

# ESERCITAZIONE CON TOOL DI KALI LINUX

## #NMAP

**NMAP** È UNO STRUMENTO DI **NETWORK EXPLORATION E AUDITING**. PUÒ SCANSIONARE SIA RETI DI GRANDI DIMENSIONI CHE SINGOLI HOST, DETERMINANDO QUALI **HOST** SONO **DISPONIBILI SU UNA RETE** E CHE **SERVIZI** OFFRONO (NOME APPLICAZIONE E VERSIONE), EVENTUALMENTE VULNERABILI. DETERMINA INOLTRE CHE **SISTEMA OPERATIVO** E CHE TIPO DI **FIREWALL E PACKET FILTERS** SONO IN USO.

PER PRENDERE CONFIDENZA CON IL TOOL L'ESERCIZIO RICHIEDE DI SCANSIONARE DA KALI LINUX (MACCHINA ATTACCANTE) LE PORTE WELL-KNOWN (1-1023) DISPONIBILI SU METASPLOITABLE (MACCHINA VITTIMA) IN TRE DIVERSE MODALITÀ:

- 1) **LA SCANSIONE "SYN"** - CON IL COMANDO **nmap -sS 192.168.50.101 -p 1-1024**. È LA MENO INVASIVA E RUMOROSA DI TUTTE, IN QUANTO, UNA VOLTA APPURATO CHE UNA PORTA È APERTA, NON CONCLUDE IL TERZO PASSAGGIO DEL THREE-WAY-HANDSHAKE CHIUDENDO LA COMUNICAZIONE CON **RST** (RESET). QUESTO EVITA L'OVERLOAD DATO DALLA CREAZIONE DEL CANALE STESSO.
- 2) **LA SCANSIONE "TCP"** - CON IL COMANDO **nmap -sT 192.168.50.101 -p 1-1024**. È UN METODO PIÙ INVASIVO, CHE PER STABILIRE SE UNA PORTA È APERTA E RECUPERARE INFORMAZIONI SUL SERVIZIO IN ASCOLTO, COMPLETA IL THREE-WAY-HANDSHAKE E STABILISCE DI FATTO UN CANALE.
- 3) **LA SCANSIONE CON LO SWITCH "-A"** - CON IL COMANDO **nmap -A 192.168.50.101 -p 1-1024**. È DI FATTO LA SCANSIONE PIÙ INVASIVA E PIÙ LENTA, MA PERMETTE DI OTTENERE MOLTI PIÙ DATI

INIZIAMO CON L'**HOST DISCOVERY** - TECNICA PER CAPIRE SE UN HOST È ATTIVO E QUINDI RAGGIUNGIBILE SU UNA RETE.

COMANDO PER PING SENZA SCAN: **nmap -sn 192.168.50.101**

DOPODICHE PROCEDIAMO CON LE TRE MODALITÀ DI SCANSIONE DELLE PORTE WELL-KNOWN E ANALIZZIAMO LE DIFFERENZE CATTURANDO I PACCHETTI CON WIRESHARK

```
(root@kali)-[/home/django]
# nmap -sn 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 16:44 EST
Nmap scan report for 192.168.50.101
Host is up (0.00037s latency).
MAC Address: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

```
(root@kali)-[/home/django]
# nmap -sS 192.168.50.101 -p 0-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 16:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00014s latency).
Not shown: 1013 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: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)
```

**PORTE APERTE = OPEN**  
**n° 12, CON SERVIZIO INDICATO**

```
(root@kali)-[/home/django]
# nmap -sT 192.168.50.101 -p 0-1024

Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 17:07 EST
Nmap scan report for 192.168.50.101
Host is up (0.00068s latency).
Not shown: 1013 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

MAC Address: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

PORTE APERTE = OPEN  
n° 12, CON SERVIZIO INDICATO

```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(root@kali)-[/home/django]
# nmap -A 192.168.50.101 -p 0-1024

Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 17:17 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 1013 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 192.168.50.101
|_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, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_DES_64_CBC_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
|_SSL2_RC2_128_CBC_EXPORT40_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
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 37423/udp mountd
|_100005 1,2,3 37692/tcp mountd
|_100021 1,3,4 46629/tcp nlockmgr
|_100021 1,3,4 54976/udp nlockmgr
|_100024 1 34673/udp status
|_100024 1 35058/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb          Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
MAC Address: 08:00:27:DC:03:D4 (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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h33m07s, deviation: 3h32m07s, median: 3m07s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2024-01-04T17:21:00-05:00
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT ADDRESS
1 1.33 ms 192.168.50.101

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 98.47 seconds
```

