Recibido: Ago. 4, 2021 | Aceptado: Ene. 10, 2022

Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI)

Security at the data link level in the Open Systems Interconnection Model (OSI)

DOI: https://doi.org/10.21803/ingecana.2.2.405

Christian Obando I[1], Martín Vásquez V[2]

[1] Ingeniero en electrónica y telecomunicaciones y especialista en seguridad informática hasta 2015. E-mail: chrisobib@gmail.com. [2] Ingeniero informatico

Resumen

Las redes de comunicaciones pueden llegar a prestar una innumerable cantidad de servicios en una organización que van a permitir satisfacer las necesidades más importantes de ésta, ayudándola con el cumplimiento de sus objetivos organizacionales con mayor eficiencia, sin embargo, la falta de implementación de seguridad de la información en sus dispositivos informáticos, puede causar una gran desventaja para dichos objetivos. La capa dos del modelo OSI se considera una de las más importantes en el flujo de la información ya que de ella prácticamente parte la comunicación con el resto de las capas de este modelo, por lo que se ve la necesidad de estudiar los ataques informáticos a esta capa e implementar técnicas que permitan mejorar la seguridad en dicha capa.

Palabras clave: Seguridad informática; Modelos de referencia, Protocolos, Redes, Dispositivos de red; Medios de transmisión.

Abstract

Communications networks can provide an innumerable amount of services in an organization that will allow it to satisfy its most important needs, helping it to fulfill its organizational objectives more efficiently.
in their computing devices can cause a great disadvantage for these objectives. Layer two of the OSI model is considered one of the most important in the flow of information, since it is practically the starting point for communication with the rest of the layers of this model, so there is a need to study computer attacks on this layer and implement techniques to improve security in this layer.

Keywords: *Computer Security, Reference Models, Protocols, Networks, Network Devices, Transmission Media.*

Introducción

Los sistemas informáticos sin importar sus características tecnológicas hardware, como por ejemplo el procesador con su capacidad de procesamiento de la información, al conectarse a una red de comunicaciones, como es el internet, es vulnerable a cualquier ataque informático ya que la forma como acceden y transmiten información en este tipo de redes no depende de esas características tecnológicas sino del medio de transmisión, y principalmente de la estructura en la cual los datos viajan de un dispositivo a otro. Esta estructura es igual para todos los dispositivos conectados y de hecho es ésta la que permite comunicar todos los dispositivos informáticos no solo localmente sino a nivel mundial. Esta estructura es conocida como el modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection). Este modelo fue creado por la Organización Internacional para la Normalización (ISO, International Organization for Standardization) en 1984 para solucionar la incompatibilidad que existía entre redes a la hora de comunicarse una con otra [1]. En la figura 1 [2] se puede observar el modelo de referencia OSI.

Desafortunadamente, las siete capas que componen a este modelo han sido objeto de muchos ataques informáticos con el fin de robar información u ocasionar percances en algún servicio de la red informática.

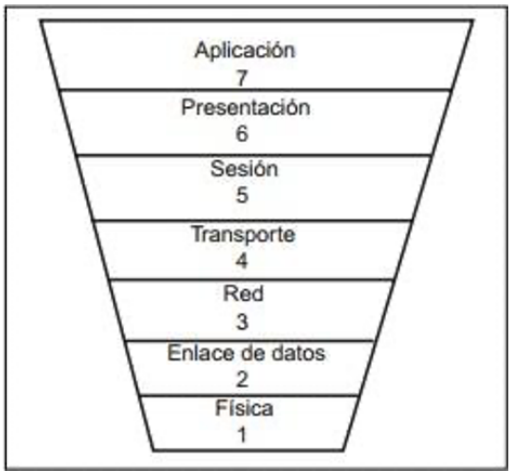

Figura 1. Modelo OSI

Este artículo es el resultado de analizar las diferentes capas del modelo OSI e identificar los ataques informáticos más relevantes que afectan a este modelo y por ende a una red de comunicaciones. El análisis detectó que la capa dos correspondiente a la de enlace de datos es una de las capas que mayor cantidad de ataques recibe por considerarse erróneamente, por algunos administradores de red, que no es importante o que no existen mecanismos de seguridad que la protejan o simplemente por falta de conocimiento de tecnologías que pueden asegurar esta capa tan importante del modelo OSI, de hecho un ataque en la capa dos podría llegar a causar el efecto dominó como se afirma en [3] el cual consiste en vulnerar esta capa y desde ella vulnerar las capas superiores que la siguen pudiendo llegar a ser catastrófico para la red de una organización.

Capa 2: Enlace de datos

Como se ha dicho con anterioridad el modelo OSI posee 7 capas, cada una de ellas cumple una determinada función en el proceso de transmisión de información desde un dispositivo origen hasta otro destino; en cada una de estas capas la información se procesa de manera diferente y tienen su propia forma de nombrar a sus unidades de datos como se indica a continuación [4]:

- Capa 1: bits
- Capa 2: tramas
- Capa 3: paquetes
- Capa 4: Segmentos
- Capa 5: SPDU (Session Protocol Data Unit)
- Capa 6: PPDU (Presentation Protocol Data Unit)
- Capa 7: APDU (Application Protocol Data Unit)

En general, en cada una de las capas la información se maneja como Unidad de Datos de Protocolo (PDU, Protocol Data Unit). Estas PDU permiten el intercambio de la información de una capa a otra, sin embargo, solo la capa homóloga será capaz de interpretar esa información, dicho de otro modo, la capa 2 de un dispositivo destino, solo puede interpretar la información que le es enviada de la capa 2 de un dispositivo origen, este tipo de comunicación es conocida como par a par [5].

Funciones de la capa 2

La tarea primordial de la capa de enlace de datos es la de corrección de errores y el control de acceso al medio. Esta capa en un dispositivo destino, hace que los bits provenientes de un dispositivo origen se transformen en tramas las cuales se transmitirán en forma secuencial hacia la siguiente capa. En sentido contrario a la comunicación, cuando los paquetes de datos llegan a la capa de enlace de datos, éstos empiezan a ubicarse en tramas, que vienen definidas por la arquitectura de red que se está utilizando (como Ethernet, Token Ring, etc.). Esta capa se encarga de desplazar los datos por el enlace físico de comunicación hasta el dispositivo destino, e identificar cada computador incluido en la red de acuerdo a su dirección física o también conocida como dirección de Control de Acceso al Medio (MAC, Media Access Control) la cual viene codificada en la Tarjeta de Interfaz de Red (NIC, Network Interface Card). La capa de enlace de datos también se asegura de que las tramas enviadas por el medio físico se recibieron sin error alguno mediante la adición de un campo en la trama llamado Chequeo de Redundancia Cíclica (CRC, Cyclical Redundancy Check), el cual básicamente es un valor que se calcula tanto en el origen como en el destino. Si los dos valores de CRC son iguales, significa que la trama se recibió correcta e íntegramente, y no recibió error alguno durante su transmisión [6].

Es también en esta capa donde se debe evitar que un transmisor muy rápido sature con datos a un receptor lento [7]. Finalmente, esta capa va a preparar los paquetes de la capa de red para ser transmitidos en el medio de transmisión.

Formato de trama de la capa 2

Como se mencionó anteriormente, el tipo de trama que se genera en la capa de enlace de datos dependerá de la tecnología de red que se está utilizando, como Ethernet, Token Ring o FDDI.

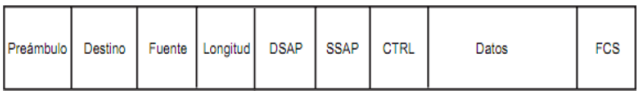

Figura 2. [7] trama Ethernet 802.2.

Preámbulo: Bits de alternación (1 y 0) que indican que se ha enviado una trama.

Destino: La dirección MAC destino

Fuente: La dirección MAC origen

Longitud: especifica el número de bytes de datos incluidos en la trama

DSAP: Punto de Acceso al Servicio de Destino (Destination Service Access Point)

SSAP: Punto de Acceso al Servicio de Origen (Source Service Access Point)

CTRL: Control Lógico de Enlace

Datos: en este segmento, la trama mantiene los datos que se han enviado o se van a enviar.

FCS: Secuencia de Comprobación de la Trama (Frame Check Sequence) el cual contiene el valor CRC de la trama. Como se puede observar, esta trama básicamente se compone de un encabezado que la describe, de los datos que la incluyen y de la información referente a la capa de enlace de datos (como los DSAP y SSAP), que no solo definen el tipo de trama que se trata (Ethernet en este caso) sino que también contribuyen a que la trama llegue a la computadora destino [2].

Dispositivos de red de la capa 2

Entre los dispositivos de red que se encuentran en la capa de enlace de datos encontramos: tarjetas de red o NIC, hub, bridge y el switch, siendo este último el objeto de estudio en este artículo ya que de todos los dispositivos presentes en esta capa, éste es el que actualmente más se utiliza en las redes de las organizaciones y por otro lado este dispositivo es el único de los cuatro que evolucionó para aprovechar sus grandes capacidades de conmutación y mejorar la velocidad de transmisión de datos de una Red Área Local (LAN, Local Area Network) a una Red de Área Amplia (WAN, Wide Area Network). Esta evolución del switch lo hace ascender a la capa de red del modelo OSI, en la cual se lo conoce como switch de capa 3 o switch multicapa y cuyas nuevas funcionalidades es la del enrutamiento entre redes [5]. En este artículo sólo se hace referencia al switch de capa 2.

Seguridad en la capa 2

Según el FBI, el 80% de los ataques informáticos provienen del interior de la organización. 99% de los puertos de las redes LAN corporativas están desprotegidos. Es decir, cualquiera puede conectarse a ellos [8].

El modelo OSI fue diseñado para que cada capa trabaje de manera independiente de las otras, su relación existe cuando una capa brinda servicios a la siguiente en jerarquía; sin embargo la capa superior no puede validar si la capa inferior fue comprometida o no. Por consiguiente, si la capa de enlace de datos es atacada, las comunicaciones se verán comprometidas sin que las otras capas se enteren del problema.

En la capa 2 los equipos son visibles unos a otros mediante una dirección física MAC. El tráfico entre equipos es administrado por un switch, el cual permite el uso de los recursos de la red de manera eficiente. El uso de switches ha creado algunos mitos, como son:

- La dirección MAC de un equipo es física por lo tanto no puede ser cambiada o falsificada.
- El switch no es vulnerable a Sniffing de tráfico.
- Las LAN Virtuales (VLAN, Virtual LAN)

están completamente aisladas unas de otras.

Ataques a la capa 2

Los ataques de capa 2 suelen requerir acceso desde el interior, ya sea un empleado o un visitante. A continuación se analizan algunos ataques a la capa de enlace de datos.

3.1.1 CAM TABLE OVERFLOW

Un switch guarda la asociación entre MAC y el puerto donde está conectado un equipo en la una tabla llamada Memoria de Contenido Direccionable (CAM, Content Addressable Memory), la cual tiene un tamaño fijo. Cuando este espacio ha sido usado en su totalidad, el switch envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM; por lo tanto, un switch se convierte en un hub para todo equipo que no esté en su tabla CAM. Si un atacante enviará hacia cualquier puerto de un switch un gran número de tramas con direcciones MAC generadas aleatoriamente hasta que se llene la tabla CAM entonces se generan problemas.

Si la tabla CAM está ll ena, no se aceptan nuevas entradas y cuando la tabla CAM no puede almacenar más asociaciones MAC-Puerto el switch empieza a enviar por todos los puertos de que dispone (Broadcast) las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM. Esto es, el switch empieza a comportarse como un hub para cualquier MAC que no haya aprendido porque su tabla CAM está llena.

Esto ocasiona dos efectos adversos graves:

Un dispositivo intruso puede conectarse a cualquier puerto del switch y capturar un tráfico que normalmente no vería por ese puerto en circunstancias normales.

El tráfico saliente del switch es claramente ineficiente e innecesariamente voluminoso, lo que puede llegar a causar que se produzca un caso de Denegación de Servicios (DoS, Denial of Service).

Este ataque puede ser mitigado configurando seguridad de puertos en el switch.

Con la seguridad de puertos, el administrador puede especificar en forma estática las direcciones MAC en un puerto particular del switch o bien puede permitir que el switch aprenda en forma dinámica un número determinado de direcciones MAC por cada puerto. En general, especificar en forma estática las direcciones MAC no es una solución administrable en un ambiente de producción. Permitir que el switch aprenda en forma dinámica un número fijo de direcciones MAC es una solución administrativamente escalable.

ARP spoofing

Para que la capa 2 pueda dar servicios a capa 3 existen dos protocolos llamados Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol) y el Protocolo de Resolución de Direcciones Inverso (RARP, Reverse Address Resolution Protocol), en los cuales cada dirección MAC está asociada a una dirección de Protocolo de Internet (IP, Internet Protocol). Estas asociaciones son almacenadas en una tabla de direcciones MAC contra direcciones IP, tanto en los switches como en los dispositivos que estén conectados en una red. ARP no proporciona seguridad o algún mecanismo para reservar direcciones IP o MAC. En algunos Sistemas Operativos (SO, Operating System) inclusive las entradas ARP estáticas son sobre escritas por las solicitudes ARP.

Mediante peticiones falsas de ARP es posible falsificar cualquier dirección MAC en una red de

cómputo; por lo tanto, cualquier tráfico puede ser redireccionado a un equipo falso y esto permite realizar varios ataques:

Tipos de ataque ARP Spoofing

a) Switch Port Stealing (Sniffing):

Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario.

b) Man in the Middle (Sniffing):

Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados).

c) Denial of service (DoS):

Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

d) Secuestro (Hijacking):

Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación y secuestrar la sesión.

Vlan hopping attack

Para que un switch administre VLANs requiere de la creación de un puerto truck que tiene acceso a todas las VLANs, este puerto se usa para transmitir tráfico de múltiples VLAN. Para la administración se usa el Protocolo de enlace Troncal Dinámico (DTP, Dynamic Trunking Protocol), el cual por defecto se encuentra configurado de manera “Automática”. El atacante puede configurar un dispositivo para que simule ser un switch y se haga pasar como tal ante otro switch permitiéndole al atacante convertirse en miembro de todas las VLAN, y por lo tanto tener acceso a servicios y/o información de toda la red.

La mejor forma de prevenir los ataques básicos de salto de VLAN consiste en deshabilitar el trunking en todos los puertos, a excepción de aquellos que lo requieran.

En los puertos donde el trunking deba estar disponible, se deben deshabilitar las negociaciones DTP y habilitar el trunking en forma manual.

Ataques A STP

El Protocolo de Árbol de Extensión (STP, Spanning Tree Protocol) permite crear topologías de red libres de bucles (forma de árbol), es decir, asegura que el tráfico broadcast no se vuelva una tormenta. Cuando un atacante logra estar conectado en dos switches, puede inundar la red con paquetes de configuración del tipo BPDU (Bridge Protocol Data Units), con lo que puede redireccionar todo el tráfico a su equipo de cómputo.

Este ataque puede ser utilizado para usurpar los tres objetivos de la seguridad: confidencialidad, integridad y disponibilidad.

Las técnicas de mitigación para la manipulación de STP incluyen la habilitación de PortFast y la utilización de root guard y BPDU guard.

Ataques de tormenta en lan

Una tormenta de LAN ocurre cuando los

paquetes inundan la LAN, creando saturación y degradando el desempeño de la red. Estas tormentas pueden ser causadas por errores en la configuración de la red, o por usuarios realizando ataques DoS. También pueden ocurrir tormentas de broadcast como se observa en la figura 8 [9].

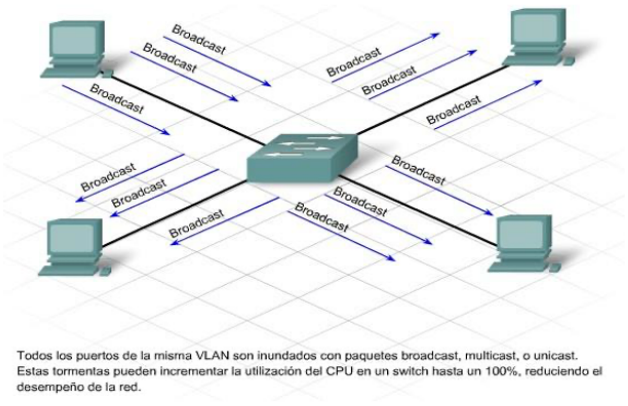

Figura 3. Tormenta LAN – broadcast.

Si bien este ataque no es posible prevenirlo en su totalidad, sí es posible mitigarlo implementando un control de tormentas. El control de tormentas previene las alteraciones en el tráfico de una LAN causadas por tormentas de broadcast, multicast o unicast provenientes de una interfaz física. El control de tormentas (o supresión de tráfico) monitorea los paquetes que pasan desde una interfaz hacia el bus de conmutación y determina si el paquete es unicast, multicast o broadcast.

El switch cuenta el número de paquetes de cada tipo específico recibidos en un cierto período de tiempo y compara estas medidas con un umbral de supresión predefinido. El control de tormentas bloquea el tráfico cuando el límite definido es alcanzado [10].

CONCLUSIONES

Los riesgos de seguridad en una red corporativa no se pueden eliminar o prevenir completamente, pero sí se pueden mitigar con una buenas políticas de seguridad de la información y haciendo uso del aseguramiento (hardening) de los dispositivos de red y servidores.

Se debe tener en cuenta que las vulnerabilidades de una red pueden ser aprovechadas por agentes externos o internos de la organización.

La seguridad de los dispositivos no es solo a nivel de red y aplicación, también hay que tener en cuenta la seguridad a nivel físico, contemplando un buen respaldo de contingencia de energía y unas buenas políticas de control de acceso hacia los lugares donde se encuentran todos los dispositivos.

El análisis de tráfico en un dispositivo consiste en “desarmar” cada trama, paquete, segmento, bloque de información y analizarlos “bit” a “bit”, aquí se esconde la razón de ser de la seguridad.

Cuando un dispositivo de red comienza a recibir información cada uno de los niveles de la pila TCP/IP comienza su tarea identificando “bit” a “bit” a qué módulo le corresponde trabajar. Un módulo no es más que un código, script o programa que tiene todas las órdenes que debe realizar en ese nivel y con esa secuencia de bits. Una vez que reúne suficiente información para identificar unívocamente a qué módulo llamar, automáticamente le pasa el control a éste y a partir de allí comienza su tarea.

Tener contingencia de los dispositivos de red y servidores, con sus respectivos respaldos de configuraciones y de información, es de vital importancia para que haya continuidad del negocio en caso de que haya un ataque de denegación de servicios.

REFERENCIAS

1]Claros Iver. Modelo OSI. Universidad Privada Cumbre. [En línea]. Disponible en: http://belarmino.galeon.com/

[2] J. Hernández. El modelo OSI y los protocols de red. (2010). [En línea]. Disponible en: http://blyx.com/public/docs/pila_OSI.pdf

[3] R. Cárdenas Gómez. Seguridad en Redes y Telecomunicaciones. (2013). [En línea]. Disponible en: http://cryptomex.org/SlidesSeguridad/SegRedesTelecom.pdf

[4]Museo de la Informática y Computación Aplicada. El modelo OSI. [En línea]. Disponible en: http://www.tecnotopia.com.mx/redes/redosi.htm

[5]Bustamante Rubén. Seguridad en Redes. Universidad Autónoma del Estado de Hidalgo. [En línea]. Disponible en: http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20 redes.pdf

[6] G. Vasquez. Redes de Comunicaciones. Universidad Autónoma de Baja California Sur. [En línea]. Disponible en: http://growitsol.com/support/UABCS/RedesI/Unidad-II-LIC.pdf

[7] IEEE. Formato de trama Ethernet. IBM. (2014). [En línea]. Disponible en: http://publib.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAJYETHERNETFRAMEFORMAT.HTM

[8] G. Arellano. Seguridad en capa 2. (2014) [en línea]. Disponible en: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fwww gabriel-arellano.com.

[9] A. Alex, O. Federico, O. Christian. Seguridad en Infraestructura de Red. Universidad Pontificia Bolivariana. (2014).

[10] J. Vicente. Network Time Protocol. (2013). [en línea].Disponible en: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.uv.es%2F~montanan%2Fredes%2Ftrabajos%2Fntp.doc&ei=YoxMUo6EB4-K9QS40YGwDw&usg=AFQjCNHfNtdIdW2FGd5lKia5IgFPSaCTnQ&sig2=anfq5t9aqDM5nczO3Ia2GA&bvm=bv.53371865,d. eWU&cad=rja