 74.55 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

No.	Time	Source	Destination	Protocol	Length	Info
3759	74.893351115	192.168.1.12	192.168.1.10	TCP	74	21 → 35212 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=524714 TSecr=3500774323 WS=64
3760	74.893360524	192.168.1.10	192.168.1.12	TCP	66	35212 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3500774323 TSecr=524714
3761	74.893394812	192.168.1.12	192.168.1.10	HTTP	71	HTTP/1.1 200 OK (text/html)
3762	74.893400092	192.168.1.10	192.168.1.12	TCP	66	36092 → 80 [ACK] Seq=66 Ack=1087 Win=64128 Len=0 TSval=3500774323 TSecr=524714
3763	74.893478418	192.168.1.10	192.168.1.12	TCP	66	36092 → 80 [RST, ACK] Seq=66 Ack=1087 Win=64128 Len=0 TSval=3500774323 TSecr=524714
3764	74.894100237	192.168.1.12	192.168.1.10	FTP	86	Response: 220 (vsFTPd 2.3.4)
3765	74.894107456	192.168.1.10	192.168.1.12	TCP	66	35212 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=3500774324 TSecr=524714
3766	74.894335575	192.168.1.10	192.168.1.12	TLSv1	197	Client Hello
3767	74.894349944	192.168.1.12	192.168.1.10	TLSv1	162	Client Hello
3768	74.894407821	192.168.1.10	192.168.1.12	TLSv1	388	Client Hello
3769	74.894511736	192.168.1.12	192.168.1.10	TLSv1	1032	Server Hello, Certificate, Server Hello Done
3770	74.894577093	192.168.1.12	192.168.1.10	TLSv1	1032	Server Hello, Certificate, Server Hello Done
3771	74.894664518	192.168.1.12	192.168.1.10	TLSv1	1032	Server Hello, Certificate, Server Hello Done
3772	74.895225360	192.168.1.10	192.168.1.12	FTP	158	Request: \026\003\001\000W\001\000\000S\003\003f\035[illegible]\005N;U\001[illegible]\U00036654zT[illegible]3S[illegible]\v[illegible]jc\016\032,\000\000
3773	74.895319075	192.168.1.12	192.168.1.10	TCP	66	21 → 35212 [ACK] Seq=21 Ack=93 Win=5824 Len=0 TSval=524714 TSecr=3500774325
3774	74.895319205	192.168.1.12	192.168.1.10	FTP	104	Response: 530 Please login with USER and PASS.
3775	74.895319265	192.168.1.12	192.168.1.10	FTP	104	Response: 530 Please login with USER and PASS.
3776	74.895682867	192.168.1.10	192.168.1.12	TCP	66	35196 → 21 [RST, ACK] Seq=518 Ack=135 Win=64256 Len=0 TSval=3500774325 TSecr=524714
3777	74.896471817	192.168.1.10	192.168.1.12	TCP	66	49462 → 25 [FIN, ACK] Seq=188 Ack=1201 Win=64128 Len=0 TSval=3500774326 TSecr=524714
3778	74.896645878	192.168.1.10	192.168.1.12	TCP	66	49484 → 25 [FIN, ACK] Seq=379 Ack=1201 Win=64128 Len=0 TSval=3500774326 TSecr=524714
3779	74.896691906	192.168.1.10	192.168.1.12	TCP	66	49468 → 25 [FIN, ACK] Seq=153 Ack=1201 Win=64128 Len=0 TSval=3500774326 TSecr=524714
3780	74.896706365	192.168.1.10	192.168.1.12	TCP	66	35212 → 21 [ACK] Seq=93 Ack=97 Win=64256 Len=0 TSval=3500774326 TSecr=524714
3781	74.896753973	192.168.1.10	192.168.1.12	TCP	66	25 → 49462 [FIN, ACK] Seq=1201 Ack=189 Win=6912 Len=0 TSval=524714 TSecr=3500774326
3782	74.896759953	192.168.1.10	192.168.1.12	TCP	66	49462 → 25 [ACK] Seq=189 Ack=1202 Win=64128 Len=0 TSval=3500774326 TSecr=524714
3783	74.897021669	192.168.1.10	192.168.1.12	TCP	66	25 → 49468 [FIN, ACK] Seq=1201 Ack=154 Win=5824 Len=0 TSval=524714 TSecr=3500774326
3784	74.897027729	192.168.1.10	192.168.1.12	TCP	66	49468 → 25 [ACK] Seq=154 Ack=1202 Win=64128 Len=0 TSval=3500774327 TSecr=524714
3785	74.897104075	192.168.1.10	192.168.1.12	TCP	66	25 → 49484 [FIN, ACK] Seq=1201 Ack=380 Win=6912 Len=0 TSval=524714 TSecr=3500774326
3786	74.897109435	192.168.1.10	192.168.1.12	TCP	66	49484 → 25 [ACK] Seq=380 Ack=1202 Win=64128 Len=0 TSval=3500774327 TSecr=524714
3787	74.897766212	192.168.1.10	192.168.1.12	TCP	66	35212 → 21 [FIN, ACK] Seq=93 Ack=97 Win=64256 Len=0 TSval=3500774327 TSecr=524714
3788	74.897889216	192.168.1.12	192.168.1.10	FTP	76	Response: 500 OOPS:
3789	74.897889326	192.168.1.12	192.168.1.10	FTP	96	Response: vsf_sysutil_recv_peek: no data
3790	74.897889366	192.168.1.12	192.168.1.10	FTP	68	Response:
3791	74.897901865	192.168.1.10	192.168.1.12	TCP	54	35212 → 21 [RST] Seq=94 Win=0 Len=0
3792	74.897909814	192.168.1.10	192.168.1.12	TCP	54	35212 → 21 [RST] Seq=94 Win=0 Len=0
3793	74.897914844	192.168.1.10	192.168.1.12	TCP	54	35212 → 21 [RST] Seq=94 Win=0 Len=0
3794	74.897966342	192.168.1.12	192.168.1.10	FTP	88	Response: 500 OOPS: child died

```
▸ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1:d0), Dst: Sercomm_75:61:e0 (b4:a5:ef:
▸ Internet Protocol Version 6, Src: fe80::a00:27ff:fe21:b1d0, Dst: fe80::1
▸ Internet Control Message Protocol v6
```

```
0000  b4 a5 ef 75 61 e0 08 00  27 21 b1 d0 86 dd 60 00   ···ua··· '!····`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 0a 00   ··· :··· ········
0020  27 ff fe 21 b1 d0 fe 80  00 00 00 00 00 00 00 00   '··!···· ········
0030  00 00 00 00 00 01 87 00  b9 3b 00 00 00 00 fe 80   ········ ·;······
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 01 01 01   ········ ········
0050  08 00 27 21 b1 d0                                 ··'!··
```



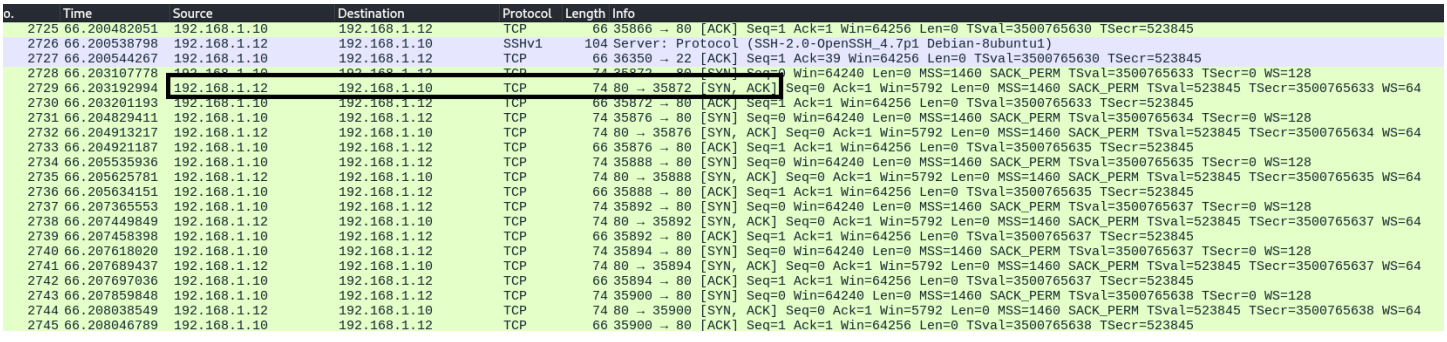
Scansion nmap -p, molto aggressiva e spam di Syn \ Ach

Scansione -sS -p più stealth perchè fa il Syn e non aspetta Ach. Se target risponde RST si suppone la porta sia chiusa, se risponde con Ach si presuppone sia aperta.

Traccia:

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.
E' molto importante in questa fase essere organizzati e strutturati.
Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 19:06 EDT
Nmap scan report for PC192.168.1.12.homenet.telecomitalia.it (192.168.1.12)
Host is up (0.000091s latency).
Not shown: 1011 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
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```