

Security Testing Report

Pace Massimiliano - efmpas@gmail.com

W11 D1

Sommario:

Scansione :

OS

Fingerprint

SynScan

Tcp connect

Version detection

Descrizione lavoro svolto

Eseguito un set di scansioni Nmap per identificare sistema operativo, porte aperte e versioni dei servizi su Metasploitable. Sono state identificate diverse porte e servizi vulnerabili (FTP, SSH, HTTP, MySQL, ecc.). Di seguito i dettagli tecnici e le raccomandazioni operative per la mitigazione.

Target

Virtual Machine Metasploitable	ip 192.168.50.101
--------------------------------	-------------------

Metodologia e comandi utilizzati

OS fingerprint	<code>sudo nmap -O 192.168.50.101</code>
SYN Scan (stealth)	<code>sudo nmap -sS -p- 192.168.50.101</code>
TCP connect scan	<code>sudo nmap -sT -p 1-65535 192.168.50.101</code>
Version detection	<code>sudo nmap -sV -p 21,22,80,3306 192.168.50.101</code>

* in TCP connect abbiamo selezionato un range di porte da 1 a 65535

* in Version detection sono state scelte la porta 21,22,80,3306

Risultati ottenuti

(sudo nmap -O 192.168.50.101)

- Comando: scansione standard con rilevamento OS (-O).
- Risultati:
 - Tante porte aperte: 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 80 (http), 139 (netbios-ssn), 445 (microsoft-ds), 3306 (mysql), ecc.
 - OS rilevato: **Linux 2.6.x**.
- Tempo di scansione: ~17 secondi.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ sudo nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 13:47 CEST
Nmap scan report for 192.168.50.101
Host is up (0.014s 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:DA:D2:25 (PCS Systemtechnik/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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.05 seconds

(kali@kali)~[~/Desktop]
$
```

Risultati ottenuti

(sudo nmap -sT -p 1-65535 192.168.50.101)

- Comando: scansione di **tutte le 65535 porte TCP**.
- Risultati:
 - Conferma le stesse porte aperte già viste prima.
 - Mostra che le altre sono “conn-refused”.
- Tempo di scansione: ~298 secondi (più lungo perché ha controllato ogni porta).

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ sudo nmap -sT -p 1-65535 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 13:51 CEST
Nmap scan report for 192.168.50.101
Host is up (0.021s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35618/tcp open  unknown
47498/tcp open  unknown
49671/tcp open  unknown
56183/tcp open  unknown
MAC Address: 08:00:27:DA:D2:25 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 298.67 seconds

(kali@kali)-[~/Desktop]
└─$
```

Risultati ottenuti

sudo nmap -sS -p- 192.168.50.101 (SYN scan / half-open scan su tutte le porte o su un range).

Effetto/interpretazione corretta:

- È una scansione **stealth** (SYN) che invia SYN e valuta le risposte (SYN/ACK = open, RST = closed).
- Fornisce un elenco di porte **aperte** più velocemente e con meno possibilità di completare connessioni TCP complete rispetto a **-sT**.
- Può comunque essere registrata da IDS/Firewall (non è invisibile), ma tende a risultare meno rumorosa sui log delle applicazioni rispetto a scansioni full connect.
- Tempo di scansione (nello screenshot) ~73s — compatibile con scansione SYN su molte porte.

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ sudo nmap -sS -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 13:49 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0034s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35618/tcp open  unknown
47498/tcp open  unknown
49671/tcp open  unknown
56183/tcp open  unknown
MAC Address: 08:00:27:DA:D2:25 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 73.58 seconds

(kali@kali)-[~/Desktop]
└─$
```


Risultati ottenuti

```
sudo nmap -sV -p 21,22,80,3306 192.168.50.101
```

(scansione mirata con detection delle versioni del servizio, `-sV`, sulle porte specificate).

output mostra banner/versioni dettagliate (vsftpd 2.3.4, OpenSSH 4.7p1, Apache 2.2.8, MySQL 5.0.51a) — tipico risultato di `-sV`.

- È una scansione **di versione** che interroga le porte selezionate per ottenere banner e fingerprinting di servizi.
- Non è una semplice scansione di porte: fornisce informazioni utili per ricerca di CVE/PoC.
- Tempo di scansione più breve rispetto a `-p-` ma più informativo su quelle porte.

```
kali@kali: ~/Desktop
File Actions Edit View Help
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
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
35618/tcp open unknown
47498/tcp open unknown
49671/tcp open unknown
56183/tcp open unknown
MAC Address: 08:00:27:DA:D2:25 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 298.67 seconds

(kali@kali)-[~/Desktop]
$ sudo nmap -sV -p 21,22,80,3306 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 13:58 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0068s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
3306/tcp  open  mysql?

MAC Address: 08:00:27:DA:D2:25 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: 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 173.71 seconds

(kali@kali)-[~/Desktop]
$
```

Report di scansione Nmap — 192.168.50.101

Autore: Pace Massimiliano

Data scansione: 2025-09-20

Host target: 192.168.50.101

MAC: 08:00:27:DA:D2:25 (Oracle VirtualBox virtual NIC)

OS stimato: Linux 2.6.x (risultato Nmap -O)

Note ambiente: Kali Linux in VirtualBox (scanner). L'host target e' una macchina vulnerabile/di laboratorio

Sintesi

È stata eseguita una serie di scansioni Nmap (scansione OS, ping/host discovery, scansione porte singole e scansione 1–65535). L'host risponde ed espone numerosi servizi TCP (sia su porte conosciute sia su alte porte non identificate). Alcuni servizi espongono versioni datate note per vulnerabilità. Il livello di rischio complessivo è **Alto** se l'host è raggiungibile da rete non fidata, dato il numero e la natura dei servizi attivi (Telnet, FTP vulnerabile, MySQL vecchio, Apache datato, servizi RPC/SMB).

Evidenze chiave

- Banner e versioni ottenute: vsftpd 2.3.4, OpenSSH 4.7p1, Apache 2.2.8, MySQL 5.0.51a. Versioni vecchie con CVE noti.
- OS fingerprint: Linux 2.6.x (compatibile con host vulnerabile).
- MAC address VirtualBox: indica ambiente virtuale.
- Scansione a tutta porta (~1–65535) conferma numerose porte aperte e molte risposte “conn-refused” o “reset” per porte chiuse.
- Scansione mirata di porte specifiche ha prodotto informazioni di versione utili per enumerazione vulnerabilità.

Porte e servizi identificati

- 21/tcp — ftp — **vsftpd 2.3.4**
- 22/tcp — ssh — **OpenSSH 4.7p1 Debian**
- 23/tcp — telnet
- 25/tcp — smtp
- 53/tcp — domain (DNS)
- 80/tcp — http — **Apache httpd 2.2.8** (Ubuntu/DAV/2)
- 111/tcp — rpcbind
- 139/tcp — netbios-ssn
- 445/tcp — microsoft-ds (SMB)
- 512/tcp — exec
- 513/tcp — login
- 514/tcp — shell
- 1099/tcp — rmiregistry
- 1524/tcp — ingreslock (porta associata a backdoor in Metasploitable)
- 2049/tcp — nfs
- 2121/tcp — ccproxy-ftp
- 3306/tcp — mysql — **MySQL** (version mostrata in uno screenshot: 5.0.51a)
- 3632/tcp — distccd
- 5432/tcp — postgresql
- 5900/tcp — vnc
- 6000/tcp — X11
- 6667/tcp — irc
- 8009/tcp — ajp13
- 8180/tcp — (unknown / web app)
- 8787/tcp — msgsrv r
- Porte alte: 35618, 47498, 49671, 56183 (unknown/open)

Valutazione rischio / Priorità

Attribuisco priorità **alta** a questi elementi:

1. **Telnet (23/tcp)** — traffico in chiaro: rischio compromissione credenziali.
2. **FTP (vsftpd 2.3.4)** — versione vulnerabile (nota per exploit in passato, es. backdoor).
3. **Apache 2.2.8** — versione datata, potenziali vulnerabilità di directory traversal, RCE tramite moduli datati.
4. **MySQL 5.0.x** — versioni vecchie con potenziali escalation/SQL injection facilità.
5. **SMB (139/445)** — esposizione di servizi di file sharing: possibile divulgazione di info sensibili.
6. **RPC/exec/login/shell (512–514)** — servizi obsoleti per login remoto, pericolosi.
7. **Altri servizi (NFS, distccd, vnc, ajp, msgsrvr)** — aumentano superficie d'attacco e possibilità di exploit.

Raccomandazioni immediate

Azioni immediate

- Isolare la macchina dalla rete (mettere in subnet di laboratorio o disconnettere).
- Disabilitare servizi non necessari: Telnet, FTP, rsh/executables remoti (512/513/514), rmiregistry, ccproxy, distccd, vnc se non richiesto.
- Configurare firewall (host-based + network) per limitare accesso alle porte critiche (solo IP amministrativi).
- Cambiare tutte le password/credenziali locali se credenziali deboli possibili.
- Abilitare logging e monitoraggio (fail2ban/IDS).