Ataqve

Conociendo distintos tipos de protocolos

Jaime Gutierrez

Grado de dificultad

El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Tenemos mucha información sobre el, ¿Pero realmente sabes que es?

En este número vamos a tratar de explicar los distintos tipos de protocolos, es decir los más importantes y métodos de ataques contra los mismos. Obviamente no vamos a analizar todos los tipos de protocolos ya que hay miles de ellos y de diferente estándar. Vamos a analizar protocolos por llamarlos de *red*.

QUE SE PUEDE DECIR QUE ES UN PROTOCOLO

Un protocolo son ¡una serie de reglas que utilizan dos ordenadores para comunicar entre sí. Cualquier producto que utilice un protocolo dado debería poder funcionar con otros productos que utilicen el mismo protocolo.

EL PROTOCOLO TCP/IP

El protocolo de red TCP/IP se podría definir como el conjunto de protocolos básicos de comunicación de redes, que permite la transmisión de información en redes de ordenadores. Una conexión TCP no es más que es una corriente de bytes, no una corriente de mensajes o textos por así decirlo.

EL PROTOCOLO ARP

El protocolo ARP (*Address Resolution Protocol*), permite realizar ciertas tareas cuyo objetivo es el asociar un dispositivo IP, que a un nivel lógico está identificado por una dirección IP, a un dispositivo de red, que a nivel físico posee una dirección física de red. Este protocolo se utiliza típicamente en dispositivos de red local, ethernet que es el entorno más extendido en la actualidad. Existe un protocolo RARP, cuya función es la inversa.

IP (Internet Protocol)

Para empezar vamos a hablar de un protocolo *básico* a nivel de red el protocolo IP o (*Internet Protocol*). El IP es un protocolo que pertenece

En este artículo aprenderás...

- Distintos tipos de protocolos,
- Protocolos complementarios.

Lo qué deberías saber...

- Conceptos de NETWORKING,
- Conocimientos de enrutación.

al nivel de red, por lo tanto, es utilizado por los protocolos del nivel de transporte como TCP para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Son números de 32 bits representados habitualmente *en formato decimal* (que varían de con valores de 255 a 0). Las direcciones ip se podría decir que son nuestro documento de identidad en la red , nos identifica a nosotros, a nuestro ISP, nuestro país de provinencia y demás datos. Un atacante podría obtener nuestra IP por muchas y diversas maneras. Por conversaciones normales de mensajería instantánea, voz sobre Ip (VoiP), logs de nuestro acceso a paginas, conexiones de distintos tipos... es decir cientos de formas distintas. Una vez el atacante allá obtenido nuestra IP se pude sacar mucha y peligrosa información de ella. Desde el país que nos conectamos hasta si buscamos páginas de datos (tipo WHOIS) la dirección a la cual esta registrada la misma linea de conexión a Internet. El atacante puede proceder a escanear la IP en busca de puertos TCP o UPD a la escucha, para poder ejecutar acciones. Un ejemplo simple, seria el puerto 139 (conocido como NETBIOS) por el cual si la víctima tiene el puerto en escucha con solo meter su dirección de IP podrías ejecutar una shell remota e incluso tener visión y control total de su computadora. Esto hace que nos pensemos dos veces antes de navegar sin un proxy.

CLASES DE DIRECCIONES IP

Hay cinco clases de direcciones IP:

A,B,C,D,E

Clase A

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección Clase A siempre es 0. Un ejemplo de una dirección IP Clase A es 124.95.44.15. El primer byte, 124, identifica el número de red. Los administradores internos de la red asignan los restantes valores. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase A es verificar el primer byte de su dirección IP, cuyo valor debe estar entre 0 y 126.

```
|número red|núm equipo|núm equipo|núm
                              equipo|
```

Todas las direcciones IP Clase A utilizan solamente los primeros 8 bits para identificar la parte de red de la dirección. Los tres bytes restantes son para los equipos de la red. A cada una de las redes que utilizan una dirección IP Clase A se les pueden asignar hasta 2 elevado a la 24 potencia (`2^24`), o 16.777.214 direcciones IP posibles para los dispositivos que están conectados. Está claro que son organismos muy grandes para poder gestionar más de 16 millones de ordenadores...

Tabla 1. *Principales tipos de mensajes ICMP*

Destino inalcanzable	No puede entregar el paquete
Tiempo excedido	Campo de tiempo de vida llegó a cero
Problema de parámetro	Campo de cabecera no valida
Supresión de origen	Paquete de estrangulamiento
Reenvío	Enseña geografía a un enrutador
Solicitud de eco	Pregunta a una máquina si está viva
Respuesta de eco	Si, estoy viva
Solicitud de marca de tiempo	Igual que la solicitud de eco, pero con marca de tiempo
Respuesta de marca de tiempo	Igual que la respuesta de eco, pero con marca de tiempo

Clase B

Los primeros 2 bits de una dirección Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP Clase B es 151.10.13.28. Los dos primeros bytes identifican el número de red. Los otros dos bytes son para numerar los equipos de la red. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase B es verificar el primer byte de su dirección IP. Las direcciones IP Clase B siempre tienen valores que van del 128 al 191 en su primer byte.

```
|número red|núm red|núm equipo|núm
                              equipo|
```

Todas las direcciones IP Clase B utilizan los primeros 16 bits para identificar la parte de red de la dirección. Los dos bytes restantes de la dirección IP se encuentran reservados para la porción del host de la dirección. Cada red que usa un esquema de direccionamiento IP Clase B puede tener asignadas hasta 2 a la 16ta potencia (`2^16`) ó `65.534` direcciones IP posibles a dispositivos conectados a su red.

Clase C

Los 3 primeros bits de una dirección Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP Clase C es 201.110.213.28. Los tres primeros bytes identifican el número de red. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase C es verificar el primer bytes de su dirección IP. Las direcciones IP Clase C siempre tienen valores que van del 192 al 223 en su primer bytes.

```
|número red|núm red|núm red|núm
equipo|
```

CLASE D

Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada

CLASE E

Las direcciones de clase E se reservan para usos en el futuro.

El PROTOCOLO HTTP

Este protocolo esta diseñado para recuperar información y llevar a cabo búsquedas indexadas permitiendo con eficacia saltos hipertextuales, además, no solo permite la transferencia de textos HTML sino de un amplio y extensible conjunto de formatos. Funciones particulares para el caso específico de la Web, creado para que resolviese los problemas planteados por un sistema hipermedial, y sobre todo distribuido en diferentes puntos de la Red.

HTTP (*HyperText Transfer Protocol*, o *Protocolo de Transferencia de Hipertexto*).

Cada vez que se activa cumple con un proceso de cuatro etapas entre el browser y el servidor que consiste en lo siguiente:

- *Conexión*: el browser busca el nombre de dominio o el número IP de la dirección indicada intentando hacer contacto con esa computadora,
- *Solicitud*: el browser envía una petición al servidor (generalmente un documento), incluyendo información sobre el método a utilizar, la versión del protocolo y algunas otras especificaciones,
- *Respuesta*: el servidor envía un mensaje de respuesta acerca de su petición mediante códigos de estado de tres dígitos,
- *Desconexión*: se puede iniciar por parte del usuario o por parte del servidor una vez transferido un archivo.

PROTOCOLO UDP

El protocolo *UDP* (*User Datagram Protocol*), pertenece a la familia de los protocolos TCP no es un protocolo tan fiable como TCP. Se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar la llegada, el protocolo exige a la maquina de destino del paquete que envíe un mensaje (un eco). Si el mensaje no llega desde la maquina de destino el mensaje se envía de nuevo. *UDP es un protocolo sencillo que implementa un nivel de transporte orientado a datagramas:*

- NO orientado a conexión.
- NO fiable.

Los datagramas UDP se encapsulan dentro de la parte de datos de un datagrama IP. Una aplicación que utilice UDP para transmitir datos, producirá exactamente un datagrama UDP por cada operación de salida que precise, el cual originará un datagrama IP encapsulándolo. Os preguntareis si , ¿pero porqué no es fiable UDP?. Os daré tres razones explicitas:

- Pueden perderse datagramas,
- Pueden duplicarse datagramas,
- Pueden desordenarse datagramas.

Pero es un protocolo más ligero que TCP, y en una LAN (hay CRC y no hay encaminadores) puede compensar. Pero recordemos que tenemos deber en cuenta la seguridad como factor principal.

PROTOCOLO ICMP

La operación de Internet es supervisada cuidadosamente por los enrutadores. Al ocurrir algo inesperado, el ICMP (*Internet Control Message Protocol*, protocolo de control de mensajes de Internet), que también se usa para probar Internet, informa del suceso. Se ha definido una docena de tipo de mensajes de ICMP; Cada tipo de mensaje de ICMP se encapsula en un paquete IP. El mensaje DESTINO INALCANZABLE se usa cuando la subred o un enrutador no pueden ubicar el destino, o un paquete con el bit DF no puede entregarse por que está en el camino una red de *paquete pequeño*. El mensaje de TIEMPO EXCEDIDO

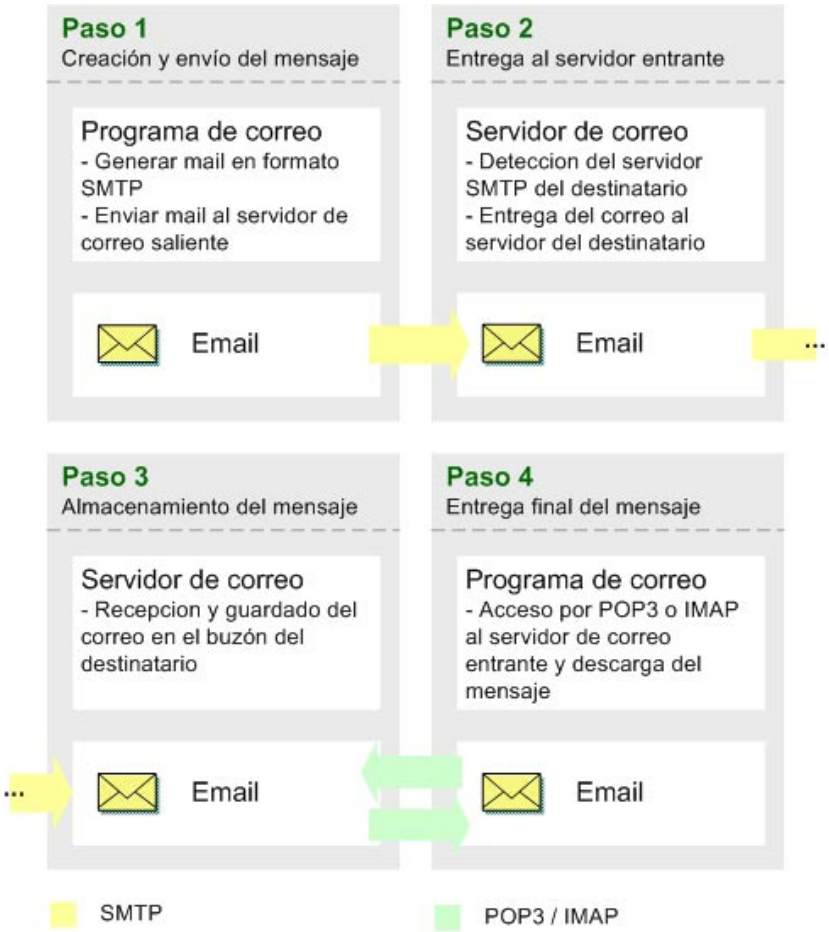

Figura 1. *Orgarnización de smtp*

se encía cuando un paquete se descarta debido a que su contador llega a cero. Este suceso es un síntoma de que los paquetes están en ciclo, de que hay un congestionamiento enorme, o de que los valores de temporización son demasiado bajos. El mensaje de PROBLEMA DE PARÁMETRO indica que se ha detectado un valor ilegal en un campo de cabecera. Este problema indica una falla en el software de IP del host, o posiblemente en el software de un enrutador transmitido.

NETBIOS

NetBIOS fue desarrollado por IBM y Systek como un intento de proveer a las aplicaciones de una interfaz para acceder a los recursos de las redes locales. Al ser solo una interfaz entre las aplicaciones y la tarjeta de red, y por tanto poder ser utilizado con independencia del hardware, hizo que pronto se convirtiera en un estándar para acceder a redes (ethernet, TokenRing, redes IBM,...). *NetBIOS ha sido utilizado ampliamente para compartir recursos de una manera simple y eficiente en redes pequeñas. Proporcionando tanto servicios orientados a conexión (sesiones) como no orientados a conexión (datagramas), al igual que soporta broadcast y multicast.*

Posteriormente surgio NetBEUI que no es mas que una versión extendida de NetBIOS que proporciono una capa de transporte que nunca fue estandarizada en NetBIOS. NetBIOS puede ser utilizado en la inmensa mayoría de los sistemas operativos de red y puede ser transportado sobre variedad de protocolos, generalmente sobre TCP/IP (NBT), IPX,...

ALGUNOS COMANDOS NETBIOS

open host: abre una conexión al host llamado. Si el número de puerto no es especificado, telnet intenta de conectar el servidor telnet desde el puerto default. La especificación del host puede ser tanto el nombre de un host o una IP.

close: cierra una sesión TELNET y te regresa al modo de comando.

Quit: cierra cualquier sesión TELNET abierta y sale de telnet. Un fin de archivo (end-of-file) (en modo de comando) también cerrará una sesión y saldrá.

Ctrl-z: suspende telnet. Este comando sólo trabaja cuando el usuario está usando csh o la el ambiente de aplicación BSD versión de ksh.

Status: muestra el status actual de telnet.

Ync: envía la secuencia SYNCH TELNET. Esta secuencia causa que el sistema remoto descarte todo lo previamente tecleado como entrada, pero que todavía no haya sido leído. Esta secuencia es enviada como un dato urgente TCP. h.

TELNET: TELNET es el protocolo de *conexión* a otro ordenador, de hecho la mayoría de los servicios posteriores, se basan en telnet (pe. FTP, HTTP). Haciendo telnet a una máquina, ejecutas programas en ella, recibiendo tu la entrada/salida de los datos. Las direcciones TELNET suelen tener el formato del nombre de dominio*maquina.remota .com* o de dirección IP `194.106.2.150` y pueden ir acompañadas de un número al final (el número del puerto) si no se nos proporciona el puerto se asume que el utilizado es el correspondiente al protocolo telnet por defecto, el 23. Una dirección típica sería: *maquina.remota.com 2010.*

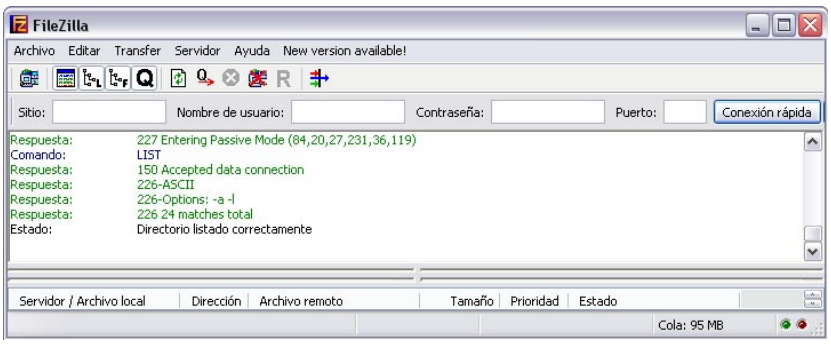

Figura 2. *Logs de conexión mediante un cliente ftp*

CUADRO APARTE (EXPLICACIÓN MÁS EXAUSTIVA)

Cómo se hace TELNET?:Ejecutando un programa cliente de telnet, prácticamente cualquier sistema *operativo lleva uno incluido de serie. Por lo tanto si nos proporcionan la dirección telnet maquina.remota.ar 2010* haríamos lo siguiente: (puede variar según sistemas):

Tecleamos en la linea de comandos *TELNET maquina.remota.ar 2010* (En otros sistemas teclearemos *TELNET* y después *OPEN maquina.remota.ar2010*) con lo que veremos algo parecido a esto:

- *telnet MAQUINA.REMOTA.AR 2010,*
- *Trying 130.132.21.53 Port 2010 ...,*
- *Connected to MAQUINA.REMOTA.COM,*
- Escape character is ...,
- Esto nos dice más o menos que está intentando conectar con la dirección, nos devuelve la dirección IP, se conecta, y nos dice cual es el *caracter escape,*
- Una vez hemos conectado se nos pide un *login* y/o *password* para entrar a la máquina remota. En algunos casos podremos conectar a la maquina remota con el login *guest* (invitado) pero la mayoría de las veces deberemos saber el login antes de conectarnos,
- El siguiente paso es configurar la emulación de terminal, es decir, decirle al sitio remoto como queremos que nos muestre los datos en nuestra pantalla. La configuración más común es la VT100, que es la estándar para las comunicaciones basadas en terminales. (algunos clientes telnet configuran ellos sólos la emulación),
- El último paso (después de haber utilizado el servicio es salir

;-) Como las pulsaciones de tecla no las hacemos *realmente* en nuestra máquina, sino en la máquina remota, necesitamos el *carácter escape* que se nos dio al conectar para pasar al *modo comando* (habitualmente teclas control + paréntesis derecho).

PROTOCOLO SMTP

SMTP (*Simple Mail Transfer Protocol*) o Protocolo Simple de Transferencia de Correo Electrónico es un conjunto de reglas que rigen el formato y la transferencia de datos en un envío de Correo Electrónico (e-mail).

Algunas ordenes *SMTP*:

- *HELO* – Abre una sesión con el servidor,
- *MAIL FROM* – Indica el autor del mensaje,
- *RCPT TO* – Indica los destinatarios del mensaje,
- *DATA* – Cuerpo del mensaje, finaliza con la orden,
- . – Final del cuerpo del mensaje (orden *DATA*),
- *QUIT* – Cierra la sesión,
- *POP3* (*Post Office Protocol*) es también un protocolo muy usado en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

Algunos comandos *POP3*:

- *USER* <*nombre*> Identificación de usuario (Solo se realiza una vez),
- *PASS* <*password*> Envías la clave del servidor,
- *STAT* Da el número de mensajes no borrados en el buzón y su longitud total,
- *LIST* Muestra todo los mensajes no borrados con su longitud,
- *RETR* <*número*> Solicita el envío del mensaje especificando el número (no se borra del buzón),
- TOP <*número*> <*líneas*> Muestra la cabecera y el número de líneas requerido del mensaje especificando el número,
- *DELE* <*número*> Borra el mensaje especificando el número,
- *RSET* Recupera los mensajes borrados (en la conexión actual),
- *QUIT* Salir.

LA IMPORTANCIA DE NO DEJAR HUELLAS (RECUADRO A PARTE)

Como hemos visto , navegar dejando a vista de malos ojos nuestra ip, puede ser realmente peligroso. ¿Pero para que los proxys?. Un proxy es un programa (generalizando) , dispositivo , servidor.... que realiza una tarea de acceso a Internet. Más específicamente es un punto intermedio entre tu y el servidor de la esquina. Al navegar bajo proxy (Ip check) podemos ocultar nuestra IP y mostrar la del servidor proxy que nos conectemos. Esto dificultara al atacante situarnos o conocer nuestro numero de IP real. También filtrar algunos contenidos potencialmente peligrosos... Hay ventajas de usar proxys , pero también hay inconvenientes la querida velocidad de navegación. Imaginemos por un momento que nos conectamos a un servidor proxy situado (o conectado) en china. La velocidad de carga de cualquier tipo se vería tremendamente reducida, al tener que pasar los datos antes por el servidor chino antes de llegar a nuestro Pc.

```
NUESTRA CONEXIÓN<<<>>
SERVIDOR PROXY<<<>>>SERVIDOR
```

Podemos encontrar servidores proxy en el mismo Internet o mediante programas de intuitiva interfaz (véase ipmask).

PROTOCOLO FTP

Ftp (*File Transfer Protocol*) es un protocolo para la transferencia remota de archivos. Lo cual significa la capacidad de enviar un archivo digital de un lugar *local* a uno *remoto* o viceversa, donde el local suele ser el computador de uno y el remoto el servidor Web.

ALGUNOS COMANDOS FTP

- *ascii*: especifica tipo de transferencia de ficheros ASCII, en contraposición a ficheros binarios (no texto),
- *binary*: especifica tipo de transferencia binaria (por defecto),
- *bell*: le indica al sistema que ejecute un pitido (bell) cuando se finalicen la ejecución de los comandos. Así podemos ejecutar bell, y dejar un fichero de gran tamaño descargándose, sabiendo que tras su finalización oiremos un BEEP, lo cual nos permite dejar la ventana minimizada y hacer cualquier otra tarea,
- *delete y mdelete*: borran uno o varios ficheros en la máquina remota,
- *user y pass*: especificar nuestro nuevo nombre y password.

PROTOCOLO SSH

El protocolo SSH (*Secure Shell*)nació para intentar que las comunicaciones en internet fuesen más seguras, esto lo consigue eliminando el envío de las contraseñas sin cifrar y mediante la encriptación de toda la información que se transmite. Se recomienda usar SSH para mantener conexiones seguras, ya que debido a las avanzadas herramientas usadas por crackers , sniffear una red se ha convertido en un juego de niños.

En la Red

- *http://es.wikipedia.org/wiki/Protocolo_de_Internet,*
- *http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol,*
- *http://usuarios.lycos.es/janjo/janjo1.html.*

SOBRE EL AUTOR

Jaime Gutierrez, Español, se interesa por la seguridad en redes y la por la programación de distintas aplicaciones en JAVA o C++. Actualmente reside en Andalucía y publico en la edición pasada el articulo *DDos un acoso constante*.

ALGUNOS COMANDOS SSH

pwd muestra el path completo del directorio en el que se encuentra.

cd cambia de directorio, por ejemplo cd directorio/subdirectorio.

cd ~ lleva a su directorio home.

cd - lleva al último directorio en el que estuvo.

cd .. sube a un directorio superior.

CONCLUSIONES

Como hemos visto a lo largo del articulo existen cientos de protocolos, pero aquí solo nos hemos parado a analizar unos pocos. Conocer como funcionan cada uno de ellos nos ayudara a saber como funciona la NET. Conocer como trabajan los paquetes, servidores, protocolos, mencionados es una de las bases del hacking y de la seguridad en sistemas. Hemos aprendido la teoría que es un poco más aburrida pero en entregas próximas vamos a ver como vulnerar estos tipos de protocolos con herramientas comunes o simplemente siendo usuarios ilegítimos. Entender como y porque, su necesidad, como se manejan y funcionan, es algo básico en este mundo.