



TECNICHE DI SCANSIONE CON NMAP

REPORT A CURA DI MORGAN PETRELLI S5/L3

INDICE

ABOUT “NMAP”

-TARGET: METASPLOITABLE

- OS FINGERPRINT.
- SYN SCAN.
- TCP CONNECT
- VERSION DETECTION.

-TARGET: WINDOWS 7

- OS FINGERPRINT.

**NMAP È UN POTENTE STRUMENTO DI SCANSIONE
DI RETE PROGETTATO PER ESPLORARE, MAPPARE E
ANALIZZARE RETI INFORMATICHE.
UNO STRUMENTO ESSENZIALE PER GLI
AMMINISTRATORI DI RETE E GLI SPECIALISTI DI
SICUREZZA INFORMATICA PER COMPRENDERE LA
TOPOLOGIA DELLA RETE, INDIVIDUARE POTENZIALI
PROBLEMI DI SICUREZZA E GARANTIRE CHE I
DISPOSITIVI E I SERVIZI SIANO CONFIGURATI IN
MODO CORRETTO E SICURO.**



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ac:eb:8f
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feac:eb8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4752 (4.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:119 errors:0 dropped:0 overruns:0 frame:0
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25313 (24.7 KB)  TX bytes:25313 (24.7 KB)

msfadmin@metasploitable:~$
```

METASPLOITABLE IP:
192.168.50.101

OS FINGERPRINT

```
—$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:05 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00095s 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:AC:EB:8F (Oracle VirtualBox virtual NIC)
Device type: general purpose
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
```

eseguendo il comando `nmap -O (ip_target)`, Nmap invierà una serie di pacchetti al dispositivo Metasploitable e analizzerà le risposte per cercare di determinare il sistema operativo in esecuzione su quel dispositivo. Utilizzerà tecniche di analisi delle risposte dei pacchetti per confrontare i pattern di risposta con i profili noti dei diversi sistemi operativi. Questo processo è noto come fingerprinting del sistema operativo.

SYS SCAN

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 15:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00058s 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:AC:EB:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

eseguendo il comando `nmap -sS (ip_target)`, Nmap invierà pacchetti SYN alle porte sul dispositivo Metasploitable e analizzerà le risposte per determinare quali porte rispondono con un pacchetto SYN/ACK (indicando che la porta è aperta) e quali non rispondono (indicando che la porta è chiusa o filtrata).

TCP CONNECT

```
—$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 16:02 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0035s 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:AC:EB:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

eseguendo il comando `nmap -sT (ip_target)`, nmap stabilirà una connessione TCP completa con ciascuna porta sul dispositivo Metasploitable e analizzerà le risposte per determinare lo stato di ogni porta (aperta, chiusa o filtrata).

differenza tra syn scan e tcp connect:

la scansione TCP Connect completa la connessione TCP con il dispositivo target, mentre la scansione SYN invia solo pacchetti SYN per determinare lo stato delle porte. La scansione SYN è più veloce e discreta, ideale per la "ricognizione" preliminare della rete, mentre la scansione TCP Connect è più accurata ma meno furtiva e può essere soggetta a rilevamento.

VERSION DETECTION

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:08 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 13:08 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0023s 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 rshcd
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:AC:EB:8F (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 66.30 seconds
```

eseguendo il comando `nmap -sV (ip_target)`, nmap invierà richieste specifiche ai servizi in esecuzione su Metasploitable per ottenere informazioni sulle versioni dei servizi. Le risposte ricevute da questi servizi aiuteranno Nmap a identificare le versioni esatte dei servizi, come ad esempio i server web, i server FTP, i server SSH e altri servizi che sono in ascolto sulle porte aperte di Metasploitable.

Informazioni preziose perché consentono agli amministratori di rete e agli esperti di sicurezza informatica di comprendere meglio le configurazioni dei servizi e di valutare le potenziali vulnerabilità specifiche per versione

Windows 7 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Prompt dei comandi

```
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\morgan>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::a9dc:8ac9:1331:c3f0%11
    Indirizzo IPv4. . . . . : 192.168.50.102
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1

Scheda Tunnel isatap.{97AE9864-9B01-4401-AC0F-F69AFF5CF97F}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\morgan>
```

WINDOWS7 IP:
192.168.50.102

OS FINGERPRINT

```
~$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:14 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D2:D5:19 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 37.64 seconds
```

Come possiamo vedere il risultato ottenuto è diverso rispetto a quello di meta, la possibile causa è che il firewall su Windows 7 potrebbe bloccare le richieste di scansione inviate da Nmap, influenzando la capacità di rilevare il sistema operativo e le porte aperte.

per provare a bypassare il firewall si potrebbe usare una scansione syn poichè Questa tecnica di scansione invia solo pacchetti SYN (parte del processo di handshake TCP) ai numeri di porta specificati sul dispositivo target. Essendo una scansione meno invasiva, può cercare di evitare la rilevazione del firewall poiché non completa la connessione TCP.

si potrebbe aggiungere anche -T Questo parametro può essere utile per controllare la velocità della scansione e ridurre il rischio di rilevazione o di sovraccarico della rete o del dispositivo target.