

M3 -> W1D1

- Esecuzione scansione -ST su host Metasploitable 192.168.50.101 dall'host Kali 192.168.50.100

Viene eseguita la scansione completa di tutte le porte, includendo il 3W-H, con in comando:

```
sudo nmap -sT 192.168.50.101
```

Vengono mostrate le seguenti porte accessibili, per un totale di 23 porte:

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
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

- Scansione SYN

Viene eseguita una scansione “leggera”, ovvero una scansione che non completa il 3W-H, che permette di non consumare troppa banda e ciò rende la scansione rapida. Viene eseguita mediante il comando:

```
sudo nmap -sS 192.168.50.101
```

Che mostra le stesse porte accessibili ma con un tempo di esecuzione inferiore 0.38s

```
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Contro 0.68s della completa

```
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

- Scansione con switch -A

Viene eseguita la scansione completa con il comando:

```
sudo nmap -A 192.168.50.101
```

Che mostra le porte accessibili, anche dalle scansioni precedenti, includendo però il nome dei servizi attivi e le relative versioni.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
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
|   100000  2                111/udp    rpcbind
|   100003  2,3,4           2049/tcp   nfs
|   100003  2,3,4           2049/udp   nfs
|   100005  1,2,3           33091/tcp  mountd
|   100005  1,2,3           34029/udp  mountd
|   100021  1,3,4           38126/udp  nlockmgr
|   100021  1,3,4           49113/tcp  nlockmgr
|   100024  1                38754/udp  status
|   100024  1                50675/tcp  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
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: 10
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, Support41Auth, Speaks41ProtocolNew, SupportsTransactions, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression
|   Status: Autocommit
|   Salt: #'8#Eq,%q/1Kd7$N-GF
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu004-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: 2025-01-14T09:42:43+00:00; 0s 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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp_methods: Failed to get a valid response for the OPTION request
8180/tcp  open  unknown
|_http_title: Apache Tomcat/5.5
|_http_favicon: Apache Tomcat
MAC Address: 08:00:27:B6:62:D1 (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: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb_security_mode:
|_account_used: <blank>
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_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: 2025-01-14T04:42:19-05:00
```

Con un tempo totale di esecuzione di :

```
Nmap done: 1 IP address (1 host up) scanned in 251.39 seconds
```