

Tecniche di scansione con Nmap su Metasploitable e Windows

Metasploitable:

La scansione Nmap **OS fingerprint**, inviando una serie di pacchetti TCP/IP all'host (Metasploitable) e confrontando le risposte con il suo database fingerprint os, appunto, ci riporta dettagli sul suo sistema operativo, le porte aperte e i servizi in ascolto su di esse.

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.20.20
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:33 EDT
Nmap scan report for 192.168.20.20
Host is up (0.0046s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds
```

La scansione Nmap **Syn Scan** ci riporta una scansione di tutte le porte aperte su un host.

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:40 EDT
Nmap scan report for 192.168.20.20
Host is up (0.0091s 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
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

La scansione Nmap **TCP Connect** ha la stessa funzionalità della SYN Scan. Non c'è molta differenza nell'uno e nell'altro, se non che nell'analisi del pacchetto.

La Syn Scan è una scansione più veloce e discreta, per cui spesso non viene registrata nei log del sistema target, host.

La TCP Connect è una scansione diretta che stabilisce una connessione completa con le porte dell'host, quindi più facilmente rilevabile nei log del sistema target.

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:41 EDT
Nmap scan report for 192.168.20.20
Host is up (0.022s 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

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

La scansione Nmap **Version Detection** ci fa una scansione delle porte, ma non si ferma alla connessione TCP. Ci dà anche la versione software, molto importante per capire la sua vulnerabilità.

Riesce a fare questo interrogando i Banner servizio per servizio e risalendo alla versione del servizio in esecuzione sull'host.

Fornisce una visione dettagliata dei servizi attivi, utile per valutazioni di sicurezza e pen testing. In sintesi, è uno strumento potente per il banner grabbing e la rilevazione delle

versioni dei servizi, automatizzando e migliorando il processo di identificazione rispetto ai metodi manuali. Utilizzare questa scansione ci consente di ottenere rapidamente una visione dettagliata dei servizi attivi su un host.

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:41 EDT
Nmap scan report for 192.168.20.20
Host is up (0.0088s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

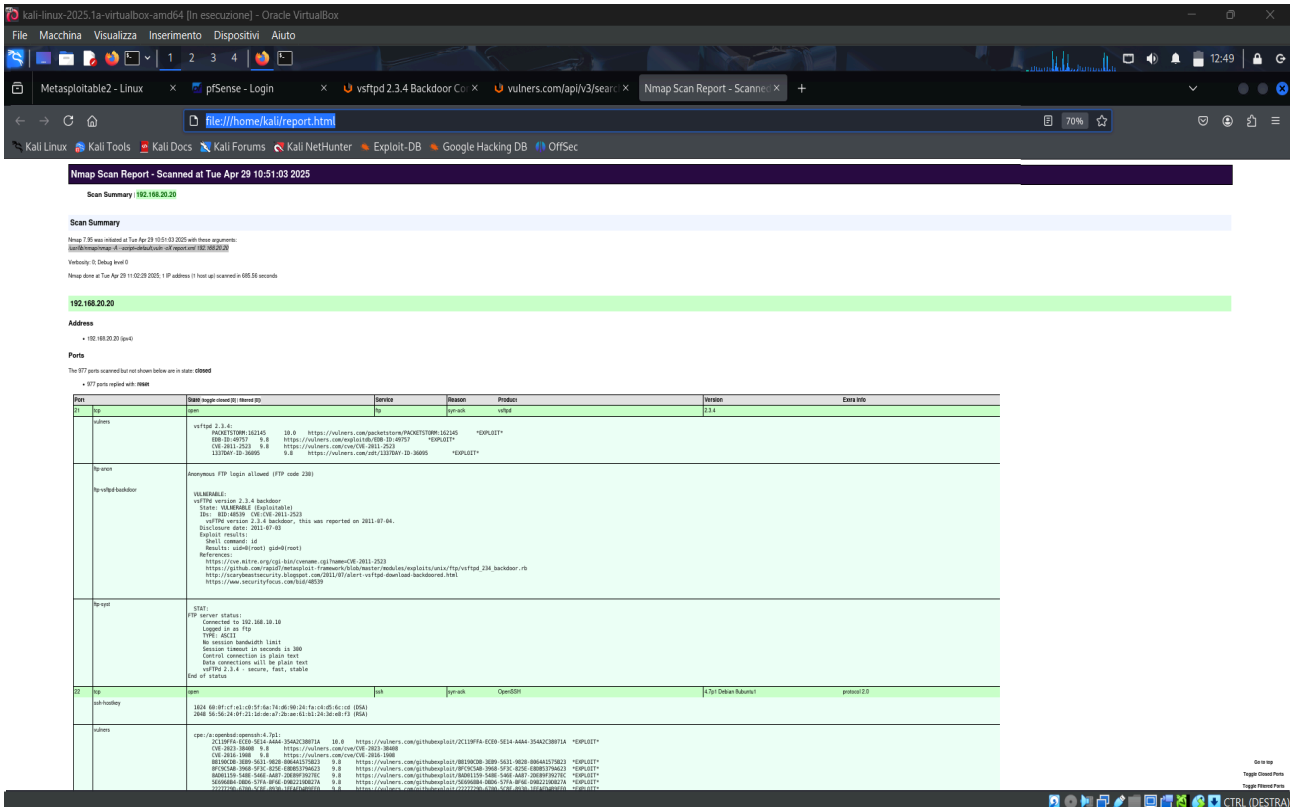
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.20 seconds
```

Eseguendo sul terminale della Kali il comando:

```
sudo nmap -A --script=default,vuln -oX report.xml 192.168.20.20
```

È possibile visualizzare un report delle scansioni effettuate, e convertire il file .xml in .html, sulla cartella della Kali, per leggerle in maniera ancora più chiara, eseguendo il comando:

```
xsltproc report.xml -o report.html
```



Windows:

```
(kali@kali)~$ sudo nmap -O 192.168.1.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:47 EDT
Nmap scan report for 192.168.1.154
Host is up (0.0033s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
5357/tcp  open  wsdapi
8443/tcp  open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.14 seconds
```

Eseguiamo stavolta la scansione Nmap OS Fingerprint sul target Windows.

Come detto prima, per la Metasploitable, esegue la sua solita scansione ma in questo caso non riesce ad identificare con precisione il sistema operativo, probabilmente a causa del Firewall di sistema attivo che modifica o blocca i pacchetti usati da Nmap per l'OS Fingerprint, a

differenza di Metasplitable.