HOST DISCOVERY

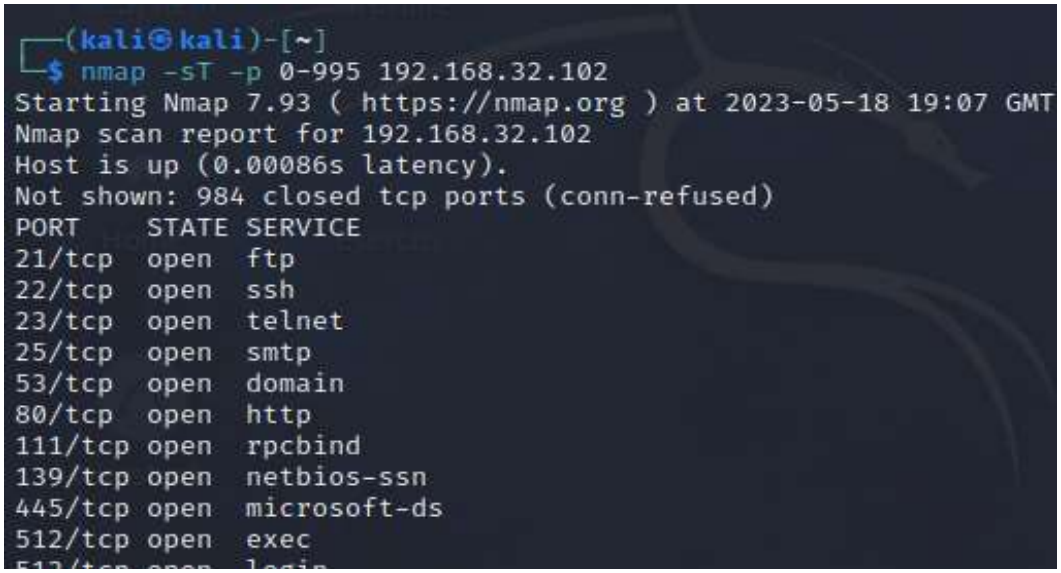
Imposto gli IP statici sulle macchine Kali Linux (Ip 192.168.32.100) e Metasploid(192.168.32.102). Dalla macchina Kali, usando il comando "**nmap -sn 192.168.32.0/24**", vado a vedere gli host che rispondono mappando la rete in modo da sapere quanti host sono attivi, in questo caso si possono vedere proprio i due che sono stati impostati.

SCANSIONE TCP SULLE PORTE WELL-KNOW

Usando il comando "**nmap -sT -p 0-995 192.168.32.102**" vado scansionare le porte well-know dalla 0 alla 995, in questo comando per indicare che stiamo scannerizzando le porte useremo -p e nello specifico si tratta di **Tcp** quindi useremo la **T** . Di seguito la tabella con il risultato della scansione, 12 porte trovate e sono tutte aperte.

FONTE	192.168.32.100
TARGET	192.168.32.102
TIPO	-sT Tpc su porte 0-995
RISULTATI	12 porte APERTE

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

```
513/tcp open  login
514/tcp open  shell

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

SCANSIONE SYN SULLE PORTE WELL-KNOW

Usando il comando "**sudo nmap -sS -p 0-995 192.168.32.102**" vado scansionare le porte well-know dalla 0 alla 995, in questo comando per indicare che si tratta di **Syn** useremo la **S** . Di seguito la tabella con il risultato della scansione, 12 porte trovate e sono tutte aperte.

FONTE	192.168.32.100
TARGET	192.168.32.102
TIPO	-sS SYN su porte 0-995
RISULTATI	12 porte APERTE

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

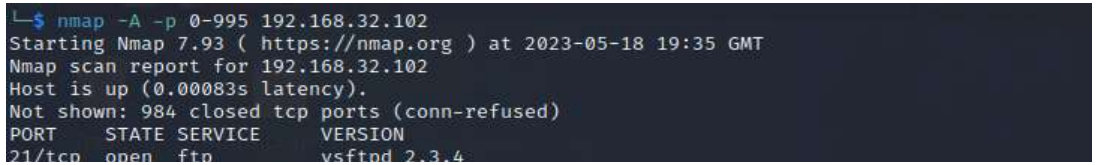
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 0-995 192.168.32.102
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 19:23 GMT
Nmap scan report for 192.168.32.102
Host is up (0.00028s latency).
Not shown: 984 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
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: 08:00:27:33:BD:A2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

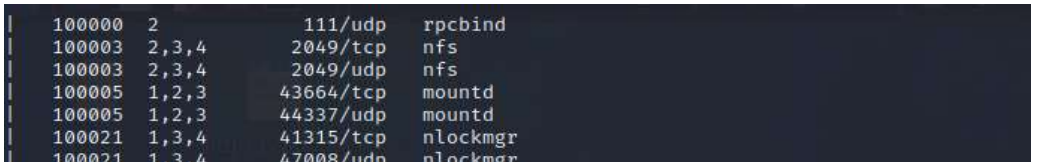
SCANSIONE CON SWITCH "-A" SULLE PORTE WELL-KNOW

Usando il comando "**nmap -A -p 0-995 192.168.32.102**" effettuiamo una nuova scansione, in questo caso avremo come informazioni aggiuntive, alle porte già viste sopra, la VERSION, di seguito inserita nella tabella.

FONTE	192.168.32.100
TARGET	192.168.32.102
TIPO	-A su porte 0-995
RISULTATI	12 porte APERTE

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSh 4.7p1 Debian 7buntu1
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache http 2.2.8
111/tcp	open	rpcbind	2 (RPC #10000)
139/tcp	open	netbios-ssn	Samba smbd 3.X -4.X
445/tcp	open	microsoft-ds	Samba smbd 3.0.20-Debian
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	
514/tcp	open	shell	Netkit rshd





```
| 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-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, START
TLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
```

```
|   100024  1          48419/tcp   status
|_  100024  1          50712/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:l
x_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 00000000
0 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T15:05:19-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h28m32s, deviation: 2h49m43s, median: -31m28s

Service detection performed. Please report any incorrect results at https://nmap.org/s
it/ .
Nmap done: 1 IP address (1 host up) scanned in 88.51 seconds
```

DIFFERENZA TRA SCANSIONE COMPLETA TCP E SYN - WIRESHARK

Avviando Wideshark che va a intercettare la scanzione TCP, si può notare in corrispondenza della **porta 80** protocollo three-way handshake proprio della ete TCP/IP col quale avviane uno scambio di pacchetti SYN e ACK tra Server e Client.

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
30	7.988085844	192.168.32.100	192.168.32.102	TCP	74	37026 → 80 [SYN] Seq=0 Win=64240 Len
51	7.990627497	192.168.32.102	192.168.32.100	TCP	74	80 → 37026 [SYN, ACK] Seq=0 Ack=1 Wi
64	7.990885732	192.168.32.100	192.168.32.102	TCP	66	37026 → 80 [ACK] Seq=1 Ack=1 Win=642

Invece durante la scansione SYN, Wideshark intercetta uno scambio di pacchetti SYN, SYN ACK, RST, quest'ultimo Reset indica che la porta non non è in ascolto e la porta quindi viene marcata come filtrata.

No.	Time	Source	Destination	Protocol	Length	Info
14	13.104092380	192.168.32.100	192.168.32.102	TCP	58	43317 → 80 [SYN] Seq=0 Win=1024 Len=
18	13.104744838	192.168.32.102	192.168.32.100	TCP	60	80 → 43317 [SYN, ACK] Seq=0 Ack=1 Wi
19	13.104758256	192.168.32.100	192.168.32.102	TCP	54	43317 → 80 [RST] Seq=1 Win=0 Len=0