

# ESERCIZIO W9D2



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.



Esercizio  
Nmap scan

## 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)

- Utilizzo setxkbmap it per cambiare il layout della tastiera .
- Effetto la Scansione TCP con il comando " **sudo nmap -sS 192.168.1.62** "

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(kali@kali)-[~]
$ setxkbmap it
(kali@kali)-[~]
$ sudo nmap -sS 192.168.1.62
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-09 18:40 EST
Nmap scan report for 192.168.1.62
Host is up (0.00037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
MAC Address: 08:00:27:39:25:7D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : nexxt
    IPv6 Address. . . . . : 2001:b07:646a:6afd:e890:a9b5:50f2:90e3
    Temporary IPv6 Address. . . . . : 2001:b07:646a:6afd:e0cb:7d13:2a2c:72f9
    Link-local IPv6 Address . . . . . : fe80::e890:a9b5:50f2:90e3%11
    IPv4 Address. . . . . : 192.168.1.62
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c29f:51ff:fea9:5860%11
                                192.168.1.254

Tunnel adapter isatap.nexxt:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : nexxt

C:\Users\admin>
```

- Notiamo attraverso la cattura dei pacchetti con Wireshark che il TCP handshake non viene concluso , ma viene solamente inviato il pacchetto SYN , subito dopo aver ricevuto il pacchetto la macchina ci risponderà con un pacchetto RST che ci indica che la porta è chiusa .
- Se la porta fosse stata aperta ci avrebbe risposto con un pacchetto SYN , ACK.

No.	Time	Source	Destination	Protocol	Length	Info
10	7.886496156	192.168.1.254	192.168.1.60	DNS	85	Standard query response 0x3b41 No such name PTR 62
11	7.909599277	192.168.1.60	192.168.1.62	TCP	58	45031 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	7.909618872	192.168.1.60	192.168.1.62	TCP	58	45031 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	7.909625852	192.168.1.60	192.168.1.62	TCP	58	45031 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	7.909667162	192.168.1.60	192.168.1.62	TCP	58	45031 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	7.909675979	192.168.1.60	192.168.1.62	TCP	58	45031 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	7.909698033	192.168.1.60	192.168.1.62	TCP	58	45031 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	7.909704547	192.168.1.60	192.168.1.62	TCP	58	45031 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	7.909737321	192.168.1.60	192.168.1.62	TCP	58	45031 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	7.909743167	192.168.1.60	192.168.1.62	TCP	58	45031 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	7.909771643	192.168.1.60	192.168.1.62	TCP	58	45031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	7.909899414	PcsCompu_39:25:7d	Broadcast	ARP	60	Who has 192.168.1.60? Tell 192.168.1.62
22	7.909908309	PcsCompu_7c:01:a2	PcsCompu_39:25:7d	ARP	42	192.168.1.60 is at 08:00:27:7c:01:a2
23	7.909978735	192.168.1.62	192.168.1.60	TCP	60	445 → 45031 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
24	7.909992371	192.168.1.60	192.168.1.62	TCP	54	45031 → 445 [RST] Seq=1 Win=0 Len=0
25	7.913244882	192.168.1.60	192.168.1.62	TCP	58	45031 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	7.913254054	192.168.1.60	192.168.1.62	TCP	58	45031 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	7.913375918	192.168.1.62	192.168.1.60	TCP	60	135 → 45031 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
28	7.913382520	192.168.1.60	192.168.1.62	TCP	54	45031 → 135 [RST] Seq=1 Win=0 Len=0
29	7.916152910	192.168.1.60	192.168.1.62	TCP	58	45031 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	7.916163158	192.168.1.60	192.168.1.62	TCP	58	45031 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

- Utilizzando “-sT ” invece andremo a completare tutti e tre i passaggi tipici del 3 way handshake infatti notiamo la ricezione dei pacchetti ACK che non erano presenti con “-sS” .

No.	Time	Source	Destination	Protocol	Length	Info
1077	5.521370775	192.168.1.60	192.168.1.62	TCP	74	38726 → 3920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1078	5.521381851	192.168.1.60	192.168.1.62	TCP	74	36316 → 10024 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1079	5.521390305	192.168.1.60	192.168.1.62	TCP	74	47900 → 3690 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1080	5.521410636	192.168.1.60	192.168.1.62	TCP	74	33672 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1081	5.521419748	192.168.1.60	192.168.1.62	TCP	74	57510 → 1093 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1082	5.521429111	192.168.1.60	192.168.1.62	TCP	74	50310 → 12174 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1083	5.521463033	192.168.1.62	192.168.1.60	TCP	74	5357 → 54488 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
1084	5.521475594	192.168.1.60	192.168.1.62	TCP	66	54488 → 5357 [ACK] Seq=1 Ack=1 Win=64256 Len=0
1085	5.521513542	192.168.1.60	192.168.1.62	TCP	74	40234 → 9618 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1086	5.521526415	192.168.1.60	192.168.1.62	TCP	74	48004 → 2111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1087	5.521570605	192.168.1.60	192.168.1.62	TCP	66	54488 → 5357 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
1088	5.521608329	192.168.1.60	192.168.1.62	TCP	74	49674 → 3800 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1089	5.521635100	192.168.1.60	192.168.1.62	TCP	74	39736 → 9 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1090	5.623311009	192.168.1.60	192.168.1.62	TCP	74	39748 → 9 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

File Actions Edit View Help

(kali@kali)-[~]

\$ sudo nmap -sT 192.168.1.62

[sudo] password for kali:

Starting Nmap 7.94 ( https://nmap.org ) at 2024-0

Nmap scan report for 192.168.1.62

Host is up (0.00067s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

5357/tcp open wsddapi

MAC Address: 08:00:27:39:25:7D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds

- Utilizzando “ sudo nmap -A ” invece riceviamo più informazioni attraverso l’ip del target come sistema operativo , nome del computer , workgroup e system time .

```
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_  message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
|   2.1.0:  
|_    Message signing enabled but not required  
| smb-os-discovery:  
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)  
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional  
|   Computer name: admin-PC  
|   NetBIOS computer name: ADMIN-PC\x00  
|   Workgroup: WORKGROUP\x00  
|_  System time: 2024-02-09T15:59:05-08:00  
|_clock-skew: mean: 2h40m00s, deviation: 4h37m07s, median: 0s  
|_nbstat: NetBIOS name: ADMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:39:25:7d (Oracle VirtualBox virtual NIC)  
  
TRACEROUTE  
HOP RTT    ADDRESS  
1   0.41 ms 192.168.1.62  
  
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 58.27 seconds
```

- Come possiamo vedere abbiamo fatto lo scan su una macchina virtuale di Oracle Virtual Box il cui sistema operativo era Windows 7 Professional 6.1 .
- Abbiamo utilizzato i comandi “ nmap -sS ”, “ nmap -sT ” e “ nmap -A ” per ottenere più informazioni sull’ip di quest’ultimo che era : “ 192.168.1.62 ”.
- Abbiamo effettuato la cattura dei pacchetti per confrontare i diversi comandi che venivano utilizzati tramite Wireshark .