

# **Martin**

# **Dalla Pozza**

## **Analisis de vulnerabilidades**

**Se debe ejecutar nmap, para comprobar que tipos de servicios funcionan y posteriormente, otro analisis para comprobar vulnerabilidades que puedan llegar a existir**

```

(kali@kali)-[~]
$ nmap -sS -sV -Pn -n 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 19:21 CEST
Nmap scan report for 192.168.1.2
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.09 seconds

```

```

(kali@kali)-[~]
$ nmap -sS -sV -Pn -n 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 19:22 CEST
Nmap scan report for 192.168.1.3
Host is up (0.0017s 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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
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

```

```

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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
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: 08:00:27:61:A2:B7 (PCS Systemtechnik/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 11.88 seconds

```

Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	0.00000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
27	0.00789929	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
32	1.319275513	192.168.1.3	192.168.1.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master
42	1.319275885	192.168.1.3	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
522	0.00951535	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
633	0.009314155	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
749	0.008510599	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
858	0.009508624	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8642e18
942	1.994147132	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x29214c3d
1025	1.992621158	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x29214c3d
11436	1.992191386	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x29214c3d
12448	1.991960893	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x29214c3d
13469	1.992766110	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x29214c3d
14496	1.37218583	fe80::22f4:e0a:b7e1:ff02::2		ICMPv6	62	Router Solicitation
15741	1.38889718	192.168.1.3	192.168.1.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master
16741	1.389752777	192.168.1.3	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
17752	1.987950243	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a
18757	1.999147577	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a

Frame 19: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0

Ethernet II, Src: PCSystemtec\_01:a2:b7 (08:00:27:61:a2:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

eth0: <live capture in progress>

Paquetes: 181

Perfil: Default

Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19763	1.987521077	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a
28775	1.987203777	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a
21794	1.987782274	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a
22804	1.987985928	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x94fe2a
23122	1.9821118	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x464dde73
24128	1.9829543	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x464dde73
251135	1.9832985	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x464dde73
261156	1.9831392	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x464dde73
271177	1.9810947	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x464dde73
281454	1.9783631	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
291457	1.9776295	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
301461	1.2977026	192.168.1.3	192.168.1.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master
311461	1.2982812	192.168.1.3	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
321462	1.9779525	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
331470	1.9776397	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
341481	1.9775265	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
351491	1.9775514	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
361502	1.9779541	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b
371504	1.9744324	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5173af2b

Frame 19: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0

Ethernet II, Src: PCSystemtec\_01:a2:b7 (08:00:27:61:a2:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

eth0: <live capture in progress>

Paquetes: 181

Perfil: Default

Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
705335	1.9455594	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
713600	1.9514574	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
723611	1.9451896	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
733621	1.2661581	192.168.1.3	192.168.1.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master
743621	1.2665022	192.168.1.3	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
753622	1.9456486	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
763634	1.9458978	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
773647	1.9452617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb162cf2d
783897	1.9419175	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x22819f24
793905	1.9407489	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x22819f24
803914	1.9406637	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x22819f24
813933	1.9406443	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x22819f24
823942	1.9413244	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x22819f24
834125	1.9396643	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6aeef2e3
844132	1.9396465	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6aeef2e3
854136	1.9957194	fe80::22f4:e0a:b7e1:ff02::2		ICMPv6	62	Router Solicitation
864144	1.9389395	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6aeef2e3
874158	1.9372092	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6aeef2e3
884165	1.9373213	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6aeef2e3

Frame 19: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0

Ethernet II, Src: PCSystemtec\_01:a2:b7 (08:00:27:61:a2:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

eth0: <live capture in progress>

Paquetes: 181

Perfil: Default

**Herramientas de Análisis de Red**

**Wireshark - Aplicación de filtro de visualización:** <Ctrl>+F

No.	Time	Source	Destination	Protocol	Length	Info
214	10635.769516	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe22ccdf
215	10649.780864	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe22ccdf
216	10661.767121	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe22ccdf
217	10668.751884	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe22ccdf
218	10681.763176	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe22ccdf
219	10821.343748	192.168.1.3	192.168.1.255	BROWSER	286	Local Master Announcement METASQLTABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master
220	10821.349696	192.168.1.3	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
221	10845.408832	fe80::22f4:e0a:b7e1:f902::2	::::	ICMPv6	62	Router Solicitation
222	11041.778896	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x84fc767
223	11049.753912	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x84fc767
224	11068.780896	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x84fc767
225	11080.757868	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x84fc767
226	11089.763374	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x84fc767
227	11356.748749	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe6578a7d
228	11362.752785	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe6578a7d
229	11371.743547	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe6578a7d
230	11393.741663	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe6578a7d
231	11499.749382	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe6578a7d

**Frame 19: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0**

- Ethernet II, Src: PCSSystematic\_b1:a2:b7 (08:00:27:61:a2:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

**Packets: 243**