APÉNDICE A

APÉNDICE A

ESTÁNDARES INTERNACIONALES

Redes inalámbricas (802.11)

Conocido también como WIFI, es una familia de estándares, especificaciones o protocolos de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y enlace de datos), especificando las normas de funcionamiento en una WLAN.

Se han desarrollado diversas especificaciones en esta familia debido a que han surgido nuevas necesidades para utilizar los medios más adecuados para lograr la implementación de una red inalámbrica en cualquier lugar.

1) 802.11a

El protocolo IEEE 802.11a se aprobó en el año de 1999. El estándar 802.11a , utiliza el mismo juego de los protocolos que tiene el estándar original 802.11, tiene una banda ancha de 5 Ghz y utiliza 52 subportadoras OFDM (Orthogonal Frequency – Division Multiplexing_ Frecuencia Ortogonal Multiplexando la División) con una velocidad máxima de 54 Mbit/s.

Utilizar la banda de 5 Ghz representa una ventaja del estándar 802.11a, dado que presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, porque restringe el uso de los equipos con este protocolo 802.11a; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como el estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

2) 802.11b

El estándar 802.11b es también un complemento del estándar 802.11; fue ratificado el mismo día que el estándar 802.11a en septiembre de 1999, con el fin de presentar mejoras y cambios al estándar 802.11.

Una WLAN (Wíreless Local Area Network _ Red de Área Local Inalámbrica) que constituye un sistema de comunicaciones de datos implementada como una extensión de una red local cableada dentro de un edificio o campus. Las redes WLAN combinan la conectividad hacia la red de datos con la movilidad del usuario. La IEEE 802.11b define dos componentes; una estación inalámbrica NIC (Network Interface Card _ Tarjeta de Red Inalámbrica), y un AP(Access Point - Punto de Acceso), el cual actúa como puente entre la estación inalámbrica y la red cableada.

3) 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo en el comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre del 2003. El 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radares y satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU (Internacional Telecommunication Union - Unión de las Telecomunicaciones Internacionales) que fueron movidas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó que los convenientes para minimizar el impacto de abrir la banda de 5 Ghz, utilizada generalmente por sistemas militares.

4) 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación 802.11g. Que es la evolución del estándar 802..11b, éste utiliza la banda de 2.4 Ghz al igual que el estándar 802.11b, pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22 Mbit/s de velocidad real de trasferencia, similar a la del estándar 802.11a.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue el día 20 de junio del 2003. Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 Km con antenas parabólicas apropiadas.

5) 802.11n

En enero de 2004, IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11n. La velocidad real de transmisión podría llegar a los 600 Mbps, y debería ser hasta 100 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output _ Entrada Mu̶últiple – Salida Múltiple), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

6) 802.11e

Las aplicaciones en tiempo real son ahora una realidad por las garantías QoS (Quality of Service -Calidad de Servicio) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC (Media Access Control Address - Dirección de Control

de Acceso al Medio) para soportar los servicios que requieren garantías de calidad de servicio. Para cumplir con su objetivo, IEEE 802.11e introduce un nuevo elemento llamado HCF(Hybrid Coordination Function - Función de Coordinación Hiíbrida) con dos tipos de acceso: EDCA (Enhanced Distributed Channel Access - Acceso al Canal Distribuido Enlazado) y HCCA (Controlled Access - Accesos Controlados)

7) 802.11 Super G

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz, alcanza una velocidad de transferencia de 108 Mbps. Esto es proporcionado por el chipset Atheros.

8) 802.11i

Está dirigido para combatir la vulnerabilidad actual en la seguridad de los protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Temporal Key Integrity Protocol - Protocolo de Claves Integrales, Seguras y Temporales) es también llamado hashing de las claves WPA2, WPE, WPA, incluyen mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricas y AES (Advanced Encryption Standard - Estándar de Cifrado Avanzado).

9) 802.11w

El estándar 802.11w está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidas, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas maliciosos. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red.

GLOSARIO

3DES	Estándar de Cifrado de Datos Triple (Triple Data Encryption Estándar). 3DES es un algoritmo de cifrado de clave simétrica implementado en 1990 y basado en DES, ya que al bloque de entrada de datos (64 bits) le son aplicadas tres iteraciones sucesivas de dicho algoritmo. 3DES parte de una clave inicial de 128 bits, la cual es dividida en dos claves diferentes de 64 bits.
A	
ACK	ACKNOWLEDGEMENT (ACK) (en español acuse de recibo), en comunicaciones entre computadoras, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.
AES	Estándar de Cifrado Avanzado (Advanced Encriyption Estándar). Es un algoritmo de cifrado de clave simétrica, adoptado como estándar en el año 1997 por el Instituto Nacional de Estándares y Tecnología, con base en una convocatoria pública lanzada a la comunidad científica internacional.
AH	Cabecera de Autenticación (Authentication Header). Proporciona autenticación e integridad de datos calculando un resumen sobre los paquetes a enviar, pero en cambio, no ofrece confidencialidad.
AMENAZA	Una amenaza es todo aquello que intenta o pretende destruir.
ANTENA	Dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre.
C	
CHROOT	chroot en un sistema operativo Unix es una operación que cambia el directorio raíz, afectando solamente al proceso actual y a sus procesos hijos. "chroot" se refiere a la llamada de sistema chroot(2) o al programa ejecutable chroot(8).
D	
DEMONIO	Un demonio, daemon o dæmon (de sus siglas en inglés *Disk And Execution MONitor*), es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita), aunque se intente cerrar o matar el proceso, éste continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

DHCP	DHCP (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de *host*) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.
DSA	Algoritmo de Firma Digital (Digital Signature Estándar). Sistema de firma digital adoptado como estándar por la organización de estándares de EEUU.
E	
ESP	Encapsulating Security Payload. Protocolo incluido dentro de IPv6 que realiza un cifrado de la información para garantizar la confidencialidad.
F	
FILEZILLA	FileZilla es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS).
FIREWALL	Dispositivo hardware o software que filtra tráfico a nivel de red y con base en unas determinadas reglas.
FTP	Protocolo de Transferencia de Ficheros (File Transfer Protocol). Protocolo perteneciente al nivel de aplicación y utilizado para transferir archivos entre diferentes equipos, ubicados éstos en redes basadas en TCP/IP. Por defecto, FTP emplea los puertos TCP 20 (Flujo de datos entre el cliente y el servidor) y 21 (transmisión de comandos de control).
G	
GUI	La interfaz gráfica de usuario, conocida también como GUI (del inglés *graphical user interface*) es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz. Su principal uso, consiste en proporcionar un entorno visual sencillo para permitir la comunicación con el sistema operativo de una máquina o computadora.

H	
HRU	El modelo de seguridad HRU (Harrison, Ruzzo, Ullman modelo) es un sistema operativo de nivel modelo de seguridad informática que se ocupa de la integridad de los derechos de acceso en el sistema. Es una extensión del modelo de Graham-Denning, en torno a la idea de que un conjunto finito de los procedimientos estén disponibles para editar los derechos de acceso de un sujeto *s* sobre un objeto *o.* Lleva el nombre de sus tres autores, Michael A. Harrison, Walter L. Ruzzo y Jeffrey D. Ullman.
HTTP	Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol). Protocolo del nivel de aplicación utilizado para la transacción de páginas o elementos web. Para ello, el cliente envía peticiones TCP al puerto 80 (por defecto) del servidor.
HUB	Concentrador elemental en una red Ethernet, que retransmite los datos que recibe de una estación a todas las démas estaciones que se encuentran conectadas en él.
I	
IDE	La interfaz ATA (Advanced Technology Attachment) o PATA, originalmente conocida como IDE (Integrated device Electronics), es un estándar de interfaz para la conexión de los dispositivos de almacenamiento masivo de datos y las unidades ópticas que utiliza el estándar derivado de ATA y el estándar ATAPI.
IEEE	Corresponde a las siglas de (Institute of Electrical and Electronics Engineers) en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en Mecatrónica.
INFORMACIÓN	Se entiende por información a todo mensaje (conjunto de datos) que al receptor le interese, lo entienda o lo ignore antes de recibirlo.
INTEGRIDAD	Característica que asegura que la información enviada a través de un canal de comunicación inseguro no haya sido alterada durante su transcurso, es decir, el mensaje a transmitr ha de ser exactamente el mismo en el origen y en el destino.

INTERNET	Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen, funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.
INTRANET	Es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización.
IP	Protocolo de Internet (Internet Protocol). Protocolo no orientado a conexión utilizado para la comunicación de datos a través de una red de paquetes conmutados.
IPSEC	Protocolo de seguridad de internet (Internet Protocol Security). Entorno de estándares abiertos basados en el protocolo IP, que ofrecen servicios de autenticación, cifrado e integridad de datos para asegurar las comunicaciones a través de dicho protocolo.
IPX	Intercambio de paquetes entre redes (Internetwork Packet Exchange). Protocolo de red no orientado a conexión, empleado para enviar y recibir informacion entre las distintas máquinas de una red Novell.
ISDN	Integrate Services Digital Network (Red Digital de Servicios Integrados). Red desarrollada por los operadores de telecomunicaciones con la intención de sustituir el sistema telefónico analógico por uno digital que permita integrar nuevos servicios (transmisión de voz, vídeo, datos).
K	
KERNEL	El núcleo o kernel (de la raíz germánica *Kern*) es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas, acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos a través de servicios de llamada al sistema.

L	
LOG	Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.
LZO	Lampel-Ziv-Oberhummer. Librería de comprensión de datos diseñada para comprimir y descomprimir en tiempo real.
O	
OUTSOURCING	Outsourcing es el proceso en el cual una firma identifica una porción de su proceso de negocio que podría ser desempeñada más eficientemente y/o más efectivamente por otra corporación, la cual es contratada para desarrollar esa porción de negocio. Esto libera a la primera organización para enfocarse en la parte o función central de su negocio.
P	
PAM	Módulo de Autenticación Enlazables (Pluggables Authentication Modules). Conjunto de módulos que se emplearán en el momento de validar el acceso a las diversas funciones y aplicaciones de un sistema operativo de tipo Unix.
PKI	Infraestructura de Clave Pública (Public Key Infraestructure). Conjunto de protocolos, servicios y estándares globales que soportan aplicaciones basadas en criptografía de clave pública. Ofrece registro, almacenamiento, selección y recuperación de claves, revocación de certificados digitales y evaluación de la confianza.
POLÍTICA	Una política representa el marco de referencia para la realización de las acciones que se deben emprender en una empresa en un periodo de tiempo. La política debe incluir tres cosas: “qué se debe hacer, cómo hacer para llegar a hacerlo y la medida empleada para evaluar lo que se ha hecho hecho”.
PPP	Protocolo de Punto a Punto (Point to Point Protocol). Protocolo que permite establecer una comunicación a nivel de enlace entre dos computadoras, a través de una línea síncrona o asíncrona.
PPTP	Protocolo de Túnel Punto a Punto (Point to Point Tunneling Protocol). Protocolo que permite la transferencia segura de datos desde el equipo remoto a una red corporativa, creando para ello una red privada virtual sobre una red física de datos TCP/IP. La conexión de control se realiza sobre el puerto 1723 (TCP).
PS	Comando del sistema operativo Unix. El comando ps muestra por pantalla un listado de los procesos que se están ejecutando en el sistema.

PSH	PSH es un bit que se encuentra en el campo del código en el protocolo TCP. Cuando PSH está activado indica que los datos de ese segmento y los datos que hayan sido almacenados anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible. A veces llegan varios segmentos que transportan datos y no tienen activado el bit PSH; el receptor almacenará esos datos pero no los entregará a la aplicación receptora hasta que reciba un segmento con el PSH activado. Con el bit a 1 está activado y a 0 desactivado.
Q	
QOS	QoS o Calidad de Servicio (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.
R	
RJ45	RJ-45 (*registered jack 45*) es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.
ROUTER	Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
RSA	(Rivest, Shamir, Adleman). Algoritmo criptográfico asimétrico basado en una pareja de claves (pública y privada). Que pueden ser utilizadas al mismo tiempo tanto para cifrar una comunicación como para autenticar a sus participantes.
RTC	Red Telefónica Conmutada. Sistema de comunicación diseñado inicialmente para la transmisión de datos a tráves de un fax o un módem analógico.
S	
SA	Asociación de Seguridad (Security Association). Acuerdo unidireccional entre los participantes de una VPN, referido a los métodos y parámetros empleados en la estructura del túnel destinados éstos a garantizar la seguridad de los datos transmitidos.

SERIAL ATA	*Serial Advanced Technology Attachment* es una interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento, como puede ser el disco duro, lectores y regrabadores de CD/DVD/BR, Unidades de Estado Sólido u otros dispositivos de altas prestaciones que están siendo todavía desarrollados. Serial ATA sustituye a la tradicional Parallel ATA o P-ATA. SATA proporciona mayores velocidades, mejor aprovechamiento cuando hay varias unidades, mayor longitud del cable de transmisión de datos y capacidad para conectar unidades al instante.
SLIP	El protocolo SLIP (Serial Line Internet Protocol) es un estándar de transmisión de datagramas IP para líneas serie, pero que ha quedado bastante obsoleto. Fue diseñado para trabajar a través de puerto serie y conexión de módem. SLIP se ha sustituido por el PPP (Point-to-Point Protocol) cuyo diseño es superior, tiene más y mejores características y no requiere de la configuración de su dirección IP antes de ser establecido. Sin embargo, con microcontroladores, se sigue utilizando el modo de encapsulación de SLIP para paquetes IP ya que usa cabeceras de tamaño reducido.
SOCKET	Un socket (enchufe), es un método para la comunicación entre un programa del cliente y un programa del servidor en una red. Un socket se define como el punto final en una conexión. Los sockets se crean y se utilizan con un sistema de peticiones o de *llamadas de función* a veces llamados interfaz de programación de aplicación de sockets (API, application programming interface).
SSH	Interfaz de Usuario Segura (Secure Shell). Protocolo que permite la autenticación y el intercambio de información a través de un canal seguro entre distintas máquinas de la red. Generalmente se emplea el puerto TCP 22 como puerto destino de la conexión.
SWITCH	Concentrador en una red Ethernet, que retransmite la información recibida sólo por el puerto al que se encuentra conectado el equipo al que va dirigida la información.
SYN	SYN es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases (3 way handshake). Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

T	
TUN	TUN o túnel es simplemente un enlace entre dos puntos a través de algún otro material. Una buena analogía es un túnel que pasa por debajo de una montaña. Ambos lados de la montaña están vinculados a través de un camino directo, en este caso la "montaña" es el Internet. Así que, esencialmente un túnel es un atajo directo a través de Internet.
U	
URL	Universal Resource Locator - Localizador de Recurso Uniforme. Sistema de direcciones que permiten identificar recursos dentro de internet (páginas web, servidores FTP, direcciones de correo).
V	
VPN	Red Privada Virtual (Virtual Private Network). Tecnología de red que permite una extensión de la red local sobre una red pública, como por ejemplo internet, con la peculiaridad de que la transmisión de datos se hace de manera privada, es decir, a tráves de unos elementos conocidos como túneles. Una VPN debe ser capaz de autenticar las comunicaciones, garantizar la integridad de la información transmitida y la confidencialidad de la misma.
W	
WINS	Servicio de nombres de internet de windows (Windows Internet Naming Service). Servidor de nombres para NetBIOS que mantiene una tabla de correspondecia entre las direcciones ethernet y los nombres de los ordenadores. Esto permite localizar rápidamente una computadora dentro de una red Windows.
WIRESHARK	Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

WPA	WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP. Los investigadores encontraron varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).
WPA2	WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA, está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.
WPE	WEP, acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.
X	
XDSL	Se conoce como xDSL a la familia de tecnologías de acceso a Internet de banda ancha basadas en la digitalización del bucle de abonado telefónico (el par de cobre). La principal ventaja de xDSL frente a otras soluciones de banda ancha (cable módem, fibra óptica, etcétera) es precisamente la reutilización de infraestructuras ya desplegadas, por tanto más baratas al estar parcial o totalmente amortizadas y con gran extensión entre la población.