



# CURSO DE HACKING ÉTICO

## ESCANER DE PUERTOS

*"No sabemos todas la respuestas. Si las tuviéramos nos aburriríamos. Sigue mirando, buscando e intentado tener más respuestas"*

**- Jack Lalanne**

# ESCANER DE PUERTOS

- ☐ Definición
- ☐ Tipos
- ☐ Herramientas
- ☐ NetDiscover
- ☐ Nmap
- ☐ Tipos de escáners con nmap
- ☐ Ejemplos

# Qué es el escaneo y tipos

El escaneo de puertos permite examinar redes o computadores en busca de objetivos o servicios que poder explotar.

**Buscar sistemas  
activos**

**Identificar SO**

**Detectar puertos  
abiertos y  
cerrados**

**Servicios  
activos**

# ¿Qué es el escaneo y tipos?

Existen diversos tipos de escaneo. Generales y concretos.

A rectangular button with a blue gradient and a 3D effect, containing the text 'Network Scan' in white.

**Network Scan**

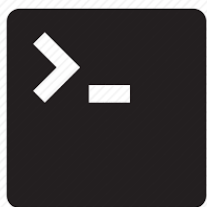
A rectangular button with a red gradient and a 3D effect, containing the text 'Port Scan' in white.

**Port Scan**

A rectangular button with a grey gradient and a 3D effect, containing the text 'Vulnerability Scan' in white.

**Vulnerability Scan**

## Herramientas utilizadas



# Descubrimiento vía ARP

**Windows: Saber si el ping lo bloquea el firewall**

<https://www.sysadmit.com/2018/05/windows-saber-si-el-ping-lo-bloquea-el-firewall.html>

**Para limpiar la caché ARP desde Linux:**

`ip neigh flush all`

```
C:\>
C:\>arp -a 1
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet      Dirección física
192.168.150.2              00-50-56-f3-96-99    dinámico
192.168.150.255           ff-ff-ff-ff-ff-ff    estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.252               01-00-5e-00-00-fc    estático

C:\>arp -d * 2
C:\>arp -a 3
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet      Dirección física
224.0.0.22                01-00-5e-00-00-16    estático

C:\>ping 192.168.150.111 4
Haciendo ping a 192.168.150.111 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.150.111:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos),

C:\>arp -a 5
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet      Dirección física
192.168.150.2              00-50-56-f3-96-99    dinámico
192.168.150.111           00-0c-29-b0-03-3b    dinámico
224.0.0.22                01-00-5e-00-00-16    estático
```

# Network Scan Ping / Netdiscover

**Entendemos por Network Scan las técnicas que permiten descubrir objetivos conectados a la red: computadores, impresoras, etc.**

```
root@educait:~# ping 10.0.0.230 -c 1
PING 10.0.0.230 (10.0.0.230) 56(84) bytes of data.
64 bytes from 10.0.0.230: icmp_seq=1 ttl=128 time=0.205 ms
root@educait:~# ping 10.0.0.235 -c 1
PING 10.0.0.235 (10.0.0.235) 56(84) bytes of data.
64 bytes from 10.0.0.235: icmp_seq=1 ttl=64 time=0.185 ms
root@educait:~# ping 10.0.0.240 -c 1
PING 10.0.0.240 (10.0.0.240) 56(84) bytes of data.
```

```
root@educait:~# netdiscover -i eth0 -r 10.0.0.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
```

IP	At MAC Address	Count	Len	MAC Vendor
10.0.0.230	00:0c:29:68:5e:75	1	60	VMware,Inc.
10.0.0.235	00:0c:29:57:de:d6	1	60	VMware,Inc.
10.0.0.240	00:0c:29:c2:69:8d	1	60	VMware,Inc.

PC → 10.0.0.240

**Iptables -A INPUT -p icmp -j DROP**





# Network Scan nping

```
root@educait:~# nping 10.0.0.229-245
```

```
Starting Nping 0.7.70 ( https://nmap.org/ at 2018-02-11 08:41 CEST
SENT (0.0427s) ICMP [10.0.0.50 > 10.0.0.229 Echo request
(type=8/code=0) id=3160 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (1.0431s) ICMP [10.0.0.50 > 10.0.0.231 Echo request
(type=8/code=0) id=40560 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (2.0450s) ICMP [10.0.0.50 > 10.0.0.231 Echo request
(type=8/code=0) id=40560 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (3.0467s) ICMP [10.0.0.50 > 10.0.0.232 Echo request
(type=8/code=0) id=32813 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (4.0483s) ICMP [10.0.0.50 > 10.0.0.233 Echo request
(type=8/code=0) id=15066 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (5.0499s) ICMP [10.0.0.50 > 10.0.0.234 Echo request
(type=8/code=0) id=28634 seq=1] IP [ttl=64 id=52894 iplen=28 ]
SENT (6.0516s) ICMP [10.0.0.50 > 10.0.0.235 Echo request
```



# Network Scan NMAP

```
root@educait:~# nmap -sn 10.0.0.0/24
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-11 08:24 CEST
```

```
Nmap scan report for 10.0.0.230
```

```
Host is up (0.000086s latency).
```

```
MAC Address: 00:0C:29:68:5E:75 (VMware)
```

```
Nmap scan report for 10.0.0.235
```

```
Host is up (0.00018s latency).
```

```
MAC Address: 00:0C:29:57:DE:D6 (VMware)
```

```
Nmap scan report for 10.0.0.240
```

```
Host is up (0.000080s latency).
```

```
MAC Address: 00:0C:29:C2:69:8D (VMware)
```

```
Nmap scan report for 10.0.0.50
```

```
Host is up.
```

```
Nmap done: 256 IP addresses (4 hosts up) scanned in 33.72  
seconds
```

# Port Scan

Entendemos por Network Scan las técnicas que permiten descubrir los puertos abiertos o cerrados de un determinado objetivo(s)

```
root@educait:~# nmap 10.0.0.230
Starting Nmap 7.70 ( https://nmap.org ) at 2018-03-11 08:44 CEST
Nmap scan report for 10.0.0.230
Host is up (0.00043s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:68:5E:75 (VMware)
```

## Port Status type

Con nmap, podemos ver diferentes tipos de estados al examinar los puertos:

- ❑ **Open**—It means that the port is accessible and an application is listening on it.
- ❑ **Closed**—It means that the port is inaccessible and no application is listening on it.
- ❑ **Filtered**—It means that nmap is not able to figure out if the port is open or closed, as the packets are being filtered, which probably means that the machine is behind a firewall.
- ❑ **Unfiltered**—It means that the ports are accessible by nmap but it is not possible to figure out if they are open or closed.



## Port Status type

```
root@educatit:~# nmap 10.0.0.240 -p80
```

PORT	STATE	SERVICE
80/tcp	open	http

```
root@10.0.0.240:~# /etc/init.d/apache2 stop
```

```
root@educatit:~# nmap 10.0.0.240 -p80
```

PORT	STATE	SERVICE
80/tcp	closed	http

```
root@10.0.0.240:~# /etc/init.d/apache2 start
```

```
root@10.0.0.240:~# iptables -A INPUT -p tcp --dport 80 -j  
DROP
```

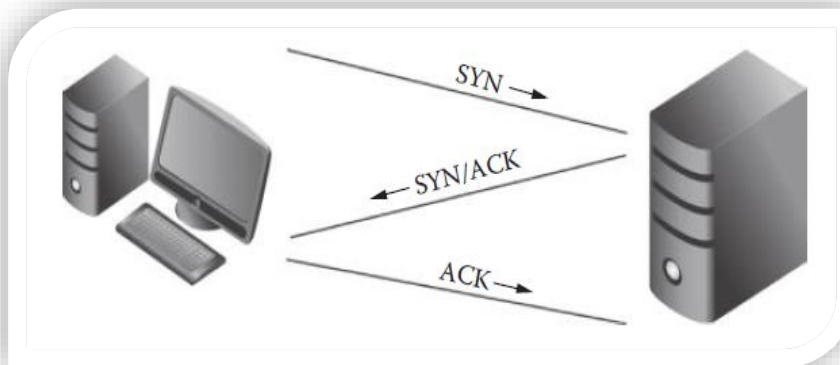
```
root@educait:~# nmap 10.0.0.240 -p80
```

PORT	STATE	SERVICE
80/tcp	filtered	http



# TCP – Three-Way Handshake

El protocolo TCP, capa de transporte del modelo OSI, es un protocolo orientado a la conexión, lo que implica que antes de intercambiar información con la capa de aplicación (http por ejemplo) examina si el puerto está a la escucha enviando tramas de sesión y utilizando los bits del campo de flags de las tramas.



## TCP Flags

- *SYN*—Initiates a connection.
- *ACK*—Acknowledges that the packet was received.
- *RST*—Resets the connections between two hosts.
- *FIN*—Finishes the connection.

Protocol	Length	Info
TCP	74	34232 → 80 [SYN] Seq=0 Win=292
TCP	74	80 → 34232 [SYN, ACK] Seq=0 Ack=1
TCP	66	34232 → 80 [ACK] Seq=1 Ack=1 W=
HTTP	376	GET / HTTP/1.1

```
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
... 0... = Congestion Window Redu
... .0.. = ECN-Echo: Not set
... ..0. = Urgent: Not set
... ...1 = Acknowledgment: Set
... .... = Push: Not set
... ..0.. = Reset: Not set
... ..1. = Syn: Set
... ..0 = Fin: Not set
[TCP Flags: .....A..S.]
```

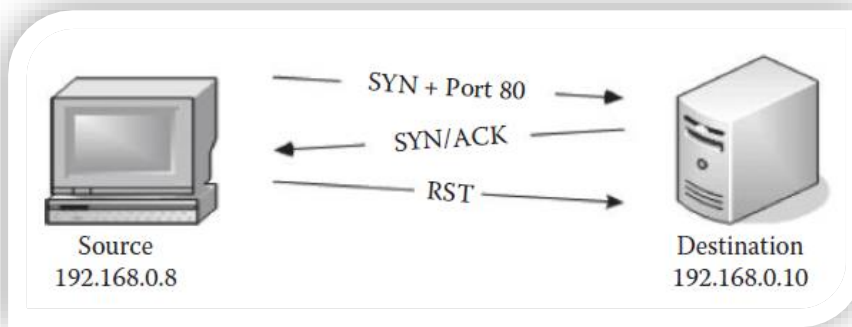


# Tipos de escaneos

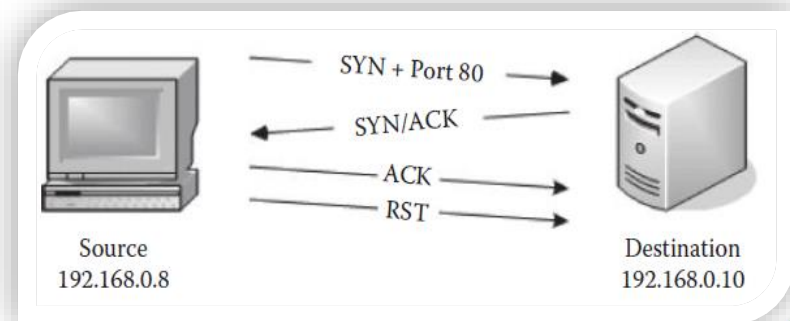
- ❑ **TCP SYN Scan** → #nmap -sS 10.0.0.240
- ❑ **TCP Connect Scan** → #nmap -sT 10.0.0.240
- ❑ **NULL Scan** → #nmap -sN 10.0.0.240
- ❑ **FIN Scan** → #nmap -sF 10.0.0.240

- ❑ **XMAS Scan** → #nmap -sX 10.0.0.240
- ❑ **Acknowledge Scan** → #nmap -sA 10.0.0.240
- ❑ **Servicios** → #nmap -sV 10.0.0.240
- ❑ **SO** → #nmap -O 10.0.0.240

## TCP SYN Scan



## TCP Connect Scan



# Host público para pruebas

Host de ejemplo donde estamos autorizados a lanzar scans:

scanme.nmap.org

Mas info: <http://scanme.nmap.org/>

Ejemplos publicados en la web:

<https://nmap.org/book/man-examples.html>



# Nmap + ejemplos

- ❑ **Scan Intensivo** → `#nmap -T4 -A -v 10.0.0.240`
- ❑ **Intensivo más UDP** → `#nmap -sS -sU -T4 -A -v 10.0.0.240`
- ❑ **Intensivo, todos los puertos TCP** → `#nmap -p 1-65535 -T4 -A -v 10.0.0.240`
- ❑ **Scan rápido** → `#nmap -T4 -F 10.0.0.240`
- ❑ **Rango de puertos** → `#nmap -p1-65535 10.0.0.240 -open`
- ❑ **Almacenamos resultados** → `#nmap -T4 -A -v 10.0.0.240 -oN /root/datos.txt`
- ❑ **Almacenamos resultados en XML** → `#nmap -T4 -A -v 10.0.0.240 -oN /root/datos.XML`
- ❑ **Idle Scan** → `#nmap -Pn -p- -sI 192.168.163.132 192.168.163.130`

Rango	Nombre	Detalle
-T0	Paranoico	Muy lento - No recomendable
-T1	Sigiloso	Útil para la evasión de IDS - Lento
-T2	Educado	No interfiere con el objetivo - Lento pero recomendable
-T3	Normal	Escaneo por defecto
-T4	Agresivo	Escaneo rápido y agresivo - No recomendable
-T5	Demente	Escaneo muy rápido y muy agresivo - No recomendable



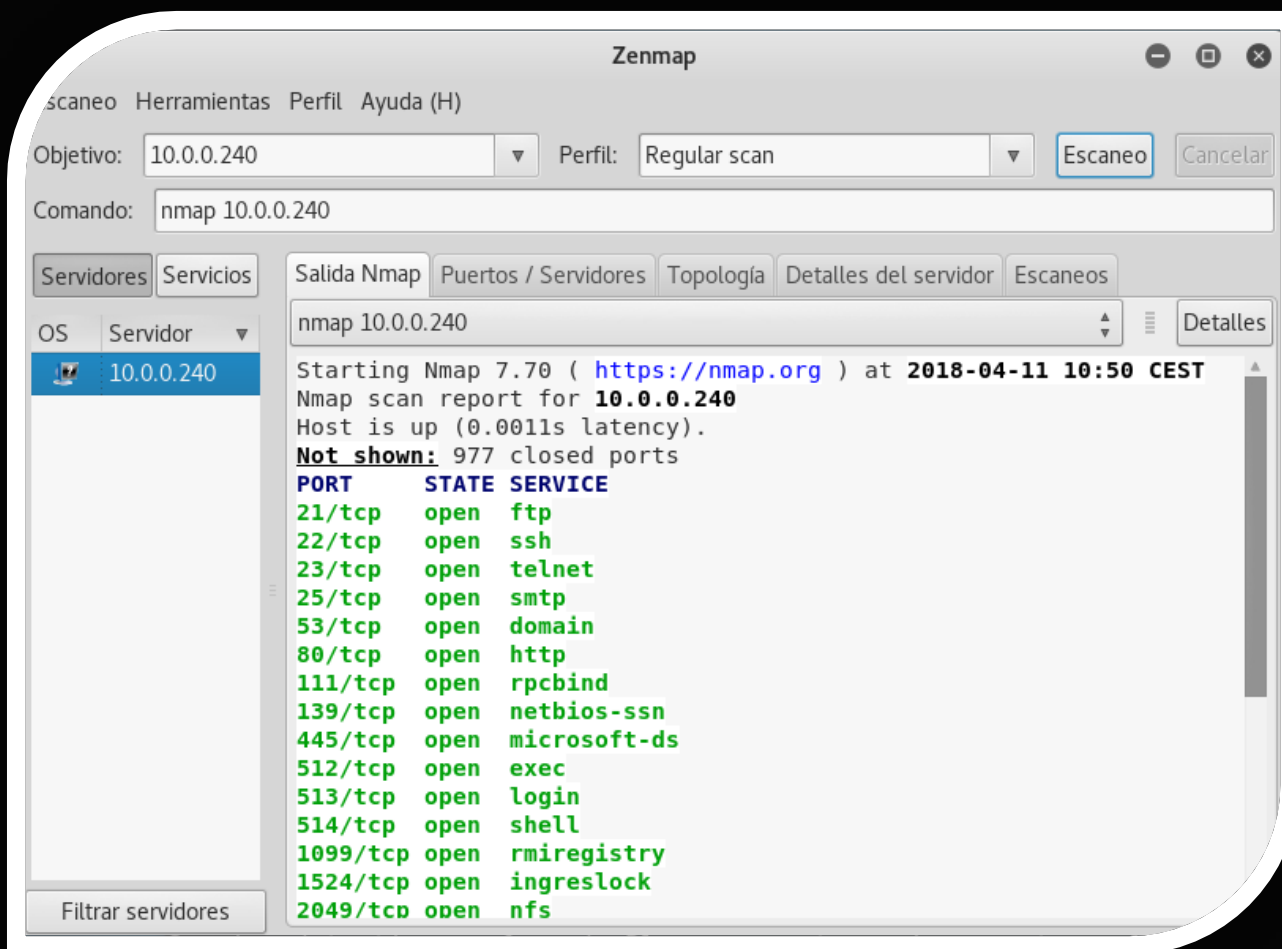
# Nmap scripts

```
root@kprofe:~# ls /usr/share/nmap/scripts/
root@kprofe:~# nmap -T3 -Pn -f -sV 10.0.0.190
root@kprofe:~# nmap -sS -sV --script auth 10.0.0.190
root@kprofe:~# nmap -sS -sV --script default 10.0.0.190
root@kprofe:~# nmap --script vuln 10.0.0.180 -p21
```

- **Auth:** ejecuta todos sus *scripts* disponibles para autenticación
- **Default:** ejecuta los *scripts* básicos por defecto de la herramienta
- **Discovery:** recupera información del *target* o víctima
- **External:** *script* para utilizar recursos externos
- **Intrusive:** utiliza *scripts* que son considerados intrusivos para la víctima o *target*
- **Malware:** revisa si hay conexiones abiertas por códigos maliciosos o *backdoors* (puertas traseras)
- **Safe:** ejecuta *scripts* que no son intrusivos
- **Vuln:** descubre las vulnerabilidades más conocidas
- **All:** ejecuta absolutamente todos los *scripts* con extensión NSE disponibles



# ZENMAP



The screenshot shows the Zenmap application window. The title bar is "Zenmap". The menu bar includes "Escaneo", "Herramientas", "Perfil", and "Ayuda (H)". The "Objetivo:" field contains "10.0.0.240" and the "Perfil:" dropdown is set to "Regular scan". The "Escaneo" button is highlighted. The "Comando:" field contains "nmap 10.0.0.240".

Below the command field, there are tabs: "Servidores", "Servicios", "Salida Nmap", "Puertos / Servidores", "Topología", "Detalles del servidor", and "Escaneos". The "Salida Nmap" tab is active, showing the scan results for "nmap 10.0.0.240".

On the left, there is a sidebar with "OS" and "Servidor" sections. The "Servidor" section shows "10.0.0.240" selected.

The main output area displays the following text:

```
nmap 10.0.0.240
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-11 10:50 CEST
Nmap scan report for 10.0.0.240
Host is up (0.0011s latency).
Not shown: 977 closed ports
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
```

At the bottom left, there is a button labeled "Filtrar servidores".

