NMAP - Herramienta de exploracion de red y escaner de seguridad.

SINOPSIS

nmap [Tipos(s)de escaneo] [Opciones] <servidor o red #1 ... [#N]>

DESCRIPCION

Nmap ha sido disenado para permitir a administradores de sistemas y gente curiosa en general el escaneo de grandes redes para determinar que servidores se encuentran activos y que servicios ofrecen. nmap es compatible con un gran numero de tecnicas de escaneo como: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, and Null scan. Vease la seccion Tipos de Escaneo para mas detalles. nmap proporciona tambien caracteristicas avanzadas como la deteccion remota del sistema operativo por medio de huellas TCP/IP , escaneo tipo stealth (oculto), retraso dinamico y calculos de retransmision, escaneo paralelo, deteccion de servidores inactivos por medio de pings paralelos, escaneo con senuelos, deteccion de filtrado de puertos, escaneo por fragmentacion y especificacion flexible de destino y puerto.

Se han hecho grandes esfuerzos encaminados a proporcionar un rendimiento decente para usuarios normales (no root). Por desgracia, muchos de los interfaces criticos del kernel (tales como los raw sockets) requieren privilegios de root. Deberia ejecutarse nmap como root siempre que sea posible.

OPCIONES

En general, pueden combinarse aquellas opciones que tengan sentido en conjunto. Algunas de ellas son especificas para ciertos modos de escaneo. nmap trata de detectar y advertir al usuario sobre el uso de combinaciones de opciones sicoticas o no permitidas.

Si usted es una persona impaciente, puede pasar directamente a la seccion ejemplos al final de este documento, donde encontrara ejemplos de los usos mas corrientes. Tambien puede ejecutar el comando nmap -h para una pagina de referencia rapida con un listado de todas las opciones.

Tipos de Escaneo

-sT Escaneo TCP connect(): Es la forma mas basica de escaneo TCP. La llamada de sistema connect() proporcionada por nuestro sistema operativo se usa para establecer una conexion con todos los puertos interesantes de la maquina. Si el puerto esta a la escucha, connect() tendra exito, de otro modo, el puerto resulta inalcanzable. Una ventaja importante de esta tecnica es que no resulta necesario tener privilegios especiales. Cualquier usuario en la mayoria de los sistemas UNIX tiene permiso para usar esta llamada.

Este tipo de escaneo resulta facilmente detectable dado que los registros del servidor de destino muestran un monton de conexiones y mensajes de error para aquellos servicios que accept() (aceptan) la conexion para luego cerrarla inmediatamente.

-sS Escaneo TCP SYN: A menudo se denomina a esta tecnica escaneo "half open" (medio abierto), porque no se abre una conexion TCP completa. Se envia un paquete SYN, como si se fuese a abrir una conexion real y se espera que llegue una respuesta. Un SYN|ACK indica que el puerto esta a la escucha. Un RST es indicativo de que el puerto no esta a la escucha. Si se recibe un SYN|ACK, se envia un RST inmediatamente para cortar la conexion (en realidad es el kernel de nuestro sistema operativo el que hace esto por nosotros). La ventaja principal de esta tecnica de escaneo es que sera registrada por muchos menos servidores que la anterior. Por desgracia se necesitan privilegios de root para construir estos paquetes SYN modificados.

-sF -sX -sN

Modos Stealth FIN, Xmas Tree o Nul scan: A veces ni siquiera el escaneo SYN resulta lo suficientemente clandestino. Algunas firewalls y filtros de paquetes vigilan el envio de paquetes SYN a puertos restringidos, y programas disponibles como Synlogger y Courtney detectan este tipo de escaneo. Estos tipos de escaneo avanzado, sin embargo, pueden cruzar estas barreras sin ser detectados.

La idea es que se requiere que los puertos cerrados respondan a nuestro paquete de prueba con un RST, mientras que los puertos abiertos deben ignorar los paquetes en cuestion (vease RFC 794 pp 64). El escaneo FIN utiliza un paquete FIN vacio (sorpresa) como prueba, mientras que el escaneo Xmas tree activa las flags FIN, URG y PUSH. El escaneo NULL desactiva todas las flags. Por desgracia Microsoft (como de costumbre) decidio ignorar el estandar completamente y hacer las cosas a su manera. Debido a esto, este tipo de escaneo no funcionara con sistemas basados en Windows95/NT. En el lado positivo, esta es una buena manera de distinguir entre las dos plataformas. Si el escaneo encuentra puertos cerrados, probablemente se trate de una maquina UNIX, mientras que todos los puertos abiertos es indicativo de Windows. Excepcionalmente, Cisco, BSDI, HP/UX, MVS, y IRIX tambien envian RSTs en vez de desechar el paquete.

-sP Escaneo ping: A veces unicamente se necesita saber que servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada direccion IP de la red que se especifica. Aquellos servidores que responden se encuentran activos. Desafortunadamente, algunos sitios web como microsoft.com bloquean este tipo de paquetes. Nmap puede enviar tambien un paquete TCP ack al puerto 80 (por defecto). Si se obtiene por respuesta un RST, esa maquina esta activa. Una tercera tecnica implica el envio de un paquete SYN y la espera de de un RST o un SYN/ACK. Para usuarios no root se usa un metodo connect().

Por defecto (para usuarios no root), nmap usa las tecnicas ICMP y ACK en paralelo. Se puede cambiar la opcion -p descrita mas adelante.

Notese que el envio de pings se realiza por defecto de todas maneras y que solamente se escanean aquellos servidores de los que se obtiene respuesta. Use esta opcion solamente en el caso de que desee un ping sweep (barrido ping) sin hacer ningun tipo de escaneo de puertos.

-sU Escaneo Udp: Este metodo se usa para saber que puertos UDP (Protocolo de Datagrama de Usuario, RFC 768) estan abiertos en un servidor. La tecnica consiste en enviar paquetes UCP de 0 bytes a cada puerto de la maquina objetivo. Si se recibe un mensaje ICMP de puerto no alcanzable, entonces el puerto esta cerrado. De lo contrario, asumimos que esta abierto.

Alguna gente piensa que el escaneo UDP no tiene sentido. Normalmente les recuerdo el reciente agujero Solaris rcpbind. Puede encontrarse a rcpbind escondido en un puerto UDP no documentado en algun lugar por encima del 32770. Por lo tanto, no importa que el 111 este bloqueado por la firewall. Pero, cquien puede decir en cual de los mas de 30000 puertos altos se encuentra a la escucha el programa? iCon un escaner UDP se puede! Tenemos tambien el programa de puerta trasera cDc Back Orifice que se oculta en un puerto UDP configurable en las maquinas Windows, por no mencionar los muchos servicios frecuentemente vulnerables que usan UDP como snmp, tftp, NFS, etc.

Por desgracia, el escaneo UDP resulta a veces tremendamente lento debido a que la mayoria de los servidores implementan una sugerencia recogida en el RFC 1812 (seccion 4.3.2.8) acerca de la limitacion de la frecuencia de mensajes de error ICMP. Por ejemplo, el kernel de Linux (en /ipv4/icmp.h) limita la generacion de mensajes de destino inalcanzable a 80 cada cuatro segundos, con una penalizacion de 1/4 de segundo si se rebasa dicha cantidad. Solaris tiene unos limites mucho mas estrictos (mas o menos 2 mensajes por segundo) y por lo tanto lleva mas tiempo hacerle un escaneo. nmap detecta este limite de frecuencia y se ralentiza en consecuencia, en vez de desbordar la red con paquetes inutiles que la maquina destino ignorara.

Como de costumbre, Microsoft ignoro esta sugerencia del RFC y no parece que haya previsto ningun tipo de limite de frecuencia para las maquinas Windows. Debido a esto resulta posible escanear los 65K puertos de una maquina Windows muy rapidamente. iWoop!

-b <ftp relay host>

Ataque de rebote FTP: Una caracteristica "interesante" del protocolo FTP (FRC 959) es la posibilidad de realizar conexiones ftp tipo "proxy". En otras palabras, ime resultaria posible conectarme desde malvado.com al servidor ftp de destino.com y pedirle a ese servidor que enviase un archivo a CUALQUIER PARTE de Internet! Aun asi, esto podria haber funcionado bien en 1985 cuando se escribio el RFC, pero en la Internet actual, no podemos permitir que la gente vaya por ahi asaltando servidores ftp y pidiendoles que escupan sus datos a puntos arbitrarios de Internet. Tal y como escribio *Hobbit* en 1985, este defecto del protocolo "puede usarse para enviar mensajes de correo y noticias cuyo rastro sera virtualmente imposible de seguir, machacar servidores en varios sitios web, llenar discos, tratar de saltarse firewalls y , en general, resultar molesto y dificil de detectar al mismo tiempo." Nosotros explotaremos este defecto para (sorpresa, sorpresa) escanear puertos TCP desde un servidor ftp "proxy". De este modo nos podriamos conectar a un servidor ftp tras una firewall, y luego escanear aquellos puertos que con mas probabilidad se encuentren bloqueados (el 139 es uno bueno). Si el servidor ftp permite la lectura y escritura en algun directorio (como por ejemplo /incoming), se pueden enviar datos arbitrarios a puertos que se encuentren abiertos (aunque nmap no realiza esta funcion por si mismo).

El argumento que se pasa a la opcion 'b' es el host que se pretende usar como proxy, en notacion URL estandar. El formato es: nombre_de_usuario:password@servidor:puerto. Todo excepto servidor es opcional. Para determinar que servidores son vulnerables a este ataque, vease mi articulo en Phrack 51. Se encuentra disponible una version actualizada en la URL de nmap (http://www.insecure.org/nmap).

Opciones Generales

No se requiere ninguna pero algunas de ellas pueden resultar de gran utilidad.

-p0 No intenta hacer ping a un servidor antes de escanearlo. Esto permite el escaneo de redes que no permiten que pasen peticiones (o respuestas)de ecos ICMP a traves de su firewall. microsoft.com es un ejemplo de una red de este tipo, y, por lo tanto, deberia usarse siempre -p0 o -PT80 al escanear microsoft.com.

-PT Usa el ping TCP para determinar que servidores estan activos. En vez de enviar paquetes de peticion de ecos ICMP y esperar una respuesta, se lanzan paquetes TCP ACK a traves de la red de destino (o a una sola maquina) y luego se espera a que lleguen las respuestas. Los servidores activos responden con un RST. Esta opcion mantiene la eficiencia de escanear unicamente aquellos servidores que se encuentran activos y la combina con la posibilidad de escanear redes/servidores que bloquean los paquetes ping. Para los usuarios no root se usa connect(). Para establecer el puerto de destino de los paquetes de prueba use -PT <numero de puerto). El puerto por defecto es el 80, dado que normalmente este puerto no es un puerto filtrado.

-PS Esta opcion usa paquetes SYN (peticion de conexion) en vez de los paquetes ACK para usuarios root. Los servidores activos deberian responder con un RST (o, en raras ocasiones, un SYN|ACK).

-PI Esta opcion usa un paquete ping (peticion de eco ICMP) verdadero. Encuentra servidores que estan activos y tambien busca direcciones de broadcast dirigidas a subredes en una red. Se trata de direcciones IP alcanzables desde el exterior que envian los paquetes IP entrantes a una subred de servidores. Estas direcciones deberian eliminarse, si se encontrase alguna, dado que suponen un riesgo elevado ante numerosos ataques de denegacion de servicio (el mas corriente es Smurf).

-PB Este es el tipo de ping por defecto. Usa los barridos ACK (-PT) e ICMP (-PI) en paralelo. De este modo se pueden alcanzar firewalls que filtren uno de los dos (pero no ambos).

-O Esta opcion activa la deteccion remota del sistema operativo por medio de la huella TCP/IP. En otras palabras, usa un punado de tecnicas para detectar sutilezas en la pila de red subyacente del sistema operativo de los servidores que se escanean. Usa esta informacion para crear una 'huella' que luego compara con una base de datos de huellas de sistemas operativos conocidas (el archivo nmap-os-fingerprints) para decidir que tipo de sistema se esta escaneando.

Si encuentra una maquina diagnosticada erroneamente que tenga por lo menos un puerto abierto, me seria de gran utilidad que me enviase los detalles en un email (es decir, se encontro la version xxx de tal cosa y se detecto este u otro sistema operativo..). Si encuentra una maquina con al menos un puerto abierto de la cual nmap le informe "sistema operativo desconocido", le estaria agradecido si me enviase la direccion IP junto con el nombre del sistema operativo y el numero de su version. Si no me puede enviar la direccion IP, una alternativa seria ejecutar nmap con la opcion -d y enviarme las tres huellas que obtendria como resultado junto con el nombre del sistema operativo y el numero de version. Al hacer esto, esta contribuyendo a aumentar el numero importante de sistemas operativos conocidos por namp y de este modo el programa resultara mas exacto para todo el mundo.

-I Esta opcion activa el escaneo TCP de identificacion contraria. Tal y como comenta Dave Goldsmith en un correo Bugtrat de 1996, el protocolo ident (rfc 1413) permite la revelacion del nombre del usuario propietario de cualquier proceso conectado via TCP, incluso aunque ese proceso no haya iniciado la conexion. De este modo se puede, por ejemplo, conectar con el puerto http y luego usar identd para descubrir si el servidor esta ejecutandose como root. Esto solo se puede hacer con una conexion TCP completa con el puerto de destino (o sea, la opcion de escaneo -sT). Cuando se usa -I,

se consulta al identd del servidor remoto sobre cada uno de los puertos abiertos encontrados en el sistema. Por supuesto, esto no funcionara si el servidor en cuestion no esta ejecutando identd.

-f Esta opcion hace que el escaneo solicitado de tipo SYN, FIN, XMAS, o NULL use pequenos paquetes IP fragmentados. La idea consiste en dividir la cabecera TCP en varios paquetes para ponerselo mas dificil a los filtros de paquetes, sistemas de deteccion de intrusion y otras inconveniencias por el estilo que tratan de saber lo uno esta haciendo. iTenga cuidado con esto! Algunos programas tienen problemas a la hora de manejar estos paquetes tan pequenos. Mi sniffer favorito produjo un error de segmentacion inmediatamente despues de recibir el primer fragmento de 36 bytes. iDespues de este viene uno de 24 bytes! Mientras que este metodo no podra con filtros de paquetes y firewalls que ponen en cola todos los fragmentos IP (como en el caso de la opcion CONFIG_IP_ALWAYS_DEFRAG en la configuracion del kernel de Linux), tambien es verdad que algunas redes no pueden permitirse el efecto negativo que esta opcion causa sobre su rendimiento y por lo tanto la dejan desactivada.

Notese que no he coseguido que esta opcion funcione con todos los sistemas. Funciona bien con mis sistemas Linux, FreeBSD y OpenBSD y algunas personas han informado de exitos con otras variantes *NIX.

-v Modo de informacion ampliada. Esta opcion resulta muy recomendable y proporciona gran cantidad de informacion sobre lo que esta sucediendo. Puede usarla dos veces para un efecto mayor. iUse -d un par veces si lo que quiere es volverse loco haciendo scroll en su pantalla!

-h Esta opcion tan practica muestra una pantalla de referencia rapida sobre las opciones de uso de nmap. Quizas haya notado que esta pagina de manual no es precisamente una "referencia rapida" :)

-o <nombre_de_archivo_de_registro>
Esta opcion guarda los resultados de sus escaneos en forma humanamente inteligible en el archivo especificado como argumento.

-m <nombre_de_archivo_de_registro>

Esta opcion guarda los resultados de sus escaneos en un formato comprensible para una maquina en el archivo especificado como argumento.

-i <nombre_de_archivo_de_entrada>

Lee especificaciones de servidores o redes de destino a partir del archivo especificado en vez de hacerlo de la linea de comandos. El archivo debe contener una lista de expresiones de servidores o redes separadas por espacios, tabuladores o nuevas lineas. Use un guion (-) como nombre_de_archivo_de_entrada si desea que nmap tome las expresiones de servidores de stdin. Vease la seccion Especificacion de Objetivo para mas informacion sobre expresiones con las que poder completar este archivo.

-p <rango de puertos>

Esta opcion determina los puertos que se quieren especificar. Por ejemplo, '-p 23' probara solo el puerto 23 del servidor(es) objetivo. '-p 20-30,139,60000-' escanea los puertos del 20 al 30, el puerto 139 y todos los puertos por encima de 60000. Por defecto se escanean todos los puertos entre el 1 y el 1024 asi como los que figuran en el archivo /etc/services.

-F Modo de escaneo rapido.

Implica que solo se desean escanear aquellos puertos que figuran en /etc/services. Obviamente esto resulta mucho mas rapido que escanear cada uno de los 65535 puertos de un servidor.

-D <senuelo1 [,senuelo2][,ME],...>

Especifica que se desea efectuar un escaneo con senuelos, el cual hace que el servidor escaneado piense que la red destino del escaneo esta siendo escaneada tambien por el servidor(es) especificados como senuelos. Asi, sus IDs pueden informar de entre 5 y 10 escaneos procedentes de direcciones IP unicas, pero no sabran que direccion IP les estaba escaneando realmente y cuales eran senuelos inocentes.

Separe cada servidor senuelo con comas, y puede usar opcionalmente 'ME' como senuelo que representa la posicion que quiere que ocupe su direccion IP. Si coloca 'ME' en la sexta posicion o superior, es muy poco probable que algunos escaneres de puertos comunes (como el excelente scanlogd de Solar Designer) lleguen incluso a mostrar su direccion IP. Si no se usa 'ME', nmap le colocara a usted en una posicion aleatoria.

Notese que aquellos servidores usados como senuelos deben escontrarse activos, o, de lo contrario podria provocar un desbordamiento (flood) SYN en su objetivo. Por otra parte, resultara bastante facil saber que servidor esta escaneando si unicamente hay uno activo en la red.

Notese tambien que algunos (estupidos) "detectores de escaneres de puertos" opondran una firewall o bien denegaran el rutaje a aquellos servidores que intenten escanear sus puertos. De este modo se podria provocar inadvertidamente que la maquina que se esta intentando escanear perdiese contacto con los servidores usados como senuelos. Esto podria causarles a los servidores escaneados verdaderos problemas si los servidores senuelo fuesen, por ejemplo, su gateway a internet o incluso "local-host". Deberia usarse esta opcion con extremo cuidado. La verdadera moraleja de este asunto es que un detector de escaneos de puertos que aparenten tener intenciones poco amistosas no deberia llevar a cabo accion alguna contra la maquina que aparentemente le esta escaneando. ¡Podria no ser mas que un senuelo!

Los senuelos se usan tanto en el escaneo ping inicial (usando ICMP, SYN, ACK, o lo que sea) como en la fase de escaneo de puertos propiamente dicha. Tambien se usan los senuelos en la fase de deteccion remota del sistema operativo (-O).

Vale la pena destacar que el uso de demasiados senuelos puede ralentizar el proceso de escaneo y, potencialmente, hacer que sea menos exacto. Por otra parte, algunos ISPs filtraran los paquetes manipulados y los desecharan, aunque muchos (actualmente la mayoria) no ponen restricciones a este tipo de paquetes.

-S <Direccion_IP>

En determinadas circunstancias, es posible que nmap no sea capaz de determinar su (de usted) direccion IP de origen (nmap se lo hara saber si este es el caso). En este caso, use -S con su direccion IP (del interfaz a traves del cual desea enviar los paquetes).

Otro posible uso de esta opcion es el de manipular el escaneo para hacer creer a los servidores de destino que alguien mas les esta escaneando. iImaginese a una compania escaneada repetidamente por una compania rival! Esta no es la funcion para la que se ha disenado esta opcion (ni su proposito principal). Simplemente pienso que revela una posibilidad que la gente deberia tener en cuenta antes de acusar a los demas de escanear sus puertos. La opcion -e sera necesaria en general para este tipo de uso.

-e <interfaz>

Le dice a nmap que interfaz ha de usar para enviar y recibir paquetes. El programa deberia detectar esto por si mismo, pero le informara si no es asi.

-g <numero_de_puerto>

Establece el numero de puerto de origen a usar en los escaneos. Muchas instalaciones de firewalls y filtros de paquetes inocentes hacen una excepcion en sus reglas para permitir que las atraviesen y establezcan una conexion paquetes DNS (53) o FTP-DATA (20). Evidentemente esto contraviene completamente las ventajas en materia de seguridad que comporta una firewall dado que los intrusos pueden enmascararse como DNS o FTP con una simple modificacion de su puerto de origen. Por supuesto, deberia probarse primero con el puerto 53 para un escaneo UDP y los escaneos TCP deberian probar el 20 antes del 53.

Notese que el uso de esta opcion penaliza levemente el rendimiento del escaneo, porque a veces se almacena informacion util en el numero de puerto de origen.

-M <max sockets>

Establece el numero maximo de sockets que se usaran en paralelo para un escaneo TCP connect() (escaneo por defecto). Resulta util a la hora de ralentizar ligeramente el proceso de escaneo con el fin de evitar que la maquina de destino se cuelgue. Otra manera de hacerlo es usar -sS, que normalmente les resulta mas facil de asumir a las maquinas de destino.

Especificacion de Objetivo

Cualquier cosa que no es una opcion (o el argumento de una opcion) en namp se trata como una especificacion de servidor de destino. El caso mas simple consiste en especificar servidores aislados o direcciones IP en la linea de comandos. Si pretende escanear una subred de direcciones IP, entonces se puede anadir '/mask' a la direccion IP o al nombre del servidor. mask debe estar entre 0 (escanea toda Internet) y 32 (escanea unicamente el servidor especificado). Use /24 para escanear una direccion de clase 'C' y /16 para la clase 'B'.

Nmap dispone tambien de una notacion mucho mas potente que permite la especificacion de direcciones IP usando listas/rangos para cada elemento. De este modo, se puede escanear la red de clase 'B' completa 128.210.*.* especificando '128.210.*.*' o '128.210.0-255.0-255' o incluso notacion de mascara: '128.210.0.0/16'. Todas ellas son equivalentes. Si se usan asteriscos ('*'), ha de tenerse en cuenta que la mayoria de los shells requieren que se salga de ellos con caracteres / o que se les proteja con comillas.

Otra posibilidad interesante consiste en dividir Internet en el otro sentido. En vez de escanear todos los servidores en una clase 'B', se puede escanear '*.*.5.6-7' para escanear todas las direcciones IP terminadas en .5.6 o .5.7 Escoja sus propios numeros. Para mas informacion sobre la especificacion de servidores a escanear, vease la seccion ejemplos a continuacion.

EJEMPLOS

A continuacion se muestran algunos ejemplos del uso de nmap que abarcan desde los usos mas normales y frecuentes a los mas complejos o incluso esotericos. Notese que se han incluido direciones IP y nombres de dominio reales para hacer las cosas mas concretas. Usted deberia sustituirlos por numeros y direcciones de su propia red. No creo que escanear otras redes sea ilegal; ni se deberian considerar los escaneos de puertos como ataques. He escaneado cientos de miles de maquinas y tan solo he recibido una queja. Pero no soy abogado y es posible que los intentos de nmap lleguen a molestar a alguna gente. Obtenga primero el permiso para hacerlo o hagalo bajo su propia responsabilidad.

nmap -v objetivo.ejemplo.com

Esta opcion escanea todos los puertos TCP reservados en la maquina objetivo.ejemplo.com. La -v implica la activacion del modo de informacion ampliada.

nmap -sS -O objetivo.ejemplo.com/24

Lanza un escaneo SYN oculto contra cada una de las maquinas activas de las 255 maquinas de la classe 'C' donde se aloja objetivo.ejemplo.com. Tambien trata de determinar el sistema operativo usado en cada una de las maquinas activas. Este escaneo requiere privilegios de roor a causa del escaneo SYN y la deteccion del sistema operativo.

nmap -sX -p 22,53,110,143 128.210.*.1-127

Envia un escaneo Xmas tree a la primera mitad de cada una de las 255 posibles subredes de 8 bits en el espacio de direcciones clase 'B' 128.210 . Se trata de comprobar si los sistemas ejecutan sshd, DNS, pop3d, imapd o el puerto 4564. Notese que el escaneo Xmas no funciona contra servidores ejecutando cualquier sistema operativo de Microsoft debido a una pila TCP deficiente. Lo mismo se aplica a los sistemas CISCO, IRIX, HP/UX, y BSDI.

nmap -v -p 80 '*.*.2.3-5'

En vez de centrarse en un rango especifico de direcciones IP, resulta a veces interesante dividir Internet en

porciones y escanear una pequena muestra de cada porcion. Este comando encuentra todos los servidores web en maquinas cuyas direcciones IP terminen en .2.3, .2.4, o .2.5 . Si usted es root podria anadir tambien -sS. Tambien encontrara maquinas mucho mas interesantes si empieza en 127. asi que es posible que desee usar '127-222' en vez de el primer asterisco dado que esa seccion tiene una densidad mucho mayor de maquinas interesantes (IMHO).

host -l compania.com | cut '-d ' -f 4 | ./nmap -v -i -

Hace una transferencia de DNS de zona para descubrir los servidores en compania.com y luego pasar las direcciones IP a nmap. Los comandos arriba indicados son para mi sistema Linux. Es posible que se necesiten comandos/opciones diferentes para otros sistemas operativos.

BUGS

cBugs? cQue bugs? Por favor, envieme cualquier bug que descubra. Los parches tampoco estarian mal :) Recuerde enviar tambien nuevas huellas de sistemas operativos para que podamos ampliar nuestra base de datos.

AUTOR

Fyodor <fyodor@insecure.org>Tipos de Escaneo

DISTRIBUCION

La ultima version de nmap se puede obtener en http://www.insecure.org/nmap