

Traccia: Tecniche di scansione con NAP

Obiettivo: Fare delle scansioni sulla Metaspotable e su Windows cercando di trovare IP, Sistema Operativo, Porte Aperte e Servizi in ascolto

Metaspotable IP 192.168.64.3

1. Sulla Metaspotable ho iniziato facendo uno Scan OS fingerprint usando il comando “map -O 192.168.64.4 dove ho potuto verificare che il sistema operativo ed alcune porte aperte, pero per avere una visione più completa ed evitare di fare più comandi ho deciso di fare “sudo nmap -A 192.168.64.3”

“nmap -A 192.168.64.3” questo comando serve a fare 4 comandi assieme ovvero:

- sV.** Identifica la versione dei servizi in esecuzione su porte aperte
- O.** Tenta di determinare il sistema operativo della macchina
- traceroute.** Traccia il percorso dei pacchetti fino al target
- script=default.** Esegue una serie di script di base (come banner grabbing, SSL check)

Eseguendo questo comando ho potuto verificare che:

IP = 192.168.64.3
Sistema Operativo = Linux karnel 2.6.x
Distribuzione = Debian
Hostname = Metaspotable.localdomain
Computer name = Metaspotable

Porte aperte e servizi attivi (Alcuni dei servizi e delle porte attive):

5900	TCP	VNC (3.3)	Accesso remoto con autenticazione VNC
6000	TCP	X11	Accesso negato, ma il servizio è visibile
6667	TCP	IRC	Server IRC attivo
8009	TCP	AJP13	Apache JServ Protocol v1.3
8180	TCP	HTTP	Apache Tomcat/Coyote JSP Engine 1.1

```
(kali@kali)-[~]
$ sudo nmap -A 192.168.64.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 14:51 BST
Nmap scan report for 192.168.64.3
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.64.2
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2025-07-04T10:59:59+00:00; -25d02h52m03s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_  program version  port/proto  service
|_  100003  2,3,4        2049/tcp    nfs
|_  100003  2,3,4        2049/udp    nfs
|_  100005  1,2,3        43594/udp   mountd
|_  100005  1,2,3        53003/tcp   mountd
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
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
|_mysql-info:
|_  Protocol: 10
|_  Version: 5.0.51a-3ubuntu5
|_  Thread ID: 19
|_  Capabilities flags: 43564
|_  Some Capabilities: SupportsTransactions, ConnectWithDatabase, SupportsCompression, Support41Auth, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake
|_  Status: Autocommit
|_  Salt: L*;%ElojGa6`0kKu,y
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-07-04T10:59:59+00:00; -25d02h52m03s from scanner time.
5900/tcp  open  vnc          VNC (protocol 3.3)
|_vnc-info:
|_  Protocol version: 3.3
|_  Security types:
```

```
|_ VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc            UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 3 days, 14:34:14
|   source ident: nmap
|   source host: 96318E76.55261F4C.FFFA6D49.IP
|_ error: Closing Link: autxjvkjd[192.168.64.2] (Quit: autxjvkjd)
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http            Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: AA:E4:EE:0C:F2:18 (Unknown)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -25d01h52m02s, deviation: 2h00m00s, median: -25d02h52m03s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable

|_ Computer name: metasploitable
|_ NetBIOS computer name:
|_ Domain name: localdomain
|_ FQDN: metasploitable.localdomain
|_ System time: 2025-07-04T06:59:50-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   0.70 ms 192.168.64.3

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 23.51 seconds
```

Windows IP 192.168.64.4

1. Sul Windows ho iniziato facendo direttamente il comando “nmap -A 192.168.64.4” ottenendo così molti dati utili come:

IP = 192.168.64.4

Sistema Operativo = Windows 10 Pro 10240

Hostname = Desktop-9k104BT

Computer name = Desktop-9k104BT

Porte aperte e servizi attivi:

```
PORT      STATE SERVICE          VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime         Microsoft Windows International daytime
17/tcp   open  qotd            Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http            Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
|_http-methods:
|_ Potentially risky methods: TRACE
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc           Microsoft Windows RPC
2105/tcp  open  msrpc           Microsoft Windows RPC
2107/tcp  open  msrpc           Microsoft Windows RPC
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
|_ssl-date: 2025-07-29T13:04:01+00:00; -2s from scanner time.
|_ssl-cert: Subject: commonName=DESKTOP-9K104BT
|_ Not valid before: 2025-04-22T21:26:00
|_ Not valid after: 2025-10-22T21:26:00
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5432/tcp  open  postgresql?
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.81
|_http-open-proxy: Proxy might be redirecting requests
8443/tcp  open  ssl/https-alt
|_ssl-cert: Subject: commonName=DESKTOP-9K104BT
|_ Not valid before: 2024-07-09T16:53:31
|_ Not valid after: 2029-07-09T16:53:31
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

Extra: Se volessi vedere tutti i dati ricavati in maniera ordinata e facile da leggere anche in futuro mi basterebbe inserire “nmap -A ipx.x.x.x -oX nomeFile.xml”.

```
(kali@kali)-[~]
└─$ nmap -A 192.168.64.3 -oX scansioneMeta.xml
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 16:33 BST
Verboesity: 0, Debug level 0
```

Dopo di che trasformo questo file in un file .html con il comando
xsltproc nomeFile.xml -o nomeFile.html

```
(kali@kali)-[~]
└─$ xsltproc scansioneMeta.xml -o scansioneMeta.html
```

Risultato:

Nmap Scan Report - Scanned at Tue Jul 29 16:33:23 2025

Scan Summary | 192.168.64.3

Scan Summary

Nmap 7.95 was initiated at Tue Jul 29 16:33:23 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -A -oX scansioneMeta.xml 192.168.64.3
Verboesity: 0; Debug level 0
Nmap done at Tue Jul 29 16:33:48 2025; 1 IP address (1 host up) scanned in 24.63 seconds

192.168.64.3

Address

- 192.168.64.3 (ipv4)
- AA:E4:EE:0C:F2:18 (mac)

Ports

The 977 ports scanned but not shown below are in state: closed

- 977 ports replied with: reset

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra Info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4
	ftp-anon	Anonymous FTP login allowed (FTP code 230)				
	ftp-syst	STAT: FTP server status: Connected to 192.168.64.2 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300				

Go to top

Toggle Closed Ports

Toggle Filtered Ports

Test fatti: Per quello che riguarda Windows ho provato inizialmente ad fare i comandi singoli come “nmap -O 192.168.64.4” pero il segnale veniva bloccato.

```
(kali㉿kali)-[~]  
$ nmap -O 192.168.64.4  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 13:51 BST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 1.66 seconds
```

Per superare questo ostacolo cerano vari comandi (es: - Pn ip) però per avere tutte le informazioni che desideravo ho usato direttamente il comando “nmap -A ip”

Conclusione: “nmap -A ip” mi ha permesso in entrambi i casi di avere tutte le informazioni che desideravo senza problemi, fornendomi una panoramica dettagliata delle macchine target, combinando rilevamento dei servizi, identificazione delle versioni, analisi del sistema operativo, traceroute e lancio di script NSE predefiniti.

Grazie a queste informazioni, è possibile ottenere un profilo preciso della superficie d’attacco della macchina analizzata.

Con queste informazioni puoi:

1. Ricercare vulnerabilità note
2. Eseguire attacchi mirati
3. Verificare la sicurezza della configurazione
4. Automatizzare con script NSE avanzati