

TCP IP: INICIACION (PARTE I)

Presentación, características y objetivos del curso de TCP/IP: Bueno, ya estamos aquí frente a la sección más ambiciosa de esta publicación. Mi intención es conseguir que quien compre esta revista no pase por alto esta sección (y eso será difícil). Para convencerte, solo tengo un argumento y está basado en mi propia experiencia personal, no seas tan tonto como fui yo, durante años esquivé el aprendizaje y comprensión del TCP/IP porque lo consideré innecesario, ¿por qué tenía que aprender TCP/IP si era capaz incluso de programar mis propias aplicaciones e incluso mis propios "sistemas de sockets"? Pues ten en cuenta una cosa, por mucho que aprendas (a veces de forma automática) a programar sockets, llegará el momento en que vuestra evolución empezará a ralentizarse, empezareis a tener dudas y esos fragmentos de código que aplicabais automáticamente empezarán a limitar (y traicionar) vuestras posibilidades reales, no hagáis como yo, no cometáis imperdonable error de "pasar" del TCP/IP. ENFRENTAROS AL RETO, NO TE ARREPENTIRÁS NUNCA!!! Es más, llegará un momento en que será imprescindible enfrentarte al TCP/IP, así que cuanto antes empecemos, mejor.

A título informativo diré que hace tan solo dos años que estudio el conjunto de protocolos TCP/IP y su entorno, fui un iluso al pensar que con las limosnas de unos míseros textos tendría más que suficiente para llegar al nirvana : Pero en estos últimos 14 meses he leído unos 30 libros, cientos de "papers" e incontables textos; pocas personas pueden saber como sabe el editor de este texto de la importancia del TCP/IP y, lo que es más, difícilmente encontrareis ningún texto que os lo explique más claramente, porque precisamente el que os escribe ha sufrido en sus propias carnes el extraño virus que parece rodear a este tema: el virus del tecnicismo extremo.

No creas que el camino será fácil, ni mucho menos, librarse de los tecnicismos es todo un alarde de imaginación y abstracción, el proceso será progresivo e intentaré que esos términos técnicos se introduzcan en vuestro vocabulario (y en concepto) poco a poco. Para conseguir esto he ideado un modo basado en tres pilares:

- Me permitiré el lujo de infringir todas las normas técnicas, es decir, que utilizaré el lenguaje como me convenga e incluso si es necesario reinventaré el significado de las palabras para hacer entender el fascinante mundo que descubriremos. Eso no implica el desconocimiento de los términos técnicos a tratar, no os librareis de ellos puesto que son necesarios para poder afrontar la lectura de otros textos... pero ya os daréis cuenta (poco a poco) de que ciertos conceptos técnicos son llamados de formas distintas según el autor y el punto de vista de quien escribe, lo que hace más difícil discernir de qué se está hablando en cada momento. Así que muchas veces veréis que junto a un concepto enumeraré las muchas formas de referirse técnicamente al mismo.
- Mantendremos siempre un paralelismo entre los conceptos explicados y una abstracción del mismo basada en el mundo real.
- Siempre que sea posible, utilizaremos diversos programas para que la teoría sea aplicada y tengamos constancia de sus utilidades.

1.- INTRODUCCIÓN SOBRE LAS DIRECCIONES IP.

Empecemos por explicar qué es una dirección IP.

Imagina que vas a Madrid (España :) y llegas al archiconocido paseo de la Castellana. Caminas por la calle y te fijas en los números de los portales, como puedes ver van desde el 1 hasta el 358 (por ejemplo). Muy bien, imagina que compras una oficina en el número 222, pues esa es TU dirección: Paseo de la Castellana 222. ----- Pues para saber la dirección de vuestro ordenador, solo tienes que abrir la consola y escribir ipconfig /all (y pulsar enter, por supuesto), os copio un ejemplo de lo que os saldrá:

Configuración IP de Windows

Nombre del host : ratorax5010

Sufijo DNS principal :

Tipo de nodo : desconocido

Enrutamiento IP habilitado. . . . : Sí

Proxy WINS habilitado. : No

La 192.168.0.1 se conoce como privada y puede haber millones de ordenadores que tienen esta dirección, por eso NO SE UTILIZA para Internet, es privada y solo tu puedes utilizarla (mas adelante os explicaré).

La 62.57.21.11 es una dirección publica y SE UTILIZA para Internet, es como la dirección de la oficina que habéis comprado, Paseo de la Castellana 222, cualquier persona podrá enviaros cartas sabiendo esta dirección, aplicándolo a TCP/IP, cualquier persona podrá enviaros "paquetes" (unidades de información) a vuestra IP.

2.- Forma de las IP:

Las IP tienen la forma X.X.X.X, siendo X un número comprendido entre 0 y 255 ambos incluidos.

Ejemplos:

10.256.1.0

198.168.200.254

0.0.0.0

255.255.255.255

127.0.0.1

.

.

Ya trataremos EN PROFUNDIDAD el mundo de las IP en próximos números de esta revista, sólo adelantar que NO TODAS ESTÁN DISPONIBLES para Internet. Hay algunas que sólo funcionarán en Intranets, otras que solo sirven para la difusión (todo llegará), otras que sólo se utilizan para "simular" una red en tu ordenador, etc.

3.- Accediendo a una Dirección de Internet tipo www.microsoft.com y los DNS.

Al comprar una oficina, tenemos la DIRECCIÓN POSTAL tipo Calle-Número-Planta-Puerta-Ciudad-Código Postal-País. Cuando conectamos un ordenador a Internet tenemos una DIRECCIÓN IP tipo xxx.xxx.xxx.xxx.

Imagina que pudiésemos llamar a nuestra Dirección Postal algo así como "LaCasadePedro" y todo el mundo pudiese relacionar ese nombre con la DIRECCIÓN POSTAL. ¿Verdad que estaría muy bien? Pues eso es posible hacerlo con la DIRECCIÓN IP :) Podemos asignar a nuestra DIRECCIÓN IP un NOMBRE, llamado NOMBRE DE DOMINIO :)

Cuando ponemos en nuestro Internet Explorer www.microsoft.com (ahora ya sabemos que eso se llama NOMBRE DE DOMINIO), lo que hace nuestro navegador es llamar a un ordenador para que TRADUZCA el NOMBRE DE DOMINIO a una DIRECCIÓN IP (el ordenador nos lo proporciona nuestro ISP y está corriendo un servicio llamado DNS=Servidor de Nombres de

Dominio).

¿Quieres verlo? Abre la consola y pica ping www.microsoft.com, os saldrá algo parecido a esto:

Haciendo ping a www.microsoft.akadns.net [207.46.197.100] 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 207.46.197.100:

Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

Fijaros en el numerito **207.46.197.100**, se parece a una IP ¿verdad? Pues habéis acertado, esa es la **IP Pública de Microsoft** en Internet.

¿Cómo es posible que escribiendo www.microsoft.com nos aparezca esa dirección que llamamos IP? Pues porque para hacernos la vida mas fácil, unos señores se reunieron un buen día en una habitación y decidieron que para no ir poniendo en nuestro ordenadores direcciones tan raras como **207.46.197.100**, tenían que idear un sistema mas humano. Pues bien, cuando en vuestro navegador de Internet ponemos www.microsoft.com, lo que hace vuestro ordenador es llamar a otro ordenador de Internet para preguntarle la dirección IP de Microsoft. Este ordenador mira en su "base de datos" y te contesta que Microsoft es en realidad 207.46.197.100 A este servicio se le llama **DNS (Servicio de Nombres de Dominio)**, recordadlo, es importante para cuando hagamos ataques de **DNS** :)

Así es como os explicaría lo que es DNS cualquier libro técnico mínimamente bueno (a ver si me sale bien) :)

DNS es un servicio de nombres estándar del IETF. Permite que un equipo cliente registre y resuelva nombres de dominio de DNS. Estos nombres se emplean para encontrar y acceder a recursos de otros equipos de la red o de redes WAN como Internet. Sus componentes principales son:

- Espacio de nombres de dominio y los registros de recursos (RR) asociados. Una base de datos distribuida de información de nombres.
- Resolutores DNS. Facilidad con la que un cliente de DNS se pone en contacto con servidores de nombre DNS y envía peticiones de nombre para obtener información de registros de recursos.

- Servidores de nombre DNS. Servidores que mantienen el espacio de nombres de dominio y los RR y responden a estas peticiones de los clientes de DNS.

¿Os ha gustado? ¿Habéis entendido algo? Pues no me lo he inventado, es prácticamente idéntico a un texto extraído de uno de los libros de TCP/IP mas importante que existe. ¿Por qué no lo entendemos? ¿somos tontos? ¿hablan en otro idioma? NO, simplemente utilizan una serie de elementos implícitos que desconocéis por ahora. Para entenderlo necesitaríais conocer lo que significan conceptos como Espacio de Nombres de Dominio, Nombres de Dominio, Dominios Superiores, Registros de Recursos (RR), Nombres canónicos, Operación de Solicitud de DNS, Actualización de DNS, Zonas DNS (Primarias, secundarias y de Active Directory) y unos 20 términos más.

No, no estoy siendo exagerado ni mucho menos, estoy incluso siendo compasivo con vosotros, porque cada uno de esos conceptos tienen detrás otros tantos y a su vez esos tienen muchos mas hasta acabar en el nirvana del TCP/IP: la construcción manual de paquetes.

¿Podemos ver ahora lo difícil que es escribir este curso? Pues intentaré llevaros poco a poco y paso a paso al Nirvana... cuando acabe este curso (aun queda mucho) podréis incluso construir y direccionar vuestros paquetes "a mano".

Ahora volved a fijaros en el resultado del ipconfig /all y mirad la referencia a Servidores DNS. En el caso expuesto hay tres IP: 212.78.133.138, 212.78.128.11 y 212.78.128.12. No os extrañéis, imaginad que el ordenador que hay en la dirección 212.78.133.138 (que es un servidor de DNS) dejase de funcionar, desde ese momento podríais acceder a Internet perfectamente, pero introduciendo directamente la IP del sitio que quisiésemos visitar, porque si pusiésemos en nuestro navegador por ejemplo www.epson.com, nos devolvería un error y una página en blanco. Porque nuestro ordenador, al intentar conectar con el equipo 212.78.133.212 no podría y sería incapaz de saber qué Dirección IP corresponde a www.epson.com. Para evitar que nos quedemos "tirados", los ISP ponen a nuestra disposición un par de máquinas (en este caso tres), si la primera no funciona pasa la petición de DNS a la segunda y así hasta que encuentra una que funciona.

Un apunte mas para que tengamos una visión mas amplia de este tema. Los Servidores de Nombre (DNS)... ¿Cómo saben que una dirección IP corresponde a un nombre determinado? ¿cómo saben que la dirección IP 207.46.197.100 corresponde a www.microsoft.com? Pues porque existe una/s organización/es que se dedica/n a asignar IPs a Nombres, para eso tenemos que rellenar un formulario y enviarlo a una de esas organizaciones para que OS REGISTREN y transmitan esa información a todos los DNS del planeta, a esto se le llama difusión de DNS y por eso, desde que se os asigna un nombre hasta que todo el planeta puede acceder a vuestra IP (X.X.X.X) con un NOMBRE DE DOMINIO (www.nuestro nombrededominio.com) pasan unos días. Ese nuevo dato que hace corresponder vuestro NOMBRE DE DOMINIO con vuestra IP debe "copiarse" a todos los servidores del planeta, y eso, aunque es un proceso automático, tarda un poco). Es como si intentásemos informar a todos nuestros conocidos (y al mundo entero) que nuestra nueva dirección es Paseo de la Castellana 222, eso implica cambiar los

listines telefónicos del País, las agendas personales de muchas personas (conocidos, familiares, etc.) ...

4.- DNS y el mundo REAL.

Ahora, para tomar un contacto un poco mas "directo" con la realidad, vamos a investigar qué es lo que saben las compañías registradoras de dominios (nombres que después se asignan a Direcciones IP) de Microsoft : Abrimos el navegador y vamos a www.networksolutions.com y una vez abierta la página picamos sobre WHOIS (está arriba a la derecha). Se abrirá una "page" con un servicio muy útil. Poned microsoft.com en el campo de búsqueda y pulsad GO, en un momento os aparecerán datos de Microsoft.

Registrant:

Microsoft Corporation (MICROSOFT-DOM)

1 microsoft way
redmond, WA 98052
US

*** la persona o compañía que registró el dominio microsoft.com (el nombre [Microsoft.com](http://microsoft.com))***

Domain Name: MICROSOFT.COM

*** Este es el nombre de dominio registrado ***

Administrative Contact:

Microsoft Hostmaster (MH37-ORG) msnhst@MICROSOFT.COM
Microsoft Corp
One Microsoft Way
Redmond, WA 98052
US
425 882 8080
Fax- - - : 206 703 2641

Technical Contact:

MSN NOC (MN5-ORG) msnnoc@MICROSOFT.COM
Microsoft Corp
One Microsoft Way

Redmond, WA 98052

US

425 882 8080

Fax- PATH

Billing Contact:

idNames, Accounting (IA90-ORG) accounting@IDNAMES.COM

idNames from Network Solutions, Inc

440 Benmar

Suite #3325

Houston, TX 77060

US

703-742-4777

Fax- - 281-447-1160

*** Estos son los contactos, vamos, que si queremos molestar un poco tenemos sus mail e incluso teléfonos ***

Record last updated on 29-Jan-2002.

Record expires on 03-May-2011.

Record created on 02-May-1991.

Database last updated on 7-Apr-2002 06:01:00 EDT.

*** Esto nos informa de cuando fue creado y actualizado el registro ***

Domain servers in listed order:

DNS1.CP.MSFT.NET	207.46.138.20
DNS1.TK.MSFT.NET	207.46.232.37
DNS3.UK.MSFT.NET	213.199.144.151
DNS3.JP.MSFT.NET	207.46.72.123
DNS1.DC.MSFT.NET	207.68.128.151

*** Servidores de Dominio ***

¿Para qué sirve todo esto? Hombre, si lo miramos desde el punto de vista de un posible atacante (o sea, tu mismo :) pues pone a tu disposición, por ejemplo, los mail de los Administradores de Red y sus nombres... ummm... ¿y qué? Pues que utilizando un buscador como www.google.com (el mejor buscador que existe) quizás encontremos consultas o consejos

que estas personas dan a sus clientes o cosas mucho mas peligrosas como explicaciones exhaustivas de cómo está formada su red. Os sorprenderíais de lo que podemos encontrar con un buen buscador.

Pero esta sección es de TCP/IP, así que dejemos el tema por ahora, que en próximos números ya os enseñaremos esas cosas :

5.- Alimentando la Curiosidad:

Bueno, venga ... A estas alturas ya debéis imaginaros qué es un ataque por DNS ¿verdad? ¿no? Venga, échale un poco de imaginación :

Un poco mas arriba tenemos los Servidores de Dominio de Microsoft

Domain servers in listed order:

DNS1.CP.MSFT.NET	207.46.138.20
DNS1.TK.MSFT.NET	207.46.232.37
DNS3.UK.MSFT.NET	213.199.144.151
DNS3.JP.MSFT.NET	207.46.72.123
DNS1.DC.MSFT.NET	207.68.128.151

Hemos dicho que los Servidores DNS "informan" del Nombre de Dominio asignado a una Dirección IP ¿verdad? Pues

- ¿qué pasaría si tomásemos el control de un Servidor DNS de Microsoft y cambiásemos los datos?
- ¿Qué pasaría si el Nombre de Dominio www.microsoft.com apuntase a otra IP en lugar de la IP de Microsoft? (por ejemplo apuntase a la Web de www.lomasguarrodeinternet.com)

Pues muy sencillo, cada vez que un ser humano introdujese en su Internet Explorer (o cualquier otro navegador) www.microsoft.com, en lugar de acceder a la Web de Microsoft, estaría accediendo a una Web de contenido erótico :

*** Los ataques de DNS son mas sencillos que un ataque en toda regla al Servidor de Páginas Web, de ahí que sean muy comunes :) ***