

La traccia di oggi ci chiedeva di prendere un po' di confidenza con i comandi di nmap nello specifico:

- Una scansione TCP sulle porte well-known, la quale verrà fatta con con il comando **sudo nmap -sS**. La quale è una scansione molto leggera che non include il 3-way-handshake, in quanto una volta ricevuto il pacchetto SYN/ACK chiude la comunicazione.

```
(root@kali)~[/home/kali]
# nmap 192.168.50.101 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.017s 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:D2:D6:E8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds
```

- Una scansione SYN sulle porte well-known, la quale verrà fatta con il comando **sudo nmap -sT**. Questa scansione è più aggressiva della precedente in quanto svolge tutti i passaggi del 3-way-handshake creando quindi un canale

```
(root@kali)~[/home/kali]
# nmap 192.168.50.101 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:42 EST
Nmap scan report for 192.168.50.101
Host is up (0.030s 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
MAC Address: 08:00:27:D2:D6:E8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.89 seconds
```

- Una scansione con “-A” sulle porte well-known, la quale verrà fatta con il comando **sudo nmap -A**, questa scansione è la più invadente delle tre questa però ci darà molte più informazioni rispetto alle precedenti due, a discapito di tempo e discrezione.

```
(root@kali)-[/home/kali]
# nmap 192.168.50.101 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.50.100
|_   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?
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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    rpcbind
```

2) Ora vediamo cosa abbiamo registrato con wireshark

- Questa è la prima scansione con -sS, come possiamo vedere in questo caso il client una volta appurato che la connessione si può interrompere la connessione senza creare un canale con il 3-handshake.

tcp.port == 21						
No.	Time	Source	Destination	Protocol	Length	Info
101	305.337015379	192.168.50.100	192.168.50.101	TCP	58	47215 → 21 [SYN] Seq=0 Win=0
121	305.341682356	192.168.50.101	192.168.50.100	TCP	60	21 → 47215 [SYN, ACK] Seq=0
125	305.342197720	192.168.50.100	192.168.50.101	TCP	54	47215 → 21 [RST] Seq=1 Win=0

Frame 101: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
 Ethernet II, Src: PcsCompu_59:c6:d1 (08:00:27:59:c6:d1), Dst: PcsCompu_d2:d6:e8 (08:00:27:d2:d6:e8)
 Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
 0000 08 00 27 d2 d6 e8 08 00 27 59 c6 d1 08 00 45 00 ..'.....'Y....E..

- Questa è invece la scansione con -sT, come si può vedere in questo caso il cliente crea un vero e proprio canale con il 3-handshake, inviando prima il segnale SYN , ricevendo poi dal server SYN,ACK, inviando a sua volta l'ACK e chiude la connessione.

tcp.port == 21

TCP port open

Time	Source	Destination	Protocol	Length	Info
33 13.181803005	192.168.50.100	192.168.50.101	TCP	74	35858 → 21 [SYN] Seq=0 Win=64240
53 13.205550096	192.168.50.101	192.168.50.100	TCP	74	21 → 35858 [SYN, ACK] Seq=0 Ack=
60 13.205868503	192.168.50.100	192.168.50.101	TCP	66	35858 → 21 [ACK] Seq=1 Ack=1 Win
83 13.210755999	192.168.50.100	192.168.50.101	TCP	66	35858 → 21 [RST, ACK] Seq=1 Ack=

0000

08 00 27 d2 d6 e8 08 00 27 59 c6 d1 08 00 45 00

.. ' ' Y E

Infine questa è la tabellazione come richiesto dalla traccia con la fonte dello scan, il ricevente dello scan, il tipo di scan e i servizi ottenuti.

INDIRIZZO SRC	INDIRIZZO DSC	SCAN	SERVIZI
192.168.50.100 (linux)	192.168.50.101 (meta)	Nmap -sT	23 - 12 (well Know)
192.168.50.100 (linux)	192.168.50.101 (meta)	Nmap -sS	23 - 12 (well Know)
192.168.50.100 (linux)	192.168.50.101 (meta)	Nmap -A	23 - 12 (well Know)