Report di Raccolta informazioni - Metasploitable

Giuseppe Gigliotti
gius199874@gmail.com

October 13, 2025

Indice

Target: 192.168.50.101 (metasploitable) **Ambiente:** Kali Linux 2025 → Metasploitable (VirtualBox)

1 Strumenti/Tool utilizzati

Utilizzando la risorsa: https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux abbiamo utilizzato alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable.

1.1 Host Discovery con Nmap

```
nmap -sn -PE 192.168.50.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 18:42 CEST
Nmap scan report for metasploitable (192.168.50.101)
Host is up (0.00059s latency).
MAC Address: 08:00:27:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

1.2 Network Discovery con Netdiscover

```
netdiscover -r 192.168.50.101 # non più utilizzato
```

Output:

```
Currently scanning: Finished!    |   Screen View: Unique Hosts

128 Captured ARP Req/Rep packets, from 5 hosts.    Total size: 7680

 IP            AT MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.50.1   52:54:00:12:35:00    13     780  Unknown vendor
192.168.50.2   52:54:00:12:35:00     1      60  Unknown vendor
192.168.50.3   08:00:27:f1:af:56     1      60  PCS Systemtechnik GmbH
192.168.50.101 08:00:27:c8:54:26     3     180  PCS Systemtechnik GmbH
192.168.50.102 08:00:27:67:de:22   110    6600  PCS Systemtechnik GmbH
```

1.3 CrackMapExec SMB Assessment

```
crackmapexec smb 192.168.50.101 # sostituito con netexec

nxc smb 192.168.50.101
```

Output:

```
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE)
                            (domain:localdomain) (signing:False) (SMBv1:True)
```

1.4 Top 10 Ports Scan

```
nmap 192.168.50.101 --top-ports 10 --open
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 18:46 CEST
Nmap scan report for metasploitable (192.168.50.101)
Host is up (0.00069s latency).
Not shown: 3 closed tcp ports (reset)
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
MAC Address: 08:00:27:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

1.5 Full Port Scan con Service Detection

```
nmap 192.168.50.101 -p- -sV --reason --dns-server ns
```

Output:

```
Nmap scan report for metasploitable (192.168.50.101)
Host is up, received arp-response (0.00027s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC
#100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubun
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/
43134/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
43620/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
48643/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
58915/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, L
Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 168.04 seconds

[... 28 porte totali identificate in 168.04 secondi]
```

1.6 Unicornscan TCP/UDP

```
sudo us -mT -Iv 192.168.50.101:a -r 3000 -R 3
 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
```

Output TCP (completato):

```
TCP open                     ftp[   21]         from 192.168.50.101  ttl 64
TCP open                     ssh[   22]         from 192.168.50.101  ttl 64
TCP open                  telnet[   23]         from 192.168.50.101  ttl 64
[... 30 porte TCP identificate]
sender statistics 1765.5 pps with 196608 packets sent total
listener statistics 196629 packets recieved 0 packets droped and 0 interface drops
```

Output UDP: Fallito per conflitto socket

1.7 SYN Scan con Service Detection

```
nmap -sS -sV -T4 192.168.50.101
```

Output: Identico al comando 1.5 (23 porte principali, 52.82 secondi)

1.8 Hping3 Port Scan

```
sudo hping3 --scan known 192.168.50.101
```

Output:

```
Scanning 192.168.50.101 (192.168.50.101), port known
266 ports to scan, use -V to see all the replies
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http)
[... tutte le porte note elencate come "Not responding"]
```

1.9 Netcat Port Scan

```
sudo nc -nvz 192.168.50.101 1-1024
```

Output:

```
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
[... 12 porte identificate nel range 1-1024]
```

1.10 Netcat Connection Test

```
nc -nv 192.168.50.101 22
```

Output:

```
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

1.11 Service Version Detection

```
nmap -sV 192.168.50.101
```

Output: Identico ai comandi 1.5 e 1.7 (52.51 secondi)

1.12 Metasploit Database Import

```
nmap -sV -oX metasploitable_scan.xml 192.168.50.101

# avviamo il tool metasploit

msfconsole

# dentro la schermata, utilizziamo il comando

db_import metasploitable_scan.xml

# vedremo l'output restituito
```

Output:

```
[] Importing 'Nmap XML' data
[] Import: Parsing with 'Nokogiri v1.14.5'
[] Importing host 192.168.50.101
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/
[*] Successfully imported /home/kali/metasploitable_scan.xml
msf > hosts
Hosts
=====
address         mac                name            os_name  os_flavor  os_sp  purpose
-------         ---                ----            -------  ---------  -----  -------
192.168.50.101  08:00:27:c8:54:2e  metasploitable  Linux                      server
msf > services
Services
========
host            port  proto  name         state  info
----            ----  -----  ----         -----  ----
192.168.50.101  21    tcp    ftp          open   vsftpd 2.3.4
192.168.50.101  22    tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protoco
192.168.50.101  23    tcp    telnet       open   Linux telnetd
192.168.50.101  25    tcp    smtp         open   Postfix smtpd
192.168.50.101  53    tcp    domain       open   ISC BIND 9.4.2
192.168.50.101  80    tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.50.101  111   tcp    rpcbind      open   2 RPC
#100000
192.168.50.101  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORK
192.168.50.101  445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORK
192.168.50.101  512   tcp    exec         open   netkit-rsh rexecd
192.168.50.101  513   tcp    login        open
192.168.50.101  514   tcp    shell        open   Netkit rshd
192.168.50.101  1099  tcp    java-rmi     open   GNU Classpath grmiregistry
192.168.50.101  1524  tcp    bindshell    open   Metasploitable root shell
```

```
192.168.50.101  2049  tcp    nfs          open   2-4 RPC
#100003
192.168.50.101  2121  tcp    ftp          open   ProFTPD 1.3.1
192.168.50.101  3306  tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
192.168.50.101  5432  tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
192.168.50.101  5900  tcp    vnc          open   VNC protocol 3.3
192.168.50.101  6000  tcp    x11          open   access denied
192.168.50.101  6667  tcp    irc          open   UnrealIRCd
192.168.50.101  8009  tcp    ajp13        open   Apache Jserv Protocol v1.3
192.168.50.101  8180  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
[22 servizi importati con versioni complete]
```

1.13 Fragmented Packets Scan

```
nmap -f --mtu=512 192.168.50.101
```

Output:

```
Starting Nmap 7.95 ( [https://nmap.org](https://nmap.org/) ) at 2025-09-14 19:26 CEST
Nmap scan report for metasploitable (192.168.50.101)
Host is up (0.00034s 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:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[... 23 porte identificate in 0.19 secondi]
```

1.14 Masscan con Banner Grabbing

```
masscan 192.168.50.0/24 -p80 --banners --source-ip 192.168.50.101
```

Output:

```
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-09-14 17:27:43 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
```

---

2 RIEPILOGO INFORMAZIONI RACCOLTE

2.1 Informazioni Generali trovate

- **Target IP:** 192.168.50.101
- **Hostname:** metasploitable.localdomain
- **Sistema Operativo:** Linux Ubuntu (identificato come Unix)
- **Virtualizzazione:** Oracle VirtualBox
- **MAC Address:** 08:00:27:C8:54:2E
- **Dominio:** localdomain
- **Workgroup SMB:** WORKGROUP

2.2 Porte e Servizi Identificati

2.2.1 SERVIZI CRITICAMENTE VULNERABILI

Porta	Servizio	Versione	Livello Rischio
1524	**bindshell**	Metasploitable root shell	**CRITICO**
23	**telnet**	Linux telnetd	**ALTO**
512	**exec**	netkit-rsh rexecd	**ALTO**

Porta	Servizio	Versione	Livello Rischio
513	**login**	Berkeley r-service	**ALTO**
514	**shell**	Netkit rshd	**ALTO**

2.2.2 DATABASE ESPOSTI

Porta	Servizio	Versione	Note
3306	MySQL	5.0.51a-3ubuntu5	Database MySQL
5432	PostgreSQL	8.3.0 - 8.3.7	Database PostgreSQL

2.2.3 SERVIZI WEB

Porta	Servizio	Versione	Note
80	HTTP	Apache 2.2.8 (Ubuntu) DAV/2	Server web principale
8180	HTTP	Apache Tomcat/Coyote JSP 1.1	Application server
8009	AJP13	Apache Jserv Protocol v1.3	Connector Tomcat

2.2.4 SERVIZI FILE TRANSFER

Porta	Servizio	Versione	Note
21	FTP	vsftpd 2.3.4	Server FTP primario
2121	FTP	ProFTPD 1.3.1	Server FTP secondario
2049	NFS	2-4 (RPC #100003)	Network File System

2.2.5 SERVIZI DI ACCESSO REMOTO

Porta	Servizio	Versione	Note
22	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Accesso sicuro
5900	VNC	VNC protocol 3.3	Desktop remoto
6000	X11	(access denied)	X Window System

2.2.6 SERVIZI DI COMUNICAZIONE

Porta	Servizio	Versione	Note
25	SMTP	Postfix smtpd	Mail server
6667	IRC	UnrealIRCd	Chat server

Porta	Servizio	Versione	Note
6697	IRC	UnrealIRCd	Chat server SSL

2.2.7 SERVIZI DI SVILUPPO/AMMINISTRAZIONE

Porta	Servizio	Versione	Note
53	DNS	ISC BIND 9.4.2	Name server
111	RPC	2 (RPC #100000)	Remote Procedure Call
139	NetBIOS	Samba smbd 3.X - 4.X	File sharing
445	SMB	Samba smbd 3.X - 4.X	File sharing
1099	Java-RMI	GNU Classpath grmiregistry	Java Remote Method
3632	distccd	distccd v1 (GNU) 4.2.4	Distributed compiler
8787	Ruby DRb	Ruby 1.8 DRb RMI	Ruby distributed objects

2.3 Vulnerabilità Identificate

2.3.1 CRITICHE

1. **Backdoor attiva porta 1524** - Accesso root diretto
2. **Telnet non cifrato** - Credenziali in chiaro
3. **Berkeley r-services** (512-514) - Protocolli obsoleti e non sicuri
4. **SMBv1 abilitato** - Protocollo vulnerabile
5. **SMB signing disabilitato** - Possibili attacchi MITM

2.3.2 ALTE

1. **Versioni software obsolete** - Molti servizi datati
2. **Database esposti** senza autenticazione apparente
3. **VNC senza autenticazione** visibile
4. **FTP vsftpd 2.3.4** - Versione con backdoor nota
5. **Multiple servizi esposti** - Attack surface molto ampia

2.3.3 MEDIE

1. **Apache 2.2.8** - Versione datata con CVE note
2. **OpenSSH 4.7p1** - Versione vecchia
3. **Bind 9.4.2** - DNS server datato
