

Report Scansioni con Nmap su Metasploitable e Windows

Scansione su Metasploitable

OS fingerprint:

L'OS fingerprint tramite nmap è una tecnica utilizzata per identificare il sistema operativo in esecuzione su un dispositivo remoto. Questa tecnica è utile per scopi di sicurezza, come l'individuazione di vulnerabilità. In questo caso, conoscendo l'indirizzo IP della metasploitable (192.168.1.20) siamo riusciti a risalire al suo sistema operativo da kali utilizzando il comando **nmap -O** (Linux 2.6.x tra la versione .9 e .33) vedi lo screenshot qui sotto:



```
(kali@kali)-[~]
$ nmap -O 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:50 EDT
Nmap scan report for 192.168.1.20 (192.168.1.20)
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
```

SYN Scan (Stealth Scan):

Lo SYN scan è una tecnica di scansione delle porte di rete che permette di determinare quali porte di un sistema sono aperte senza stabilire una connessione completa. In pratica, il client invia un pacchetto SYN al server, aspettandosi una risposta SYN-ACK (se la porta è aperta). A questo punto, invece di completare l'handshake TCP con un pacchetto ACK, invia un pacchetto RST (reset) per chiudere la connessione. Per questa scansione abbiamo utilizzato il comando **nmap -sS**. Andiamo a vedere nello screenshot qui sotto quali porta sono risultate aperte:

```
(kali㉿kali)-[~]
$ nmap -sS 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:51 EDT
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.000081s 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:FF:AC:20 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

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

TCP Connect Scan:

Il TCP Connect Scan è una tecnica di scansione delle porte che, a differenza dello SYN Scan, tenta di stabilire una connessione TCP completa con ogni porta target (quindi completa l'handshake SYN, SYN-ACK-, ACK senza chiudere la connessione in anticipo). Abbiamo utilizzato il comando **nmap -sT** per questa operazione. Come si può notare dagli screenshot non c'è nessuna differenza tra questa scansione e quella effettuata con il comando **nmap -sS** se non una leggera maggiore velocità di questa scansione con TCP Connect scan, fatto strano ma possibile quando si fanno queste operazioni su una singola macchina (Il SYN Scan dovrebbe essere più veloce e sprecare meno

risorse di rete in quanto fa un passaggio in meno). Qui sotto lo screen con il risultato della scansione:

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.1.20  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:52 EDT  
Nmap scan report for 192.168.1.20 (192.168.1.20)  
Host is up (0.000080s 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:FF:AC:20 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Version Detection:

La "Version Detection" in Nmap è una funzionalità che permette di identificare il servizio in esecuzione su una porta aperta e la sua versione. In pratica, Nmap non si limita a rilevare quali porte sono aperte (come per SYN Scan e TCP Connect Scan), ma cerca anche di capire quale applicazione o servizio le sta utilizzando e che versione ha. Per questa scansione abbiamo utilizzato il comando **nmap -sV**. Qui sotto ecco lo screenshot della scansione con le porte e il relativo servizio in ascolto su ogni porta trovata aperta:

```

(kali㉿kali)-[~]
$ nmap -sV 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:54 EDT
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.00043s 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  ftp          ProFTPD 1.3.1
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  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FF:AC:20 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 99.03 seconds

```

Scansione su Windows 10

OS fingerprint:

Per windows l'unico target richiesto è stato quello di risalire al sistema operativo tramite il comando **nmap -O** dalla macchina Kali. Avendo il suo indirizzo IP (192.168.1.38) siamo riusciti ad utilizzare il comando e risalire alla versione di Windows (Windows 10 tra la versione 1507 e 1607).

Nota bene: nmap-O sfrutta bug presenti in queste versioni e riesce a penetrare la macchina e risalire al sistema operativo attivo su essa, dà un range di versioni perché lo stesso bug è presente in tutte queste. Sotto lo screenshot dimostrativo:

```
(kali㉿kali)-[~]  
$ nmap -O 192.168.1.38  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 10:03 EDT  
Nmap scan report for 192.168.1.38 (192.168.1.38)  
Host is up (0.00013s latency).  
Not shown: 981 closed tcp ports (reset)  
PORT      STATE SERVICE  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
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  
3389/tcp  open  ms-wbt-server  
5357/tcp  open  wsapi  
5432/tcp  open  postgresql  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
8443/tcp  open  https-alt  
MAC Address: 08:00:27:8F:37:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 10  
OS CPE: cpe:/o:microsoft:windows_10  
OS details: Microsoft Windows 10 1507 - 1607  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
```