Unidad II: Servicios de Red

2.1 DHCP

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma *dinámica* (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero desde sus inicios se diseñó como un complemento del protocolo BOOTP (Protocolo Bootstrap), que se utiliza, por ejemplo, cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host.

2.2 DNS

Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio

adirecciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos. El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul V. Mockapetris publicó los RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y RFC 1035).

2.3 Telnet

El término TELNET se refiere a la conexión remota a un ordenador, esto es posible en Internet gracias al TELNET Protocol. Es habitual usar la expresión "hacer un TELNET", con ello estamos expresando que vamos a realizar una conexión en modo terminal remoto con una máquina en la que estamos autorizados. Sin embargo, muchas máquinas permiten que les hagamos un TELNET como invitados para que podamos acceder a la información pública de la que disponen, y para lo cual no necesitamos autorización.

2.4 SSH

SSH (**S**ecure **SH**ell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas

remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionarclaves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

2.5 FTP y TFTP

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entreordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza los puertos 20 y 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

FTP (siglas en inglés de ***F****ile* ***T****ransfer* ***P****rotocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de

archivosentre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

- El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.
- Para solucionar este problema son de gran utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

2.6 WWW: HTTP y HTTPS

Para empezar, una buena idea es conocer que significa la “S” y no es otra cosa que el vocablo en inglés “secure” . Cuando navegamos por Internet la mayoría de las páginas empiezan por http://. Esto quiere decir que utiliza lenguaje normal, pero que podría no ser seguro.

En otras palabras, alguien podría estar espiando la “conversación” entre tu ordenador y la página sin demasadas complicaciones. Cualquiera podía obtener alguno de tus datos, algo crucial si hablamos de servicios en los que manejamos dinero. Así que ya tenemos un buen motivo para no dar ninguna tarjeta de crédito en estos tipo de páginas.

HTTPS, una forma de dar seguridad a tus datos

2.7 NFS

El Network File System *(Sistema de archivos de red)*, o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que sea independiente de la máquina, el sistema operativo y el protocolo de transporte, esto fue posible gracias a que está implementado sobre los protocolos XDR (presentación) y ONC RPC (sesión).[1] El protocolo NFS está incluido por defecto en los Sistemas Operativos UNIX y la mayoría de distribuciones Linux.

2.8 CIFS

CIFS: Common Internet File System (Sistema de Archivo Común de Internet) en cuanto a RVS suele ser también llamado "reverse" y procede del francés "Response s'il vous plait" (Responder por favor"). Aunque en la actualidad se empieza a ver con más frecuencia el vocablo en castellano SRC que es la sigla de "se ruega contestación".

2.9 e-mail: SMTP, POP, IMAP y SASL