

# Report su scan effettuato su Metasploitable

```
(nicholas@kali)-[~]
$ sudo nmap -sn -PE 192.168.50.2
[sudo] password for nicholas:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-31 11:21 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
Nmap scan report for 192.168.50.2
Host is up (0.00092s latency).
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

(nicholas@kali)-[~]
$
```

File Actions Edit View Help						
Currently scanning: Finished!   Screen View: Unique Hosts						
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60						
IP	At	MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.50.2		ca:01:f0:3e:dd:b1	1	60	Unknown vendor	

- Comando utilizzato: map -sn -PE per verificare che l’host sia attivo

- Comando utilizzato per contro prova: netdiscover -r

```
$ nmap 192.168.50.2 -top-ports 10 -open
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-31 11:24 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
Nmap scan report for 192.168.50.2
Host is up (0.0011s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

```
(nicholas@kali)-[~]
$ sudo hping3 --scan known 192.168.50.2
Scanning 192.168.50.2 (192.168.50.2), port known
264 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+
|port| serv name | flags | ttl | id | win | len |
+-----+-----+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 r
miregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)

(nicholas@kali)-[~]
```

- Comando utilizzato: nmap -top-ports 10 -open, per verificare le 10 porte aperte più importanti

- Comando utilizzato hping3 —scan known, per un ulteriore prova per verificare porte aperte

# Report completo

- Comando utilizzato: `nmap -p- -sV -reason`, che effettua una scansione in SYN scan elencandoci consecutivamente le porte aperte con i relativi servizi con le relative versioni

```
(nicholas@kali)-[~]
$ nmap 192.168.50.2 -p- -sV -reason -dns-server ns
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-31 11:24 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.2
Host is up, received syn-ack (0.00097s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack  Linux telnetd
25/tcp    open  smtp         syn-ack  Postfix smtpd
53/tcp    open  domain       syn-ack  ISC BIND 9.4.2
80/tcp    open  http         syn-ack  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack  2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack  netkit-rsh rexecd
513/tcp   open  login?       syn-ack
514/tcp   open  shell        syn-ack  Netkit rshd
1099/tcp  open  java-rmi     syn-ack  GNU Classpath grmiregistry
1524/tcp  open  bindshell    syn-ack  Metasploitable root shell
2049/tcp  open  nfs          syn-ack  2-4 (RPC #100003)
2121/tcp  open  ftp          syn-ack  ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack  MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      syn-ack  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack  VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack  (access denied)
6667/tcp  open  irc          syn-ack  UnrealIRCd
6697/tcp  open  irc          syn-ack  UnrealIRCd
8009/tcp  open  ajp13        syn-ack  Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack  Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          syn-ack  Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
41978/tcp open  nlockmgr     syn-ack  1-4 (RPC #100021)
42088/tcp open  mountd       syn-ack  1-3 (RPC #100005)
52830/tcp open  status       syn-ack  1 (RPC #100024)
58829/tcp open  java-rmi     syn-ack  GNU Classpath grmiregistry
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 150.33 seconds
```

# Report di Scan su Metasploitable con Nmap da Kali Linux

Data dello scan: 31 luglio 2023, 11:24 CEST  
Indirizzo IP scansionato: 192.168.50.2

Risultati dello scan:

Informazioni generali sul sistema:

Host up: Si

Latenza: 0.00097 secondi

Porte aperte e servizi attivi:

Porta 21/tcp (ftp): Servizio vsftpd 2.3.4

Porta 22/tcp (ssh): Servizio OpenSSH 4.7p1 Debian 8ubuntu1 (protocollo 2.0)

Porta 23/tcp (telnet): Servizio Linux telnetd

Porta 25/tcp (smtp): Servizio Postfix smtpd

Porta 53/tcp (domain): Servizio ISC BIND 9.4.2

Porta 80/tcp (http): Servizio Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Porta 111/tcp (rpcbind): Servizio 2 (RPC #100000)

Porta 139/tcp (netbios-ssn): Servizio Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Porta 445/tcp (netbios-ssn): Servizio Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Porta 512/tcp (exec): Servizio netkit-rsh rexecd

Porta 513/tcp (login?): Servizio sconosciuto

Porta 514/tcp (shell): Servizio Netkit rshd

Porta 1099/tcp (java-rmi): Servizio GNU Classpath grmiregistry

Porta 1524/tcp (bindshell): Servizio Metasploitable root shell

Porta 2049/tcp (nfs): Servizio 2-4 (RPC #100003)

Porta 2121/tcp (ftp): Servizio ProFTPD 1.3.1

Porta 3306/tcp (mysql): Servizio MySQL 5.0.51a-3ubuntu5

Porta 3632/tcp (distccd): Servizio distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Porta 5432/tcp (postgresql): Servizio PostgreSQL DB 8.3.0 - 8.3.7

Porta 5900/tcp (vnc): Servizio VNC (protocollo 3.3)

Porta 6000/tcp (X11): Accesso negato

Porta 6667/tcp (irc): Servizio UnrealIRCd

Porta 6697/tcp (irc): Servizio UnrealIRCd

Porta 8009/tcp (ajp13): Servizio Apache Jserv (Protocollo v1.3)

Porta 8180/tcp (http): Servizio Apache Tomcat/Coyote JSP engine 1.1

Porta 8787/tcp (drb): Servizio Ruby DRb RMI (Ruby 1.8; percorso /usr/lib/ruby/1.8/drb)



Porta 41978/tcp (nlockmgr): Servizio 1-4 (RPC #100021)  
Porta 42088/tcp (mountd): Servizio 1-3 (RPC #100005)  
Porta 52830/tcp (status): Servizio 1 (RPC #100024)  
Porta 58829/tcp (java-rmi): Servizio GNU Classpath grmiregistry  
Informazioni sul sistema operativo e CPE (Common Platform Enumeration):  
Hosts: metasploitable.localdomain, irc.Metasploitable.LAN  
Sistemi operativi: Unix, Linux  
CPE: cpe:/o:linux:linux\_kernel  
Note aggiuntive:

Durante la scansione, è stato rilevato un warning riguardo l'incapacità di determinare i server DNS. Reverse DNS è stato disabilitato.  
Per eventuali segnalazioni di risultati incorretti, si può fare riferimento a <https://nmap.org/submit/>.