

## M3\_W9D3

Scansione dei Servizi di Rete attivi tramite il tool **Nmap** di Kali Linux su macchina Metasploitable (192.168.50.101).

Prima scansione completa delle porte incluse nel range 1-1024 con la flag **-sT**.

The image shows two windows from a Kali Linux system. The top window is a terminal running Nmap. The bottom window is Wireshark showing a network capture of the scan.

**Terminal Output:**

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nmap -sT 192.168.50.101 -p 1-1024  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 18:48 GMT  
Nmap scan report for 192.168.50.101  
Host is up (0.0013s latency).  
Not shown: 1012 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  
  
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

**Wireshark Capture:**

Capturing from eth0

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1883	2.709450899	192.168.50.101	192.168.50.100	TCP	54	308 → 36032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1884	2.709453566	192.168.50.100	192.168.50.101	TCP	74	58522 → 678 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1885	2.709463066	192.168.50.100	192.168.50.101	TCP	74	33496 → 234 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1886	2.709466733	192.168.50.100	192.168.50.101	TCP	74	60316 → 978 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1887	2.709469858	192.168.50.100	192.168.50.101	TCP	74	51290 → 249 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1888	2.709473442	192.168.50.100	192.168.50.101	TCP	74	42336 → 732 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1889	2.709478609	192.168.50.100	192.168.50.101	TCP	74	57948 → 163 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1890	2.709482443	192.168.50.100	192.168.50.101	TCP	74	46542 → 985 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1891	2.709485943	192.168.50.100	192.168.50.101	TCP	74	56130 → 1016 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1892	2.709486109	192.168.50.101	192.168.50.100	TCP	54	500 → 56872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1893	2.709489401	192.168.50.100	192.168.50.101	TCP	74	48604 → 583 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1894	2.709492901	192.168.50.100	192.168.50.101	TCP	74	43044 → 327 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1895	2.709496360	192.168.50.100	192.168.50.101	TCP	74	57568 → 270 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1896	2.709499777	192.168.50.100	192.168.50.101	TCP	74	46564 → 231 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1897	2.709503152	192.168.50.100	192.168.50.101	TCP	74	46828 → 776 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1898	2.709506444	192.168.50.100	192.168.50.101	TCP	74	36090 → 916 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
1899	2.709506944	192.168.50.101	192.168.50.100	TCP	54	519 → 47154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1900	2.709506986	192.168.50.101	192.168.50.100	TCP	54	321 → 60144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1901	2.709509736	192.168.50.100	192.168.50.101	TCP	74	47692 → 860 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on eth0  
Ethernet II, Src: ZyxelCommuni\_43:ef:80 (f0:87:56:43:ef:80), Dst: Br...  
Address Resolution Protocol (request)

La scansione **-sT** è una delle opzioni disponibili in Nmap,

La flag **-sT** indica a Nmap di eseguire una scansione TCP connect.

Quando si esegue una scansione TCP connect (**-sT**), Nmap tenta di stabilire una connessione TCP completando.

Tuttavia, è importante notare che l'utilizzo di una scansione TCP connect può essere più rumorosa e meno furtiva rispetto ad altre tecniche di scansione offerte da Nmap, come **-sS** (scansione SYN).

Seconda scansione completa delle porte incluse nel range 1-1024 con la flag **-sS**.

The image shows two windows from a Kali Linux system. The top window is a terminal running an Nmap scan. The bottom window is Wireshark capturing network traffic on the eth0 interface.

**Terminal Window:**

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.50.101 -p 1-1024  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 18:50 GMT  
Nmap scan report for 192.168.50.101  
Host is up (0.00068s latency).  
Not shown: 1012 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  
MAC Address: CA:D0:F2:82:E7:85 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

**Wireshark Window:**

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
44	6.419218927	192.168.50.100	192.168.50.101	TCP	58	34899 → 900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	6.419220177	192.168.50.100	192.168.50.101	TCP	58	34899 → 552 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	6.419221469	192.168.50.100	192.168.50.101	TCP	58	34899 → 43 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	6.419223886	192.168.50.100	192.168.50.101	TCP	58	34899 → 897 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	6.419225344	192.168.50.100	192.168.50.101	TCP	58	34899 → 896 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	6.419226761	192.168.50.100	192.168.50.101	TCP	58	34899 → 311 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50	6.419227969	192.168.50.100	192.168.50.101	TCP	58	34899 → 103 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	6.419229219	192.168.50.100	192.168.50.101	TCP	58	34899 → 737 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	6.419562445	192.168.50.101	192.168.50.100	TCP	54	554 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53	6.419562528	192.168.50.101	192.168.50.100	TCP	58	80 → 34899 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
54	6.419511862	192.168.50.100	192.168.50.101	TCP	54	34899 → 80 [RST] Seq=1 Win=0 Len=0
55	6.419584409	192.168.50.101	192.168.50.100	TCP	54	110 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	6.419584450	192.168.50.101	192.168.50.100	TCP	58	139 → 34899 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
57	6.419584492	192.168.50.101	192.168.50.100	TCP	54	113 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	6.419594201	192.168.50.100	192.168.50.101	TCP	54	34899 → 139 [RST] Seq=1 Win=0 Len=0
59	6.419651996	192.168.50.101	192.168.50.100	TCP	54	256 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	6.419652079	192.168.50.101	192.168.50.100	TCP	54	587 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	6.419652121	192.168.50.101	192.168.50.100	TCP	54	443 → 34899 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	6.419781754	192.168.50.101	192.168.50.100	TCP	58	445 → 34899 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0  
Ethernet II, Src: ZyXelCommuni\_43:ef:80 (f0:07:56:43:ef:80), Dst: Br...  
Address Resolution Protocol (request)

Quando si esegue una scansione SYN stealth (-sS), Nmap invia pacchetti SYN al target su porte specifiche e analizza le risposte per determinare lo stato dei porti sul sistema di destinazione.

La scansione SYN stealth è considerata una delle tecniche di scansione più furtive, poiché non completa la connessione TCP come la scansione TCP connect (-sT). Invece, Nmap invia solo il pacchetto di SYN e analizza le risposte senza completare la connessione TCP. L'utilizzo della scansione SYN stealth è spesso preferito per eseguire scansioni di rete in modo discreto, in particolare quando si vuole evitare il rilevamento da parte dei sistemi di difesa della rete.

Terza scansione completa delle porte nel range 1-1024 con la flag **-A**.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -A 192.168.50.101 -p 1-1024  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 18:53 GMT  
Nmap scan report for 192.168.50.101  
Host is up (0.0045s latency).  
Not shown: 1012 closed tcp ports (conn-refused)  
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 192.168.50.100  
|     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  
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTT  
  
513/tcp   open  login  
514/tcp   open  shell        Netkit rshd  
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux  
_kernel  
  
Host script results:  
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (u  
nknown)  
|_smb-os-discovery:  
|   OS: Unix (Samba 3.0.20-Debian)  
|   Computer name: metasploitable  
|   NetBIOS computer name:  
|   Domain name: localdomain  
|   FQDN: metasploitable.localdomain  
|_ System time: 2024-02-07T13:53:12-05:00  
|_smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s  
|_smb2-time: Protocol negotiation failed (SMB2)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submi  
t/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds  
  
(kali@kali)-[~]  
$
```

La scansione con la flag **-A** in Nmap è una delle opzioni avanzate che fornisce un insieme completo di informazioni sull'host e sulle porte scansionate. Questa flag combina diverse tecniche di scansione e l'analisi dei dati raccolti per fornire una visione dettagliata delle caratteristiche del sistema target.

L'utilizzo della flag **-A** è consigliato quando si desidera ottenere informazioni complete e dettagliate sull'host di destinazione, inclusi dettagli sulla versione del servizio e sul sistema operativo. Tuttavia, è importante notare che l'utilizzo della flag **-A** può richiedere più tempo e risorse rispetto alle scansioni standard.

REPORT						
TCP SCAN (-sT)						
FONTE		TARGET	SCAN TYPE	SERVIZI ATTIVI		
Indirizzo IP	Range di Porte	Indirizzo IP	TCP	PORT	STATO	SERVIZIO
192.168.50.100	1-1024	192.168.50.101	TCP	21	OPEN	ftp
192.168.50.100	1-1024	192.168.50.101	TCP	22	OPEN	ssh
192.168.50.100	1-1024	192.168.50.101	TCP	23	OPEN	telnet
192.168.50.100	1-1024	192.168.50.101	TCP	25	OPEN	smtp
192.168.50.100	1-1024	192.168.50.101	TCP	53	OPEN	domain
192.168.50.100	1-1024	192.168.50.101	TCP	80	OPEN	http
192.168.50.100	1-1024	192.168.50.101	TCP	111	OPEN	rpcbind
192.168.50.100	1-1024	192.168.50.101	TCP	139	OPEN	netbios-ssn
192.168.50.100	1-1024	192.168.50.101	TCP	445	OPEN	microsoft-ds
192.168.50.100	1-1024	192.168.50.101	TCP	512	OPEN	exec
192.168.50.100	1-1024	192.168.50.101	TCP	513	OPEN	login
192.168.50.100	1-1024	192.168.50.101	TCP	514	OPEN	shell
SYN SCAN (-sS)						
192.168.50.100	1-1024	192.168.50.101	TCP	21	OPEN	ftp
192.168.50.100	1-1024	192.168.50.101	TCP	22	OPEN	ssh
192.168.50.100	1-1024	192.168.50.101	TCP	23	OPEN	telnet
192.168.50.100	1-1024	192.168.50.101	TCP	25	OPEN	smtp
192.168.50.100	1-1024	192.168.50.101	TCP	53	OPEN	domain
192.168.50.100	1-1024	192.168.50.101	TCP	80	OPEN	http
192.168.50.100	1-1024	192.168.50.101	TCP	111	OPEN	rpcbind
192.168.50.100	1-1024	192.168.50.101	TCP	139	OPEN	netbios-ssn
192.168.50.100	1-1024	192.168.50.101	TCP	445	OPEN	microsoft-ds
192.168.50.100	1-1024	192.168.50.101	TCP	512	OPEN	exec
192.168.50.100	1-1024	192.168.50.101	TCP	513	OPEN	login
192.168.50.100	1-1024	192.168.50.101	TCP	514	OPEN	shell