

INFO GATHERING OPEN SOURCE INTELLIGENCE #YEAHHUB.COM MACCHINA: METASPLOITABLE

SFRUTTANDO I SUGGERIMENTI DEL SITO:

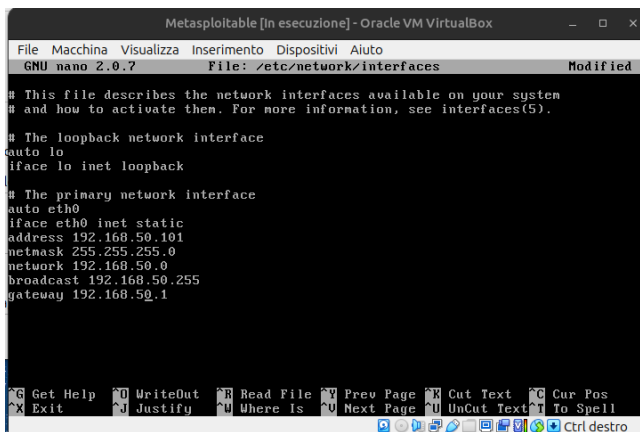
<https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/>

UTILIZZARE ALCUNI DI QUESTI STRUMENTI PER RACCOGLIERE INFORMAZIONI SULLA MACCHINA METASPLOITABLE E PRODURRE UN REPORT, IN CUI INDICARE:

SOPRA -> L'ESECUZIONE DEGLI STRUMENTI

NELLA PARTE FINALE -> RECAP DELLE INFORMAZIONI TROVATE

AL FINE DELL'ESERCIZIO NON SERVE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SU RETI DIVERSE, QUINDI REIMPOSTO L'IP DI **METASPLOITABLE** SU **192.168.50.101**, MENTRE QUELLO DI KALI LINUX RESTA 192.168.50.100



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
Ctrl destro
```

SELEZIONO IN SEGUITO ALCUNI DEI COMANDI SHELL INTERESSANTI SUGGERITI DALLA FONTE DI "YEAHHUB":

Here is the list of 15 most useful host scanning commands for [Kali Linux](#) are as listed below:

- 1. nmap -sn -PE <target>
- 2. netdiscover -r <target>
- 3. crackmapexec <target>
- 4. nmap <target> -top-ports 10 -open
- 5. nmap <target> -p- -sV -reason -dns-server ns
- 6. us -mT -lv <target>;a -r 3000 -R 3 && us -mU -lv <target>;a -r 3000 -R 3
- 7. nmap -sS -sV -T4 <target>
- 8. hping3 -scan known <target>
- 9. nc -nvz <target> 1-1024
- 10. nc -nv <target> 22
- 11. nmap -sV <target>
- 12. db_import <file.xml> (For Metasploit Framework)
- 13. nmap -f -mtu=512 <target>
- 14. masscan <network> -p80 -banners -source-ip <target>
- Never ending process.....

#NMAP:

PROVO PRIMA I COMANDI COL IL TOOL PIÙ FAMILIARE:

- **nmap -sn -PE 192.168.50.101**
- **nmap 192.168.50.101 -top-ports 10 -open**
- **nmap 192.168.50.101 -p -sU -reason -dns-server ns**
- **nmap -sS -sU -T4 192.168.50.101**
- **nmap -sU 192.168.50.101**
- **nmap -f -mtu=512 192.168.50.101**

-sn: "no port scan" controlla che l'host è attivo tramite ping senza effettuare scan

-PE: "echo request" - Nmap manda un pacchetto ICMP type 8 ("echo request") all'indirizzo IP di destinazione, aspettandosi un type 0 ("echo reply") di ritorno dagli host disponibili. Tuttavia molti host e firewall ora bloccano questo tipo di pacchetti. È utile x tenere sotto controllo una rete interna.

-top-ports 10 -open: effettua la scansione di <10> porte presenti nel file "nmap-services" con il maggior rapporto, nel caso aperte

-p: range di porte, è possibile specificare un protocollo **T**: per TCP, **U**: per UDP, **S**: per SCTP o **P**: per IP Protocol

-sU: "version detection" - identifica un servizio/versione associato ad una porta aperta

-dns-servers: Nmap cercherà di determinare i server DNS da usare per le reverse query usando il file resolv.conf (UNIX) o il Registro (Win32) sulla macchina su cui viene eseguito

-sS: TCP SYN scan, detto anche "stealth scan". Effettua una scansione non invasiva senza terminare il TCP 3-way-handshake

-T4: "timing templates", in questo caso livello 4 è definito "aggressivo: incrementa la velocità assumendo che si è su una rete veloce ed affidabile, impedisce al ritardo dinamico per una scansione di andare al di sotto della soglia dei 10 millisecondi per le porte TCP

-f: obbliga la scansione (anche i ping scan) a usare pacchetti IP frammentati (frammentando l'header su più pacchetti) in modo da rendere più difficile per un packet filter

-mtu=512: si può indicare lo spiazzamento ("offset") dei pacchetti desiderato, che deve essere multiplo di 8. Si usa o **-f** o **-mtu**

```
(django@kali)-[~]
└─$ sudo su
[sudo] password for django:
(root@kali)-[/home/django]
# nmap -sn -PE 192.168.50.101/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 18:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 6.07 seconds
```

```
(root@kali)-[/home/django]
# nmap 192.168.50.101 --top-ports 10 --open
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 18:01 EST
Nmap scan report for 192.168.50.101
Host is up (0.0076s 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

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
# nmap 192.168.50.101 -sV -reason -dns-server ns
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 18:16 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.87% done; ETC: 18:16 (0:00:06 remaining)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00016s latency).
Not shown: 977 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
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
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
MAC Address: 08:00:27:A3:DF:62 (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 53.07 seconds
```

```
(root@kali)-[/home/django]
# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 06:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.00016s 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) 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  unknown
MAC Address: 08:00:27:A3:DF:62 (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 173.00 seconds
```

```
(root@kali)-[/home/django]
# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 06:52 EST
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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) 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
MAC Address: 08:00:27:A3:DF:62 (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 52.91 seconds
```

```
(root@kali)-[/home/django]
# nmap -f -mtu=512 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 06:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.00014s 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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

#NETCAT:

- nc -nvz 192.168.50.101 1-1024
 - nc -nv 192.168.50.101 22
- nvz: fa uno scan verboso -v scan solo su un indirizzo IP numerico
- n, non su un DNS con zero-I/O mode -z
- 1-1024; 22: indicazioni sulle porte; range 1-1024; specifico 22

```
(root@kali)-[/home/django]
# nc -nvz 192.168.50.101 1-1024
(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

(root@kali)-[/home/django]
# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

#UNICORNSCAN:

È UN OSINT TOOL DI KALI LINUX DA RIGA DI COMANDO:

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

-mT: scan mode TCP

-mU: scan mode UDP

-Iv: modalità verbosa -v e immediata -I, visualizza le cose così come le troviamo

-r: pacchetti per secondo (totali, non per host, e man mano che aumentano lo scan diventa meno accurato)

-R: ripetizione di pacchetti N volte

```
(root@kali)-[/home/django]
# us -mT -Iv 192.168.50.101:a -r 3000 -R 3 66 us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode 'TCPscan' ports 'a' pps 3000
using interface(s) eth1
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 1
2 Seconds
TCP open 192.168.50.101:2049 ttl 64
TCP open 192.168.50.101:58353 ttl 64
TCP open 192.168.50.101:21 ttl 64
TCP open 192.168.50.101:23 ttl 64
TCP open 192.168.50.101:6697 ttl 64
TCP open 192.168.50.101:53 ttl 64
TCP open 192.168.50.101:445 ttl 64
TCP open 192.168.50.101:80 ttl 64
TCP open 192.168.50.101:47562 ttl 64
TCP open 192.168.50.101:3306 ttl 64
TCP open 192.168.50.101:139 ttl 64
TCP open 192.168.50.101:6000 ttl 64
TCP open 192.168.50.101:51385 ttl 64
TCP open 192.168.50.101:8180 ttl 64
TCP open 192.168.50.101:513 ttl 64
TCP open 192.168.50.101:3632 ttl 64
TCP open 192.168.50.101:2121 ttl 64
TCP open 192.168.50.101:514 ttl 64
TCP open 192.168.50.101:60405 ttl 64
TCP open 192.168.50.101:8009 ttl 64
TCP open 192.168.50.101:8787 ttl 64
TCP open 192.168.50.101:5432 ttl 64
TCP open 192.168.50.101:1524 ttl 64
TCP open 192.168.50.101:512 ttl 64
TCP open 192.168.50.101:6667 ttl 64
TCP open 192.168.50.101:1099 ttl 64
TCP open 192.168.50.101:22 ttl 64
TCP open 192.168.50.101:5900 ttl 64
TCP open 192.168.50.101:111 ttl 64
TCP open 192.168.50.101:25 ttl 64
sender statistics 2696.8 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets dropped and 0 interface drops
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
TCP open smtp[ 25] from 192.168.50.101 ttl 64
TCP open domain[ 53] from 192.168.50.101 ttl 64
TCP open http[ 80] from 192.168.50.101 ttl 64
TCP open sunrpc[ 111] from 192.168.50.101 ttl 64
TCP open netbios-ssn[ 139] from 192.168.50.101 ttl 64
TCP open microsoft-ds[ 445] from 192.168.50.101 ttl 64
TCP open exec[ 512] from 192.168.50.101 ttl 64
TCP open login[ 513] from 192.168.50.101 ttl 64
TCP open shell[ 514] from 192.168.50.101 ttl 64
TCP open rmiregistry[ 1099] from 192.168.50.101 ttl 64
TCP open ingreslock[ 1524] from 192.168.50.101 ttl 64
TCP open shilp[ 2049] from 192.168.50.101 ttl 64
TCP open scientia-ssdb[ 2121] from 192.168.50.101 ttl 64
TCP open mysql[ 3306] from 192.168.50.101 ttl 64
TCP open distcc[ 3632] from 192.168.50.101 ttl 64
TCP open postgresql[ 5432] from 192.168.50.101 ttl 64
TCP open winvnc[ 5900] from 192.168.50.101 ttl 64
TCP open x11[ 6000] from 192.168.50.101 ttl 64
TCP open irc[ 6667] from 192.168.50.101 ttl 64
TCP open unknown[ 6697] from 192.168.50.101 ttl 64
TCP open unknown[ 8009] from 192.168.50.101 ttl 64
TCP open unknown[ 8180] from 192.168.50.101 ttl 64
TCP open msgsrvr[ 8787] from 192.168.50.101 ttl 64
TCP open unknown[47562] from 192.168.50.101 ttl 64
TCP open unknown[51385] from 192.168.50.101 ttl 64
TCP open unknown[58353] from 192.168.50.101 ttl 64
TCP open unknown[60405] from 192.168.50.101 ttl 64
adding 192.168.50.101/32 mode 'UDPscan' ports 'a' pps 3000
using interface(s) eth1
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 1
2 Seconds
```

```
(root@kali)-[/home/django]
# us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode 'UDPscan' ports 'a' pps 3000
using interface(s) eth1
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 1
2 Seconds
UDP open 192.168.50.101:2049 ttl 64
UDP open 192.168.50.101:111 ttl 64
UDP open 192.168.50.101:49291 ttl 64
UDP open 192.168.50.101:53 ttl 64
UDP open 192.168.50.101:137 ttl 64
UDP open 192.168.50.101:60464 ttl 64
UDP open 192.168.50.101:48952 ttl 64
sender statistics 2818.2 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets dropped and 0 interface drops
UDP open domain[ 53] from 192.168.50.101 ttl 64
UDP open sunrpc[ 111] from 192.168.50.101 ttl 64
UDP open netbios-ns[ 137] from 192.168.50.101 ttl 64
UDP open shilp[ 2049] from 192.168.50.101 ttl 64
UDP open unknown[48952] from 192.168.50.101 ttl 64
UDP open unknown[49291] from 192.168.50.101 ttl 64
UDP open unknown[60464] from 192.168.50.101 ttl 64
```

#RECAP INFORMAZIONI TROVATE:

ALLA FINE DEGLI SCAN CONOSCIAMO IL MAC ADDRESS DELL'HOST 08:00:27:A3:DF:62 (ORACLE VIRTUAL BOX NIC), ABBIAMO INDIVIDUATO 2 HOST (METASPLOITABLE.LOCALDOMAIN, IRC.METASPLOITABLE.LAN), IL SISTEMA OPERATIVO (UNIX, LINUX KERNEL), LE PORTE TCP APERTE COI RELATIVI SERVIZI E VERSIONI (ES. PORTA 21-FTP-VERSIONE VSFTP 2.3.4, PORTA 80-HTTP-VERSIONE APACHE HTTPD 2.2.8 UBUNTU DAV/2, PORTA 6667-IRC-VERSIONE UNREALIRC, ECC.) E LE PORTE UDP APERTE CON IL RELATIVO SERVIZIO (ES. PORTA 111-SUNRPC, PORTA 137-NETBIOS-NS).