SEGURIDAD DE LAS TIC BAJO PROTOCOLOS TCP/IP - ANÁLISIS PARTICULAR EN ECUADOR MEDIANTE ESCANEO DE PUERTOS

Jorge I. Ortiz M.
Corporación CENTRO NACIONAL DE CONTROL DE ENERGÍA -CENACE-

Juan C. Vallecilla M.
Corporación CENTRO NACIONAL DE CONTROL DE ENERGÍA -CENACE-

RESUMEN

En el presente artículo se describe lo relacionado a seguridad en redes de comunicación con protocolos TCP/IP, sus potenciales vulnerabilidades, tipos de ataques informáticos y nuevas tecnologías en cuanto a seguridad. Se presenta una estadística a nivel país sobre las vulnerabilidades encontradas en distintas redes de comunicación que trabajan bajo protocolos TCP/IP mediante escaneo de puertos.

1. PROTOCOLOS DE COMUNICACIÓN TCP/IP

En la actualidad, la familia de protocolos de Internet, o más conocida como protocolos de comunicación TCP/IP, se han difundido masivamente en todo el mundo, convirtiéndose en la base de Internet, permitiendo la transmisión de información entre redes de computadoras.

Efectivamente, TCP/IP es un conjunto de protocolos, siendo los más importantes el Protocolo de Control de Transmisión (TCP), y el Protocolo de Internet (IP), que fueron los primeros en definirse y los más utilizados. A la familia de protocolos de Internet, pertenecen alrededor de 100 protocolos, entre los cuales se mencionan: HTTP (Hyper Text Transfer Protocol) utilizado para acceder a páginas web, FTP (File Transfer Protocol) utilizado para transferencia de archivos, SMTP (Simple Mail Transfer Protocol) y POP (Post Office Protocol) utilizados para correo electrónico, TELNET para acceder a equipos remotos, etc.

1.1 Capas o Niveles de TCP/IP

Con el modelo de capas o niveles se simplificó el intercambio de información entre equipos de cómputo, ya que cada capa tiene como entradas la información de su nivel inmediatamente inferior, y sus resultados o salidas son las entradas para su nivel inmediatamente superior.

1.1.1 Capa Física y Enlace (Ethernet)

La capa física se refiere a los medios físicos de comunicación (cable, radio, fibra óptica), y a las actividades necesarias para tener un desempeño óptimo de dichos medios como: código de canales, modulación, potencias de señales, longitudes de onda, sincronización, temporización y distancias máximas.

La capa física Ethernet utiliza direcciones de red de 48 bits, estas direcciones de red vienen impresas de fábrica en todas las placas de red Ethernet.

Debido a que las direcciones Ethernet e IP son dos números distintos y que no guardan ninguna relación, para efectuar la comunicación a un host a través de su dirección IP, se necesita convertir ésta a la correspondiente dirección Ethernet. ARP (Address Resolution Protocol) es el protocolo encargado de realizar las conversiones de dirección correspondientes a cada host.

Ningún paquete de datos puede salir de la red sin tener la dirección Ethernet y la dirección IP de la máquina de destino. La gestión de las direcciones Ethernet, se la realiza en la capa de red.

1.1.2 Capa de Red

La capa de red se encarga de establecer los caminos para efectuar la transferencia de datos a través de la red, es decir, se ocupa del direccionamiento en la red, el ruteo, la fragmentación y desfragmentación de datagramas, los mensajes de control de Internet, y las tablas de direcciones físicas locales. Cada uno de estos servicios los administra un protocolo diferente.

Los protocolos más importantes que se encuentran en esta capa son: el protocolo IP (Internet Protocol) se encarga del direccionamiento, ruteo y fragmentación de los datagramas, ICMP (Internet Control Message Protocol) maneja los mensajes de control de Internet, ARP/RARP gestionan las direcciones Ethernet locales.

Cada equipo tiene una dirección IP única, compuesta por 32 bits en numeración binaria, por facilidad, se los separa en cuatro grupos de 8 bits y se los traduce a numeración decimal. Debido a que con 8 bits binarios