

Security Testing Report

TEST SCANSIONE HOST METASPLOITABLE

Pace Massimiliano - efmpas@gmail.com

17/09/2025

CONTENUTO

Sommario:

- utilizzo del tool Nmap per la scansione della VM Meta
- valutazione rischi

Descrizione lavoro svolto

Analizzeremo come la VM si comporta con il tool Nmap .
Utilizzeremo 11 comandi Nmap per ottenere piu' informazioni possibili

Target

Metasploitable ip : 192.168.50.101

Vulnerabilità - se presenti

Metasploitable è una macchina virtuale intenzionalmente vulnerabile progettata per scopi didattici e per testare strumenti e tecniche di penetration testing in ambiente isolato. Contiene numerosi servizi e applicazioni configurati con vulnerabilità note (vecchie versioni di server web, database, servizi di rete, ecc.), in modo da permettere agli studenti e ai security tester di esercitarsi nell'enumerazione, nello sfruttamento controllato e nella redazione di report senza rischiare sistemi di produzione.

Metodi usati e risultati ottenuti

Comando:

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

Spiegazione: fa un **ping scan** (**-sn**) con pacchetti **ICMP Echo** (**-PE**).

Risultato: conferma che l'host **192.168.50.101** è **up** (attivo).

Qui non scansiona porte, controlla solo se il target risponde al ping.

Comando :

- strumento: **arp-scan** (non nmap).
- Risultato: hai rilevato l'host **192.168.50.101** con MAC address **08:00:27:DA:D2:25** (VirtualBox). Serve per mappare la rete locale e trovare i dispositivi connessi.
- Comando:

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

- Spiegazione: scansiona le **10 porte più comuni** e mostra solo quelle **aperte**.
- Risultato: host attivo con queste porte aperte:
 - 21 (ftp)
 - 22 (ssh)
 - 23 (telnet)
 - 25 (smtp)
 - 80 (http)
 - 139 (netbios-ssn)
 - 445 (microsoft-ds)

Queste sono tipiche di una macchina vulnerabile come **Metasploitable**.

- Comando:

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

- Opzioni:

- **-p-** → tutte le 65535 porte

- **-sV** → rileva la versione dei servizi

- **--reason** → mostra il motivo per cui una porta è marcata open/closed

- **--dns-server**

Risultato: warning → “Unable to determine any DNS servers”.

La scansione comunque parte ma senza DNS reverse lookup.

- Strumento: **hping3**

- Comando:

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

Risultato: mostra tantissime porte conosciute (risposte da hping).

Conferma che molte porte su Metasploitable sono raggiungibili.

Strumento: **netcat (nc)**

- Comando:

```
nc -nv 192.168.50.101 22
```

- Risultato: connessione su porta 22 riuscita → SSH aperto.

Banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntul

Ottima informazione: puoi sapere la **versione del servizio SSH**.

- Comando:

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

- Opzioni:

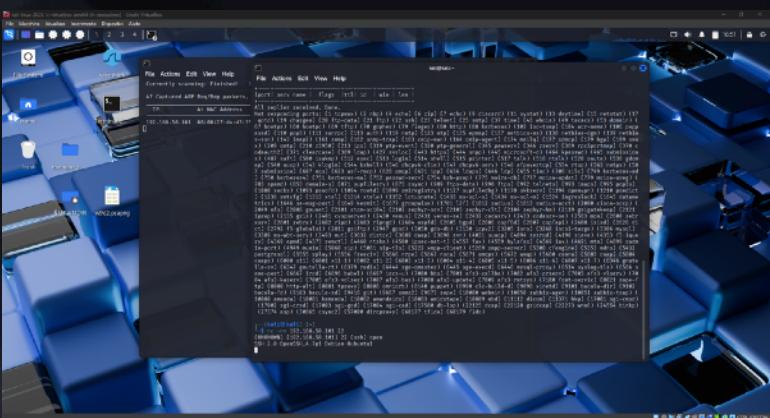
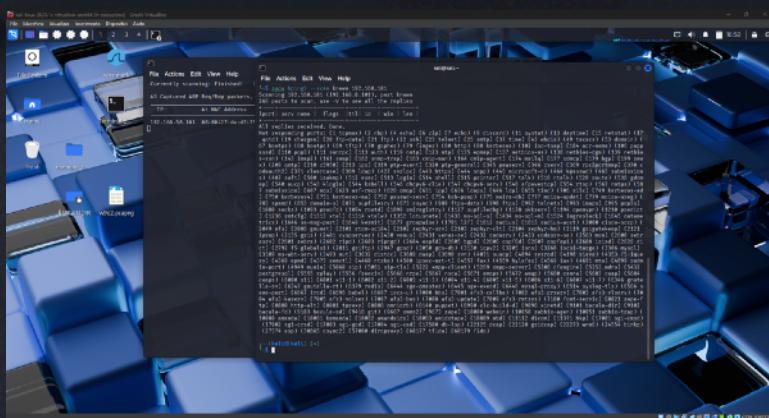
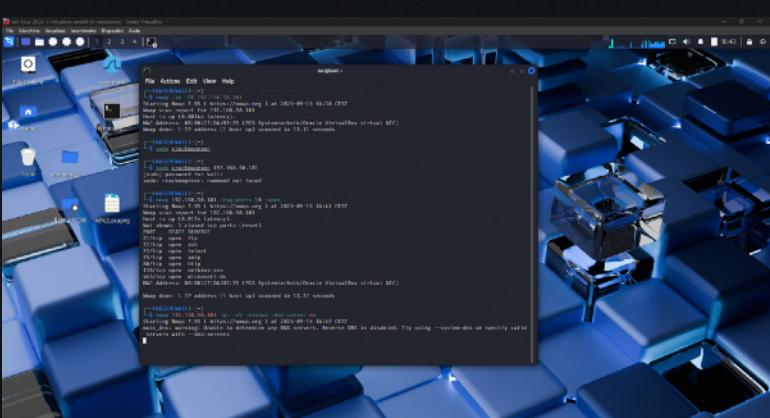
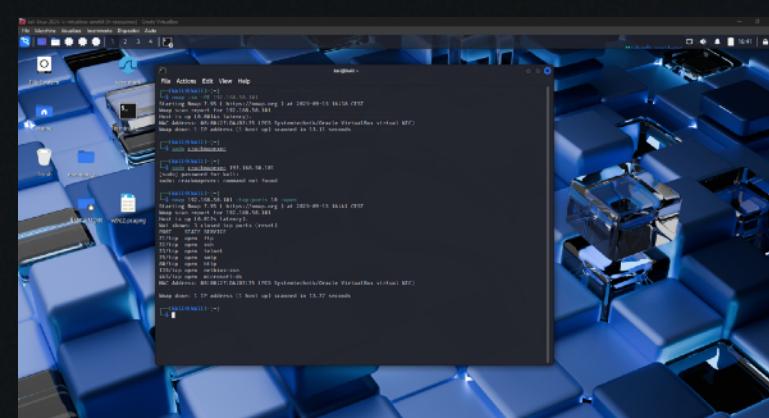
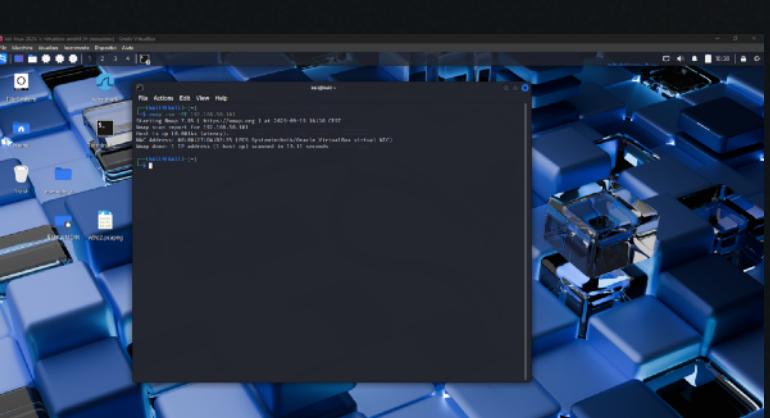
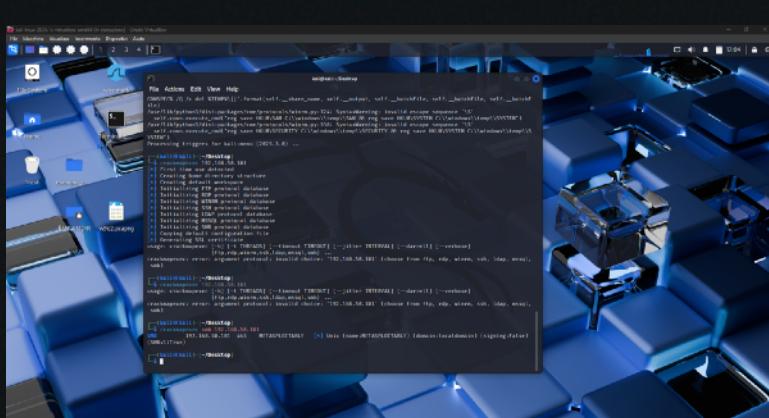
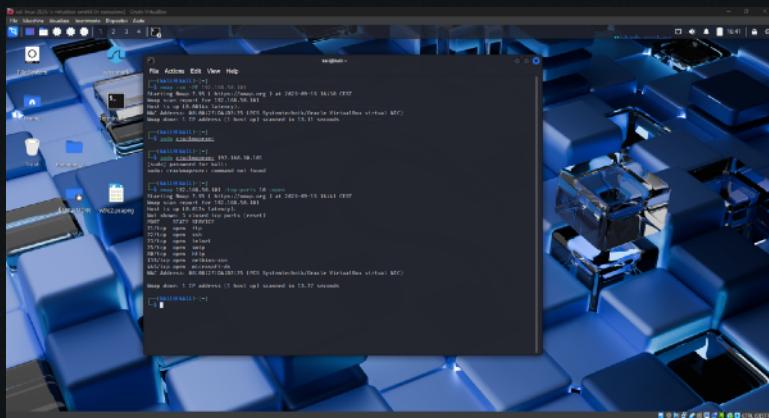
- **-f** → frammenta i pacchetti per bypassare firewall/IDS

- **--mtu 512** → imposta dimensione massima dei pacchetti

- Risultato: trovate molte porte aperte (21, 22, 23, 25, 53, 80, 139, 445, 3306, 5432, 5900, 6000, 8009, 8180...).

È una scansione “evasiva” che cerca di confondere sistemi di difesa.

Documentazione fotografica



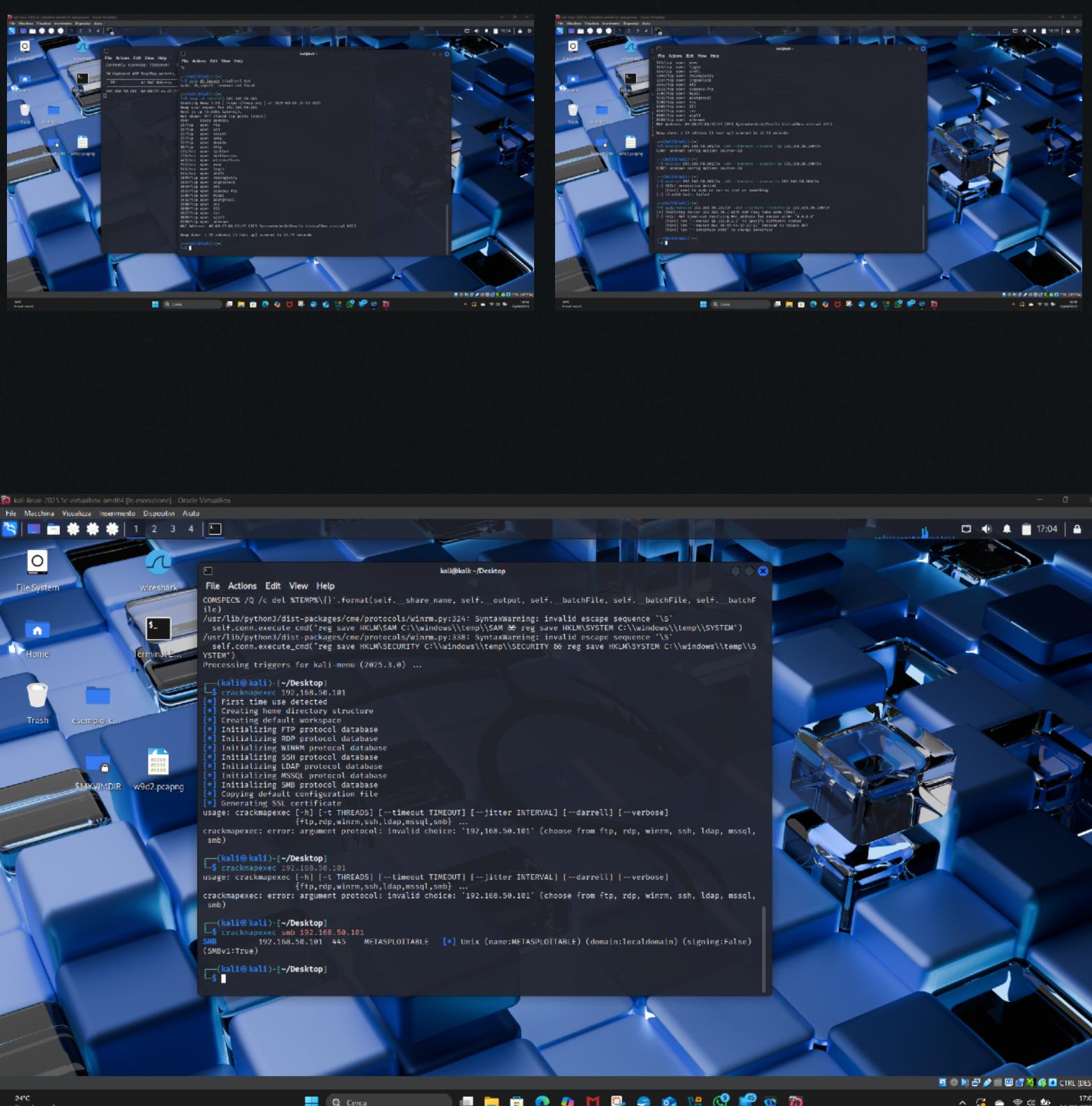


Tabella riepilogativa

Comando (esempio)	Cosa fa / perché lo hai usato	Opzioni chiave (spiegate)	Output osservato dalle tue foto
arp-scan / arp-scan -l (o arp-scan integrato nello screenshot)	Scansione ARP per scoprire host nella LAN (livello 2). Ottimo per trovare MAC e IP attivi su rete locale.	N/A (tool ARP)	Ha rivelato 192.168.50.101 con MAC 08:00:27:DA:D2:25 (VirtualBox).
nmap -sn -PE 192.168.50.101	Ping scan: verifica se l'host è up senza scansionare porte. -PE usa ICMP Echo.	-sn (no port scan), -PE(ICMP Echo)	Host up; conferma presenza di 192.168.50.101.
nmap 192.168.50.101 --top-ports 10 --open	Scansiona le 10 porte più comuni e mostra solo quelle aperte (veloce, orientata a trovare servizi comuni).	--top-ports 10, --open	Porte aperte trovate: 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 80 (http), 139 (netbios-ssn), 445 (microsoft-ds) (tipiche di Metasploitable).
nmap -p- -sV --reason 192.168.50.101	Scansione di tutte le porte con service/version detection; --reason mostra perché sono state classificate.	-p- (tutte le porte), -sV(version detection), --reason	ricevuto warning su DNS ma nmap ha iniziato la scansione. (Reverse DNS disabilitato)
sudo hping3 --scan known 192.168.50.101 (o simile)	Uso di hping3 per inviare pacchetti TCP e vedere risposte — utile per fingerprinting e scan personalizzati	--scan (scan note), opzioni TCP personalizzate	Moltissime risposte elencate (conferma che molte porte sono raggiungibili).
nc -nv 192.168.50.101 22	Netcat per testare connessione TCP e leggere banner; utile per banner grabbing.	-n no DNS, -v verbose	Connessione aperta su 22 → banner SSH-2.0-OpenSSH_4.7p1 ... (versione SSH visibile).
nmap -f --mtu 512 192.168.50.101	Scan con frammentazione pacchetti (-f) e MTU impostato per tentare di eludere IDS/firewall.	-f (fragment), --mtu 512	Scansione ha mostrato molte porte aperte: oltre a quelle sopra anche 111, 512, 513, 1524, 2049, 3306, 5432, 5900, 6000, 6667, 8009,
masscan 192.168.50.101 -p1-65535 --rate 1000(suggerito)	Scansione ultra-veloce porte su larga scala (masscan vs nmap).	-p1-65535(range), --rate(pps)	
crackmapexec smb 192.168.50.101	Tool di enumerazione/attacco SMB (hai provato, ha risposto con smb info).	crackmap exec smb <ip>	CrackMapExec ha mostrato SMB 192.168.50.101:445 METASPLOITABLE (host riconosciuto come Metasploitable/SMBv1).
nmap -f -mtu=512 -sV -sC -A -p <ports> 192.168.50.101	Comando combinato per rilevare versioni, eseguire script di default e fingerprinting avanzato.	-sV, -sC, -A, -p	— (da eseguire come passo successivo)

Conclusione

192.168.50.101 è una macchina VM Metasploitable con moltissimi servizi legacy e versioni datate — risultano numerose porte e servizi aperti (SMB, FTP, Telnet, SSH, DB, web, VNC, NFS, ecc.), rendendola **ottima per esercizi di enumerazione e exploitation** in ambiente controllato

Valutazione delle vulnerabilità probabili (priorità)

1. SMB (445) — alta priorità

- SMB aperto e macchina Metasploitable → probabile SMBv1 e condivisioni/credenziali deboli. Strumenti: enum4linux, smbclient, smbmap, crackmapexec.

2. Telnet / FTP (23,21) — alta

- Servizi non criptati, probabile uso di credenziali predefinite anonime.

3. SSH (22) — media/alto

- Banner mostra versione vecchia (OpenSSH_4.7). Verificare user enumeration, brute-force in lab, chiavi deboli.

4. Web apps (80,8180,8009) — media

- Controllare applicazioni web vulnerabili (directory bruteforce, file upload, XSS, RCE).

5. DB (3306 mysql, 5432 postgres) — media

- Possibile accesso senza password o con credenziali di default.

6. NFS / rpcbind / rlogin / backdoors (111,2049,512,513,1524) — alta/critica per Metasploitable (accessi remoti, root escalation possibili).

7. VNC/X11 (5900,6000) — media: potenziale accesso remoto a desktop.

8. Servizi legacy (irc / rmiregistry / ajp / etc.) — vario rischio, può offrire exploit noti su VM didattiche.