ESERCIZIO M3 D4 – scansione METASPOLITABLE2 192.168.50.101

1- nmap -sn -PE 192.168.1.101

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 14:50 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00049s latency).
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

2- netdiscover -r

```
 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:a0:26:54      1      60  PCS Systemtechnik GmbH
```

3-crackmapexec

```
┌──(marco㉿kali)-[~]
└─$ crackmapexec ssh 192.168.50.101/24
SSH         192.168.50.101  22     192.168.50.101   [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

┌──(marco㉿kali)-[~]
└─$ crackmapexec winrm 192.168.50.101/24

┌──(marco㉿kali)-[~]
└─$ crackmapexec smb 192.168.50.101/24
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)

┌──(marco㉿kali)-[~]
└─$ crackmapexec mssql 192.168.50.101/24

┌──(marco㉿kali)-[~]
└─$ crackmapexec ldap 192.168.50.101/24
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)

┌──(marco㉿kali)-[~]
└─$ crackmapexec ftp 192.168.50.101/24
FTP         192.168.50.101  21     192.168.50.101   [*] Banner: (vsFTPd 2.3.4)

┌──(marco㉿kali)-[~]
└─$ crackmapexec rdp 192.168.50.101/24
```

4- nmap 10 top ports

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 15:00 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00069s 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:A0:26:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

5- DNS slow scan

```
┌──(root㉿kali)-[/home/marco]
└─# nmap 192.168.50.101 -p- --version-all --reason --dns-servers ns
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 15:12 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00018s latency).
Not shown: 65505 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
1099/tcp open  rmiregistry  syn-ack ttl 64
1524/tcp open  ingreslock   syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
3632/tcp open  distccd      syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
6667/tcp open  irc          syn-ack ttl 64
6697/tcp open  ircs-u       syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64
```

```
8787/tcp  open  msgsrvr      syn-ack ttl 64
45417/tcp open  unknown      syn-ack ttl 64
54763/tcp open  unknown      syn-ack ttl 64
56231/tcp open  unknown      syn-ack ttl 64
57278/tcp open  unknown      syn-ack ttl 64
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```

6- TCP Syn scan nmap

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 15:30 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00024s 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?
25/tcp   open  smtp?
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?
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  ccproxy-ftp?
3306/tcp open  mysql?
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:A0:26:54 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.24 seconds
```

7- SCAN con HPING3

```
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)
```

8-Port scanning Netcat

```
(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
```

9- Banner grabbing Netcat

Porta 21

```
(UNKNOWN) [192.168.50.101] 21 (ftp) open
220 (vsFTPd 2.3.4)
```

Porta 22

```
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

10- Version scanning Nmap

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 15:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000068s 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?
25/tcp   open  smtp?
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?
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  ccproxy-ftp?
3306/tcp open  mysql?
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:A0:26:54 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

11- firewall bypass

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 15:51 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000088s 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:A0:26:54 (Oracle VirtualBox virtual NIC)
```

Informazioni Target

name:METASPLOITABLE

IP: 192.168.50.101

Mac Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)

Porte aperte:

- 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

PORTA 21 - Versione Ftp: vsftpd 2.3.4

PORTA 22 - Versione Secure shell: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

PORTA 53 - tcp ISC BIND 9.4.2

PORTA 80 – HTTP - Apache httpd 2.2.8 ((Ubuntu) DAV/2)

PORTA 111 - 2 (RPC #100000)

PORTA 139 - netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

PORTA 445 - netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

PORTA 5432 – DATABASE SYSTEM - postgresql PostgreSQL DB 8.3.0 – 8.3.7

PORTA 5900 – VIRUAL NETWORK COMPUTING - VNC (protocol 3.3)

PORTA 8009 - ajp13 Apache Jserv (Protocol v1.3)

PORTA 8180 - http Apache Tomcat/Coyote JSP engine 1.1