

Práctica 31 Escaneadores y exploración de puertos. (Por HxC Mods-Adm)

Fireport

Es un sencillo escaneador que nos muestra los puertos TCP abiertos en la máquina, basta con indicar el puerto de inicio (Start Port) y el puerto final (End Port) para que encuentre los servicios disponibles.

El apartado Sockets es de especial interés, puesto que nos permitirá un escaneo más rápido dependiendo del número de sockets a usar.

Muchas de las herramientas que utilizaremos a partir de ahora pueden utilizar uno o varios sockets, así que voy a explicar “algo más de ello”

Socks es un protocolo de red, como lo puede ser TCP, UDP, FTP, http, etc., socks afecta exclusivamente a las conexiones TCP/IP.

Se utiliza en proxys, VPN, Firewall, etc y su función es probar los paquetes de datos entrantes y salientes

La versión de Socks puede ser la 4 ó la 5, ésta última además de ser más robusta permite:

- autenticación
- UDP
- DNS

Para usar socks necesitamos un cliente Sockets y un servidor de Socks + un puerto.

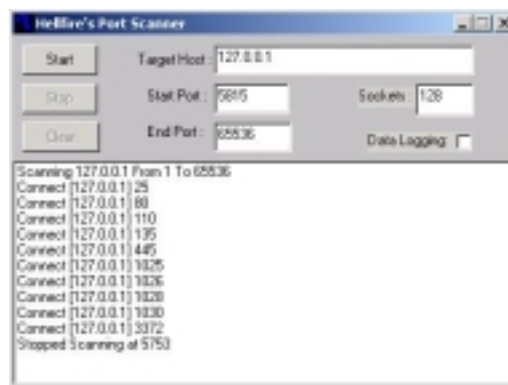
Para establecer conexiones Socks, Windows utiliza una librería llamada Ws2_32.dll y los programas que usan winsock pueden realizar conexiones ocultando la IP, debido a que el protocolo socks lo permite.

Dicho de otra forma, que si “anonimizamos” éste escaneador mediante socksCap y Socks Chain como ya se aprendió anteriormente, el escaneado será anónimo.

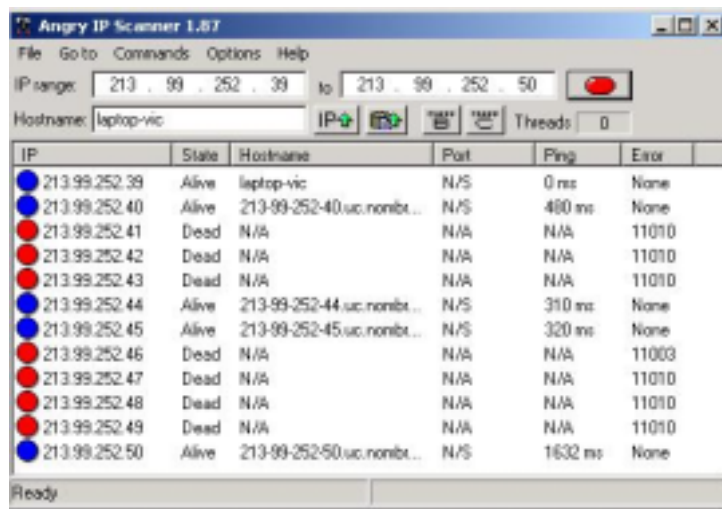
Las aplicaciones que dependen de NetBios (ya veremos que es esto) utilizan netbt.sys no ws2_32.dll y no se pueden anonimizar porque Netbios no utiliza Sockets.

El número de sockets en windows es de aproximadamente 32.000 así que no pongas un número muy elevado, muchas de las aplicaciones que usas utilizan un gran número de sockets para establecer conexiones y si “se te acaban” los sockets disponibles no funcionarán, lo mismo le ocurriría al equipo destino, si usamos muchos sockets por cada conexión puede rechazar el escaneado.

Por el momento piensa que un socket lo compone una conexión + dirección ip + puerto



IpScan



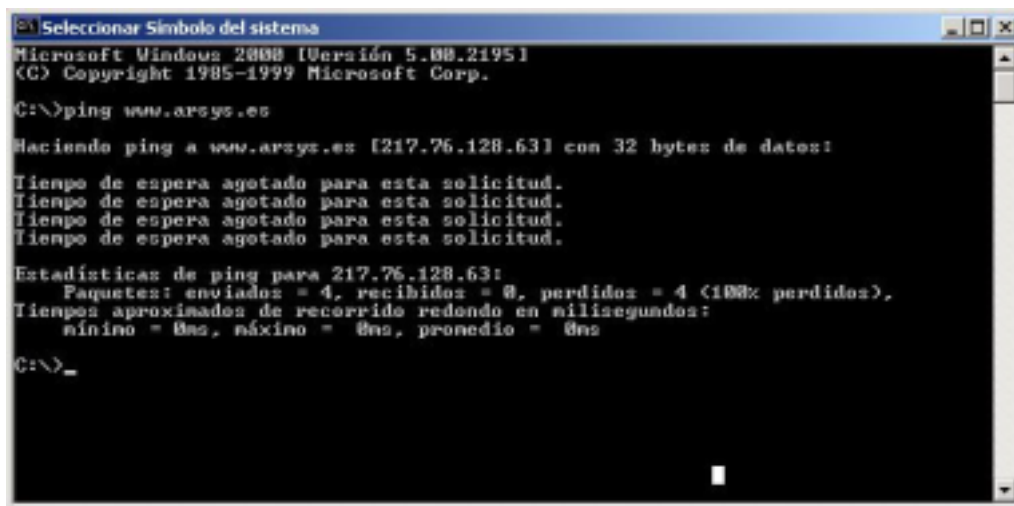
IpScan sería el equivalente al comando ping del Sistema Operativo, con la ventaja de poder explorar un rango de red completo y de ser extremadamente rápido.

Además *IpScan* mediante el *menú de Options-Options* puede establecer el puerto de conexión, esto es que podemos determinar la existencia o no de la máquina destino por sus servicios.

Vamos a ver, ya hemos comentado que muchos firewalls, routers, etc. pueden filtrar las peticiones ping echo y rechazar sistemáticamente los barridos ping y escaneados de puertos, pues bien con éste podemos “saltarnos” esa restricción

Ejemplo:

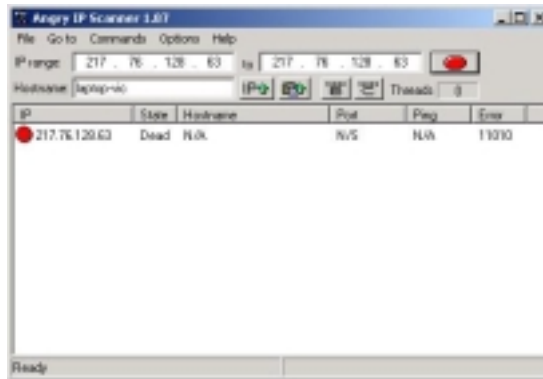
Vamos a realizar un ping desde una shell a www.arsys.es



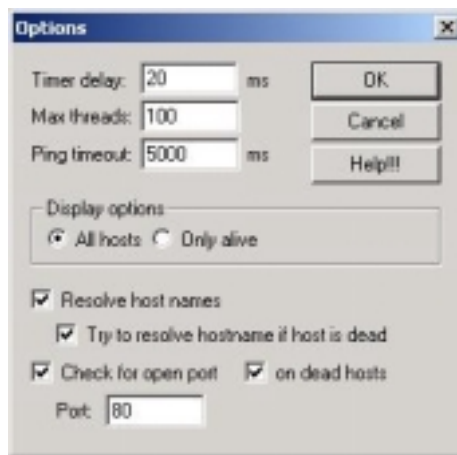
Como ves, el host rechaza la petición y “parece” que no está disponible, si abrimos Internet Explorer y accedemos a www.arsys.es verás que SI EXISTE y que SI ESTA DISPONIBLE.

Foro de HackXcrack

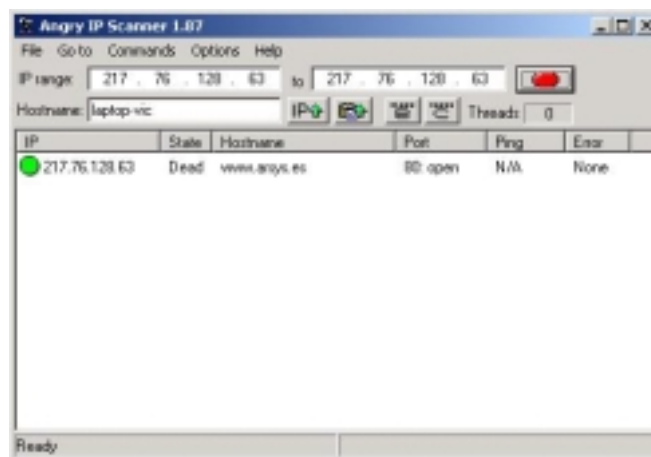
Ahora vamos a **IPScan** y lo probamos con la dirección IP 217.76.128.63 que es la IP de arsys según nos informó el mandato ping, el resultado sigue siendo negativo, el host no existe.



Bien pues ahora, el *menú de options-options* selecciona esto:

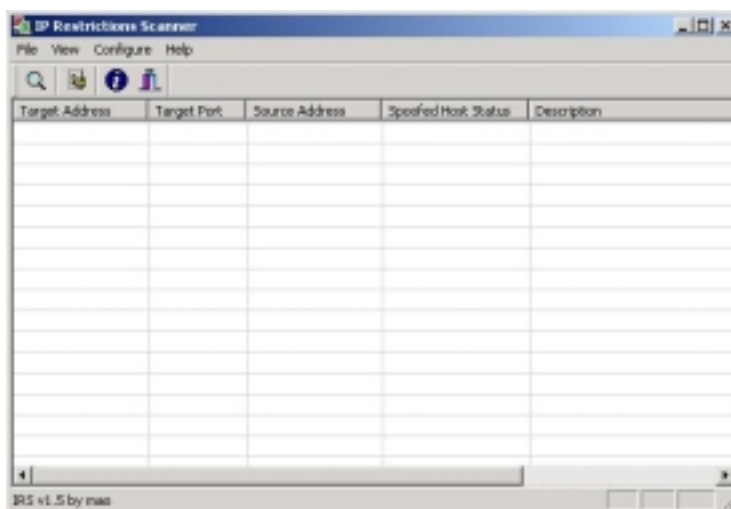


Pulsa OK y volvemos a escanear la dirección de arsys (217.76.128.63)



Como ves aunque la columna state aparece como “muerto” dead, responde positivamente al puerto escaneado que no es otro que el 80 (servidor Web)

Irs



Ip Restrictions Scanner, suena bien, Escaneado de IP restringidas.

Lo primero, ésta herramienta necesita de un nuevo protocolo de disco, llamado *winpcap*, no es la única, por ejemplo *nmapwin* también la necesitará, así que no se te olvide instalarlo.

La principal “*virtud*” de IRS es que combina “*envenenamientos ARP*” (ARP Poisoning) y “*medio-escaneado*” (Half-Scan), éstas son técnicas que nos permiten encontrar los servicios activos de un host que tiene restringido el acceso.

Además y por si fuera poco, IRS aplica técnicas de *spoof* en sus conexiones de puertos TCP sobre el objetivo.

Vamos a explicar todo estos términos extraños:

Envenenamiento ARP

ARP es “otro protocolo”, Protocolo de Resolución de Direcciones y asigna direcciones IP a direcciones hardware físicas, es como si fuese una tabla relaciones entre la dirección IP y dirección MAC de la tarjeta o tarjetas de red.

Claro, pues el envenenamiento ARP consiste en trucar la caché de ARP y hacerse pasar por otro de forma que la máquina objetivo “nos reconozca” como un equipo de confianza.

Half Scan

Realmente tendría que haber comenzado explicando los diferentes tipos de escaneado y aburrirte con las explicaciones técnicas de cada uno de ellos o “deslumbrarte” con mis conocimientos técnicos “oh! Gran voz del saber, explícame todos los tipos de escaneado...”

Foro de HackXcrack

Una conexión TCP es un acuerdo entre **dos máquinas** mediante **tres caminos**

Camino 1 CLIENTE ----- paquete SYN enviado por el cliente -----> SERVIDOR

Camino 2 CLIENTE <-----paquete SYN/ACK enviado por el servidor----- SERVIDOR

Camino 3 CLIENTE -----paquete ACK enviado por el cliente-----> SERVIDOR

Dicho de otra forma:

- 1º) El cliente “pide” al servidor que se quiere comunicar (SYN)
- 2º) El servidor “concede” la petición (SYN/ACK)
- 3º) El cliente “confirma” la concesión (ACK)

Esta sería una conexión completa TCP, pero ¿Qué pasaría si uno de los dos extremos “se olvidase” de algo?, ¿Qué pasa si el servidor rechaza SYN o no envía ACK?

Vale, vale es algo complicado, comprende lo que sigue:

Exploración TCP SYN: Conocida como la exploración “medio abierta” (Half Scan) en la que el cliente no envía el paso 3 (ACK) sino que envía un RST/ACK para que no se establezca nunca una conexión completa. Esta técnica es más sigilosa y puede no ser detectada por la máquina objetivo (servidor)

¿Hay más técnicas de escaneado?

Si, vete entendiendo bien, esto:

Exploración TCP FIN: El cliente envía un paquete FIN (en lugar de SYN) al puerto destino de tal forma que el servidor responde con un RST por todos los puertos cerrados

Exploración de árbol TCP: El cliente envía paquetes FIN, URG y PUSH, el servidor responde con un RST de todos los puertos cerrados

Exploración Nula o P0: Esta técnica desactiva todas las banderas y el servidor responderá con un RST de sus puertos cerrados.

Exploración del puerto Origen: El cliente especifica el puerto origen (normalmente del 1 al 1023) para realizar el escaneado, de ese modo se pueden escanear otros puertos a partir del indicado. Esta técnica permite “saltarse” algunos firewalls.

Exploración UDP: consiste en lo mismo pero para puertos UDP, la principal desventaja es que como UDP no es fiable (no confirma) podemos encontrar falsos positivos.

Todavía hay más: **Exploración ACK, Exploración de Ventanas TCP, Exploración RPC**, etc., e incluso una variación de la exploración SYN que no envía nunca el paso 3, por lo que el servidor se queda esperando.... si enviamos muchos de esos paquetes así podemos “tirar abajo” el servidor, esto se conoce como inundación SYN.

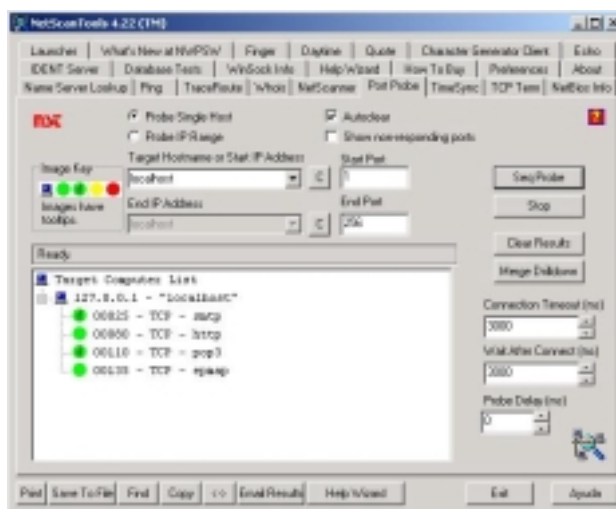
IRS, utiliza o puede utilizar el escaneado SYN, para probar los otros tipos de escaneo puedes ir descargando e instalando nmapwin, que utiliza todas estas técnicas y mas.

Spoof

Consiste en falsificar la dirección de origen del paquete IP

Bueno, para un simple escaneo puede resultarte “algo complejo” cuando toquemos el tema de los sniffers comprenderás mejor todos éstos términos y te enseñaré a aplicarlos, incluso usaremos IRS para ello, de momento basta con que recuerdes la terminología y comprendas sus acciones.

NetScanTools

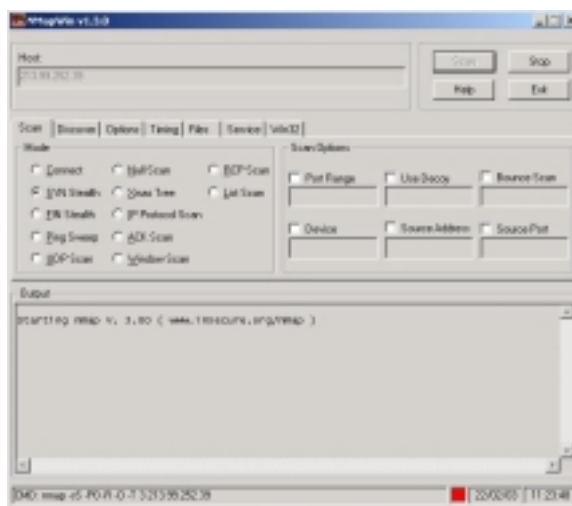


Net Scan Tools, es más que una herramienta de simple escaneado, comprende muchas utilidades en sí misma: Consultas DNS, Transferencias de Zona, whois, NetBios, Finger, etc... y además es multitarea, puedes escanear un rango de Ip's y realizar la tranferencia de zona de un DNS simultáneamente.

Puede escanear puertos TCP y UDP, admite múltiples procesos (thread) simultáneos con lo cual es bastante rápido, además es un escaneador bastante fiable.

Su inconveniente es que no es gratis

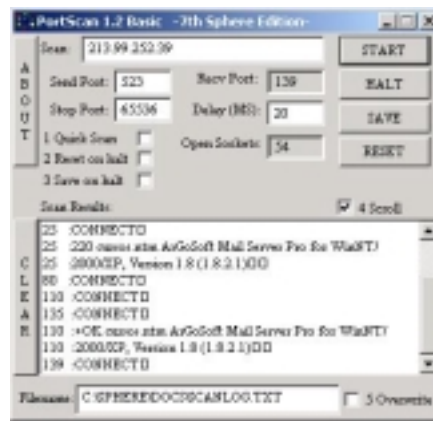
NmapWin



Nmap es un clásico entre los clásicos, en un principio sólo para el mundo unís y ahora también disponible en Windows, precisa de WinPcap y puede ser usado desde su interface gráfica como desde la línea de comandos, con la ventaja de poder así crearnos nuestros propios scripts.

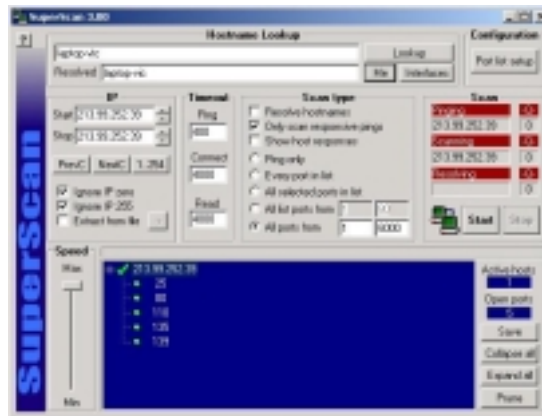
Nmap permite todos los tipos de escaneado descritos anteriormente y alguno más como el escaneo paranoico o con “otra máquina por medio” de forma que el objetivo tiene doble trabajo, identificar qué es un escaneo y qué no lo es, en la parte de prácticas nmap sera uno de nuestros ejercicios.

PortScan



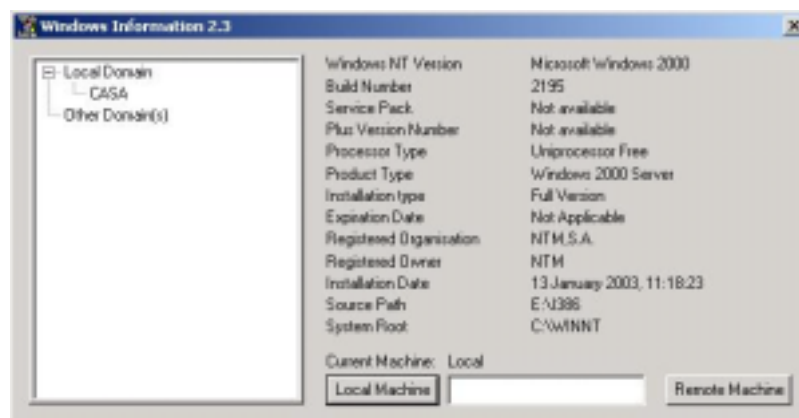
Después de Nmap o NetScanTools, port scan te resultará simple e incluso algo soso, no te olvides de él, es de lo más rápido y fiable que conozco.

SuperScan



Es otro de los clásicos, rápido, sencillo y configurable. Ah! Y GRATIS. Úsalo es de los buenos.

WinInfo



Realmente no es un escáner, pero te puede ir muy bien si deseas conocer las características de una máquina Windows.