

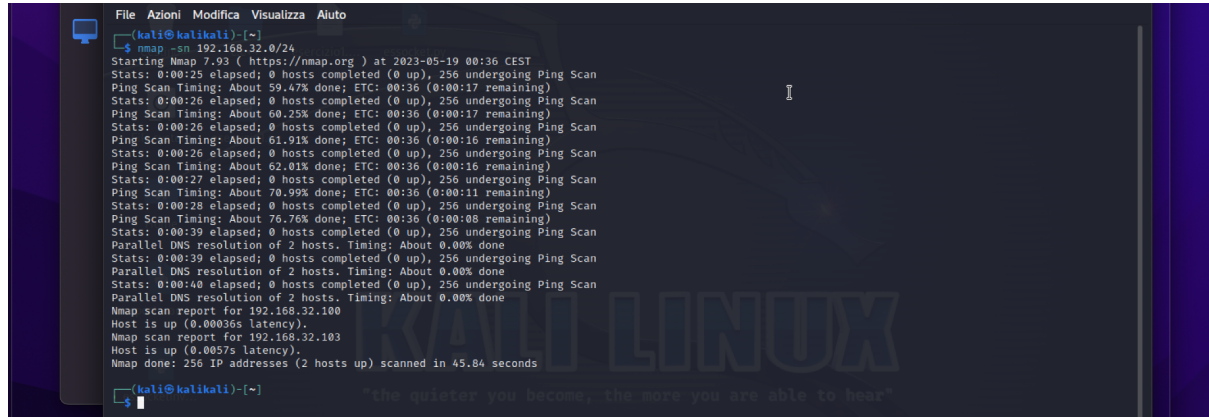
ESERCIZIO NMAP

- Host discovery

Dopo aver messo kali e metasploitable su rete interna con gli indirizzi:

kali 192.168.32.100 e meta 192.168.32.103, effettuo un Host discovery sulla rete

192.168.32.0/24 con nmap, con il comando: `nmap -sn 192.168.32.0/24` nmap riconosce i 2 Host.



```
(kali@kalikali)~$ nmap -sn 192.168.32.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 00:36 CEST
Stats: 0:00:25 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 59.47% done; ETC: 00:36 (0:00:17 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 60.25% done; ETC: 00:36 (0:00:17 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 61.91% done; ETC: 00:36 (0:00:16 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 62.01% done; ETC: 00:36 (0:00:16 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 70.99% done; ETC: 00:36 (0:00:11 remaining)
Stats: 0:00:28 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 76.76% done; ETC: 00:36 (0:00:08 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 2 hosts. Timing: About 0.00% done
Stats: 0:00:39 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 2 hosts. Timing: About 0.00% done
Stats: 0:00:40 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 2 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.32.100
Host is up (0.00036s latency).
Nmap scan report for 192.168.32.103
Host is up (0.0057s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 45.84 seconds
```

Scansione TCP sulle porte Well-Known

Con il comando `nmap -sT -p 0-1023 192.168.32.103`

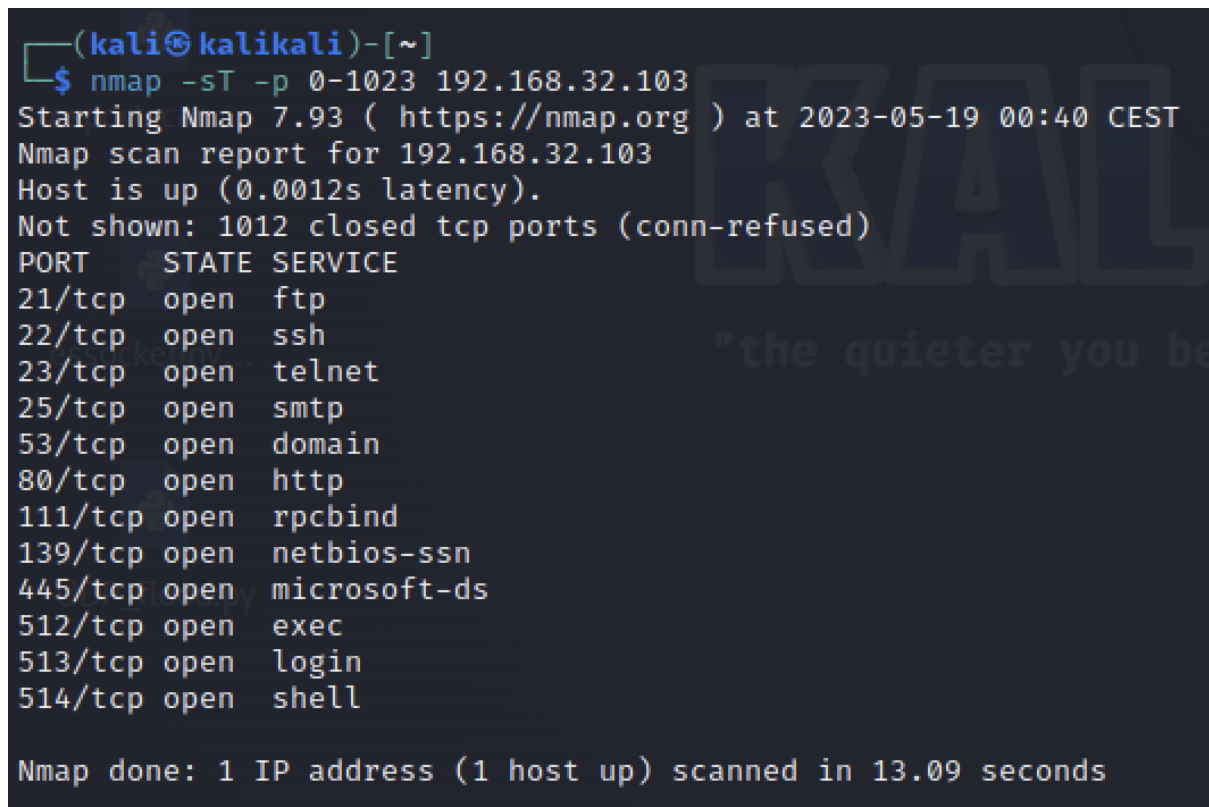
Report della scansione:

Fonte scan: 192.168.32.100 (kali)

Target scan: 192.168.32.103 (meta)

Tipo di scan: -sT (TCP SCAN) porte 0-1023

Risultato: 12 servizi attivi



```
(kali@kalikali)~$ nmap -sT -p 0-1023 192.168.32.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 00:40 CEST
Nmap scan report for 192.168.32.103
Host is up (0.0012s 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 13.09 seconds
```

Scansione SYN sulle porte well-known

Con il comando: `nmap -sS -p 0-1023 192.168.32.103` Report scansione:

Fonte scan: 192.168.32.100

Target scan: 192.168.32.103

Tipo di scan: -sS (SYN SCAN) sulle porte 0-1023

Risultato: 12 servizi attivi

```
(kali@kalikali)-[~]
$ sudo su
(root@kalikali)-[/home/kali]
# nmap -sS -p 0-1023 192.168.32.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 01:18 CEST
Nmap scan report for 192.168.32.103
Host is up (0.00077s 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
```

Scansione con switch -A sulle porte well-known

con il comando: `nmap -a -p 0-1023 192.168.32.103` Report scansione approfondita:

Altre info riportate nella scansione:

```
(kali@kalikali)-[~]
$ nmap -A -p 0-1023 192.168.32.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 01:28 CEST
Nmap scan report for 192.168.32.103
Host is up (0.0013s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.32.100
|_   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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkeys:
|_   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_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
```

```

|_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         46459/udp  mountd
|   100005   1,2,3         51930/tcp  mountd
|   100021   1,3,4         38571/udp  nlockmgr
|   100021   1,3,4         59875/tcp  nlockmgr
|   100024   1             51787/tcp  status
|   100024   1             55736/udp  status
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  shell       Netkit rshd
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h02m41s, deviation: 2h49m43s, median: 2m40s
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-05-18T19:31:47-04:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.51 seconds

```

Ciandri Leonardo