

# W11D2

SCANSIONE SERVIZI NMAP SU METASPLOITABLE

# La traccia

## Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- ❑ OS fingerprint
- ❑ Syn Scan
- ❑ TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- ❑ Version detection

# La traccia

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

<https://www.poftut.com/nmap-output/>

```
nmap -oN report1 IP
```

# Os Fingerprint

Per sapere il sistema operativo del target senza utilizzare il ping abbiamo usato il comando in figura. La differenza tra il primo e il secondo è che col primo non abbiamo avuto risultati, col secondo invece anche se più aggressivo e meno accurato nmap ci da dei possibili risultati.

```
(kali@kali)~$ sudo nmap -Pn -O --osscan-limit 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:38 EST
Nmap scan report for 192.168.100.4
Host is up (0.011s latency).
Not shown: 931 closed tcp ports (reset), 49 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
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  cproxy-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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN&E=4&D=1/17&OT=21&CT=1&CU=35476&PV=Y&DS=2&DC=I&G=Y&TM=65A8
OS:6517&P=x86_64-pc-linux-gnu)SEQ(SP=C7&GCD=1&ISR=C&TI=Z&II=I&TS=5)SEQ(SP=
OS:C7&GCD=1&ISR=C&TI=Z&II=I&TS=6)OPS(O1=M5B4ST11NW7&O2=M5B4ST11NW7&O3=M5B4
OS:NNT11NW7&O4=M5B4ST11NW7&O5=M5B4ST11NW7&O6=M5B4ST11)WIN(W1=16A0&W2=16A0&W
OS:3=16A0&W4=16A0&W5=16A0&W6=16A0)ECN(R=Y&DF=Y&T=4&QW=16D0&O=M5B4NNSNW7&CC=
OS:Y&Q=)T1(R=Y&DF=Y&T=4&QS=O&A=S+&F=AS&RD=O&Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y
OS:DF=Y&T=4&QW=O&S=Z&A=S+&F=AR&O=O&RD=O&Q=)T6(R=N)T7(R=N)U1(R=Y&DF=N&T=4&QI
OS:L=164&UN=O&RIPL=G&RID=G&RIPCK=G&RUCK=G&RUD=G)IE(R=Y&DFI=N&T=4&QCD=S)

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 26.83 seconds
```

```
(kali@kali)~$ sudo nmap -Pn -O --osscan-guess 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:39 EST
Nmap scan report for 192.168.100.4
Host is up (0.0055s latency).
Not shown: 931 closed tcp ports (reset), 49 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
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  cproxy-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
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.18 (9
4%), Kyocera CopyStar CS-2560 printer (93%), Linux 2.6.16 - 2.6.28 (92%), Linux 2.6.22 (92%), Linux 2.6.24 (92%),
Linux 2.4.21 (embedded) (92%), Linux 2.6.29 (Gentoo) (92%), Linux 2.6.9 (92%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN&E=4&D=1/17&OT=21&CT=1&CU=38207&PV=Y&DS=2&DC=I&G=Y&TM=65A8
OS:6553&P=x86_64-pc-linux-gnu)SEQ(SP=BE&GCD=2&ISR=D&TI=Z&II=I&TS=6)SEQ(SP=
OS:BF&GCD=1&ISR=D&TI=Z&II=I&TS=5)SEQ(SP=BF&GCD=1&ISR=D&TI=Z&II=I&TS=6)SEQ
OS:(SP=BF&GCD=1&ISR=D&TI=Z&II=I&TS=5)SEQ(SP=BF&GCD=1&ISR=D&TI=Z&II=I&TS=6
OS:)OPS(O1=M5B4ST11NW7&O2=M5B4ST11NW7&O3=M5B4NNT11NW7&O4=M5B4ST11NW7&O5=M5B
OS:4ST11NW7&O6=M5B4ST11)WIN(W1=16A0&W2=16A0&W3=16A0&W4=16A0&W5=16A0&W6=16A0
OS:)ECN(R=Y&DF=Y&T=4&QW=16D0&O=M5B4NNSNW7&CC=NXQ=)T1(R=Y&DF=Y&T=4&QS=O&A=S+
OS:Y&F=AS&RD=O&Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y&DF=Y&T=4&QW=O&S=Z&A=S+&F=AR&O=
OS:Y&RD=O&Q=)T6(R=N)T7(R=N)U1(R=Y&DF=N&T=4&QIPL=164&UN=O&RIPL=G&RID=G&RIPCK=
OS:G&RUCK=G&RUD=G)IE(R=Y&DFI=N&T=4&QCD=S)

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 26.91 seconds
```

# SYN e TCP Scan and version detection

Si può evincere dalle scansioni che non vi sono differenze in quanto dal TCP Scan, solitamente più invasivo, risultano gli stessi servizi attivi elencati nonostante dovrebbero esserne di più. In questo caso invece no. Avendo attivato l'opzione dei servizi(-sV) possiamo anche vedere le versioni dei servizi scansionati.

```
(kali@kali)-[~]
$ sudo nmap -sV -sS 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:48 EST
Nmap scan report for 192.168.100.4
Host is up (0.019s latency).
Not shown: 931 closed tcp ports (reset), 49 filtered tcp ports (no-response)
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?
25/tcp    open  smtp?
53/tcp    open  domain       ISC BIND 9.4.2
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
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?
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: Host: 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 195.16 seconds
```

```
(kali@kali)-[~]
$ sudo nmap -sV -sT 192.168.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 18:54 EST
Nmap scan report for 192.168.100.4
Host is up (0.018s latency).
Not shown: 931 closed tcp ports (conn-refused), 49 filtered tcp ports (no-response)
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?
25/tcp    open  smtp?
53/tcp    open  domain       ISC BIND 9.4.2
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
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?
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: Host: 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 194.93 seconds
```

# Scansione di meta su stessa rete di Kali

```
kali@kali: ~  
File Actions Edit View Help  
  
❏(kali@kali)-[~]  
$ nmap -sV 192.168.50.4 -oN reportIP  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 07:09 EST  
Nmap scan report for 192.168.50.4  
Host is up (0.031s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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?  
25/tcp    open  smtp?  
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?  
513/tcp   open  login?  
514/tcp   open  shell?  
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?  
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: Host: 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 194.02 seconds  
  
❏(kali@kali)-[~]  
$
```

In questo caso la scansione dei servizi viene innanzitutto salvata in un file. Facendo un confronto tra la scansione attuale e quella della stessa macchina ma su rete diversa notiamo che i servizi rilevati sono di più servizi nell'attuale scansione in quanto non stando sulla stessa rete il traffico non viene filtrato dal firewall (per esempio il firewall filtrava di pfsense filtrava il traffico sulla porta 80)