UNIVERSIDAD DEL CENTRO DEL BAJIO.

LICENCIATURA EN SISTEMAS COMPUTACIONALES.

TÍTULO:

"Seguridad a nivel de red.
Seguridad a nivel de enlace.
Seguridad en redes locales inalámbricas: amenazas y ataques, mecanismos básicos".

MATERIA:

SEGURIDAD INFORMATICA.

DOCENTE:

FILIBERTO DURAN GARCIA.

PRESENTA

PABLO SÁNCHEZ UGALDE.

Celaya, Guanajuato , 9 de Marzo del año 2019.

Seguridad de redes.

La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red. Los usuarios eligen o se les asigna una identificación y contraseña u otra información de autenticación que les permite acceder a información y programas dentro de sus autorizaciones. La seguridad de red cubre una variedad de redes de computadoras, tanto públicas como privadas, que se usan en trabajos cotidianos; realizar transacciones y comunicaciones entre empresas, agencias gubernamentales e individuos. Las redes pueden ser privadas, como dentro de una empresa, y otras que pueden estar abiertas al público. La seguridad de la redes está presente en organizaciones, empresas y otros tipos de instituciones. Hace como su nombre indica: protege la red, además de proteger y supervisar las operaciones que se realizan. La forma más común y simple de proteger un recurso de red es asignándole un nombre único y la contraseña correspondiente.

Capa de enlace de datos.

Pila del modelo OSI.

El nivel de enlace de datos (en inglés: data link level) o capa de enlace de datos, es la segunda capa del modelo OSI,1 es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. 2Recibe peticiones de la capa de red y utiliza los servicios de la capa física.

El objetivo de la capa de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a la conexión). Para lograr este objetivo tiene que montar bloques de información (llamados tramas en esta capa), dotarles de una dirección de capa de enlace (Dirección MAC), gestionar la detección o corrección de errores, y ocuparse del “control de flujo” entre equipos (para evitar que un equipo más rápido desborde a uno más lento).

Cuando el medio de comunicación está compartido entre más de dos equipos es necesario arbitrar el uso del mismo. Esta tarea se realiza en la subcapa de control de acceso al medio.

Seguridad en redes inalámbricas.

Lamentablemente, la seguridad en estas redes no se ha considerado suficientemente por parte de sus usuarios y han quedado vulnerables a diversos tipos de ataques. Aunque es muy común asociar el término "redes inalámbricas" a las redes conocidas como WiFi, en la actualidad esta familia incluye muchas otras tecnologías. Es posible encontrar tecnologías que se mueven entre tres grupos distintos. El primero se denomina redes WWAN (Wireless Wide Area NetworkRedes Inalámbricas de Área Amplia) cuya potencia y alcance permiten abarcar grandes espacios e incluso ciudades. Dentro de este grupo se ubican las tecnologías celulares (GSM, GPRS, CDPD, TDMA.). Las redes WLAN (Wireless Local Area NetworkRedes Inalámbricas de Área Local) integran el segundo grupo y se caracterizan por una potencia y alcance medios utilizados ampliamente en entornos cerrados, como edificios o áreas de pocos kilómetros. Este grupo es dominado por las tecnologías 802.11 (WiFi). Al tercer y último grupo WPAN (Wireless Personal Area NetworkRedes Inalámbricas de Area Personal) pertenecen aquellos equipos que utilizan potencia reducida para abarcar espacios pequeños en el entorno de una oficina o una persona. Dentro de las WPAN se encuentran las tecnologías 802.15, Bluetooth, HomeRF, IrDA o similares. Recientemente fue creado el nuevo estándar 802.16 (WiMax) para cubrir distancias superiores a WiFi. WiMax, que también es mucho más tolerante a la falta de visibilidad, fue concebido para competir con tecnologías ubicadas en el grupo WWAN, pero es un complemento de WiFi y no su sustituto. Esta tecnología, que se populariza en los últimos dos años para el acceso inalámbrico de Banda Ancha.

Métodos de ataques.

En la actualidad, las redes inalámbricas cuentan con numerosos mecanismos y protocolos que aunque no garantizan de forma absoluta la integridad y confidencialidad de la información que por ellas transita, sí proporcionan barreras que reducen de forma considerable la cantidad de personas capaces (por sus conocimientos y recursos) de efectuar ataques exitosos que llegan al punto de competir con muchas de las soluciones cableadas actualmente disponibles. Desafortunadamente, al igual que sucede muchas veces con las redes cableadas, la complejidad de algunas de estas medidas y el desconocimiento por parte de usuarios y administradores, trae como resultado que proliferen muchos sistemas desprotegidos, donde la gran mayoría no cuenta incluso con los requerimientos mínimos recomendados. Debido a la gran extensión que tiene su uso a nivel global, se le dedicará un aparte especial a los tipos de ataques más comunes en las redes 802.11. 802.11: Favorito de los atacantes La amplia cobertura de las zonas de las redes 802.11 es uno de los principales motivos para tener presente una constante preocupación e interés por su seguridad. Un atacante puede ubicarse en un lugar en el que nadie espere encontrarlo y

mantenerse lo suficientemente lejos del área física de la red sin ser detectado. Otro motivo fundamental es el extenso uso, pues en el 2006 la cantidad de dispositivos de hardware con capacidades 802.11 superaba los cuarenta millones de unidades. Defcon, un concurso de búsqueda de redes 802.11 que se realiza anualmente en Estados Unidos arrojó en su edición del 2002 un alarmante 61.2% de redes que no tenían habilitado el protocolo WEP y un 18.6% que tenía como valor ESSID el predeterminado por el fabricante. En Europa, durante el año 2003, se detectaba en el Reino Unido un 70% de puntos de acceso sin WEP, muchos de los cuales servían adicionalmente como puerta de enlace para Internet. En el caso de Cuba sucede un fenómeno similar, y quizás de forma más marcada en los últimos años. Las tecnologías 802.11 se han convertido en el estándar para redes inalámbricas en nuestro país, popularizadas por medio de los equipos como AOpen, NetGear y Cisco. En un estudio realizado en el 2005 por la Agencia de Control y Supervisión del MIC, al menos el 85,6% de las redes detectadas en Ciudad de La Habana no tenían habilitado WEP y en algunos casos fue posible explorar estas intranets desde el exterior de las edificaciones que las alojaban. Aunque actualmente esa situación se ha revertido en gran medida gracias a la acción de varias entidades involucradas en la seguridad de redes, son muchos los usuarios cubanos que optan cada día por soluciones 802.11 para sus empresas, en muchos casos sin contar con el conocimiento necesario para ejecutar implementaciones medianamente seguras. En conclusión, las redes 802.11 son omnipresentes, fáciles de encontrar y no requieren un esfuerzo especial para conectarse a ellas, características que las hacen convertirse en la actualidad en uno de los objetivos favoritos de muchos atacantes.

REFERENCIAS.

CAPA DE ENLACE DE DATOS

En el texto: ("Capa de enlace de datos", 2019)

Bibliografía: Capa de enlace de datos. (2019). Retrieved from https://es.wikipedia.org/wiki/Capa_de_enlace_de_datos

SEGURIDAD DE REDES

En el texto: ("Seguridad de redes", 2019)

Bibliografía: Seguridad de redes. (2019). Retrieved from https://es.wikipedia.org/wiki/Seguridad_de_redes

SEGURIDAD EN REDES INALÁMBRICAS - ECURED

En el texto: ("Seguridad en redes inalámbricas - EcuRed", 2019)

Bibliografía: Seguridad en redes inalámbricas - EcuRed. (2019). Retrieved from https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas#Seguridad_en_redes_inal.C3.A1mbricas