

## Advanced And Comprehensive Use Of Nmap

```
.....  
[+] Title:      Advanced And Comprehensive Use Of Nmap  
[+] Author:     Juh...  
[+] Contact:    juhscr@hotmail.es  
[+] Date:       December 2010  
[+] Software Link: http://nmap.org  
[+] Tested On: Windows, Linux, Unix, Server's, Solaris  
[+] A little paper about types of scan with nmap tool  
.....
```

- 0v01- Introduction
- 0v02- Little Example
- 0v03- Types of scan
- 0v04- Options 4 scan
- 0v05- Creating and testing our type of scan (legal)
- 0v06- Conclusion

-----++Introduction++-----

Hello my friends soy juh y bueno lo prometido es deuda y bueno Feliz Navidad y Año Nuevo a todos espero la pasen bien y vamos a darle ...

Bueno en esto del pentesting lo mas basico y mas eficaz es obtener la mayor informacion que podamos sobre nuestra victima hablo a nivel general (webs, servers, redes, ordenadors, routers, etc...).

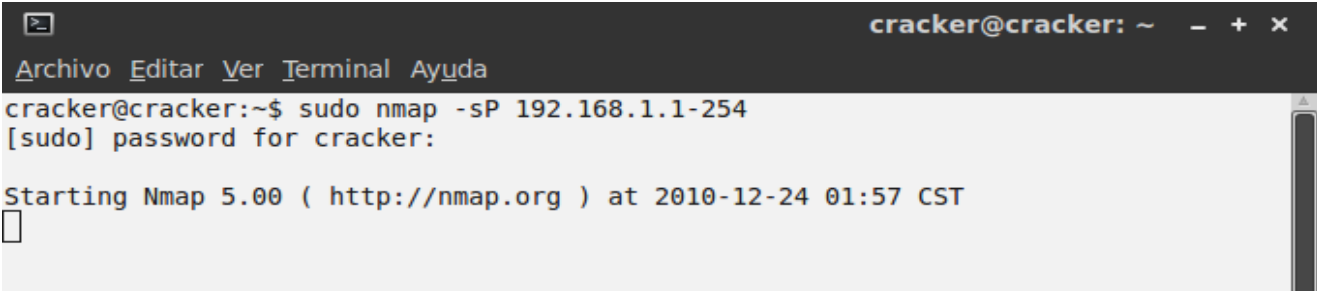
Y como es basico tener una buena informacion recolectada para saber por donde podemos atacar seria bueno comenzar con este potente scanner se llama Nmap y ya vimos en el cuaderno pasado como instalarlo.

Bueno en general hice un 'resumen' de los tipos de scaneo y opciones que podemos usar en nmap basicas y avanzadas (algunas que no puse pero son muy avanzada y aurita no necesitamos tanto XD)

Vamos bueno aqui esta y lean con atencion por que este les servira para crear un tipo de scaneo lo mas cercano a lo que desean obtener y de lo que desean vurlar o scanear y estos es MUY IMPORTANTE.

-----++Pequeño ejemplo++-----

La forma de llamar a nmap serla la siguiente:



```
cracker@cracker: ~ - + x  
Archivo Editar Ver Terminal Ayuda  
cracker@cracker:~$ sudo nmap -sP 192.168.1.1-254  
[sudo] password for cracker:  
  
Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 01:57 CST  
□
```

OK veamos abren su terminal y damos lo siguiente:

sudo : si no tiene permisos root lo usan, si los tienen no lo usan y si lo usan da igual

nmap : llamamos al scanner

-sP : Metodo de scaneo no afuerza es este puede ser -sT -sP -sX -sS -sF -sX -sN (veremos las diferencias mas adelante)

192.168.1.1-254 : nuestro host a scanear en este caso scane 192.168.1.1 hasta el host 192.168.1.254 (tambien veremos mas adelante esto)

Lo importante es que tenga la estructura de como escribir un scaneo.

Ahora si pasemos con los tipos de scaneo y las distintas opciones que tenemos disponibles en nmap, tratare de ser lo mas claro y explicito posible para que sepan como funciona cada uno y en base a esto sepan que tipo de scaneo les sirve mas o si su tipo de scaneo no les sirve lo puedan modificar un poco y mejorarlo segun las necesidades ;D .....

-----++TIPOS DE SCANEO:++-----

-sT :

La mas basica de scaneo tcp si el puerto esta a escuchando "connect()" se mostrara, de lo contrario aparecera como cerrado.

Pros:

Cualquier usuario sin privilegios o con puede lanzarlo.

Contras:

Facil de detectar por filtro firewalls etc..

-sS :

TCP SYN es llamada como la "half open" por que no se abre una conexion tcp completa, se envia un paquete SYN como si fuera a abrir una conexion y espera respuesta, un SYN|ACK muestra el puerto que esa a la escucha, un RST indica que el puerto no esta a la escucha (cerrado). Cuando el escaneo recibe un SYN|ACK inmediatamente manda un RST para cerra la conexion.

Pros:

Dificil de detectar por filtros firewalls etc...

Contras:

Se necesitan permisos de root para construir estos paquetes SYN modificados.  
(usamos la palabra sudo para obtener los permisos recuerden el primer ejemplo XD)

-sF -sX -sN :

Modo Stealth, FIN, Xmas Tree o Null Scan.

Algunos firewalls y filtros vigilan el envío de paquetes SYN en puertos restringidos como por ejemplo Synlogger detecta este tipo de scaneo y a veces pueden ser bypassados.

El escaneo FIN utiliza un paquete vacío (FIN) para enviar, el Xmas Tree activa las flags FIN, URG y PUSH, y el NULL ignora el estándar y hace todo a su forma y debido a esto no funciona con S.O.'s basados en Windows95/NT y podremos distinguir entre dos S.O.'s distintos. Si detecta puertos cerrados lo más seguro es que sea una máquina con UNIX y si encuentra abiertos es probable que sea Windows.

-sP :

Escaneo ping.

Este lo recomiendo más para red local para ver que hosts están arriba para esto este scan envía peticiones de respuesta ICMP a cada ip de la red que especifiquemos, los que responden están activos y los que no pues están down. También puede enviar un paquete TCP ACK al puerto 80(predeterminado) y si obtiene respuesta de RST la máquina está activa. O también puede enviar paquetes SYN y la espera de un RST o un SYN|ACK y con usuarios que no tienen privilegios usa el método connect()

-sU:

Escaneo UDP. (Protocolo de Datagrama de Usuarios)

Este scan envía paquetes UDP de 0 bytes a cada puerto en la ip y si recibe mensaje ICMP de puerto inalcanzable el puerto está cerrado y de lo contrario pues está abierto XD.

-pO :

Ignora el ping

No hace un ping antes de scanearlo es decir se brinca este paso y sirve para brincar firewalls que no permiten ecos de ICMP.

Y se usa generalmente cuando tu sabes que realmente el host que scaneas está UP (osea arriba, online, conectado etc...)

-PT :

Usa el ping TCP para saber que host's están activos en vez de enviar ecos ICMP y esperar respuesta, se envían paquetes TCP|ACK a través de la red y espera respuesta, los host's activos responden con un RST (Para usar ponemos -PT<numero de puerto> ej. -PT143)

-PS :

Usa paquetes SYN en vez de paquetes ACK los host's activos responden con RST .

-PI :

Usa ping (petición de eco ICMP) para encontrar host's activos y direcciones broadcast dirigidas a

subredes.

-PB :

Scaneo ping por defecto pero usa barridos ACK(-PT) e ICMP(-PI) en paralelo.

-----++Opciones De Escaneo++-----

-O :

Detección de sistema operativo

Este detecta el sistema operativo por medio de huellas TCP/IP. Usa técnicas para detectar en la pila de red subyacente del sistema operativo de los host's que se escanen y después las huellas las compara con una base de datos(nmap-os-fingerprint)

-f :

Este hace scaneo de tipo SYN, FIN, XMAS o NULL usando paquetes IP fragmentados. La idea es dividir la cabecera TCP en varios paquetes para así burlar filtros y firewalls

-v :

Información ampliada.

Este arroja muchos resultados sobre lo que esta sucediendo

-D:

Decoys.

Este nos sirve para como su nombre lo dice usar señuelos se usa de esta forma (-D1.2.3.4,5,6,7,8) es un ejemplo ustedes pueden usar de otra forma pero con eso basta.

-h :

Pantalla de referencia parida.

-p :

Rango de puertos.

Sirve para scanear un rango de host's o algunos específicos según el scan (ej. -p 20-30,80,1200)

escanearía del 20 al 30 el puerto 80 y el 1200 se separa por comas si es un puerto en concreto y por guión (-) si es un rango

(si recordamos el ejemplo hacemos algo similar pero con la direccion ip)

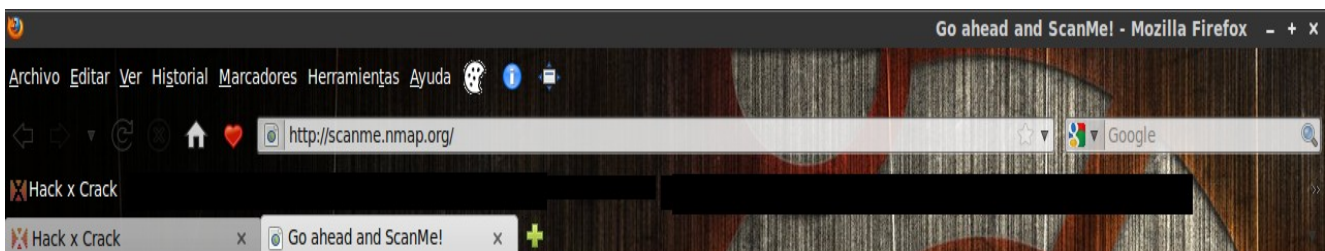
-F : Modo de escaneo rápido.

Esto se debe a que solo escanea aquellos puertos que configura en /etc/services.

-----++Creando y probando tipos de scan's++-----

Ya que vimos en gran parte los tipos de scans y opciones que nos brinda Nmap podremos proceder. Hay una forma legal de probar nuestros scans y tipos de escaneo por que recordemos que todo tiene una ética y muchas veces escaneamos una web sin tener idea de términos legales y muchas veces como no sabes técnicas de privacidad u ofuscación (ip, datos, proxys, metadatos, entre otros ) podemos meternos en problemas por un simple escaneo a una web donde puedes o no dejar un log (Recordemos que siempre hay alguien que sabe mas que nosotros ) y por ello debemos tener cuidado soy muy enfático en esta parte por que la ética en estos ámbitos es muy importante.

Bueno después de mi sermoneo de ética y bla bla bla vamos a ver hay una web que los mismo creadores de nmap nos ofrecen y es scanme.nmap.org y nos permite una serie de 'servicios' en el cual podemos escanear la web y ver los resultados de cada scan y opciones.



Hello, and welcome to Scanme.Nmap.Org, a service provided by the [Nmap Security Scanner Project](#) and [Insecure.Org](#).

We set up this machine to help folks learn about Nmap and also to test and make sure that their Nmap installation (or Internet connection) is working properly. You are authorized to scan this machine with Nmap or other port scanners. Try not to hammer on the server too hard. A few scans in a day is fine, but dont scan 100 times a day or use this site to test your ssh brute-force password cracking tool.

Thanks  
[Fyodor](#)

Bueno hay vemos un pantallazo de la web.

Ahora ire poniendo el tipo de scan y el resultado para que vayamos comparando... (todos van dirigidos a la web scanme.nmap.org y sirve tanto para webs como para servers o computadores normales poniendo la ip en lugar de la direccion web)

-sT

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sT scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:34 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    closed smtp
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth

Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds
```

-sS

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:51 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 37.04 seconds
```

-sF

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sF scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:54 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 995 open|filtered ports
PORT      STATE SERVICE
70/tcp    closed gopher
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 33.43 seconds
```

-sX

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sX scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:56 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 995 open|filtered ports
PORT      STATE SERVICE
70/tcp    closed gopher
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 33.59 seconds
```

-sN

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sN scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:57 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 997 open|filtered ports
PORT      STATE SERVICE
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 9.44 seconds
```

-sP

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sP scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 02:59 CST
Host scanme.nmap.org (64.13.134.52) is up (0.068s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

-sU

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sU scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:01 CST
All 1000 scanned ports on scanme.nmap.org (64.13.134.52) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 74.46 seconds
```

Ahora yo tomare el tipo de scan -sS y le iremos complementando con mas opciones me iran entendiendo jejej ...

-pO

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -pO scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:06 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
PORT STATE SERVICE
0/tcp filtered unknown
Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
```

-PT<numero de puerto>

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -pT113 scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:09 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
PORT STATE SERVICE
113/tcp closed auth
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

-PS



```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PS scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:10 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 31.40 seconds
```

-PI

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PI scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:12 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```

-PB

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PB scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:14 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 34.48 seconds
```

Ahora agreguemos mas opciones jejeje ...

-O

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PB -O scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:17 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (96%), Gemtek embedded (96%), Siemens embe
dded (96%), Aastra embedded (94%), Belkin Linux 2.4.X (92%), Inventel embedded (92%),
Telekom embedded (92%), USRobotics embedded (92%)
Aggressive OS guesses: Linux 2.6.24-1 (Fedora Core 5) (96%), Gemtek P360 WAP or Siemen
s Gigaset SE515dsl wireless broadband router (96%), Linux 2.6.15 - 2.6.26 (95%), Linux
2.6.23 (Gentoo) (95%), Aastra RFP L32 IP DECT WAP (94%), Linux 2.6.13 - 2.6.24 (94%),
Linux 2.6.13 - 2.6.27 (94%), Linux 2.6.15 - 2.6.18 (94%), Linux 2.6.18 (94%), Linux 2
.6.18 - 2.6.24 (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 23.86 seconds
```

-f

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PB -f scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:21 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 10.67 seconds
```

-v

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PB -v scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:22 CST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 03:22
Scanning 64.13.134.52 [3 ports]
Completed Ping Scan at 03:22, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:22
Completed Parallel DNS resolution of 1 host. at 03:22, 0.05s elapsed
Initiating SYN Stealth Scan at 03:22
Scanning scanme.nmap.org (64.13.134.52) [1000 ports]
Discovered open port 22/tcp on 64.13.134.52
Discovered open port 53/tcp on 64.13.134.52
Discovered open port 80/tcp on 64.13.134.52
Completed SYN Stealth Scan at 03:22, 26.07s elapsed (1000 total ports)
Host scanme.nmap.org (64.13.134.52) is up (0.17s latency).
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 992 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
31337/tcp closed Elite

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.43 seconds
Raw packets sent: 2010 (88.416KB) | Rcvd: 24 (1006B)
```

-p

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -p 100-115,230,1120 scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:25 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
PORT      STATE SERVICE
100/tcp    filtered newacct
101/tcp    filtered hostname
102/tcp    filtered iso-tsap
103/tcp    filtered gppitnp
104/tcp    filtered acr-nema
105/tcp    filtered unknown
106/tcp    filtered pop3pw
107/tcp    filtered unknown
108/tcp    filtered snagas
109/tcp    filtered pop2
110/tcp    filtered pop3
111/tcp    filtered rpcbind
112/tcp    filtered mcidas
113/tcp    closed  auth
114/tcp    filtered audionews
115/tcp    filtered sftp
230/tcp    filtered unknown
1120/tcp   filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
```

-F

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -F scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:27 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 94 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed auth
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.38 seconds
```

Bueno ya vimos todos ahora voy crear uno a mis necesidades para que vean a que me refiero...

OK yo necesito un scaneo que sea “half open” para poder “bypasear” el firewall supongamos, que también tenga barrido ACK y me de el S.O. Del target (host) que me scane del puerto 22 al 55 y los puertos específicos 55 60 113 y 445 para saber si esta abiertos o no entonces mi scan quedaría así...  
sudo nmap -sS -PB -O -p 22-55,80,113,445 scanme.nmap.org

```
cracker@cracker: ~ - + x
Archivo Editar Ver Terminal Ayuda
cracker@cracker:~$ sudo nmap -sS -PB -O -p 22-55,80,113,445 scanme.nmap.org

Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-24 03:30 CST
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 32 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
113/tcp   closed auth
445/tcp   closed microsoft-ds
Device type: general purpose|WAP|broadband router
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (95%), Gemtek embedded (95%), Siemens
embedded (95%), Aastra embedded (93%), Belkin Linux 2.4.X (92%), Inventel embedded
(92%), Telekom embedded (92%), USRobotics embedded (92%)
Aggressive OS guesses: Linux 2.6.20-1 (Fedora Core 5) (95%), Linux 2.6.15 - 2.6.26
(95%), Gemtek P360 WAP or Siemens Gigaset SE515dsl wireless broadband router (95%
), Linux 2.6.13 - 2.6.20 (94%), Linux 2.6.13 - 2.6.24 (94%), Linux 2.6.13 - 2.6.27
(94%), Linux 2.6.18 (94%), Linux 2.6.18 - 2.6.24 (94%), Linux 2.6.18 - 2.6.26 (94
%), Linux 2.6.23 (Gentoo) (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.32 seconds
```

y listo ya tenemos nuestro scaneo personalizado que se adapta a nuestras necesidades.

-----++Conclusiones++-----

Ya vimos una gran cantidad de opciones y parámetros a configurar y apuesto que si usan google podrán encontrar cosas mas avanzadas y mas y mas pero en general ya vimos como crear nuestro propio scaneo y tengan en cuenta que también sirve para ordenadores servers entre otras cosas practiquen los scaneos y configurar distintos scaneos por que en el siguiente cuaderno mezclaremos nmap con Metaplasmo y veremos que nos da un resultado bastante interesante vale ?

Bueno pues después de la clase de nmap los dejo hasta pronto ya saben, feliz navidad y año nuevo a todos les dejo mi correo hay pueden enviarme o contactarme por cualquier duda saludos amigos!  
juh@hackxcrack.es