

## REPORT SCANSIONE METASPLOITABLE-IP 192.168.50.101

IP	SISTEMA OPERATIVO	PORTE APERTE	SERVIZI IN ASCOLTO CON VERSIONE
192.168.50.101	Unix (Samba 3.0.20-Debian)	21/ftp	Vsftpd 2.3.4
		22/ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
		23/telnet	Linux telnetd
		25/smtp	Postfix smtpd
		53/domain	ISC BIND 9.4.2
		80/http	Apache https 2.2.8 ((Ubuntu) DAV/“)
		111/rpcbind	2 (RPC #100000)
		139/netbios-ssn	Samba sbd 3.x - 4.x
		445/microsoft-ds	Samba sbd 3.x - 4.x
		512/exec	Netkit-rsh rexecd
		513/login	
		514/shell	Netkit rshd

### SCANSIONE NMAP CON SCRIPT - INFORMAZIONI SISTEMA OPERATIVO

```

root@kali:~/home/luca
# nmap -O report6 192.168.50.101 -p 0-1024 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:46 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00082s latency). OS: 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 50.56 seconds
[output truncated]
MAC Address: 2E:29:34:08:0D:08 (Unknown)
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)(request)
|   Computer name: metasploitable
|   NetBIOS computer name: metasploitable
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-08-03T10:50:25-04:00
Nmap done: 1 IP address (1 host up) scanned in 13.69 seconds

```

# SCANSIONE CON METODO TCP E VERSION DETECTION CON RANGE DI PORTE DALLA 0 ALLA 1024

```
(root㉿kali)-[~/home/luca]# nmap -Ov report5 192.168.50.101 -p 0-1024 -sV -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 1013 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4|101
21/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?  login? 100
514/tcp   open  shell   Netkit rshd
MAC Address: 2E:29:34:08:0D:08 (Unknown)
Service Info: Host: metasploitable.localdomain; 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 50.63 seconds
# [root@kali:~/home/luca]# protocol (request)

0000 ff ff ff ff ff ff 52 4c ff e7 b6 8b 08 00 00 01 ..... RL .....
0010 08 00 06 04 00 01 52 4c ff e7 b6 8b c0 a8 32 64 ..... RL ..... 2d
0020 00 00 00 00 00 00 c0 a8 32 01 ..... 2

● wireshark_eth0FREQ1.pcapng | Pacchetti: 2644 - visualizzati: 2644 (100.0%) | Profilo: Default
Python
```

QUESTO TIPO DI SCANSIONE E MOLTO INVASIVA PERCHE VA A CHIUDERE IL 3-WAY-HANDSHAKE COME SI PUO VEDERE DALLA FOTO QUI SOTTO (ES. PORTA 80 )

```
(root㉿kali)-[~/home/luca]# nmap -Ov report5 192.168.50.101 -p 0-1024 -sV -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 1013 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4|101
21/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?  login? 100
514/tcp   open  shell   Netkit rshd
MAC Address: 2E:29:34:08:0D:08 (Unknown)
Service Info: Host: metasploitable.localdomain; 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 50.56 seconds
# [root@kali:~/home/luca]# protocol (request)

0000 ff ff ff ff ff ff 52 4c ff e7 b6 8b 08 00 00 01 ..... RL .....
0010 08 00 06 04 00 01 52 4c ff e7 b6 8b c0 a8 32 64 ..... RL ..... 2d
0020 00 00 00 00 00 00 c0 a8 32 01 ..... 2

● wireshark_eth0FREQ1.pcapng | Pacchetti: 2644 - visualizzati: 2644 (100.0%) | Profilo: Default
Python
```

## SCANSIONE CON METODO SYN (STEALTH) E VERSION DETECTION

```

root@kali:[/home/luca]
# nmap -ON report5 192.168.50.101 -p 0-1024 -sV -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:37 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00068s latency).
Not shown: 1013 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntul (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 #10000)
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 rexd
513/tcp   open  login?      rlogn
514/tcp   open  shell        Netkit rshd/ps2tel
MAC Address: 2E:29:34:08:0D:08 (Unknown)

Service Info: Host: metasploitable.localdomain; 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 50.63 seconds

root@kali:[/home/luca]
# nmap -ON report5 192.168.50.101 -p 0-1024 -sV -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:41 CEST
[...]

```

eth0:<live capture in progress>

Pacchetti: 14 · visualizzati: 14 (100.0%) | Profilo: Default

Python

QUESTA SCANSIONE RISPETTO ALLA PRECEDENTE E MENO INVASIVA PERCHE NON CHIUDA IL 3-WAY-HANDSHAKE COME SI PUO NOTARE NELLA FOTO QUI SOTTO. UNA VOLTA CHE CONTROLLA SE LA PORTA APERTA CHIUDA LA CONNESSIONE

```

root@kali:[/home/luca]
# nmap -ON report5 192.168.50.101 -p 0-1024 -sV -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:41 CEST
[...]

```

Source	Destination	Protocol	Length	Info
28909925	192.168.50.100	TCP	58	59768 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28914633	192.168.50.100	TCP	58	59768 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28923842	192.168.50.100	TCP	58	59768 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28928383	192.168.50.100	TCP	58	59768 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32632407	192.168.50.101	TCP	54	587 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33041675	192.168.50.101	TCP	58	445 → 59768 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33041883	192.168.50.101	TCP	54	995 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33041967	192.168.50.101	TCP	54	110 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33089342	192.168.50.100	TCP	54	59768 → 445 [RST] Seq=1 Win=0 Len=0
33311717	192.168.50.101	TCP	54	443 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33312133	192.168.50.101	TCP	54	554 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33312217	192.168.50.101	TCP	54	113 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33666592	192.168.50.101	TCP	58	53 → 59768 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33666800	192.168.50.101	TCP	58	80 → 59768 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33666883	192.168.50.101	TCP	54	993 → 59768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33674175	192.168.50.100	TCP	54	59768 → 53 [RST] Seq=1 Win=0 Len=0
33691508	192.168.50.100	TCP	54	59768 → 80 [RST] Seq=1 Win=0 Len=0

Frame 203: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
 Ethernet II, Src: 52:4c:ff:e7:b6:8b (52:4c:ff:e7:b6:8b), Dst: 2e:29:34:08:0d:08 (2e:29:34:08:0d:08)
 Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
 Transmission Control Protocol, Src Port: 59768, Dst Port: 626, Seq: 0, Len: 0

0000 2e 29 34 08 0d 08 52 4c ff e7 b6 8b 08 00 45 00 .4 .RL .....E.
0010 00 2c dd d8 00 00 35 06 c1 d9 c0 a8 32 64 c0 a8 ,.. 5 ..2d .
0020 32 65 e9 78 02 72 c5 73 ac b5 00 00 00 00 60 02 2e x r s .....
0030 04 00 4f f8 00 00 02 04 05 b4 ..0 ..0 ..0 ..0 ..

wireshark\_eth0EZ1P1.pcapng

Pacchetti: 2148 · visualizzati: 2148 (100.0%) · marcati: 5 (0.2%) · scartati: 0 (0.0%) | Profilo: Default

Python

REPORT SCANSIONE WINDOWS 7 INDIRIZZO IP:192.168.50.102

IP	SISTEMA OPERATIVO	PORTE APERTE	SERVIZI IN ASCOLTO CON VERSIONE
192.168.50.102	WINDOWS 7 ULTIMATE 7600 / WINDOWS 7 ULTIMATE 6.1)	135/MSRPC	Microsoft Windows ppc
		139/NETBIOS-SSN	Windows netbios-ssn
		445/MICROSOFT-DS	Microsoft windows 7-10 microsoft-ds
		554/RTSP	
		2869/ICSLAP	Microsoft httpapi httpd 2.0
		5357/WSDAPI	Microsoft httpapi httpd 2.0

## SCANSIONE NMAP CON SCRIPT - INFORMAZIONI SISTEMA OPERATIVO

SCANSIONE CON METODO TCP E VERSION DETECTION SENZA RANGE DI PORTE

```
File Azioni Modifica Visualizza Aiuto Analizza Statistiche Telefonia Wireless Strumenti Aiuto
5357/tcp open wsapi
10243/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
MAC Address: 16:EA:F7:02:36:0A (Unknown)
Destination Protocol Length Info
192.168.50.101 TCP 74 886 - 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
192.168.50.101 TCP 74 39228 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
192.168.50.101 TCP 74 513 - 886 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 TSval=39228 TStamp=1628338248.100000000
192.168.50.101 TCP 74 80 - 39228 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 TSval=39228 TStamp=1628338248.100000000
192.168.50.101 TCP 66 39228 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=39228 TStamp=1628338248.100000000
# nmap -oh repow4 192.168.50.102 -sV -ST
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 17:53 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0076s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
PORT 2569/STATE SERVICE      VERSION
135/tcp   open msrpc        Microsoft Windows RPC
139/tcp   open netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5544/tcp  open rtsp?
2869/tcp  open http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc        Microsoft Windows RPC
49153/tcp open msrpc        Microsoft Windows RPC
49154/tcp open msrpc        Microsoft Windows RPC
49155/tcp open msrpc        Microsoft Windows RPC
49156/tcp open msrpc        Microsoft Windows RPC
MAC Address: 16:EA:F7:02:36:0A (Unknown)
Service Info: Host: LUCA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.23 seconds

[root@kali)-[/home/luca]
#
```

#### SCANSIONE CON METODO SYN (STEALTH) E VERSION DETECTION

Kali Linux

File Azioni Modifica Visualizza Aiuto Analizza Statistiche Telefonia Wireless Strumenti Aiuto

Nmap done: 1 IP address (1 host up) scanned in 25.85 seconds

(root@kali)-[~/home/luca]

```
# nmap -oN repow2 192.168.50.102 -p 0-1024 -sV -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:50 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0031s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
MAC Address: 16:EA:F7:02:36:0A (Unknown)
Service Info: Host: LUCA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. .
Nmap done: 1 IP address (1 host up) scanned in 136.88 seconds
```

(root@kali)-[~/home/luca]

```
[  ]# nmap -oN repow3 192.168.50.102 -p 0-1024 -T5 -sV -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:53 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0029s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
MAC Address: 16:EA:F7:02:36:0A (Unknown)
Service Info: Host: LUCA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. .
Nmap done: 1 IP address (1 host up) scanned in 132.59 seconds
```

(root@kali)-[~/home/luca]

```
[  ]#
```

## SCANSIONE OS FINGERPRINTING SENZA SCRIPT DI METASPLOITABLE

```
Kali Linux
root@kali: /home/luca

File Azioni Modifica Visualizza Aiuto

# nmap -O 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 15:47 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0044s 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  cccproxy-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: 2E:29:34:08:0D:08 (Unknown)
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/submit/
Nmap done: 1 IP address (1 host up) scanned in 14.74 seconds
Nmap usage: nmap [options] 
          --script [-f] 
          --scriptdir <dir>
          --scriptlist <list>
          --scriptfile <file>
```

## SCANSIONE OS FINGERPRINTING SENZA SCRIPT DI WINDOWS 7

```
Kali Linux
root@kali: /home/luca

File Azioni Modifica Visualizza Aiuto

MAC Address: 2E:29:34:08:0D:08 (Unknown)
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/submit/
Nmap done: 1 IP address (1 host up) scanned in 14.74 seconds
Nmap usage: nmap [options] 
          --script [-f] <script>[,<script>...]
          --scriptdir <dir>
          --scriptlist <list>
          --scriptfile <file>
```

  

```
# nmap -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 15:53 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0008s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 16:EA:F7:02:36:0A (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone|fingerprint
Running: Microsoft Windows Server 2008 R2|Windows 8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8_1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 19.30 seconds
Nmap usage: nmap [options] <target>
          --script [-f] <script>[,<script>...]
          --scriptdir <dir>
          --scriptlist <list>
          --scriptfile <file>
```

## SCANSIONE METODO SYN METASPLOITABLE

## SCANSIONE METODO TCP METASPLOITABLE

## SCANSIONE CON METODO VERSION DETECTION DI METASPLOITABLE

```
root@kali:~/home/luca
# nmap -O report3 192.168.50.101 -T5 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 16:21 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000725 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 rexec
513/tcp   open  login?      rlogin
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?     http-wordpress-brute.nse
8180/tcp  open  unknown     http-wordpress-users.nse
MAC Address: 2E:29:34:08:0D:08 (Unknown)

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

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@kali:~/home/luca
#
```

LA SCANSIONE VERSION DETECTION E COME UNA SCANSIONE TCP CON L'AGGIUNTA DI SPECIFICI TEST PER LA RILEVAZIONE DEI SERVIZI IN ASCOLTO SU UNA PORTA , ANCHE QUESTA SCANSIONE E' MOLTO INVASIVA PERCHE GENERA MOLTO TRAFFICO DI RETE



