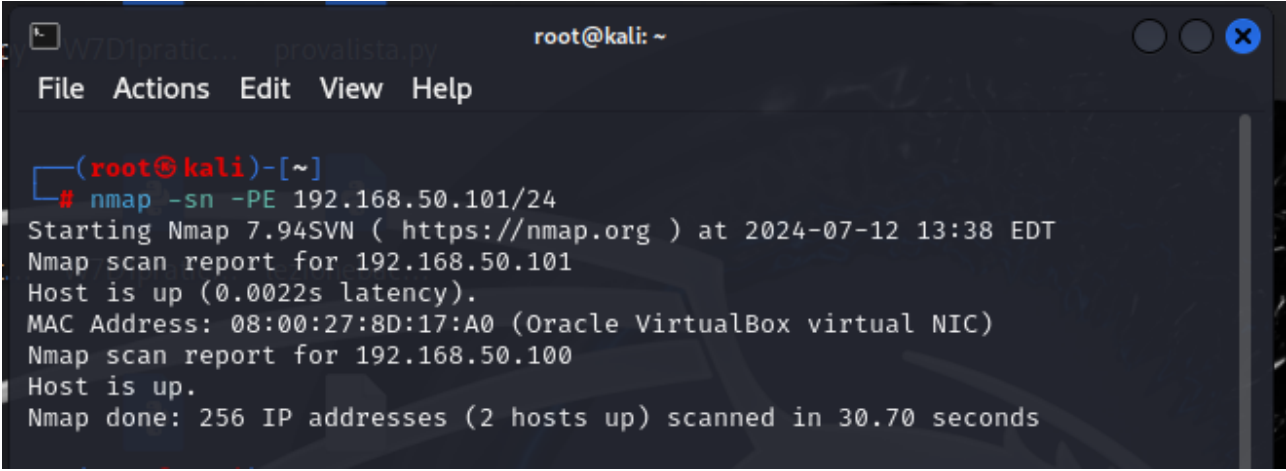


W10D4 – Scansioni

Esercizio obbligatorio e facoltativo.

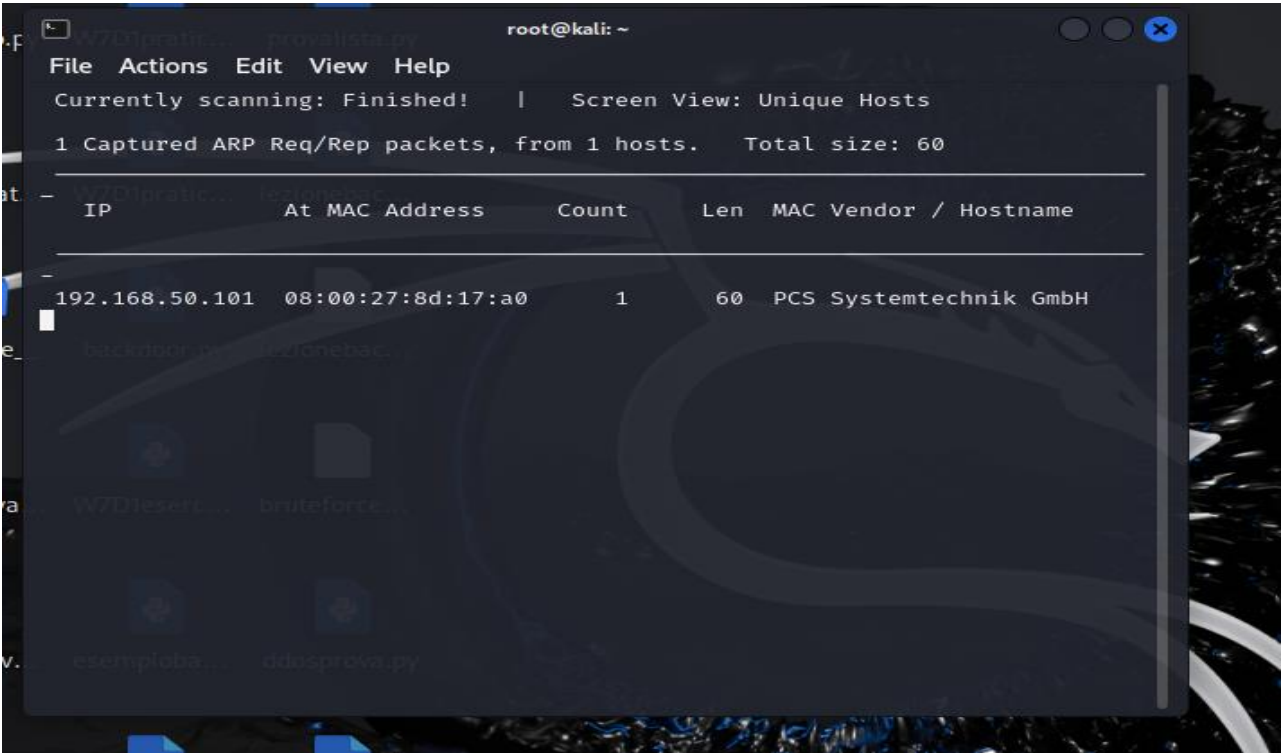
I seguenti screenshot riportano le diverse scansioni che ho svolto, prendendo come target la macchina Metasploitable 2 con IP 192.168.50.101.

Ricognizione attiva con Nmap.



```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nmap -sn -PE 192.168.50.101/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 13:38 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0022s latency).  
MAC Address: 08:00:27:8D:17:A0 (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 30.70 seconds
```

Scansione con Netdiscover.



```
root@kali: ~  
File Actions Edit View Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60  


| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------------|-------------------|-------|-----|------------------------|
| 192.168.50.101 | 08:00:27:8d:17:a0 | 1     | 60  | PCS Systemtechnik GmbH |


```

Scansione con CrackMapExec.

```
root@kali: ~
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history

(root@kali)-[~]
# crackmapexec ftp 192.168.50.101
FTP 192.168.50.101 21 192.168.50.101 [*] Banner: (vsFTPd 2.3.4
)
```

Scansione top ports con Nmap.

```
(root@kali)-[~]
# nmap 192.168.50.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 06:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0036s 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
MAC Address: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Ricognizione approfondita DNS con Nmap.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nmap 192.168.50.101 -p- -sV --reason --dns-server ns  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 06:40 EDT  
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: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 90.00% done; ETC: 06:41 (0:00:02 remaining)  
Nmap scan report for 192.168.50.101  
Host is up, received arp-response (0.00044s latency).  
Not shown: 65505 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 (pro  
tocol 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: W  
ORKGROUP)  
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: W  
ORKGROUP)  
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  
3632/tcp  open  distccd      syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.  
2.4-1ubuntu4))  
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)
```

```
root@kali: ~  
File Actions Edit View Help  
  
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  
3632/tcp   open  distccd      syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.  
2.4-1ubuntu4))  
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  
6697/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  
8787/tcp   open  drb          syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/  
lib/ruby/1.8/drbr)  
37336/tcp  open  nlockmgr     syn-ack ttl 64 1-4 (RPC #100021)  
47658/tcp  open  java-rmi     syn-ack ttl 64 GNU Classpath grmiregistry  
56788/tcp  open  status       syn-ack ttl 64 1 (RPC #100024)  
57578/tcp  open  mountd       syn-ack ttl 64 1-3 (RPC #100005)  
MAC Address: 08:00:27:8D:17:A0 (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://n  
map.org/submit/  
Nmap done: 1 IP address (1 host up) scanned in 180.29 seconds  
  
(root@kali)-[~]  
#
```

Scansione con Unicornscan.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# 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) eth0  
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a littl  
e longer than 1 Minutes, 12 Seconds  
TCP open 192.168.50.101:512 ttl 64  
TCP open 192.168.50.101:8180 ttl 64  
TCP open 192.168.50.101:3306 ttl 64  
TCP open 192.168.50.101:6697 ttl 64  
TCP open 192.168.50.101:22 ttl 64  
TCP open 192.168.50.101:2049 ttl 64  
TCP open 192.168.50.101:3632 ttl 64  
TCP open 192.168.50.101:6000 ttl 64  
TCP open 192.168.50.101:80 ttl 64  
TCP open 192.168.50.101:514 ttl 64  
TCP open 192.168.50.101:445 ttl 64  
TCP open 192.168.50.101:2121 ttl 64  
TCP open 192.168.50.101:53 ttl 64  
TCP open 192.168.50.101:25 ttl 64  
TCP open 192.168.50.101:56788 ttl 64  
TCP open 192.168.50.101:21 ttl 64  
TCP open 192.168.50.101:23 ttl 64  
TCP open 192.168.50.101:37336 ttl 64  
TCP open 192.168.50.101:8009 ttl 64  
TCP open 192.168.50.101:1099 ttl 64  
TCP open 192.168.50.101:8787 ttl 64  
TCP open 192.168.50.101:139 ttl 64  
TCP open 192.168.50.101:1524 ttl 64  
TCP open 192.168.50.101:47658 ttl 64  
TCP open 192.168.50.101:57578 ttl 64  
TCP open 192.168.50.101:513 ttl 64  
TCP open 192.168.50.101:5900 ttl 64  
TCP open 192.168.50.101:5432 ttl 64  
TCP open 192.168.50.101:111 ttl 64  
TCP open 192.168.50.101:6667 ttl 64
```

```
root@kali: ~  
File Actions Edit View Help  
TCP open 192.168.50.101:111 ttl 64  
TCP open 192.168.50.101:6667 ttl 64  
sender statistics 2170.8 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[37336] from 192.168.50.101 ttl 64  
TCP open unknown[47658] from 192.168.50.101 ttl 64  
TCP open unknown[56788] from 192.168.50.101 ttl 64  
TCP open unknown[57578] from 192.168.50.101 ttl 64  
adding 192.168.50.101/32 mode 'UDPscan' ports 'a' pps 3000  
using interface(s) eth0
```



```

TCP open      unknown[55895]      from 192.168.50.101  ttl 64
adding 192.168.50.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a littl
e longer than 1 Minutes, 12 Seconds
UDP open 192.168.50.101:53  ttl 64
UDP open 192.168.50.101:111  ttl 64
UDP open 192.168.50.101:137  ttl 64
UDP open 192.168.50.101:42628  ttl 64
UDP open 192.168.50.101:2049  ttl 64
UDP open 192.168.50.101:52333  ttl 64
UDP open 192.168.50.101:45746  ttl 64
sender statistics 2923.8 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets dropped and 0 interface drop
s
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[42628]   from 192.168.50.101  ttl 64
UDP open      unknown[45746]   from 192.168.50.101  ttl 64
UDP open      unknown[52333]   from 192.168.50.101  ttl 64

```

```

(root@kali)-[~]
#

```

Scansione SYN con Nmap.

```

File Actions Edit View Help
(root@kali)-[~]
# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 07:01 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00045s 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: 08:00:27:8D:17:A0 (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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.85 seconds

```

Scansioni con HPING3 e con Netcat

```
(root@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) (3
306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-
u) w7D1eserc... bruteforce...

(root@kali)-[~]
# 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)-[~]
#
```

Scansione banner grabbing con Netcat

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

Scansione Nmap con versioni.

```
File Actions Edit View Help
(root@kali)-[~]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 07:21 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00083s 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
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: 08:00:27:8D:17:A0 (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 65.74 seconds
```

Scansione Firewall Bypass.

```
File Actions Edit View Help
(root@kali)-[~]
# nmap -f --mtu=512 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 13:00 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0024s 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: 08:00:27:8D:17:A0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Report finale delle scansioni.

Con la prima scansione, sono stati trovati due host attivi nella rete, ovvero la macchina Kali e la macchina Metasploitable, rispettivamente con gli IP 192.168.50.100 e 192.168.50.101. Anche la seconda scansione con netdiscover ha rilevato che l'host 192.168.50.101, ossia la macchina Metasploitable, è attivo sulla rete e ne ha rilevato anche l'indirizzo MAC. Crackmapexec ha esaminato il banner della porta 21, dove è attivo stp. La quarta scansione, che ha preso come target le top ports, ha ritrovato che 7 di queste top ports sono aperte, ovvero le porte 21,22,23,25,80,139 e 445, mentre 3 porte sono chiuse. Il quinto scanner, invece, va più in profondità ed indica il motivo per il quale una porta è risultata aperta, riportando ad esempio lo scambio di pacchetti syn-ack e la versione del servizio attivo su quella porta. La scansione con Unicornscan, invece, ha controllato tutte le porte, svolgendo sia una scansione TCP che una UDP e riportando tutte le porte aperte e i relativi servizi, partendo da TCP. Le porte UDP trovate sono le porte 53,111,137,2049,42628,45746 e 52333, nelle quali sono attivi i servizi domain, sunrpc, netbios-ns, shilp e 3 servizi non noti. La settima scansione è una normale scansione SYN che riporta le versioni dei servizi trovati. Le porte aperte trovate sono 23 e sono le porte numero 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000, 6667,8009 ed 8180 e i servizi attivi sono, rispettivamente, ftp,ssh,telnet, smtp, domain, http, rpcbind, netbios-ssn su due porte, exec, login, shell, java-rmi, bindshell, nfs, ftp, mysql, postgresql, vnc,X11, irc, ajp13 ed http. La scansione successiva con HPING3 ha scansionato in tutto 264 porte, ricevendo risposta da tutte tranne che da 22, mentre la scansione semplice con netcat ha rilevato 12 porte aperte, ossia le porte numero 514,513,512,445,139,111,80,53,25,23,22 e 21. La successiva scansione con netcat si è concentrata sulla lettura del banner della porta 22. La scansione con nmap -sV ha riportato la versione di tutti i servizi trovati sulle 23 porte riportate, mentre l'ultima scansione cerca di aggirare il firewall inviando dei pacchetti frammentati alle 23 porte riportate prima.