

SCANSIONI NMAP

METASPOITABLE (192.168.50.101)

OS fingerprint:

```
(kali㉿kali)-[~]
$ sudo nmap -Pn -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:36 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 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
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
MAC Address: 08:00:27:3A:A0:2B (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

OS detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

Syn Scan:

```
(kali㉿kali)-[~]  
$ sudo nmap -Pn -sS 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:38 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00055s latency).  
Not shown: 977 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  
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  
MAC Address: 08:00:27:3A:A0:2B (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
```

TPC Connect Scan:

```
(kali㉿kali)-[~]  
$ sudo nmap -Pn -sT 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:51 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0011s latency).  
Not shown: 977 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  
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  
  
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
```

Version Detection:

```
(kali㉿kali)-[~]
```

```
$ sudo nmap -Pn -sV --version-all 192.168.50.101
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 08:57 EDT
```

```
Nmap scan report for 192.168.50.101
```

```
Host is up (0.0011s latency).
```

```
Not shown: 977 closed tcp ports (reset)
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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 httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (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
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

```
MAC Address: 08:00:27:3A:A0:2B (Oracle VirtualBox virtual NIC)
```

```
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 110.19 seconds
```

```
(kali㉿kali)-[~]
```

```
$
```

WINDOWS 7 (192.168.50.102)

OS fingerprint:

```
(kali㉿kali)-[~]  
└─$ sudo nmap -Pn -O 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:48 EDT  
Nmap scan report for 192.168.50.102  
Host is up (0.00072s latency).  
Not shown: 987 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
554/tcp   open  rtsp  
2869/tcp  open  icslap  
5357/tcp  open  wsdaapi  
10243/tcp open  unknown  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
MAC Address: 08:00:27:09:02:67 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 7|2008|8.1  
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

REPORT

METASPLOITABLE:

IP:

192.168.50.101

SO:

Linux 2.6.9 - 2.6.33

PORTE APERTE:

21/tcp, 22/tcp, 23/tcp, 25/tcp, 53/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512/tcp, 513/tcp, 514/tcp, 1099/tcp, 1524/tcp, 2049/tcp, 2121/tcp, 3306/tcp, 5432/tcp, 5900/tcp, 6000/tcp, 6667/tcp, 8009/tcp, 8180/tcp

SERVIZI IN ASCOLTO E VERSIONE:

Servizio: ftp	vsftpd 2.3.4,
Servizio: ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Servizio: telnet	Linux telnetd
Servizio: smtp	Postfix smtpd
Servizio: domain	ISC BIND 9.4.2
Servizio: http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
Servizio: rpcbind	2 (RPC #100000)
Servizio: netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Servizio: netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Servizio: exec	netkit-rsh rexecd
Servizio: shell	Netkit rshd
Servizio: java-rmi	GNU Classpath grmiregistry
Servizio: bindshell	Metasploitable root shell
Servizio: nfs	2-4 (RPC #100003)
Servizio: ftp	ProFTPD 1.3.1
Servizio: mysql	MySQL 5.0.51a-3ubuntu5
Servizio: postgresql	PostgreSQL DB 8.3.0 - 8.3.7
Servizio: vnc	VNC (protocol 3.3)
Servizio: X11	(access denied)
Servizio: irc	UnrealIRCd
Servizio: ajp13	Apache Jserv (Protocol v1.3)
Servizio: http	Apache Tomcat/Coyote JSP engine 1.1