



MATTIA PASTORELLI

SCANSIONE DEI SERVIZI CON **NMAP**

1

> COMANDA:

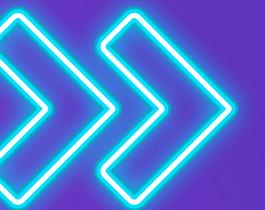
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection. E la seguente sul target Windows 7
- OS fingerprint.



COS'È NMAP?

Nmap, acronimo di "Network Mapper", è uno strumento di scansione di rete open source utilizzato per esaminare e mappare dispositivi su una rete, rilevando porte aperte, servizi in esecuzione, e altre informazioni rilevanti sulla sicurezza



The screenshot shows the official Nmap website at nmap.org. The header features the Nmap logo (an eye icon) and navigation links for Npcap.com, Seclists.org, Sectools.org, and Insecure.org. Below the header is a search bar and a menu bar with links for Download, Reference Guide, Book, Docs, Zenmap GUI, and In the Movies. A prominent button says "Get Nmap 7.94 here". The main content area is titled "News" and lists several bullet points about recent releases and developments, such as the redesign of the site, the release of Nmap 7.90, and the announcement of Npcap version 1.00. Other news items include DEFCON 27, the 20th anniversary of Nmap, the release of Nmap 7.50, and the release of Nmap 7. It also mentions the "Icons of the Web" project and its appearance in movies like Elysium and G.I. Joe: Retaliation. The news section concludes with details about Nmap 6.01, the relaunch of SecTools.Org, the release of Nmap 5.50, and the presentation video for Defcon.

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [Insecure.org](#), and [Sectools.org](#).
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [[Release Announcement](#) | [Download page](#)]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [[Release Announcement](#) | [Download page](#)]
- Nmap 7.80 was released for DEFCON 27! [[release notes](#) | [download](#)]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article](#). #Nmap20!
- Nmap 7.50 is now available! [[release notes](#) | [download](#)]
- Nmap 7 is now available! [[release notes](#) | [download](#)]
- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation](#)!
- We're delighted to announce Nmap 6.40 with 14 new [NSE scripts](#), hundreds of new [OS](#) and [version detection](#) signatures, and many great new features! [[Announcement/Details](#)], [[Download Site](#)]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [[Announcement/Details](#)], [[Download Site](#)]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01](#)!
- Nmap 6 is now available! [[release notes](#) | [download](#)]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- [Nmap 5.50 Released](#): Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [[Download page](#) | [Release notes](#)]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam—all in 38 minutes! ([Presentation video](#))
- [Icons of the Web](#): explore favicons for the top million web sites with our [new poster](#) and [online viewer](#).
- We're delighted to announce the immediate, free availability of the [Nmap Security Scanner version 5.00](#). Don't miss the [top 5 improvements in Nmap 5](#).
- After years of effort, we are delighted to release [Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning](#)!
- We now have an active Nmap [Facebook page](#) and [Twitter feed](#) to augment the [mailing lists](#). All of these options offer RSS feeds as well.

Nmap: Discover your network



OS FINGER PRINT

Un OS fingerprint, o "fingerprinting" dell'OS, si riferisce al processo di identificazione del sistema operativo in esecuzione su un determinato host in una rete.

In figura possiamo vedere il comando nmap (ip) --script smb-os-discovery, il quale effettua uno script dell'ip al fine di individuare le porte presenti sulla rete e l'OS dell'Host analizzato (in questo caso Metasploitable)



```
(root㉿kali)-[~/home/kali]
└─# nmap 192.168.50.100 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:46 EST
Nmap scan report for 192.168.50.100
Host is up (0.012s 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: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)

Host script results:
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2024-01-10T09:42:34-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.77 seconds
```

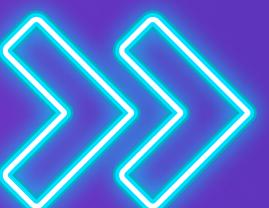
➤SYN SCAN

Lo "SYN SCAN" è una tecnica di scansione di porte attraverso l'invio di un solo pacchetto, il quale non comporta il completamento della 3 way - handshake (mancano SYN/ACK e ACK).

Viene utilizzato principalmente per analizzare le porte disponibili e aperte su un determinato indirizzo IP

Questo scan è meno intrusivo rispetto ad una scansione completa, di conseguenza è più rapida e fa "meno rumore"

Comando : nmap -sS (IP destinatario META)



```
└─(root㉿kali)-[~/home/kali]
# nmap -sS 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:45 EST
Nmap scan report for 192.168.50.100
Host is up (0.0017s 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: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

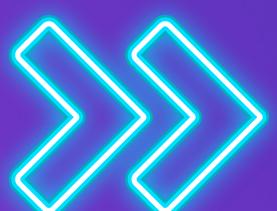


➤TCP CONNECT

Il TCP CONNECT è sempre una scansione di porte utilizzata per verificare l'apertura o la chiusura di porte su un host, ma a differenza della SYN SCAN, questa completa la 3 way - handshake

Questa scansione è più completa ed utile se stiamo effettuando un controllo di rete o un PT, per quanto riguarda un attaccante questa è una soluzione poco adottata perché genera parecchio "rumore".

Comando: nmap -sT (IP destinatario META)



```
(root㉿kali)-[~/home/kali]
# nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:58 EST
Nmap scan report for 192.168.50.100
Host is up (0.0031s 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: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

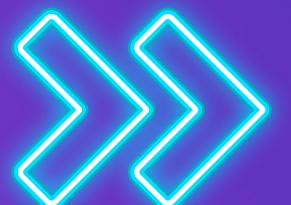
➤ VERSION DETECTION

La VERSION DETECTION o anche detto "Banner Grabbing", consiste nel recupero delle informazioni esposte da un determinato software o demone di un servizio (Es: Versione e nome del software/servizio)

Può essere utilizzato per verificare eventuali vulnerabilità su alcuni servizi.

Comando: nmap -sV (IP destinatario META)

```
Multipath: 1/2
└─(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 09:19 EST
Nmap scan report for 192.168.50.100
Host is up (0.00051s 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?
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
6000/tcp  open  X11             (access denied)
6667/tcp  open  irc              UnrealIRCd
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
MAC Address: 08:00:27:7B:7F:8E (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



OS FINGER PRINT

WINDOWS 7

Questa volta è stato effettuato L'OS fingerprinting sulla macchina di Windows 7 al fine di scoprire la versione dell'OS.

E' stato possibile disattivando il Firewall di Windows. Altrimenti non ci sarebbe stato nessun riscontro e nessun risultato.

Possiamo notare che a differenza di Metasploit, windows non mostra tutte le porte (ES. 21,22 ecc..), questo può essere successo per diversi motivi:

- 1) Diversità di sistema operativo
- 2) Il firewall di windows blocca determinati accessi, bisogna inserire una regola all'interno che lasci passare il segnale da Kali verso windows. Quindi Problemi di Autorizzazione e Sicurezza per firewall e scansione porte

```
└─(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:53 EST
Nmap scan report for 192.168.50.102
Host is up (0.00097s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:DA:A2:FD (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
| OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: win7
| NetBIOS computer name: WIN7\x00
| Workgroup: WORKGROUP\x00
| System time: 2024-01-10T14:53:15+01:00
```