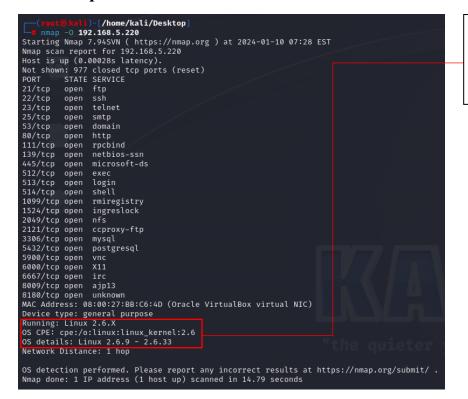
[CONSEGNA SETTIMANA 5 LEZIONE 3]

Identificazione dei servizi e scansione della rete

La seconda fase di un pentesting è definita come *scansione della rete*, durante la quale ci si avvale del software **nmap**, il quale permette di eseguire diversi tipologie di scansione sulla rete.

Come target oggi useremo la macchina metasploitable e il sistema operativo Windows 10.

IP Metasploitable: 192.168.5.220



Tipologia di scansione : -O
Risultato ottenuto : sistema operativo linux 2.6.x

```
Transport 192.168.5.220

Starting Mmap 7.95VN (https://mmap.org ) at 2024-01-10 07:35 EST
Nmap scan report for 192.168.5.220
Not shown: 977 Closed tep ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open smt opens ship opens ship of the post simple o
```

Tipologia di scansione : -sV

Risultato ottenuto : Versione dei servizi in ascolto

Possiamo notare come in entrambe le scansioni siano state elencate tutte le porte aperte e i relativi servizi associati. La differenza sostanziale tra le due scansione risiede nei risultati ottenuti. La prima scansione mirava all ottenere il sistema operativo della macchina, mentre

la seconda cercava nello specifico la versione dei servizi in ascolto. Possiamo notare inoltre che tra le porte aperte, molte sono a rischio di un potenziale attacco (ad esempio la porta 21 ftp o la porta 23 telnet).

```
inmap 7.94SVN (https://nmap.org) at 2024-01-10 07:31 EST
Numap scan report for 192.168.5.220
Host is up (0.000093s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
          open ftp
open ssh
 22/tcp
23/tcp
25/tcp
53/tcp
80/tcp
             open domain
open http
             open rpcbind
open netbios-ssn
 l11/tcp
l39/tcp
 45/tcp
12/tcp
             open login
open shell
 14/tcp
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
  121/tcp open
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open
 3009/tcp open ajp13
 3180/tcp open
 MAC Address: 08:00:27:BB:C6:4D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

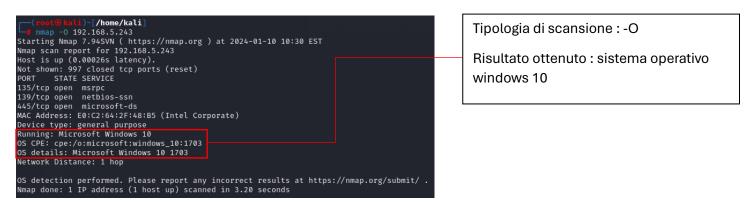
```
root@ kali)-[/home/kali/Desktop
nmap\-sT 192.168.5.220
Immap -sT 192.168.5.220
Starting Nmap 7.94SVN (https://nmap.org ) at 2024-01-10 07:33 EST Nmap scan report for 192.168.5.220
Host is up (0.00018s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp
23/tcp
               open ssh
open telnet
 53/tcp
               open
                          domain
                         http
rpcbind
80/tcp
111/tcp
               open
139/tcp
445/tcp
                         netbios-ssn
microsoft-ds
512/tcp
513/tcp
               open login
open shell
                          rmiregistry
1099/tcp open
1524/tcp open
2049/tcp open
                          ingreslock
2121/tcp open
3306/tcp open
                         mysql
5432/tcp open
5900/tcp open
                         postgresql
6000/tcp open
6667/tcp open
8009/tcp open ajp13
8180/tcp open unkno
MAC Address: 08:00:27:BB:C6:4D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Tra le varie tipologie di scansione possiamo trovare -sS, che esegue l'invio solo del pacchetto SYN, per poi terminare con un RESET, questa scansione risulta molto meno invasiva e quindi più difficile da notare.

Un altra scansione, ma che al contrario può risultare più invasiva è -sT che esegue il completo 3-way handshake (SYN - SYN/ACK – ACK), risultando più facile da notare.

Nel caso della scansione sulla macchina metasploitable si può notare che non vi è una differenza tra le due scansioni, se non per la latenza.

IP Windows 11: 192.168.5.243



Nel caso della scansione sulla macchina Windows 10, dopo aver temporaneamente disabilitato il firewall, possiamo notare che le porte aperte sono decisamente inferiori. Nel caso non avessi disabilitato il firewall, nmap avrebbe riportato che le porte non hanno dato alcuna risposta (*no-response*)