

Martin

Dalla Pozza

Analisis de vulnerabilidades

- 1.....Escaneo por defecto. Descubrimiento de Hosto (Ping Scan)**
- 2.....Si queremos ver el servicio y ping para ver como responde nuestro objetivo**
- 3.....Escaneo ACK**
- 4.....Escaneo Xmas**
- 5.....Escaneo para averiguar servicio y version**
- 6.....Escaneo UDP**

1.....Escaneo por defecto. Descubrimiento de Host (Ping Scan)

```
(kali@kali)-[~]
$ nmap 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 11:28 CEST
Nmap scan report for 192.168.1.2
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

```
(kali@kali)-[~]
$ nmap 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 11:30 CEST
Nmap scan report for 192.168.1.3
Host is up (0.0021s 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
```

```
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: 08:00:27:61:A2:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

2.....Si queremos ver el servicio y ping para ver como responde nuestro objetivo

```
(kali㉿kali)-[~]  
$ nmap -sS -Pn -n 192.168.1.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 11:41 CEST  
Nmap scan report for 192.168.1.2  
Host is up (0.012s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

```
(kali㉿kali)-[~]  
$ nmap -sS -Pn -n 192.168.1.3  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 11:42 CEST  
Nmap scan report for 192.168.1.3  
Host is up (0.0022s 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
```

```
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: 08:00:27:61:A2:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

3.....Escaneo ACK

```
(kali㉿kali)-[~]
└─$ nmap -sA -Pn -n 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 12:24 CEST
Nmap scan report for 192.168.1.2
Host is up (0.12s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds

(kali㉿kali)-[~]
└─$ nmap -sA -Pn -n 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 12:24 CEST
Nmap scan report for 192.168.1.3
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:61:A2:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

4.....Escaneo Xmas

```
(kali㉿kali)-[~]
└─$ nmap -sX -Pn -n 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 12:26 CEST
Nmap scan report for 192.168.1.3
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

```
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:61:A2:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

5.....Escaneo para averiguar servicio y version

```
(kali@kali)-[~]
$ nmap -sS -sV -Pn -n 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 12:36 CEST
Nmap scan report for 192.168.1.3
Host is up (0.0066s 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
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)
nmap done: 1 IP address (1 host up) scanned in 11.00 seconds
```

```
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
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 12.07 seconds
```

6.....Escaneo UDP

```
(kali@kali)-[~]
$ nmap -sU -sV -Pn -n 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 12:40 CEST
Stats: 0:06:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 26.02% done; ETC: 13:05 (0:18:43 remaining)
Stats: 0:13:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.92% done; ETC: 13:23 (0:30:34 remaining)
Stats: 0:35:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 43.70% done; ETC: 14:02 (0:46:10 remaining)
Stats: 1:23:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 72.69% done; ETC: 14:35 (0:31:31 remaining)
Stats: 1:58:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 93.83% done; ETC: 14:46 (0:07:49 remaining)
Stats: 2:44:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 52.56% done; ETC: 15:55 (0:30:42 remaining)
Stats: 2:44:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 54.78% done; ETC: 15:53 (0:28:33 remaining)
Stats: 3:14:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 99.74% done; ETC: 15:54 (0:00:10 remaining)
Nmap scan report for 192.168.1.2
Host is up (0.00094s latency).
Not shown: 762 open|filtered udp ports (no-response), 237 closed udp ports (port-unreach)
PORT      STATE SERVICE      VERSION
137/udp open  netbios-ns  Microsoft Windows netbios-ns (workgroup: WORKGROUP)
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-GKFKCPM; 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 11770.16 seconds
```

```
(kali@kali)-[~]
$ nmap -sU -sV -Pn -n --top-port 1000 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 15:30 CEST
Warning: 192.168.1.3 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).
Not shown: 949 closed udp ports (port-unreach), 47 open|filtered udp ports (no-response)
PORT      STATE SERVICE      VERSION
53/udp open  domain       ISC BIND 9.4.2
111/udp open  rpcbind      2 (RPC #100000)
137/udp open  netbios-ns   Microsoft Windows netbios-ns (workgroup: WORKGROUP)
2049/udp open  nfs          2-4 (RPC #100003)
MAC Address: 08:00:27:61:A2:B7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: METASPLOITABLE; 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 1937.30 seconds
```

```
(kali@kali)-[~]
$ nmap -sU -sV -Pn -n --top-port 1000 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 17:30 CEST
Stats: 0:52:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 63.00% done; ETC: 18:53 (0:30:46 remaining)
Nmap scan report for 192.168.1.2
Host is up (0.0011s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE      VERSION
137/udp open  netbios-ns   Microsoft Windows netbios-ns (workgroup: WORKGROUP)
MAC Address: 08:00:27:04:F0:92 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-GKFKCPM; 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 5085.21 seconds
```