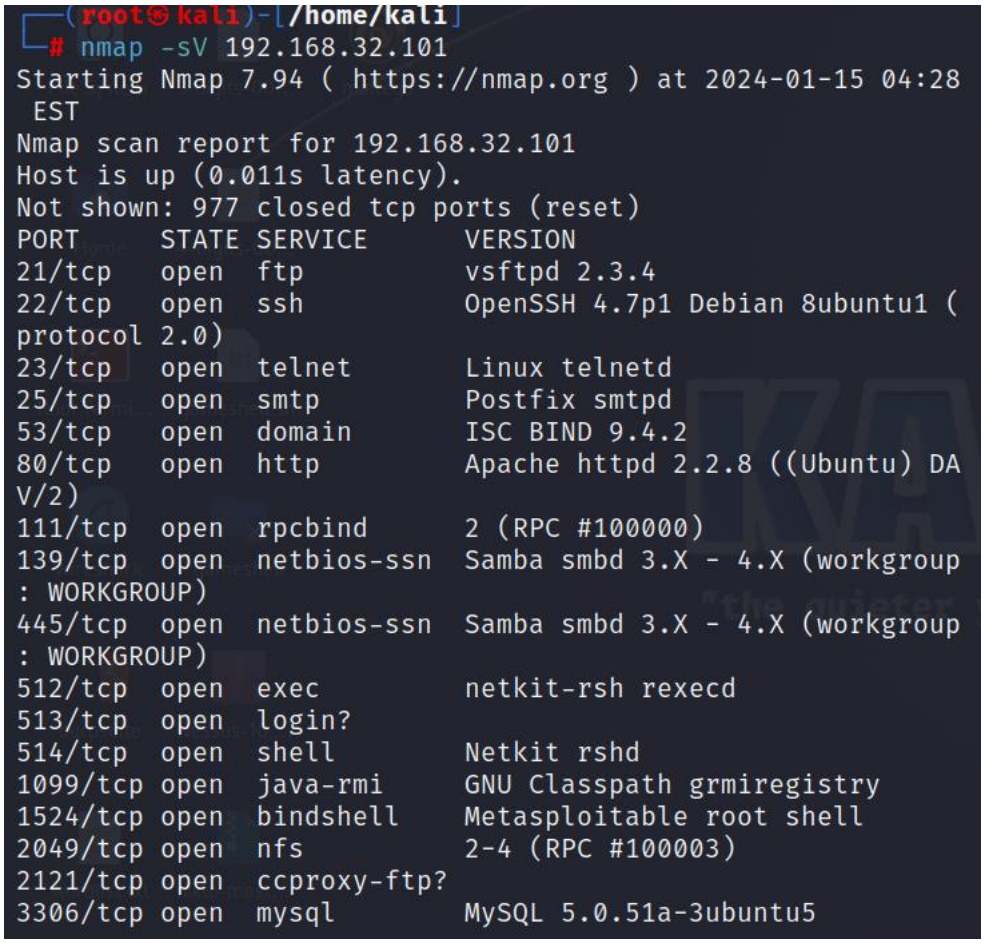
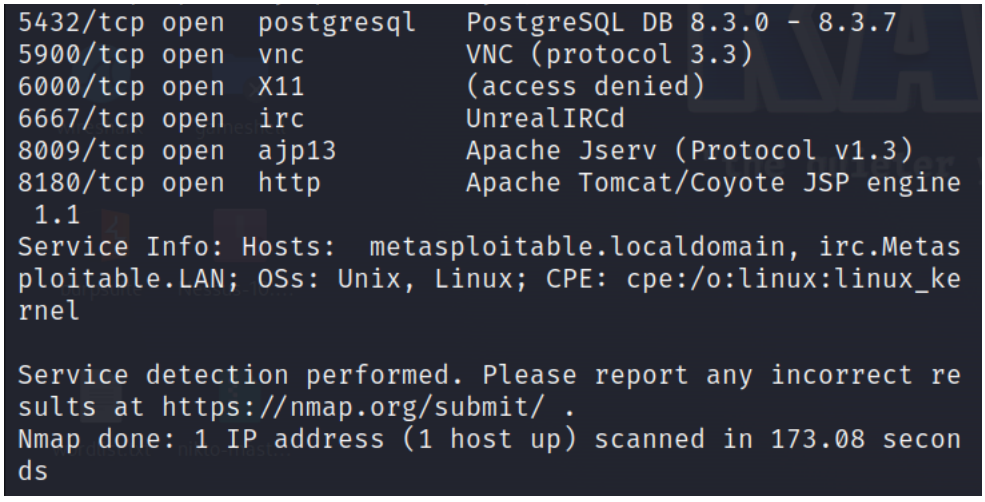
Utilizzo del comando nmap -sV



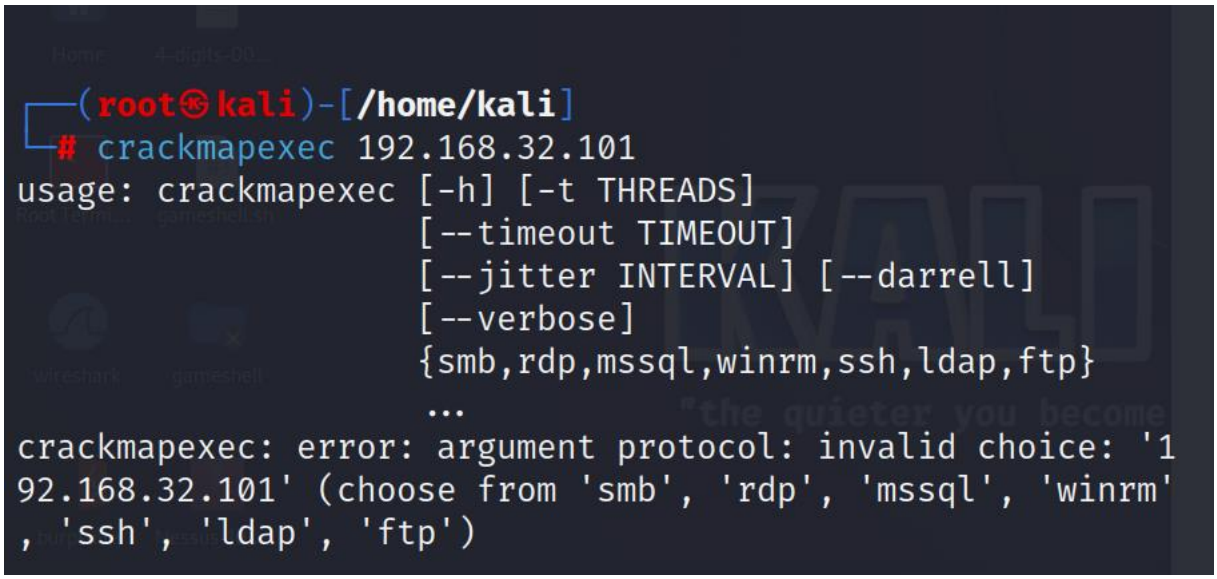
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 04:28
 EST
Nmap scan report for 192.168.32.101
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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) DA
V/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  ccproxy-ftp?
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```



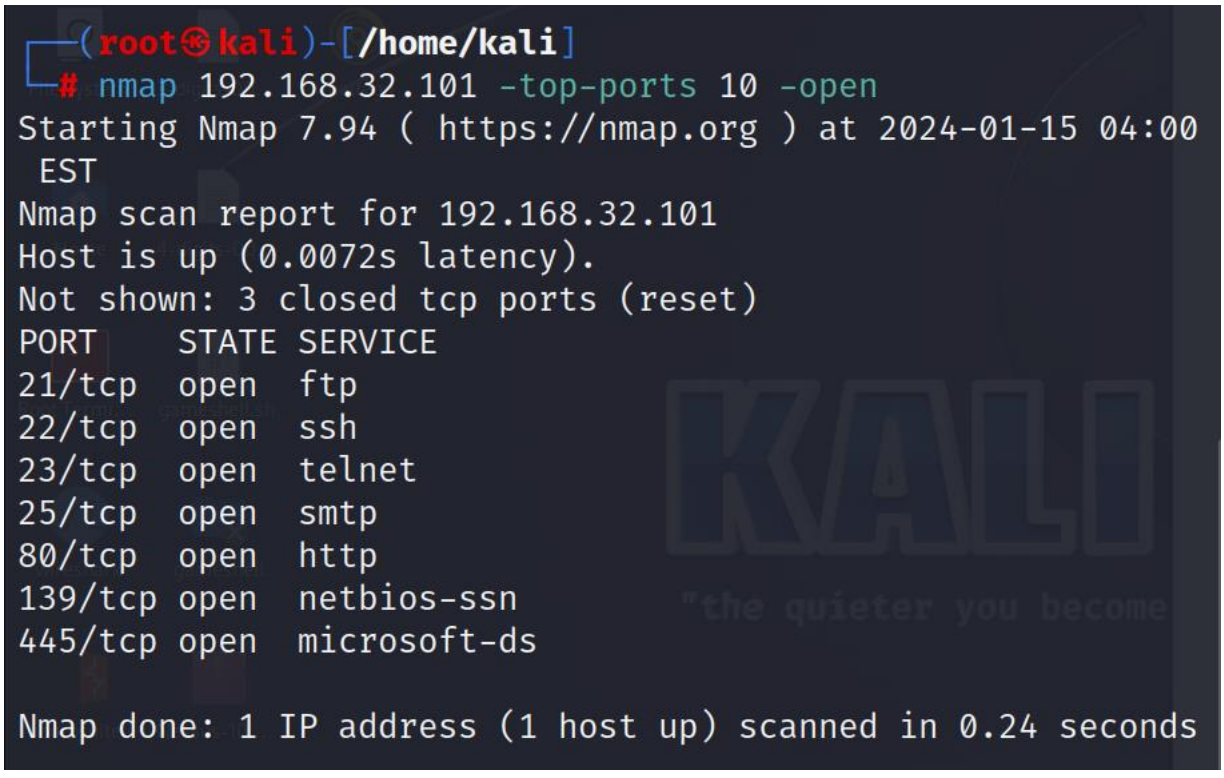
```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine
 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metas
ploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel

Service detection performed. Please report any incorrect re
sults at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.08 secon
ds
```

L'utilizzo del seguente comando ha permesso di evidenziare tutte le porte aperte in protocollo tcp su metasploit

Il comando crackmapexec no



Il comando nmap -top-ports 10 -open ha evidenziato 7 porte con protocollo tcp su 10, fra le porte aperte risultano aperte quella della ssh, telnet, netbios.



Con il comando netdiscover -r è stato messo in chiaro l'IP, Gateway e MAC address di metasploit.

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

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.32.1    08:00:27:e1:d1:55      1      60  PCS Systemtechnik GmbH
192.168.32.101  08:00:27:6e:a9:f1      1      60  PCS Systemtechnik GmbH
```

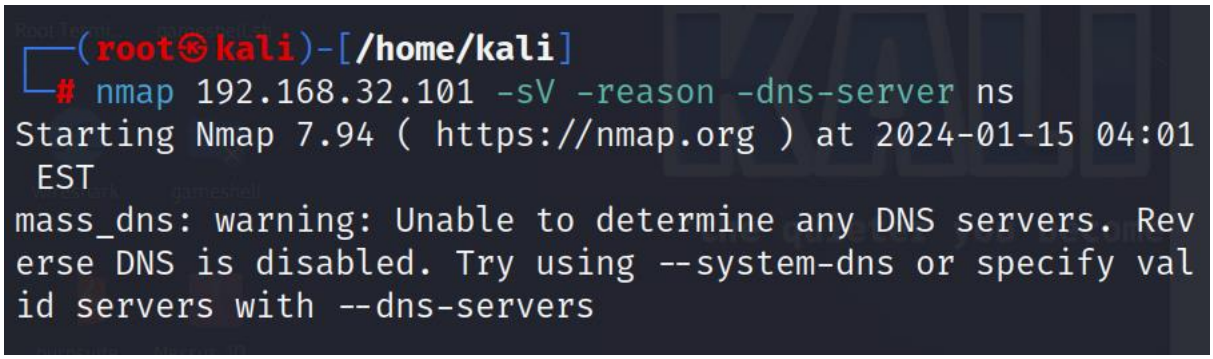
Il comando nmap -f -mtu=512 ha evidenziato 977 porte con protocollo tcp chiuse; fra le porte aperte si evidenzia la 513, una probabile vulnerabilità.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f -mtu=512 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 04:38 EST
Nmap scan report for 192.168.32.101
Host is up (0.026s 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

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 --scan known 192.168.32.1
Scanning 192.168.32.1 (192.168.32.1), 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: (1 tcpmux) (2 nbp) (4 echo) (6 zip) (7 echo) (9 discard) (11 systat
) (13 daytime) (15 netstat) (17 qotd) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 te
lnet) (25 smtp) (37 time) (43 whois) (49 tacacs) (53 domain) (67 bootps) (68 bootpc) (69
tftp) (70 gopher) (79 finger) (80 http) (88 kerberos) (102 iso-tsap) (104 acr-nema) (106
poppassd) (110 pop3) (111 sunrpc) (113 auth) (119 nntp) (123 ntp) (135 epmap) (137 netbio
s-ns) (138 netbios-dgm) (139 netbios-ssn) (143 imap2) (161 snmp) (162 snmp-trap) (163 cmi
p-man) (164 cmip-agent) (174 mailq) (177 xdmcp) (179 bgp) (199 smux) (209 qmtp) (210 z395
0) (213 ipx) (319 ptp-event) (320 ptp-general) (345 pawserv) (346 zserv) (369 rpc2portmap
) (370 codaauth2) (371 clearcase) (389 ldap) (427 svrloc) (443 https) (444 snpp) (445 mic
rosoft-d) (464 kpasswd) (465 submissions) (487 saft) (500 isakmp) (512 exec) (513 login)
(514 shell) (515 printer) (517 talk) (518 ntalk) (520 route) (538 gdomap) (540 uucp) (543
 klogin) (544 kshell) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (554 rtsp) (56
3 nntps) (587 submission) (607 nqs) (623 asf-rmcp) (628 qmqp) (631 ipp) (636 ldaps) (646
ldp) (655 tinc) (706 silc) (749 kerberos-ad) (750 kerberos4) (751 kerberos-ma) (752 passw
d-serv) (754 krb-prop) (775 moira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (853
 domain-s) (871 supfilesrv) (873 rsync) (989 ftps-data) (990 ftps) (992 telnets) (993 ima
ps) (995 pop3s) (1080 socks) (1093 proofd) (1094 rootd) (1099 rmiregistry) (1127 supfiled
bg) (1178 skkserv) (1194 openvpn) (1210 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw) (
1352 lotusnote) (1433 ms-sql-s) (1434 ms-sql-m) (1524 ingreslock) (1645 datametrics) (164
6 sa-msg-port) (1649 kermit) (1677 groupwise) (1701 l2f) (1812 radius) (1813 radius-acct)
 (2000 cisco-sccp) (2049 nfs) (2086 gnunet) (2101 rtcm-sc104) (2102 zephyr-srv) (2103 zep
hyr-clt) (2104 zephyr-hm) (2119 gsigatekeep) (2121 iprop) (2135 gris) (2401 cvspserver) (
```


```
 klogin) (544 kshell) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (554 rtsp) (56
3 nntps) (587 submission) (607 nqs) (623 asf-rmcp) (628 qmqp) (631 ipp) (636 ldaps) (646
ldp) (655 tinc) (706 silc) (749 kerberos-ad) (750 kerberos4) (751 kerberos-ma) (752 passw
d-serv) (754 krb-prop) (775 moira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (853
 domain-s) (871 supfilesrv) (873 rsync) (989 ftps-data) (990 ftps) (992 telnets) (993 ima
ps) (995 pop3s) (1080 socks) (1093 proofd) (1094 rootd) (1099 rmiregistry) (1127 supfiled
bg) (1178 skkserv) (1194 openvpn) (1210 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw) (
1352 lotusnote) (1433 ms-sql-s) (1434 ms-sql-m) (1524 ingreslock) (1645 datametrics) (164
6 sa-msg-port) (1649 kermit) (1677 groupwise) (1701 l2f) (1812 radius) (1813 radius-acct)
 (2000 cisco-sccp) (2049 nfs) (2086 gnunet) (2101 rtcm-sc104) (2102 zephyr-srv) (2103 zep
hyr-clt) (2104 zephyr-hm) (2119 gsigatekeep) (2121 iprop) (2135 gris) (2401 cvspserver) (
2430 venus) (2431 venus-se) (2432 codasrv) (2433 codasrv-se) (2583 mon) (2600 zebrasrv) (
2601 zebra) (2602 ripd) (2603 ripngd) (2604 ospfd) (2605 bgpd) (2606 ospf6d) (2607 ospfap
i) (2608 isisd) (2628 dict) (2792 f5-globalsi) (2811 gsiftp) (2947 gpsd) (3050 gds-db) (3
130 icpv2) (3205 isns) (3260 iscsi-targe) (3306 mysql) (3389 ms-wbt-serv) (3493 nut) (363
2 distcc) (3689 daap) (3690 svn) (4031 suucp) (4094 sysrqd) (4190 sieve) (4353 f5-iquery)
 (4369 epmd) (4373 remctl) (4460 ntske) (4500 ipsec-nat-t) (4557 fax) (4559 hylafax) (456
9 iax) (4691 mtn) (4899 radmin-port) (4949 munin) (5060 sip) (5061 sip-tls) (5222 xmpp-cl
ient) (5269 xmpp-server) (5308 cfengine) (5353 mdns) (5432 postgresql) (5555 rplay) (5556
 freeciv) (5666 nrpe) (5667 nsca) (5671 amqps) (5672 amqp) (5680 canna) (6000 x11) (6001
x11-1) (6002 x11-2) (6003 x11-3) (6004 x11-4) (6005 x11-5) (6006 x11-6) (6007 x11-7) (634
6 gnutella-sv) (6347 gnutella-rt) (6379 redis) (6444 sge-qmaster) (6445 sge-execd) (6446
mysql-proxy) (6514 syslog-tls) (6566 sane-port) (6667 ircd) (6696 babel) (6697 ircs-u) (7
000 bbs) (7001 afs3-callba) (7002 afs3-prserv) (7003 afs3-vlserv) (7004 afs3-kaserv) (700
5 afs3-volser) (7007 afs3-bos) (7008 afs3-update) (7009 afs3-rmtsys) (7100 font-servic) (
8021 zope-ftp) (8080 http-alt) (8081 tproxy) (8088 omniorb) (8140 puppet) (8990 clc-build
-d) (9098 xinetd) (9101 bacula-dir) (9102 bacula-fd) (9103 bacula-sd) (9418 git) (9667 xm
ms2) (9673 zope) (10000 webmin) (10050 zabbix-agen) (10051 zabbix-trap) (10080 amanda) (1
0081 kamanda) (10082 amandaidx) (10083 amidxtape) (10809 nbd) (11112 dicom) (11371 hkp) (
17001 sgi-cmsd) (17002 sgi-crsd) (17003 sgi-gcd) (17004 sgi-cad) (17500 db-lsp) (22125 dc
ap) (22128 gsidcap) (22273 wnn6) (24554 binkp) (27374 asp) (30865 csync2) (57000 dircprox
y) (60177 tfido) (60179 fido)
```

Nmap -sV -reason -dns-server ns



Riepilogo

L'utilizzo di alcuni dei tool consigliati per questo esercizio, con le dovute scansioni, hanno evidenziato alcune possibili vulnerabilità in base alla presenza di alcune porte aperte come il comando nmap -f -mtu=512, lo stesso con il comando nmap -top-ports 10 -open. Le maggiori vulnerabilità sono emerse a livello di porte tcp. Ricapitolando le maggiori vulnerabilità di metasploit si possono riscontrare a livello di porte.