# Introducción a la seguridad en redes IP

**Tabla de Contenidos**

1. Introducción a la seguridad en redes IP..... 2
1.1 Funcionamiento de TCP e IP..... 2
Interfaces de protocolo..... 3
1.2 El protocolo Internet..... 4
Servicios IP..... 4
Protocolo IP..... 4
El datagrama tiene varios campos , entre los que se encuentran :..... 4
Direcciones IP..... 5
El protocolo de mensajes de error de Internet ( ICMP )..... 5
DNS..... 5

# 1. Introducción a la seguridad en redes IP

Este curso contiene los conocimientos necesarios para configurar, utilizar las herramientas de seguridad y administrar una red con acceso a Internet basados en servidores Windows 2000 y UNIX.

Red es una configuración de computadores que intercambian información. Pueden proceder de una variedad de fabricantes y es probable que tenga diferencias tanto en hardware como en software, para posibilitar la comunicación entre estas es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos. **Un protocolo es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos.**

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más universalmente utilizado es el **Internet Protocol Suite**, comúnmente conocido como **TCP / IP.** Es un protocolo **DARPA** que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP Proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto. El TCP / IP es la base de Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

Las tareas en los sistemas de comunicación son:

- Utilización del sistema de transmisión
- Implementación de la interfaz
- Generación de la señal
- Sincronización
- Gestión del intercambio
- Detección y corrección de errores
- Control de flujo

## *1.1 Funcionamiento De TCP E IP*

IP está en todos los computadores y dispositivos de encaminamiento y se encarga de retransmitir datos desde un

computador a otro pasando por todos los dispositivos de encaminamiento necesarios .

TCP está implementado sólo en los computadores y se encarga de suministrar a IP los bloques de datos y de comprobar que han llegado a su destino .

Cada computador debe tener una dirección global a toda la red . Además , cada proceso debe tener un puerto o dirección local dentro de cada computador para que TCP entregue los datos a la aplicación adecuada .

Cuando por ejemplo u computador A desea pasar un bloque desde una aplicación con puerto 1 a una aplicación con puerto 2 en un computador B , TCP de A pasa los datos a su IP , y éste sólo mira la dirección del computador B , pasa los datos por la red hasta IP de B y éste los entrega a TCP de B , que se encarga de pasarlos al puerto 2 de B .

La capa IP pasa sus datos y bits de control a la de acceso a la red con información sobre qué encaminamiento tomar , y ésta es la encargada de pasarlos a la red .

Cada capa va añadiendo bits de control al bloque que le llega antes de pasarlo a la capa siguiente . En la recepción , el proceso es el contrario .

TCP adjunta datos de : puerto de destino , número de secuencia de trama o bloque y bits de comprobación de errores .

IP adjunta datos a cada trama o bloque de : dirección del computador de destino , de encaminamiento a seguir .

La capa de acceso a la red adhiere al bloque : dirección de la subred de destino y facilidades como prioridades .

Cuando el paquete llega a su primera estación de encaminamiento , ésta le quita los datos puestos por la capa de acceso a la red y lee los datos de control puestos por IP para saber el destino , luego que ha seleccionado la siguiente estación de encaminamiento , pone esa dirección y la de la estación de destino junto al bloque y lo pasa a la capa de acceso a la red .

**Interfaces de protocolo**

Hay muchas aplicaciones que no requieren todos los protocolos y pueden utilizar sólo algunos sin problemas

*Las aplicaciones*

Hay una serie de protocolos implementados dentro de TCP/IP :

- **Protocolo sencillo de transferencia de correo ( SMTP ).** Es un protocolo de servicio de correo electrónico ,

listas de correo , etc...y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP .

- **Protocolo de transferencia de ficheros ( FTP ).** Permite el envío y recepción de ficheros de cualquier tipo hacia un usuario . Cuando se desea el envío , se realiza una conexión TCP con el receptor y se le pasa información sobre el tipo y acciones sobre el fichero así como los accesos y usuarios que pueden acceder a él . Una vez realizado esto , se envía el fichero . Finalizado esto , se puede cortar la conexión .
- **TELNET .** Es un protocolo para que dos computadores lejanos se puedan conectar y trabajar uno en el otro como si estuviera conectado directamente . Uno de ellos es el usuario y el otro el servidor . TCP se encarga del intercambio de información .

## *1.2 El Protocolo Internet*

**Servicios IP**

Los servicios que proporciona IP a TCP son : **Send** ( envío ) y **Deliver** ( entrega ) .

TCP utiliza Send para solicitar el envío de una unidad de datos y Delive es utilizada por IP para notificar a TCP que una unidad de datos ha llegado . Los campos incluidos en estas dos llamadas son : dirección origen y destino de los datos , usuario IP , identificador de bloque de datos , indicador sobre si está permitida la segmentación del bloque , tipo de servicio , tiempo de vida , longitud de los datos , datos . Algunos campos no son necesarios para Deliver .

El tipo de servicio solicitado puede ser de encaminamiento lo más rápido posible , lo más seguro posible , prioridad , etc...

**Protocolo IP**

**El datagrama tiene varios campos , entre los que se encuentran :**

- Versión . Para futuras versiones .
- Longitud de la cabecera Internet .
- Tipo de servicio . Seguridad , prioridades , etc...
- Longitud total del datagrama .
- Identificador del datagrama .
- Indicadores de permiso de segmentación . Para poder usarse en sistemas en los que se deba segmentar en el destino o en dispositivos intermedios .

- Desplazamiento del fragmento . Identifica dónde va el fragmento dentro del datagrama fragmentado .
- Tiempo de vida . Tiempo de espera antes de destruir el datagrama .
- Suma de comprobación de la cabecera . Para detección de errores .
- Dirección de origen .
- Dirección de destino .
- Opciones variadas . Solicitadas por el usuario que envía los datos .
- Relleno . Bits para asegurar la multiplicidad para 32 bits .
- Datos . Datos de usuario .

**Direcciones IP**

La dirección de origen y destino en la cabecera IP es una dirección global de Internet de 32 bits . De estos 32 bits , algunos identifican al computador y el resto a la red . Estos campos son variables en extensión para poder ser flexibles al asignar direcciones de red . Hay diferentes tipos de redes que se pueden implantar en la dirección de red . Unas son grandes ( con muchas subredes ) , otras medianas y otras pequeñas . Es posible y adecuado mezclar en una dirección los tres tipos de clases de redes .

**El protocolo de mensajes de error de Internet ( ICMP )**

Este protocolo es utilizado para enviar mensajes en caso de error . Por ejemplo , cuando un datagrama no puede llegar a su destino , cuando llega con error , cuando el dispositivo de encaminamiento no tiene espacio de almacenamiento suficiente , etc...

ICMP , aunque está en el mismo nivel que IP , le pasa sus mensajes a IP para encapsularlos y enviarlos a su destino ( en forma de datagrama , por lo que no se asegura que llegue a su destino ) . Los datagramas suministrados por ICMP contienen su cabecera y parte de los datos del datagrama erróneo para que el IP que los reciba sepa qué protocolos había implicados en el error.

Los casos de error más habituales son que no se encuentre el destino , que se haga necesaria la segmentación pero esté prohibida por el propio datagrama , que haya pasado el tiempo permitido para el envío , que el destinatario no pueda procesar aún el datagrama porque esté sobrecargado de trabajo ( el emisor debe de disminuir la velocidad de envío cuando reciba el mensaje de error ) , etc...

Además de los mensajes de error , son posibles mensajes de control para por ejemplo establecer una conexión , para saber si es posible una conexión con una determinada dirección ( el mensaje llega al destinatario y es devuelto con una confirmación o denegación de posibilidad de conexión ) , para comprobar el tiempo de propagación de datos através de un camino , etc...

**DNS**

DNS son las siglas de *"Domain Name Service"* y, básicamente es usado para traducir direcciones IP. Por ejemplo, necesito saber la dirección IP del servidor indetec.tk y usando el DNS puedo obtener la dirección IP 213.216.96.90. Sin DNS no es posible establecer comunicación por web o por otros protocolos utilizados en internet.