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, SwitchToSSLAfterH
andshake
|   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:
```

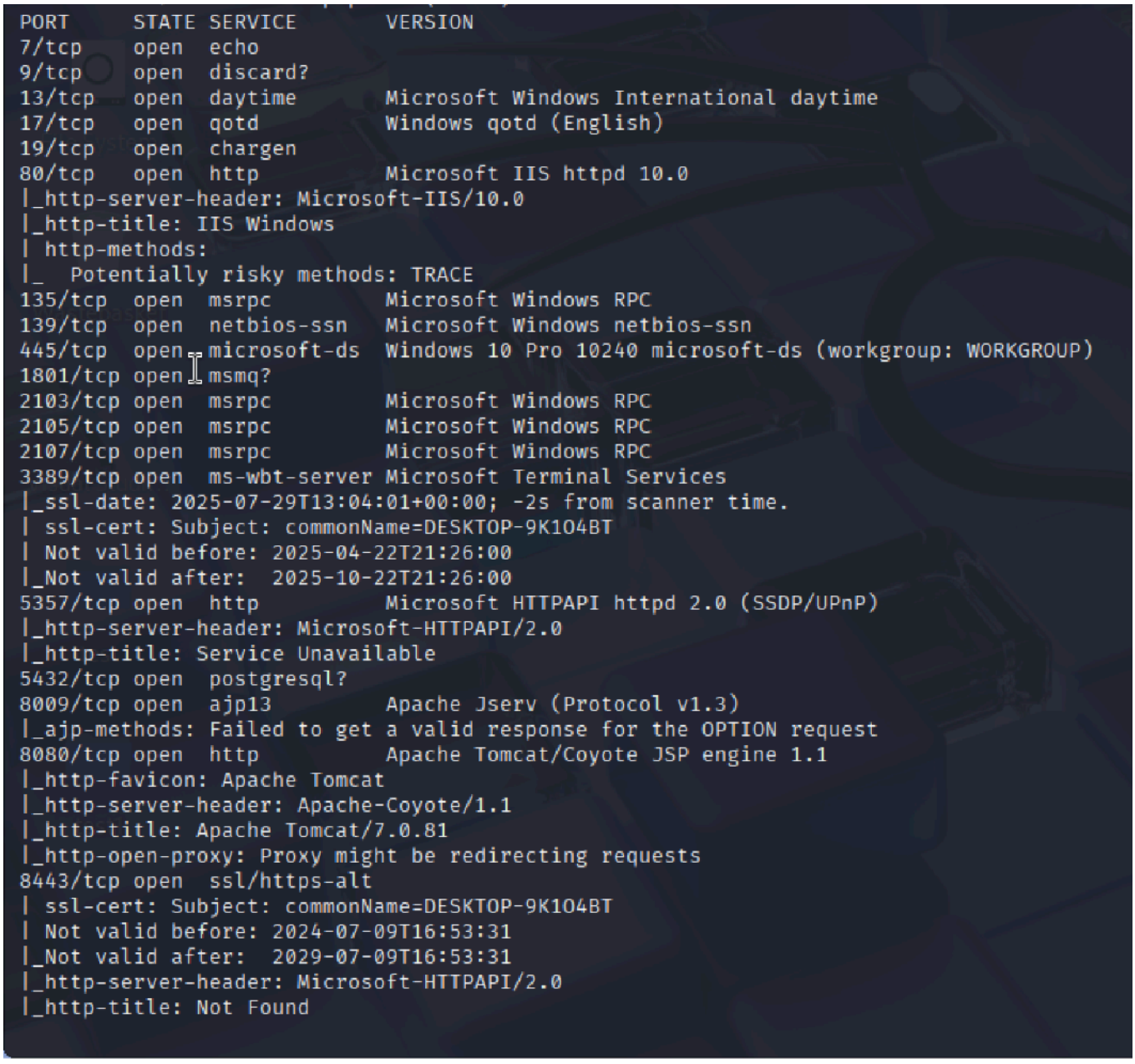
```
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 3 days, 14:34:14
|   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
|   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 cosi 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:



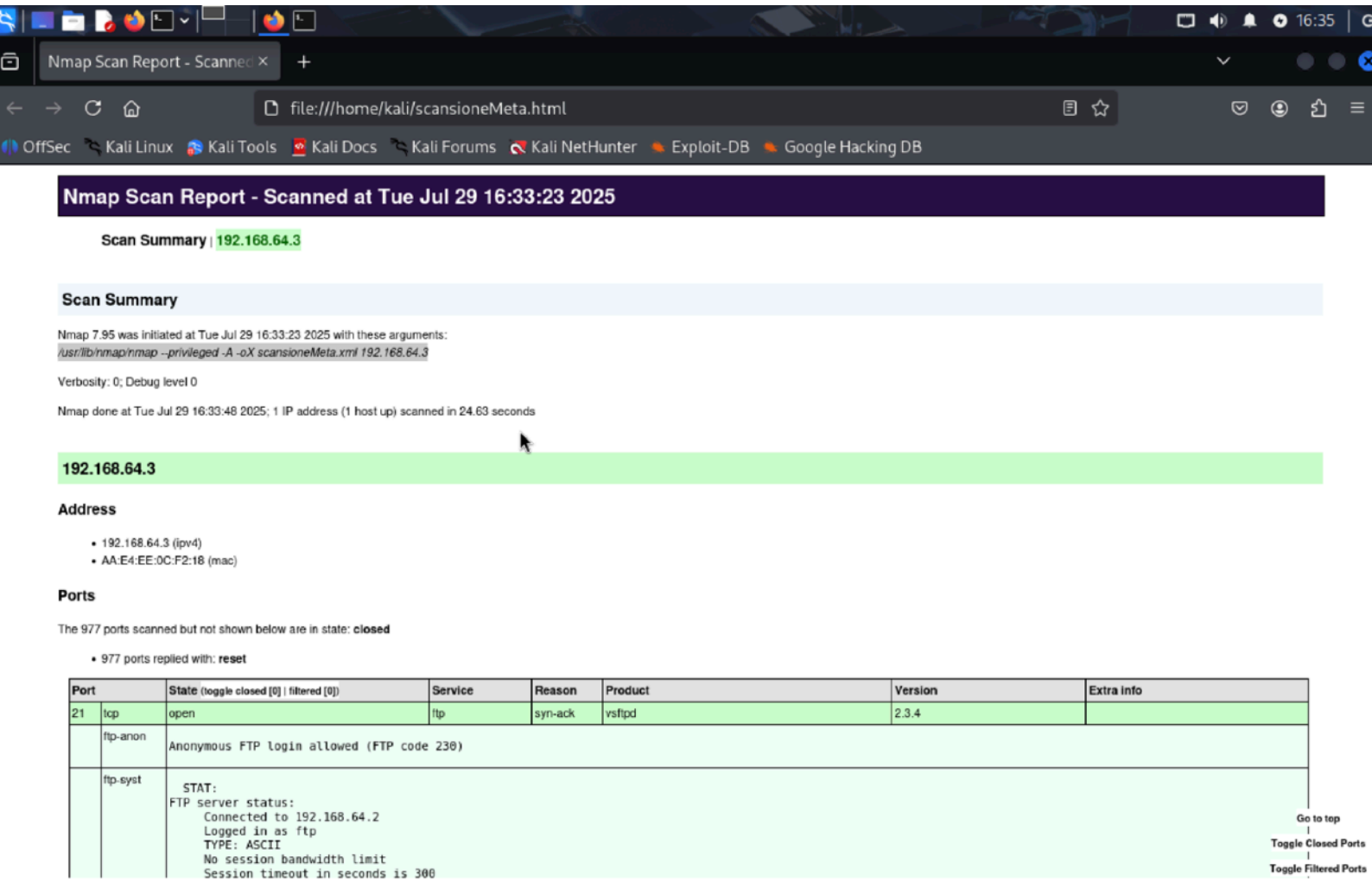
Extra: Se volessi vedere tutti i dati ricavati in maniera ordinata e facile da leggere anche in futuro mi basterebbe inserire “nmap -A ipx.x.x.x -oX nomeFile.xml.

```
┌──(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
```

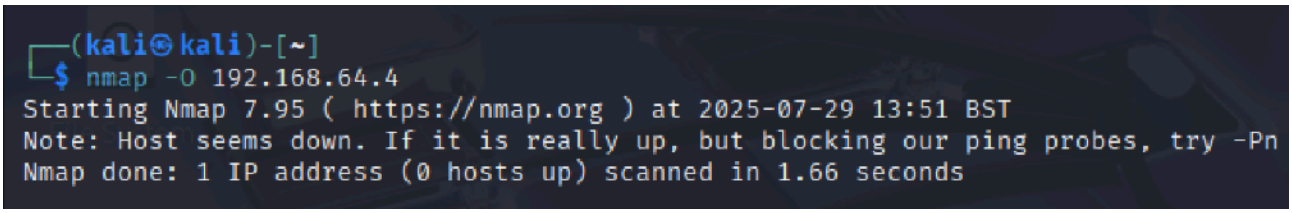
Dopo di che trasformo questo file in un file .html con il comando
xsltproc nomeFile.xml -o nomeFile.html

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

Risultato:



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.



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