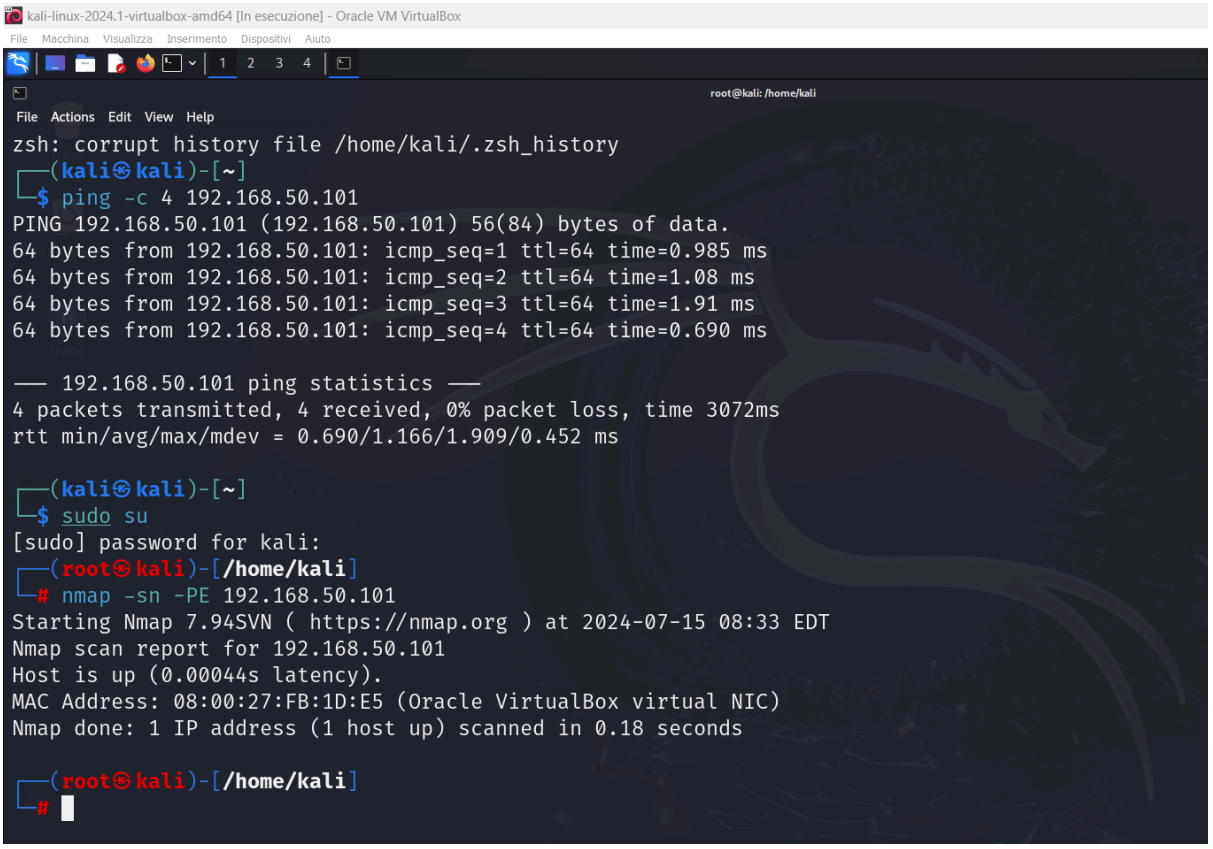
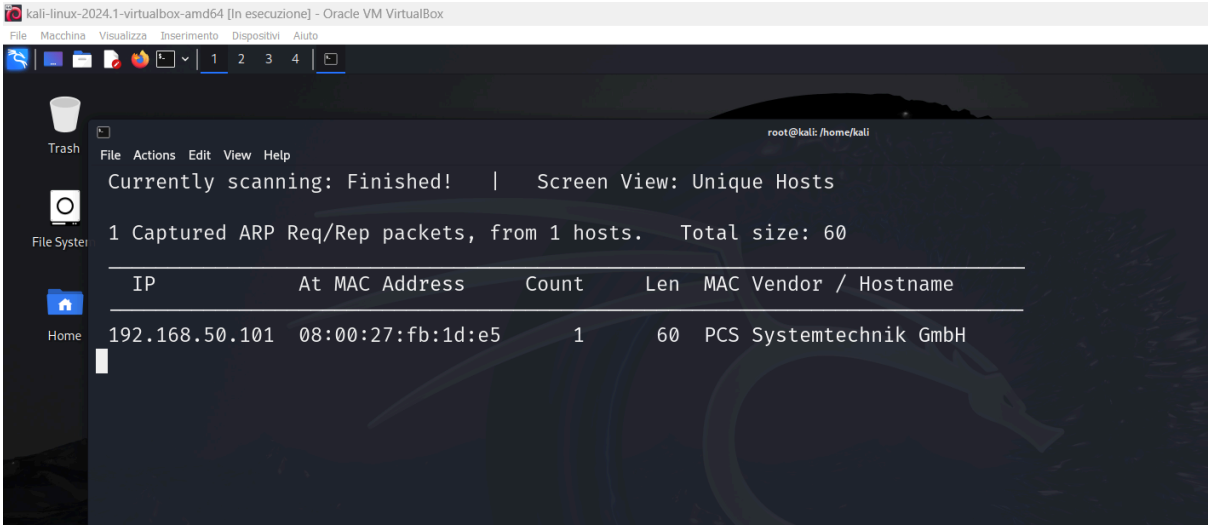
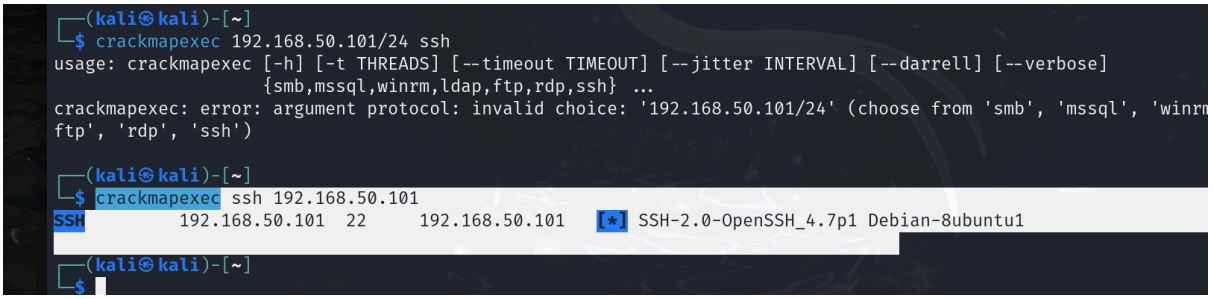


netdiscover -r 192.168.50.101

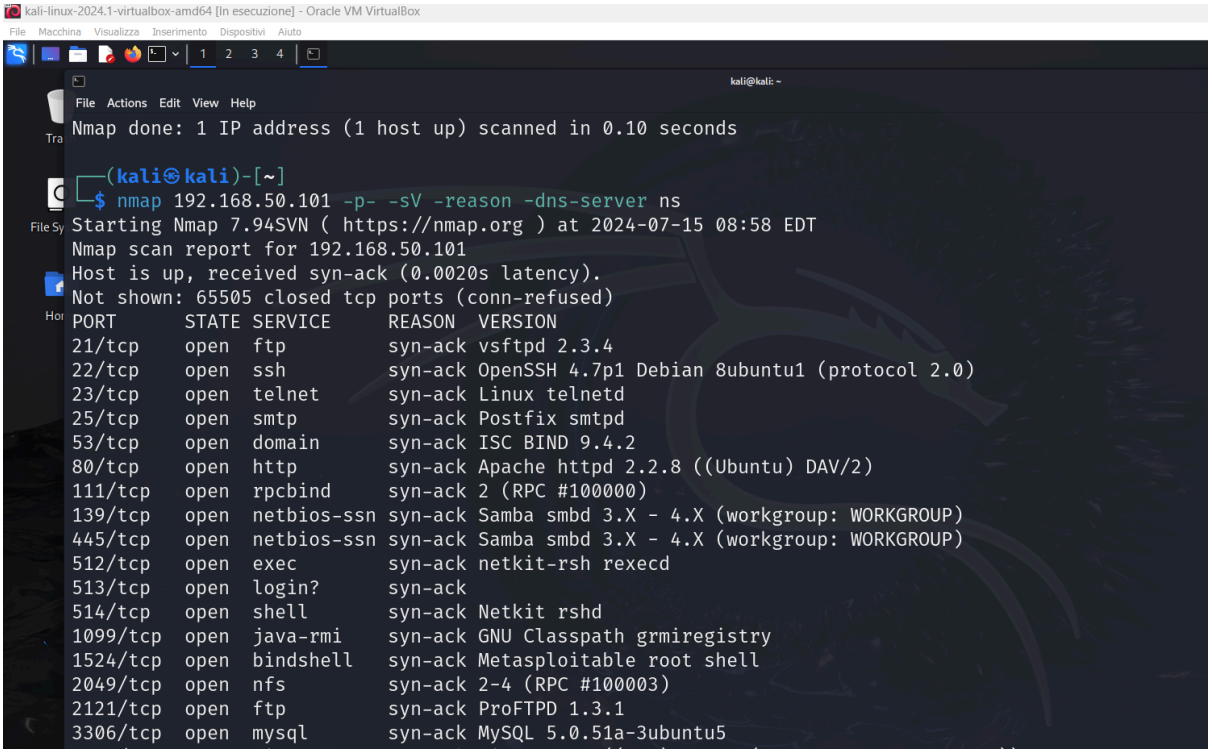


Crackmapsense



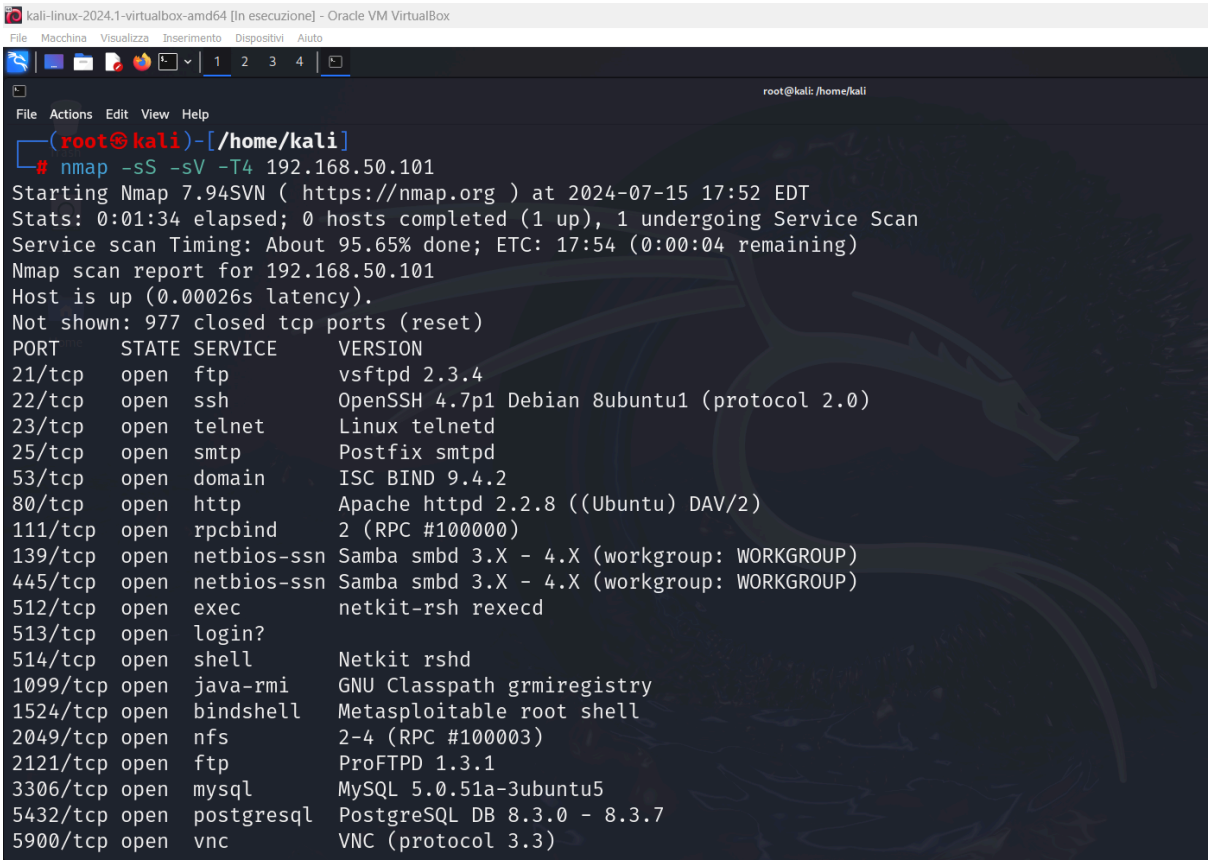
Nmap top port - “Migliori” 10 porte aperte

Lettura informazioni DNS



Unicornscan

NMAP formato ridotto, con versione servizi

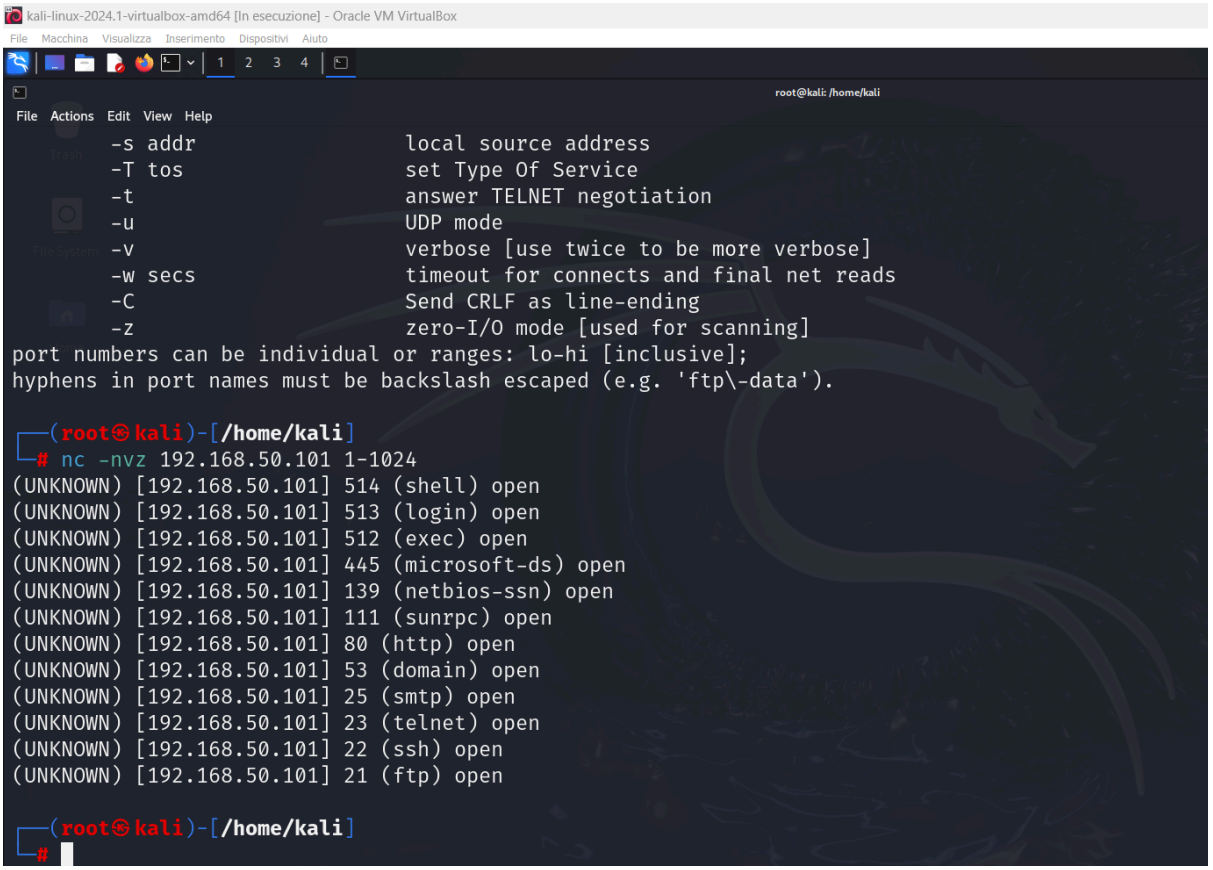



```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
MAC Address: 08:00:27:FB:1D:E5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.99 seconds
```

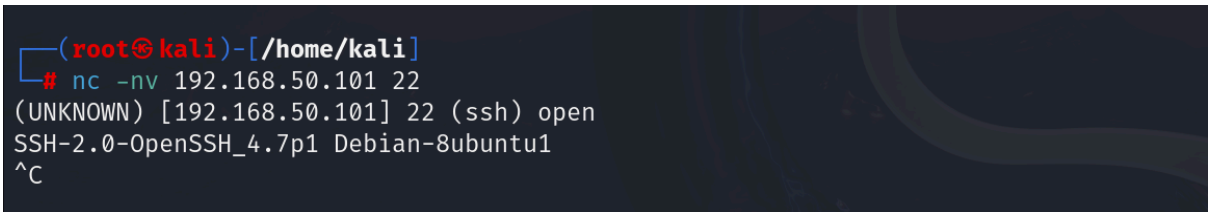
Hping3

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -scan known 192.168.50.101
hping3: option requires an argument -- s
Try hping3 --help

┌──(root㉿kali)-[/home/kali]
└─# hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), 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 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

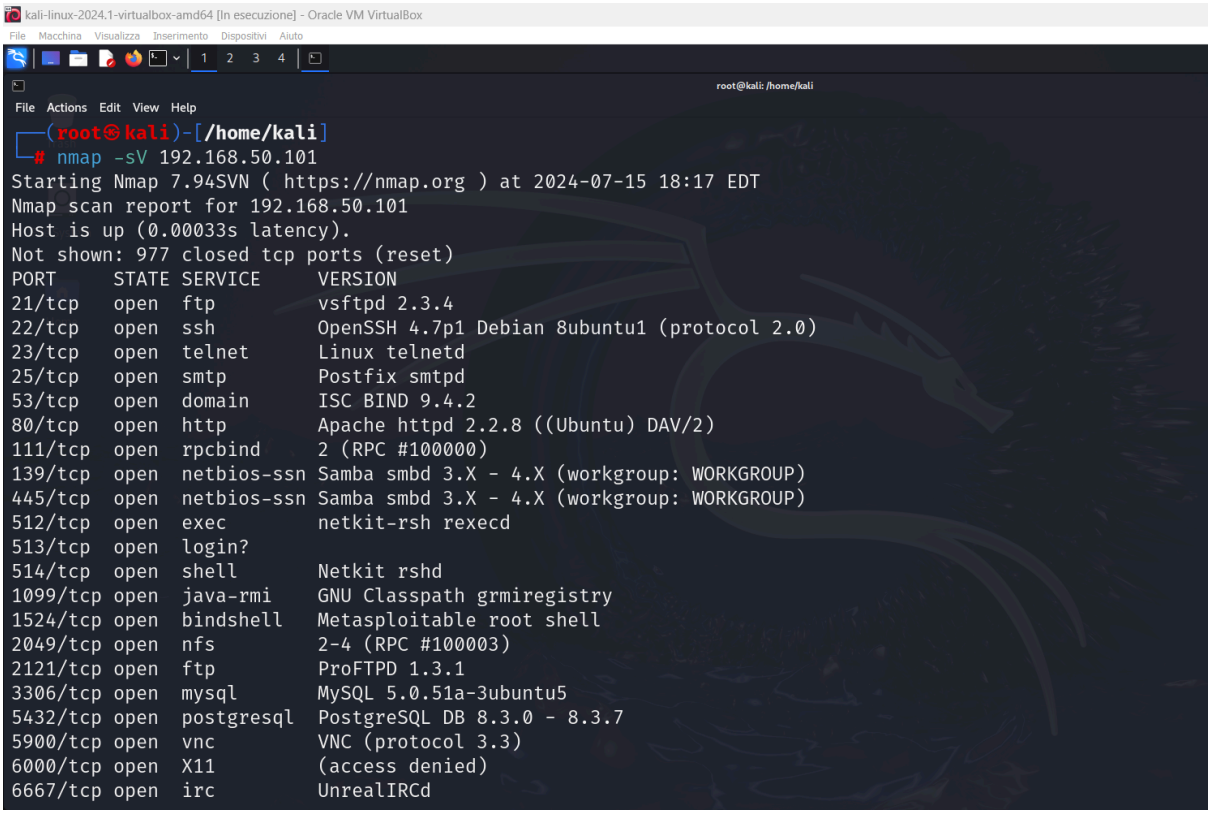
Netcat con scansione dettagliata e stato porte



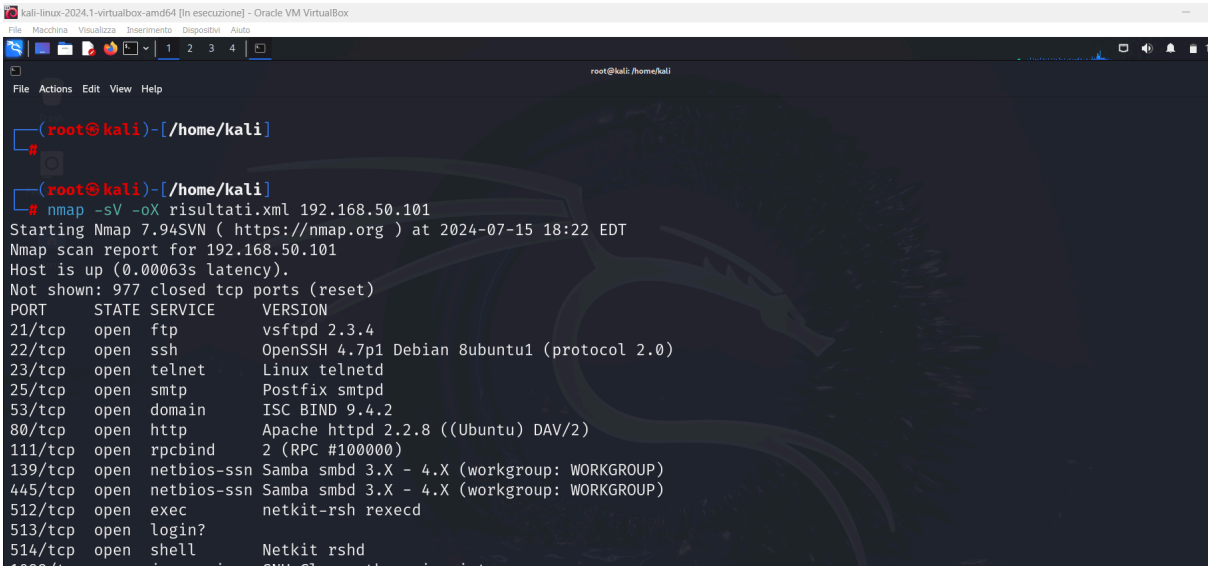
NETCAT in ascolto



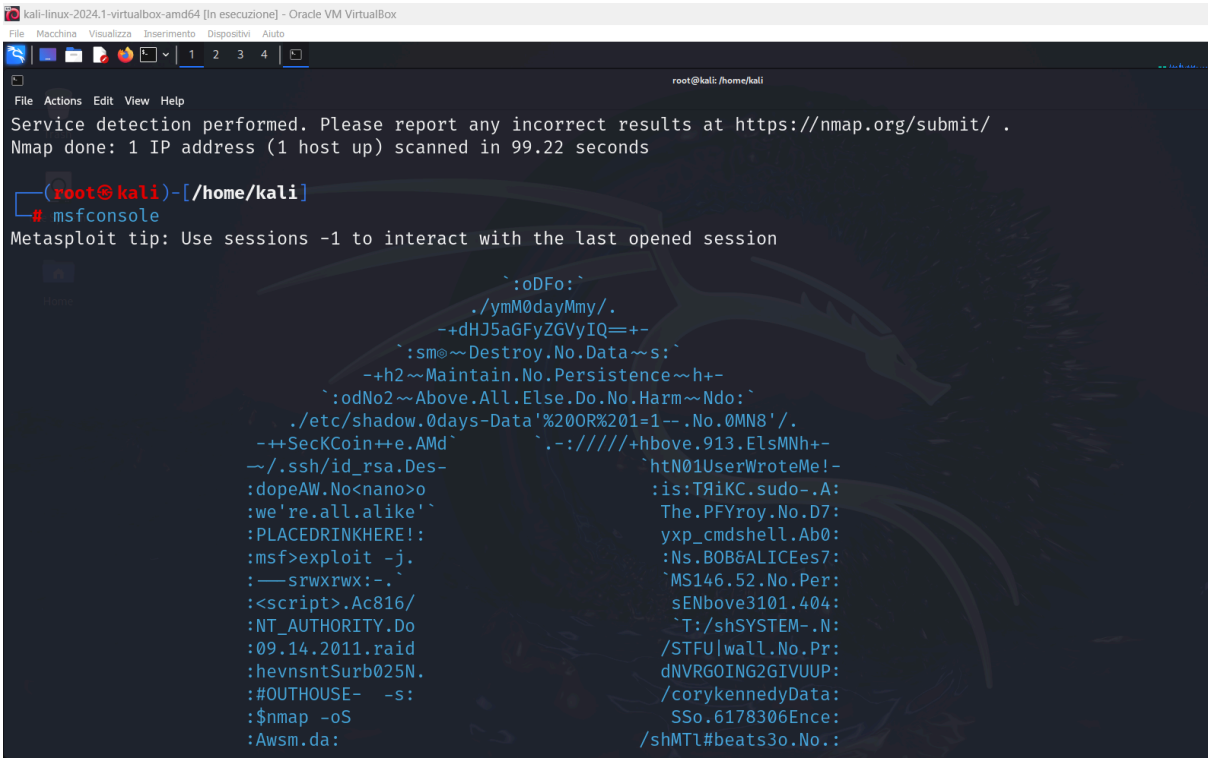
NMAP con versione servizi



Salvataggio su file XML



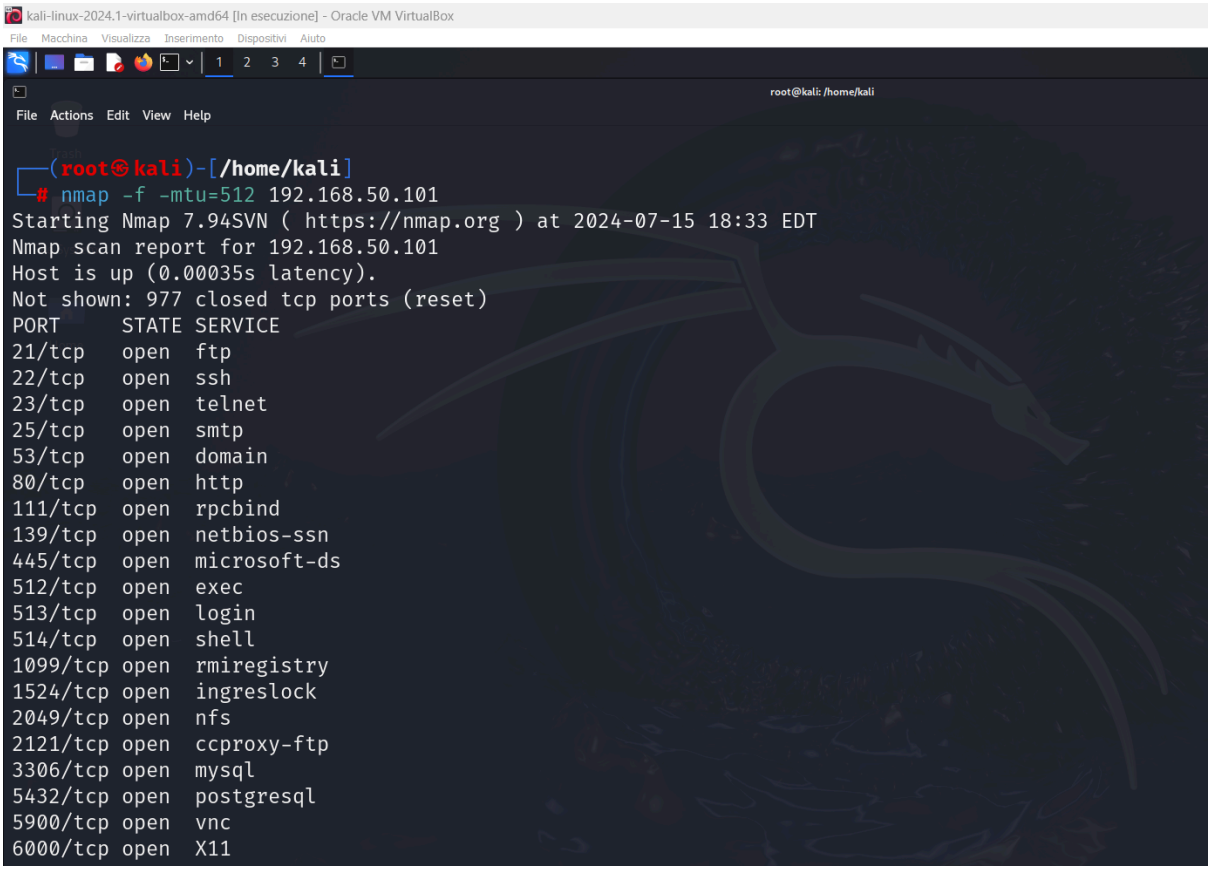
_faccio partire Msfconsole



_non sono connesso al database

```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] postgresql selected, no connection
msf6 > db_import risultati.xml
[-] Database not connected
msf6 > db_import ./risultati.xml
[-] Database not connected
msf6 > db_status
[*] postgresql selected, no connection
msf6 > db_connect
[-] A URL or saved data service name is required.
```

Bypassare i filtri del FIREWALL rimpicciolendo i pacchetti



Report 192.168.50.101

- **Indirizzo IP**: 192.168.50.101
- **MAC Address**: 08:00:27:FB:1D
  (Oracle VirtualBox virtual NIC)
- **Sistema Operativo**: Unix, Linux
- **Nome Host**: metasploitable.localdomain, irc.Metasploitable.LAN

PORTE INTERESSANTI

Porta	Stato	Servizio	Versione
21/tcp	Open	ftp	vsftpd 2.3.4
22/tcp	Open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
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 rexecd
513/tcp	Open	login?	-
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	Apache Jserv (Protocol v1.3)
8180/tcp	Open	http	Apache Tomcat/Coyote JSP engine 1.1

Le porte più comuni si espongono tutte ad exploit noti per l’obsolescenza delle versioni dei servizi in uso.