Anexo I

Instalación de software necesario para la realización de la práctica # 7

Guía rápida de instalación de los programas NMAP y NESSUS

Instalación de NMAP

1. Iniciamos el instalador de la aplicación permitiendo la ejecución del programa. Presionamos el botón Ejecutar Figura AI.1

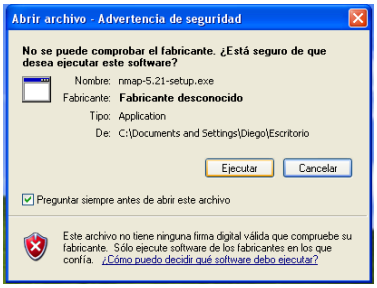

Figura AI.1 Ejecución del instalador

2. En este paso aceptamos los términos de la licencia (I AGREE) Figura AI.2

Se recuerda que NMAP tiene una licencia tipo GNU

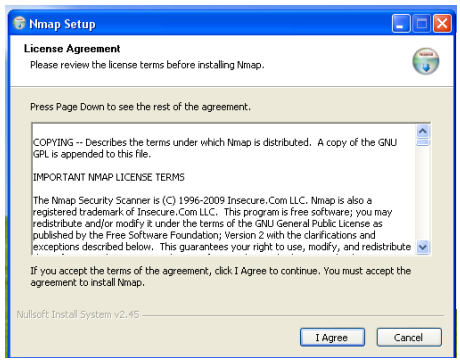

Figura AI.2 Términos de la licencia de NMAP

3. Seleccionamos los componentes a instalar, para fines de esta práctica dejaremos todos los componentes seleccionados. Pulsamos el botón NEXT Figura AI.3

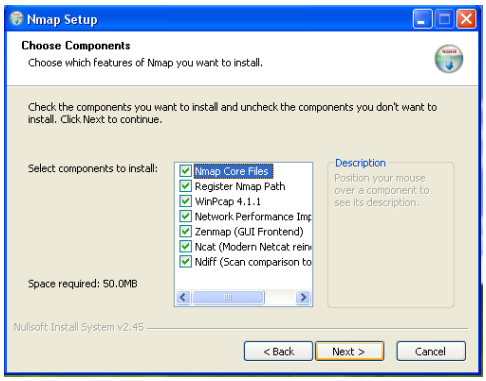

Figura AI.3 Selección de componentes de NMAP

4. Seleccionamos la ubicación donde quedaran instalados los archivos de ésta aplicación. Presionamos el botón INSTALL Figura AI.4

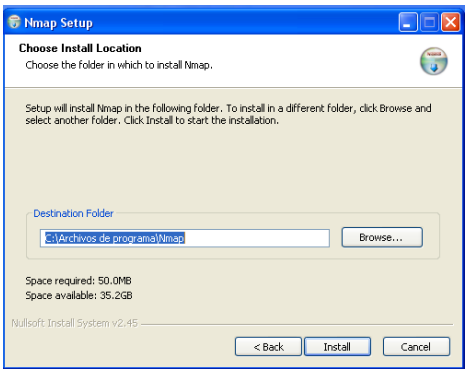

Figura AI.4 Selección del directorio de instalación de NMAP

5. Uno de los paquetes que vienen incluidos en ésta distribución de NMAP es WinPcap, ésta solicitará la configuración de preferencias de inicio, por el momento deseleccionáremos ambas casillas. Presionamos el botón NEXT. Figura AI.5

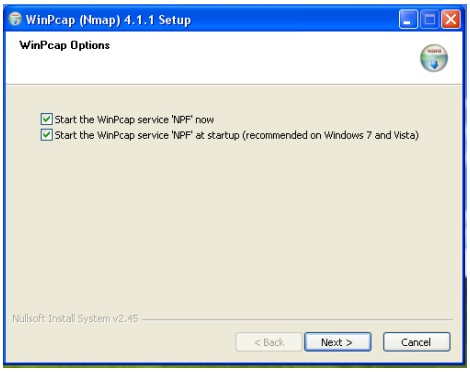

Figura AI.5 Preferencias de NMAP

6. Seleccionamos los accesos directos al programa. Presionamos el botón NEXT Figura AI.6

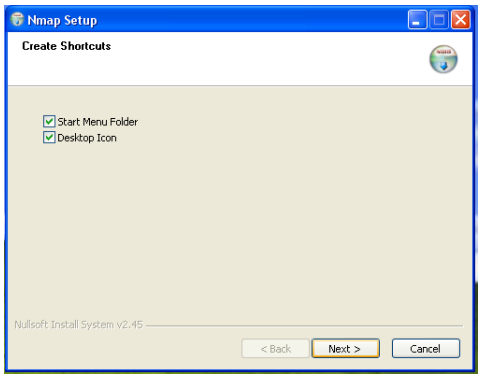

Figura AI.6 Creación de Accesos de NMAP

7. Finalizamos la instalación del programa presionado el botón de FINISH Figura AI.7

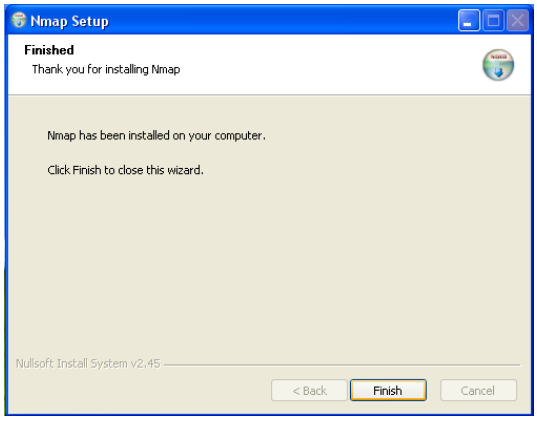

Figura AI.7 Finalización de la instalación de NMAP

Instalación de Nessus

1. Ejecutamos el instalador de la aplicación. Presionamos el Botón NEXT Figura AI.8

Figura AI.8 Instalador de NESSUS

2. Aceptamos los términos de la licencia. Presionamos el botón NEXT. Figura AI.9

NOTA a diferencia de NMAP NESSUS tiene una licencia COMERCIAL

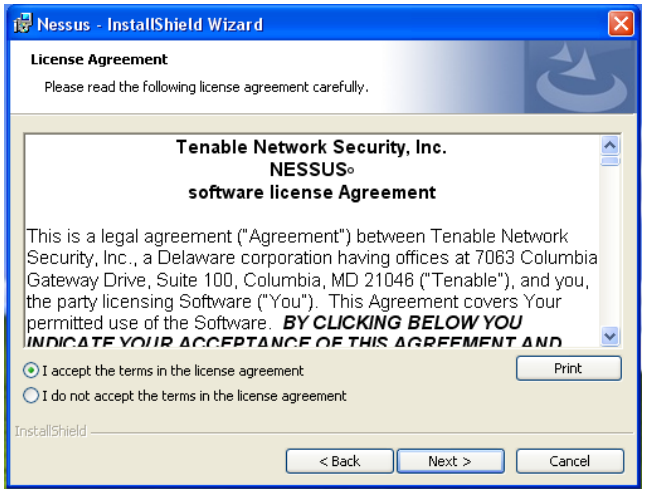

Figura AI.9 Términos de la licencia de NESSUS

3. Seleccionamos la ubicación donde quedaran instalados los archivos de ésta aplicación. Presionamos el botón NEXT. Figura AI.10

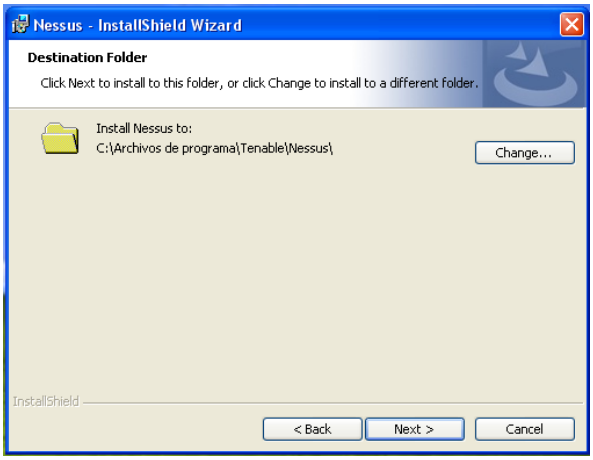

Figura AI.10 Selección del directorio de instalación de NESSUS

4. Seleccionamos el tipo de instalación que queremos llevar a cabo. Para fines de esta práctica elegimos COMPLETE. Presionamos el botón NEXT Figura AI.11

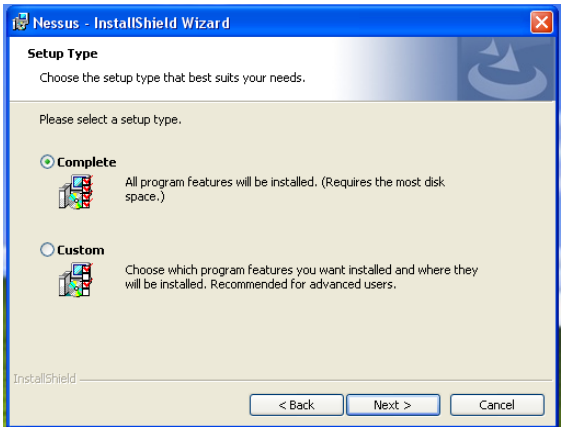

Figura AI.11 Tipo de instalación de NESSUS

Al termino de la instalación nosmostrará la sigueinte pantalla. Terminamos la instalación presionando el Botón FINISH Figura AI.12

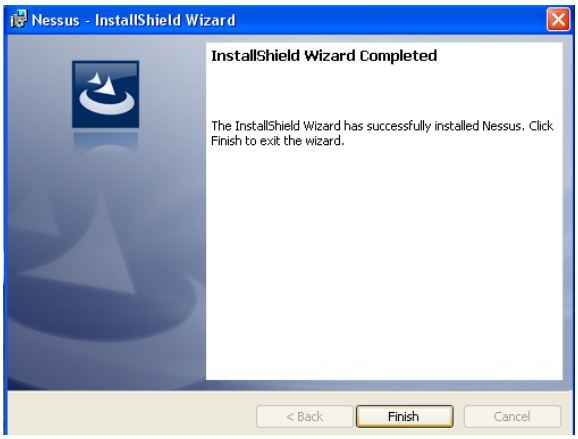

Figura AI.12 Instalación terminada de NESSUS

Configuración de NESSUS

1. Iniciamos la aplicación de Nessus Server Manager Figura AI.13

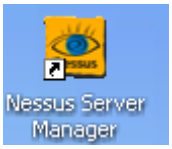

Figura AI.13 NESSUS Server Manager

2. Al iniciar nos aparecerá una ventana como la siguiente: Figura AI.14

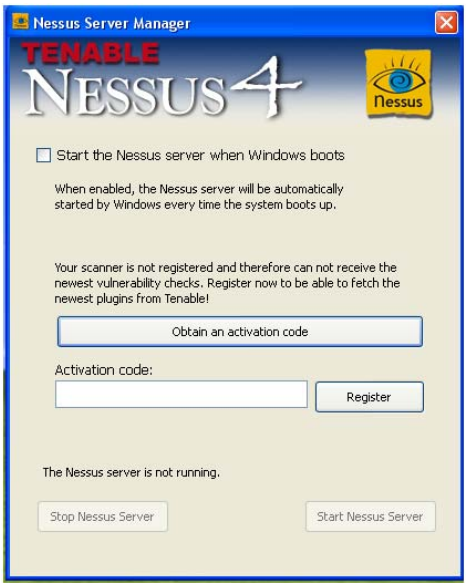

Figura AI.14 Configuraciones del servidor de NESSUS

Damos click en el botón OBTAIN AN ACTIVATION CODE

3. Se abrirá una ventana del navegador predeterminado de internet mostrando las 2 opciones de suscripción para el uso de ésta herramienta, para fines de la práctica seleccionaremos HomeFeed Figura AI.15

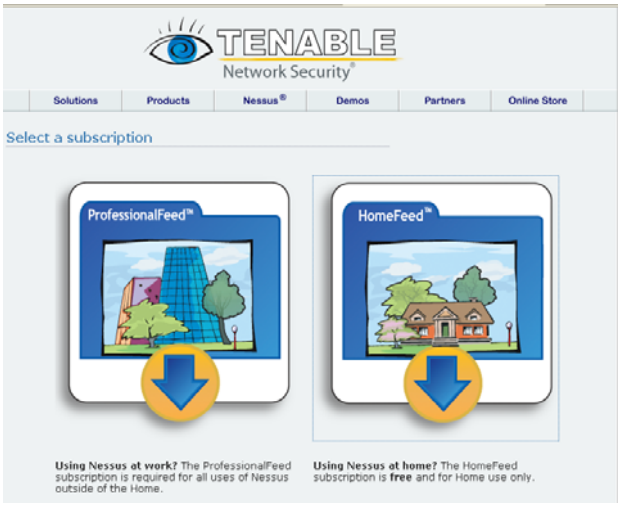

Figura AI.15 Selección de la suscripción de NESSUS

4. Aceptamos los términos de uso Figura AI .16

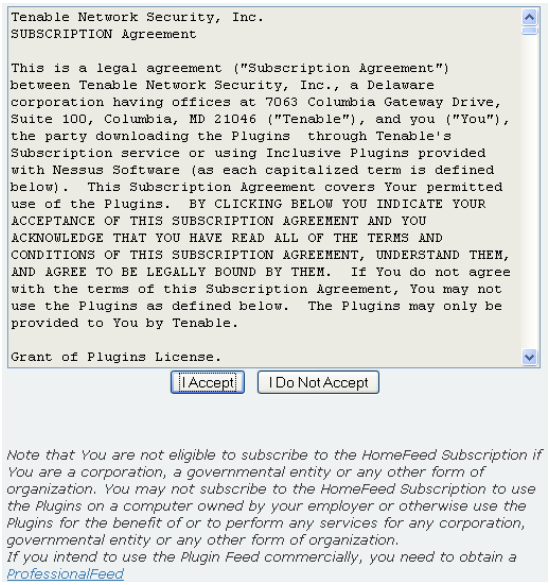

Figura AI.16 Licencia de NESSUS

5. A continuación escribimos una dirección de correo válida donde recibiremos la llave para usar el producto Figura AI.17

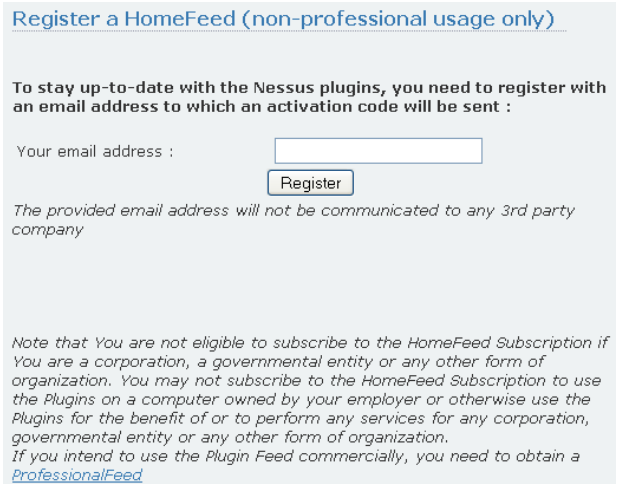

Figura AI.17 Registro de email para recibir clave de activación de NESSUS

6. Revisamos nuestra bandeja de entrada de nuestro correo y buscamos un mensaje con el encabezado "Nessus Plugin Feed" abrimos el correo y verificamos la clave adjunta en él Figura AI.18

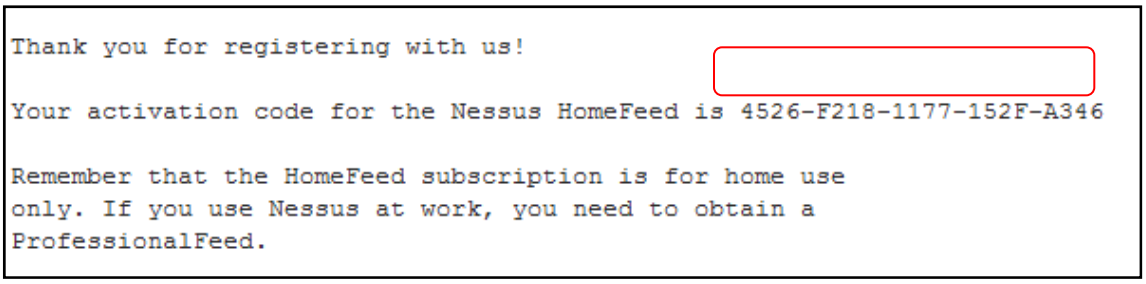

Figura AI.18 Clave de validación para NESSUS

7. Insertamos la clave y presionamos el botón Register para validar el producto. Después de ser activado iniciara la actualización de plug-ins de la aplicación, puede que tome varios minutos realizar la operación. Figura AI.19

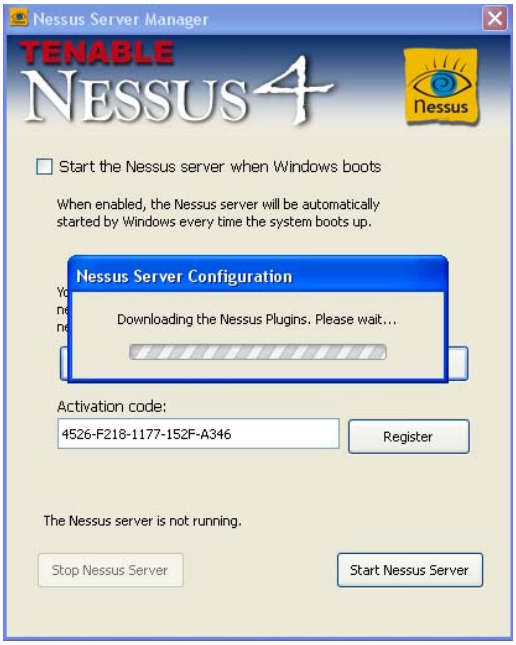

Figura AI.19 Registro de clave de NESSUS

8. Una vez que aparezca ésta pantalla podemos iniciar la práctica # 7 Figura AI.20

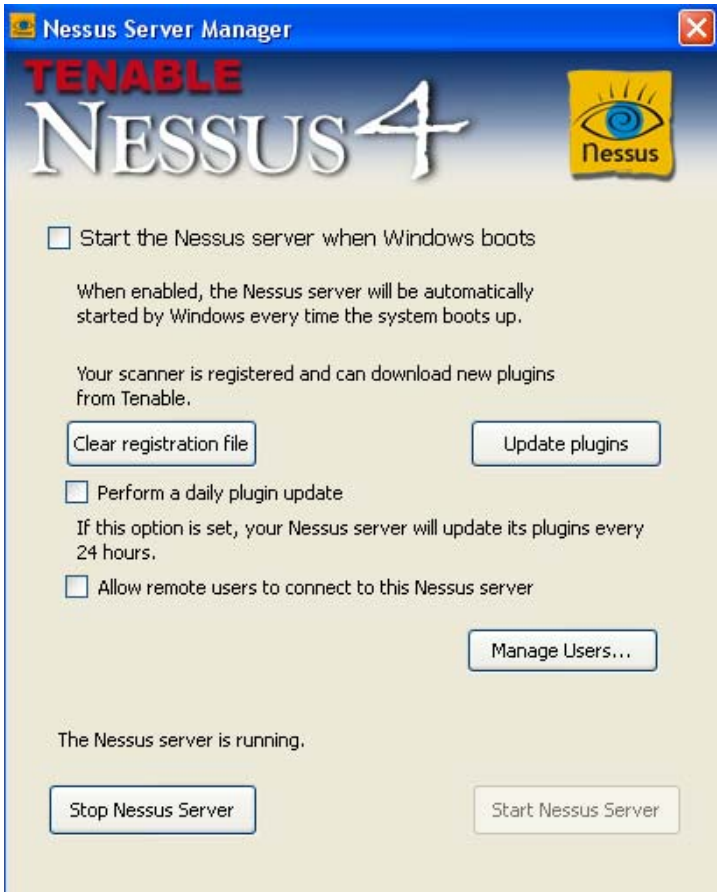

Figura AI.20 Panel de Control del servidor de NESSUS

Anexo II

Cuestionario Práctico

Cuestionario implementado para la obtención de datos estadísticos

Universidad Nacional Autónoma de México
Facultad de Ingeniería
División de Ingeniería Eléctrica

Cuestionario Estadístico

Condiciones de Uso

Se proveerá al participante material electrónico, impreso y digital para la consulta y realización de prácticas de seguridad informática. Algunos elementos tales como dispositivos físicos serán sujetos únicamente a préstamo durante la realización de determinadas prácticas, el uso de estos dispositivos estará sujeto a disponibilidad. Se brindará asesoría gratuita en caso de ser requerida.

Política de Privacidad

La recopilación de datos tales como: información personal y resultados obtenidos mediante el presente cuestionario solo serán con fines estadísticos y de mejora de las prácticas realizadas.

Acepto condiciones de uso y política de privacidad

_____
Nombre y Firma del Participante

Datos del Participante

Nombre del Alumno_____
Número de Cuenta_____ ¿Es Ud. pasante (si/no)?_____
Semestre Actual (aprox.)_____

Anexo II

Llena la siguiente tabla marcando con una x cada una de las preguntas:

Indica qué práctica(s) has realizado y ¿cuánto tiempo te ha llevado aproximadamente?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	45 min	1hr	1.25hr	1.5hr	1.75hr	2hr	2.5hr
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente contestar el cuestionario inicial?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente leer la introducción de la práctica?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									

7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente la toma de datos?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

¿Cuánto tiempo te ha llevado aproximadamente rellenar el informe y terminar el cuestionario final?

Número de la Práctica	Realizo		Tiempo Estimado de Realización						
	Si	No	T<5min	5min	10min	15min	20min	25min	T>25min
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

Selecciona una de las siguientes Opciones:

¿Por qué medio recibiste las prácticas?

1.-USB 2.-Email 3.-Prácticas impresas 4.-Otro

Anexo II

¿Cuál es tu principal fuente de información adiciona para realizar las prácticas de laboratorio de Seguridad Informática?

1. Soy pasante, tengo la información de otros años
2. En clase (apuntes, diapositivas, etc.)
3. Internet

¿Requeriste asesoría durante la realización de las prácticas?

1.-Si 2.-No

En tu opinión, ¿son útiles las actividades y prácticas en el laboratorio de Seguridad informática?

1.- Útiles 2.- Adecuadas 3.- Inútiles

¿Prefieres las prácticas virtuales o las de campo?

1.-Simulaciones 2.-De campo (con equipo físico)

¿Son útiles las prácticas para consolidar lo que se estudia en la teoría, o son complementarias?

1.- Refuerzan conocimiento 2.- Complementan

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando su consideración personal acerca de la información presentada en introducción.

1.- Suficiente 2.- Adecuada 3.-Deficiente

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando su consideración personal acerca del material empleado

1.- Suficiente 2.- Adecuada 3.- Deficiente

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando el nivel de dificultad de cada práctica

4 Muy difícil | 3 Difícil | 2 Normal | 1 Fácil

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Tomando en cuenta la siguiente escala llena la siguiente tabla indicando el nivel interés en las prácticas que hayas realizado

4 Muy interesante | 3 Interesante | 2 Poco Interesante | 1 Aburrido

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Índice de figuras y tablas

Listado indexado de figuras y tablas que aparecen en el presente trabajo

Índice de figuras

Tablas

Glosario

Definiciones de conceptos utilizados en el marco de la seguridad informática

802.11

802.11: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas (wireless). Permite la conexión de dispositivos móviles (laptop, PDA, teléfonos celulares a una red cableada, por medio de un Punto de Acceso (Access Point). La conexión se realiza a través de ondas de Radio Frecuencia. Originalmente ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz Se le conoce popularmente como WIFI. Tiene un área de cobertura aproximada de 100 ms.

802.11a: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz Utiliza la tecnología OFDM (Orthogonal Frecuency División Multiplexing. Esta banda de 5GHz no se pudo utilizar en muchos países, al comienzo, por estar asignada a las fuerzas y organismos de seguridad.

802.11b: Estándar de conexión wireless que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. Fue ratificado en 1999. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.

802.11g: Estándar de conexión wireless que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz Se basa en la tecnología OFDM, al igual que el estándar 802.11a. Fue ratificado en Junio de 2003. Una de sus ventajas es la compatibilidad con el estándar 802.11b.

802.11n: Estándar en elaboración desde Enero 2004. Tiene como objetivo conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps Hay 2 propuestas distintas. En 2006 se aprobará una de las dos. La de TGn Sync o la WWiSE.

• 802.16: Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz La interoperabilidad es certificada por el WIMAX FORUM

• 802.16d: Estándar de transmisión wireless (WIMAX*) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la “primer milla”.

• 802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

A

AAA: Abreviatura de autenticación, autorización y accounting, sistema de redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

Autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

Autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

Accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, billing, auditoría y cost allocation.

A menudo los servicios AAA requieren un servidor dedicado. RADIUS es un ejemplo de un servicio AAA.

ACCESS POINT (PUNTO DE ACCESO): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

ACCESO REMOTO (REMOTE ACCESS): Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

ACREDITACIÓN VOLUNTARIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (1): Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

ACTIVE-X: Los denominados controles Active-X son componentes adicionales que se pueden incorporar a las páginas web, para dotar a éstas de mayores funcionalidades (animaciones, video, navegación tridimensional, etc.). Escritos en un lenguaje de programación como Visual Basic, C o C++, que no es el propio de las páginas web (HTML) y podrían estar infectados con virus.

AD HOC: Una WLAN bajo una topología “Ad Hoc” consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones “Ad Hoc” son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal

ADWARE: Es una variante comercial del Spyware. Se trata de un pequeño trozo de código que tiene como finalidad recolectar datos a efectos de marketing. Es difícil distinguirlo del malware.

AES: Estándar de cifrado avanzado (Advanced Encryption Standar): También conocido como “Rijndael”, algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST).

AGUJERO (HOLE): Una vulnerabilidad en el diseño del software y/o hardware que permite engañar a las medidas de seguridad

ALIAS (ALIAS): Nombre diferente por el cual se conoce un virus.

ALGORITMO DE ENCRIPTACIÓN (ENCRIPTYON ALGORITHM): Codificaciones de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma / producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños.

AMPLIFICADOR (AMPLIFIER): Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido preamplificado y un amplificador lineal de salida de radio frecuencia (RF).

ANTENA (ANTENNA): Dispositivo generalmente metálico capáz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia qué punto se emita la señal podemos encontrar direccionales u omnidireccionales.

APPLIANCE SERVER: Servidores (dedicados a Internet sharing servicios FTP, e-mail, conexiones VPN, servicios de cortafuegos, de impresora y archivo y también operan como servidores web) que incorporan hardware y software en el mismo producto de modo que las aplicaciones se encuentran pre instaladas. El appliance está plug-in dentro de una red existente y puede comenzar a funcionar casi de inmediato con una mínima configuración y mantenimiento.

ANÁLISIS EURÍSTICO (HEURISTIC ANALIST): Se trata de un análisis adicional que solamente algunos programas anti-virus pueden realizar para detectar virus que hasta ese momento son desconocidos.

ANALIZADOR DE COMPORTAMIENTO (BEHAVIOR BLOCKER): Un programa anti-virus emplea una técnica para comprobar si un archivo incorpora los comportamientos habituales de un virus. Un Behavior blocker trabaja bajo un conjunto de reglas de funcionamiento que legitima programas bajo las reglas de comportamiento que siguen los virus. Además analiza y determina las tareas y comportamientos que han sido diseñadas para un archivo y averigua si el éste contiene algún virus.

ANCHO DE BANDA (BANDWIDTH): Este término define la cantidad de datos que pueden ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

ANTI-VIRUS: Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos

APPENDER (APPENDER): Es un virus que afecta una copia de su código al final del archivo de la víctima.

ARMOURING (ARMOURING): Mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de los virus, éstos son abiertos como archivos, utilizando programas especiales que permiten descubrir cada una de las líneas de su código. De un virus que utilice esta técnica no se podrá leer su código.

ATAQUE ACTIVO (ACTIVE ATTACK): Ataque al sistema para insertar información falsa o corromper la ya existente.

ATAQUES A PASSWORDS (PASSWORD ATTACK): Es un intento de obtener o descifrar un password legítima de usuario. Las medidas de seguridad contra estos ataques son muy limitadas, consistiendo en una política de passwords, que incluye una longitud mínima, palabras no reconocibles y cambios frecuentes.

ATAQUE DE DICCIONARIO (DICCIONARY ATTACK): Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente no se introducen manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.

ATAQUE DE FUERZA BRUTA (BRUTE FORCE ATTACK): Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

AUDITORÍA: Análisis de las condiciones de una instalación informática por un auditor extremo e independiente que realiza un dictamen sobre diferentes aspectos. Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

AUTENTIFICACIÓN (AUTHENTICATION): Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

AUTO – ENCRIPTACIÓN (AUTO – ENCRYPTION): Capacidad de algunos virus para esconderse de posibles programas anti-virus. Las soluciones anti-virus se encargan de encontrarlos buscando determinadas cadenas de caracteres (firma del virus), identificativas de cada una de ellos. Para evitar este mecanismo de búsqueda, algunos virus consiguen codificar o cifrar estas cadenas de texto de forma diferente en cada nueva infección. Esto supone que en la nueva infección, el anti-virus no encontrará la cadena que busca para detectar a un virus en concreto, pues éste la habrá modificado. No obstante, existen otros mecanismos alternativos para detectarlos.

AUTORIZACIÓN (AUTHORISATION): Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

B

BACKGROUND (BACKGROUND): Se dice que una aplicación funciona “en background” cuando está trabajando sin afectar la actividad del usuario.

BIOMÉTRICA (BIOMETRIC): Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc.…) para su aplicación a la seguridad informática como medio de identificación del usuario.

BLOWFISH: es un codificador simétrico de bloques. Toma una clave de longitud variable, entre 32 y 448 bits.

BRIDGE (PUENTE): elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

BOMBA DE E-MAIL (MAILBOMB): son mensajes de correo electrónico excesivamente largos enviados a la cuenta de correo de un usuario con el propósito de provocar la caída del sistema o evitar que los mensajes verdaderos sean recibidos.

BOMBA DE TIEMPO (TIME BOMB): Programa que se activa en una determinada hora.

BOMBA LÓGICA (LOGIC BOMB): programa que se ejecuta cuando existen condiciones específicas para su activación. Los suelen utilizar muchos virus como mecanismo de activación.

BOTS (BOTS): Término utilizado en Internet y que se deriva de la palabra “robot”. Con él se denomina a pequeños trozos de software que tienen la finalidad de actuar de manera independiente en un computador, como un “robot” controlado remotamente.

BUGTRAG: lista de correo de divulgación completa, moderada para la discusión detallada y anuncio de vulnerabilidades en seguridad informática; qué son, cómo explotarlas y cómo solucionarlas.

BÚSQUEDA EXAUSTIVA DE CLAVE (EXHAUSTIVE KEY SEARCH): Consiste en descubrir la clave empleada en un sistema de encriptación, probando todas las posibles.

C

CADENA (CHAIN): Una consecución de caracteres de texto, dígitos, números, signos de puntuación o espacios en blanco consecutivos. Alguna de las técnicas empleadas por los anti-virus para la detección de virus es buscar determinadas cadenas de texto (o código) que estos incluyen de manera frecuente.

CENTRINO: Tecnología móvil desarrollada por Intel compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada.

CHAP – CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL: Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafió al solicitante de la conexión, el cual responde a un valor hash que será comparado por el servidor con sus cálculos de valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario0 finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafió. Debido a que los identificadores cambian frecuentemente y por que la autenticación puede ser solicitada en cualquier momento.

CLIENTE INALÁMBRICO (WIRELESS CLIENT): Todo dispositivo susceptible de integrarse en una red wireless como PDAs, portátil, cámaras inalámbricas, impresoras, etc.…

CERTIFICADO DIGITAL (1) (CERTIDFICATE): Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del

emisor. Los Certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona.

CHEQUEADOR DE INTEGRIDAD (INTEGRITY CHECKER): Es un programa que determina si otro programa ha sido alterado. Para que una infección de virus ocurra, el código ejecutable necesita haber sido alterado por un virus. Un chequeador de integridad investiga tales cambios y los marca como sospechosos.

CHECKSUM CRIPTOGRÁFICO (CRYPOGRAPHIC CHECKSUM): Checksum calculado mediante la utilización de un algoritmo como base criptográfica. Es imposible cambiar unos datos sin que el checksum criptográfico cambie.

CHECSUMMER: Herramienta que calcula un único número asociado a determinados archivos que habitualmente no cambia para protegerlos. Checksummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección.

CLAVE DE ENCRIPTACIÓN (ENCRYPTION KEY): Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

CLAVE DE REGISTRO (REGISTRY KEY): El registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiarán de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.

CODIFICADOR OR BLOQUES (BLOCK CIPHER): Ciencia que estudia las características biológicas del ser humano (el iris, huella dactilar, la voz, etc.…) para su aplicación a la seguridad informática como medio de identificación del usuario.

COMPSEC: Abreviatura de COMPuter SECurity (Seguridad Informática).

CONFIDENCIALIDAD (CONFIDENTIALITY): Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

CONTROL DE ACCESOS (ACCESS CONTROL): Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc.,… El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de usuario y password, certificados del cliente, protocolos de seguridad de redes, etc.

COPIA DE SEGURIDAD (BACKUP): Es una copia de todos los datos originales contenidos en redes y PC’s que puede ser usado en caso de que estos se destruyan por diversas causas.

CORTAFUEGOS (FIREWALL): Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.…

CRACKER: Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

CRIPTOANÁLISIS (CRYPTANALYSIS): Estudio de un sistema de encriptación con la intención de detectar cualquier punto débil dentro de su algoritmo clave.

CRIPTOLOGÍA (CRYPTOLOGY): Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.

CRON (UNIX): En el sistema operativo Unix, cron es un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero crontab.

CROSSTALK (RUIDO, INTERFERENCIA): Ruido o interferencia que fluye entre los cables de comunicación o dispositivos.

D

DELITO INFORMÁTICO (COMPUTER CRIME): Delito cometido utilizando una PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

DENEGACIÓN DE SERVICIOS (Denial of Service) (DoS): O ataque DoS. Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES: algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmos DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

DESBORDAMIENTO DE BÚFFER (BUFFER OVERFLOW): Error de software que se produce cuando se copia una cantidad más grande de datos sobre un área más pequeña sin interrumpir la operación sobre-escribiendo otras zonas de datos no previstas. En algunas ocasiones eso puede suponer la posibilidad de alterar el flujo del programa pudiendo hacer que este realice operaciones no previstas. Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte además en un fallo de seguridad. El código copiado especialmente reparado para obtener los privilegios del programa atacado se llama shellcode.

DESENCRIPTAR (DESCRYPTION): Proceso de transformación en cyphertext – texto encriptado o cifrado – a plaintext (Es la acción inversa de encriptar).

DESINFECCIÓN (DISINFECTION): Acción que realizan los programas anti-virus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan o restauran la información infectada.

DHA (DIRECTORY HARVEST ATTACK): Llamado el "Asesino Silencioso". Este ataque consiste en el envío masivo de emails a un dominio determinado con el fin de "cosechar" y recolectar direcciones válidas de emails, para ser incorporadas a las listas de spam.

RELLAMADA (DIALBACK): Rasgo de seguridad que asegura que las personas sin autorización no conecten con módems a los que no deben tener acceso. Cuando se pide una conexión, el sistema verifica el nombre del usuario para validarlo, e inicia una re llamada al número asociado con ese nombre de usuario.

DIALER: Programa que permite cambiar el número de acceso telefónico automáticamente de acuerdo a la situación geográfica del usuario. Estos códigos (que se descargan de sites a veces sin darnos cuenta) toman el control sólo de la conexión telefónica vía módem, desviando las llamadas normales que efectúas a través de tu proveedor hacia una número del tipo 908, 906, etc.…, números de tarifa especial y bastante cara por lo general. Últimamente se han detectado un aumento de incidentes relativos a “dialers porno” que permiten visualizar páginas pornográficas de forma gratuita pero que sin embargo se pagan cuando llega la escandalosa factura telefónica.

DISPOSITIVO MOVIL (MOBILE DEVICE): Ya sea una tarjeta PCMIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red. Su función es la de recibir/enviar información desde la estación en que están instaladas (portatileslaptops, netbooks, PDAs, móviles, cámaras, impresoras)

DSSS- ESPECTRO AMPLIO MEDIANTE SECUENCIA DIRECTA (DIRECT SEQUENCE SPREAD SPECTRUM): A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos. Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b

DISPOSITIVO DE CREACIÓN DE FIRMA ELECTRÓNICA (1): Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma (electrónica).

DISPOSITIVO DE VERIFICACIÓN DE FIRMA ELECTRÓNICA (1): Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma (electrónica).

DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA ELECTRÓNICA (1): Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

DONGLE: Hardware de seguridad que se debe conectar al sistema informático antes de que se ejecute una determinada aplicación; previene las copias ilegales de los programas informáticos.

DROPPER: Usado como portador de virus, un dropper es un programa ejecutable que instala el virus en memoria, en el disco o en un archivo (aunque un dropper por sí mismo no tiene capacidades de infección ni de replicación).

E

EAP – PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE (EAP – EXTENSIBLE AUTHENTICATION PROTOCOL): Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por

clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

ECHELON: Sistema internacional de interceptación mediante satélites de las telecomunicaciones iniciado como proyecto en 1947 e implementado en 1960. Desde su nacimiento en plena Guerra Fría ha evolucionando con los tiempos incluyendo actualmente actividades de espionaje industrial. Su dirección está al cargo de la NSA (National Security Agency, Estados Unidos) y de la GCHQ (Government Communications Headquarters, Gran Bretaña) aunque también tiene estaciones de control en Australia, Canadá y Nueva Zelanda.

ENCRIPTACIÓN (ENCRYPTION): Proceso para transformar la información escrita en plaintext a ciphertext.

ENCRIPTACIÓN ASIMÉTRICA (ASYMMETRIC ENCRYPTION): Encriptación que permite que la clave utilizada para encriptar sea diferente a la utilizada para desencriptar. El algoritmo de encriptación asimétrico más difundido es RSA.

ENCRIPTACIÓN DE ARCHIVOS (FILE ENCRYPTION): transformación de los contenidos plaintext de un archivo (texto sin cifrar) a un formato ininteligible mediante algún sistema de encriptación.

EN EL TERRENO (IN THE WILD): Clasificación utilizada por la organización Wildlist que recoge todos aquellos virus sobre los que más de una persona ha notificado alguna incidencia.

EN EL ZOO (IN THE ZOO): Describe un virus que únicamente existe dentro de un entorno de investigación.

ENGAÑO (HOAX): No se trata de virus, sino de falsos mensajes de alarma (bromas o engaños) sobre virus que no existen. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes. En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. , mensajes que simulan a los reales, alertas de nuevos virus, anuncios de nuevas soluciones, cadena de correos a reenviar,…, etc. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa (CBS…) en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.

ESCÁNER (SCANNER): Programa que busca virus en la memoria del PC o en los archivos.

ESCÁNER BAJO DEMANDA (SCANNER ON DEMAND): Programa escáner antivirus que el usuario ejecuta manualmente cuando lo estima conveniente.

ESCÁNER HEURÍSTICO (HEURISTIC SCANNER): Programa escáner antivirus que busca virus nuevos y desconocidos.

ESCÁNER RESIDENTE (RESIDENT SCANNER): Programa escáner antivirus que está buscando virus recursivamente en background.

ESTÁNDAR (STANDAR): Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.…

ETHERNET: Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

EXCEPCIONES (EXCEPTIONS): Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso, lo que el programa anti-virus puede chequear es el cambio en las cadenas (excepciones).

EXPLOTAR (EXPLOIT): Método de utilizar un bug o fallo para penetrar en un sistema.

F

FALLO (BUG): O error en un programa. Cuando uno de ellos tiene errores, se dice que tiene Bugs. Como los virus son programas, también pueden contener bugs. Esto implicaría que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

FALSO NEGATIVO (FALSE NEGATIVE): Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.

FALSO POSITIVO (FALSE POSITIVE): Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio.

FAST – FLEXIBLE AUTHENTICATION SECURE TUNNELING : Protocolo de seguridad WLAN del tipo EAP. Desarrollado por Cisco y presentado a la IETF como borrador a principios de 2004. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

FHSS – ESPECTRO AMPLIO MEDIANTE SALTOS DE FRECUENCIA (FHSS – FREQUENCY HOPPING SPREAD SPECTRUM): Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar a cabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este “Hopping Pattern”. El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.

FICHERO (FILE): Todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

FILTRADO (FILTERING): Proceso mediante el cual un puente o conmutador Ethernet lee el contenido del paquete y descubre que éste no necesita volver a ser enviado, por lo que lo desprecia. La velocidad de filtrado es la velocidad a la que un dispositivo puede recibir paquetes y desecharlos sin ninguna pérdida de paquetes entrantes o demoras en su procesado.

FILTROS ANTI-SPAM (ANTI-SPAM FILTERS): Son herramientas para filtrar el spam o correo basura no solicitado en los programas de correo.

FIRMA ELECTRÓNICA O FIRMA DIGITAL (DIGITAL SIGNATURE): El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.

FIRMA ELECTRÓNICA AVANZADA (ADVANCED DIGITAL SIGNATURE) : Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

FIRMWARE: Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es una combinación de software y hardware. ROMs, PROMs e EPROMs que tienen datos o programas grabados dentro son firmware.

ENTRAMADO (FRAMING): División de datos para su transmisión en grupos de bits a los que se les añade una cabecera y un código de verificación para formar una trama.

FTP – PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP – FILE TRANSFER PROTOCOL) : Protocolo de transferencia de archivos que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

G

GALLETA (COOKIE): Rastro que el servidor de un sitio web deja en nuestro PC cuando lo visitamos por primera vez; cada vez que volvemos a dicho sitio, la señal se actualiza, dando información al servidor de nuestro paso por la página. Con estas señales, los servidores pueden saber por dónde navegamos, cuáles son nuestros intereses, etc.…

GATEWAY (PASARELA/PUERTA): Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

GPS – SISTEMA DE POSICIONAMIENTO GLOBAL (GPS – GLOBAL POSITION SYSTEM): Sistema de navegación por satélite con cobertura global y continua que ofrece de forma rápida y temporalmente bastante precisa una posición geográfica de un elemento. El primer satélite para esta técnica de seguimiento se lanzó en

1978, pero sin embargo el sistema no estuvo operativo hasta 1992 y fue desarrollado por las fuerzas aéreas de los EE.UU.

GESTIÓN DE CLAVES (KEY MANAGEMENT): Proceso para generar, transportar, almacenar y destruir claves de encriptación de modo seguro.

GNU: Es un acrónimo recursivo que significa **GNU No es Unix** (*GNU is Not Unix*). Puesto que en inglés "*gnu*" (en español "ñu") se pronuncia igual que "*new*", Richard Stallman recomienda pronunciarlo "*guh-noo*". En español, se recomienda pronunciarlo ñu como el antílope africano o fonéticamente;[2] por ello, el término mayoritariamente se deletrea (G-N-U) para su mejor comprensión. En sus charlas Richard Stallman finalmente dice siempre «Se puede pronunciar de cualquier forma, la única pronunciación errónea es decirle 'linux'».

GPL: Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Inglés como copyleft -'copia permitida'- (en clara oposición a copyright -'derecho de copia'-), y está contenida en la Licencia General Pública de GNU

H

HACKER: Persona que accede a un sistema informático sin autorización para “cotillear”, ver su funcionamiento interno y explotar vulnerabilidades. Este término se suele utilizar indistintamente con el término cracker (intruso), pero supuestamente hacker no implica necesariamente malas intenciones, mientras que cracker sí.

HASH: Un valor hash, también conocido como “message digest”, es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

HONEYPOTS (TARROS DE MIEL EN CASTELLANO): Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del “pirata” con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc.

HOTSPOT (PUNTO CALIENTE): Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc.…) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

I

IRC WORMS (GUSANOS DE INTERNET RELAY CHAT): Infectan solamente a usuarios del software MIRC para acceder a los canales IRC (Internet Relay Chat). El gusano se aprovecha de cualquier desperfecto en el diseño de seguridad del software mIRC PARA sobre-escribir el archivo Script omitido (Script.ini) cuando los archivos son transferidos utilizando el protocolo DCC.

IEEE – INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS (- INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS)
Formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo (http://www.ieee.org).

IETF – THE INTERNET ENGINEERING TASK FORCE: Grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet (http://www.ietf.org).

INFRAESTRUCTURA (INFRAESTRUCTURE): Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso

IPSEC – IP SECURITY: Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

INFECCIÓN (INFECTION): Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.

INTEGRIDAD DE ARCHIVOS: Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

ISO 17999: Estándar para la gestión de la seguridad de la información.

L

LAN – RED DE ÁREA LOCAL (LOCAL AREA NETWORK): Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)… Sus características son: Topología en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

LDAP – Protocolo de Acceso Ligero a Directorio (Lightweight Directory Access Protocol): Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más

simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

LEAP – LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL: Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

M

MAC – DIRECCIÓN DE CONTROL DE ACCESO A MEDIOS (MEDIA ACCESS CONTROL ADDRESS): Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexadecimal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

MALWARE (CÓDIGO MALICIOSO): Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

MBPS (MEGABITS POR SEGUNDO): Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

MD5: Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, EL PRIMERO SE ENVÍA sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

MHZ (MEGAHERTZIO): Unidad empleada para medir la “velocidad bruta” de los microprocesadores equivalente a un millón de hertzios.

MS-CHAP – PROTOCOLO DE AUTENTICACIÓN POR DESAFÍO MUTUO (MS-CHAP – CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL): Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto. Microsoft ha creado una variante de CHAP específica de Windows denominada MS-CHAP. Challenge Handshake Authentication Protocol se llama también CHAP.

N

NCSC – CENTRO NACIONAL DE SEGURIDAD INFORMÁTICA (NATIONAL COMPUTER SECURITY CENTER): Institución de EEUU responsable de fomentar el desarrollo de sistemas informáticos seguros y de su implantación en las oficinas del gobierno para la clasificación de la información.

O

OFDM – ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING: Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

P

PAP – PROTOCOLO DE AUTENTICACIÓN DE CLAVES (PASSWORD AUTHENTICATION PROTOCOL): El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.

PAYLOAD: Efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows,…).

PEAP – PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL: Protocolo del tipo EAP desarrollado conjuntamente por Microsoft, RSA Security y Cisco para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS encriptado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

PHISHING: Técnica en auge que consiste en atraer mediante engaños a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc.… Uno de los métodos más comunes para hacer llegar a la “víctima” a la página falsa es a través de un e-mail que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que el “phiser” ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.
Una de las consecuencias más peligrosas de este fraude es que la barra “falsa” queda en memoria aún después de salir de la misma pudiendo hacer un seguimiento de todos los sitios que visitamos posteriormente y también el atacante puede observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.
Una manera para el usuario de descubrir el engaño es que no se muestra la imagen del candado en la parte inferior del navegador que indica que la navegación es segura.

PIN – PERSONAL IDENTIFIER NUMBER (NÚMERO DE IDENTIFICACIÓN PERSONAL): Número generalmente de 4 dígitos que actúa como contraseña de acceso para el uso de una diversidad de servicios: cajeros automáticos, conexión de teléfono móvil, etc..

PKI – INFRAESTRUCTURA DE CLAVE PÚBLICA (PUBLIC KEY INFRASTRUCTURE): Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet. Los estándares de PKI siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. La infraestructura de claves públicas se llama también PKI.

POLIMORFISMO (POLYMORPHISM): Característica que presentan algunos virus consisten en que su código no siga un patrón fijo de caracteres de modo que es muy difícil detectarlo.

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (CERTIFICATE SERVICE PROVIDER): Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

PROCEDIMIENTO DE DISOCIACIÓN: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

PRODUCTO DE FIRMA ELECTRÓNICA (PRODUCT OF DIGITAL SIGNATURE): Es un programa o aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

PROTECCIÓN CONTRA COPIADO (COPY PROTECTION): Método para impedir hacer copias de programas de software. Es una forma de evitar el robo de aplicaciones informáticas.

PROTECCIÓN DE DATOS (DATA PROTECTION): Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

PROTOCOLO (PROTOCOL): Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

PUERTA TRASERA (BACKDOOR): No se trata de un virus, sino de una herramienta de administración remota. Si es instalada por un hacker tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar passwords y datos confidenciales y enviarlos vía mail a un área remota.

R

RADIUS – REMOTE AUTHENTICATION DIAL-IN USER SERVICE: Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISP's) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y

contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAS – SERVIDOR DE ACCESO REMOTO (REMOTE ACCESS SERVER): Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

ROUTER: Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LAN's o WAN's o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.

ITINERANCIA (ROAMING): En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

S

SECTOR DE ARRANQUE (BOOT SECTOR): Todo disco tiene un sector de arranque que el PC lee cuando se enciende. Este sector contiene todos los códigos necesarios para cargar los archivos de sistema DOS.

SECTOR DE PARTICIÓN (PARTITION SECTOR): Todo disco duro o disquete tiene un sector de partición que es leído después de que se ha arrancado el PC. Contiene datos sobre el disco tales como el número de sectores de cada partición y la ubicación de las particiones.

SECTORES DEFECTUOSOS (BAD SECTORS): Aquellos que, tras formatear el disco duro en MS-DOS, se revelan inutilizables. Algunos virus tienen la capacidad de renombrar sectores útiles como “defectuosos” para almacenar en ellos su código, de modo que el usuario y el sistema operativo no accedan a él y garantizando así la infección del PC.

SERVIDOR DE AUTENTICACIÓN (AUTHENTICATION SERVER): Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.

SHELLCODE: En términos underground, shellcode son una serie de órdenes de ensamblador que, beneficiándose de fallos informáticos, que ejecutan un código después de sobrescribir la dirección de retorno (ret) de un programa o función mediante un desbordamiento (overflow) u otro método válido. Si el atacante consigue insertar su shellcode sobre el ret, cuando se produzca el desbordamiento y el salto, se ejecutará sus órdenes.

SIGNATARIO (SIGNATORY): Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

SISTEMA DE ENCRIPTACIÓN (CRYPTOSYSTEM): Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para encriptar.

SOBREPASAMIENTO (TUNNELING): Técnica diseñada para impedir que las aplicaciones anti-virus trabajen correctamente.

SPYWARE (SPYWARE): Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se dé cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

STEALTH: Característica que tienen los virus para pasar inadvertidos ante el usuario al que infectan.

TARJETA INTELIGENTE (SMART CARD): Pequeño dispositivo electrónico del tamaño de una tarjeta de crédito que contiene memoria digital y posiblemente un circuito integrado, llamándose entonces Integrated Circuit Cards (ICCs). Sus usos son variados: para almacenar historiales médicos, como monedero digital, para generar IDs (similar a un Token). Para utilizarla, y bien capturar los datos en ella almacenada o bien añadirlos, es necesario un pequeño lector especial para estos dispositivos.
SNIFFER: Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras…

SPAM: También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

SPOOFING: Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Otros ataques de falseamiento conocidos son:
• DNS Spoofing: En este caso se falsea una dirección IP ante una consulta de resolución de nombre (DNS) o viceversa, resolver con un nombre falso una cierta dirección IP.
• ARP Spoofing: Hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que un determinado equipo de una red local envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
• Web Spoofing: El pirata puede visualizar y modificar una página web (incluso conexiones seguras SSL) solicitada por la víctima.
• E.mail Spoofing: Falsifica la cabecera de un e-mail para que parezca que proviene de un remitente legítimo. El principal protocolo de envío de e-mails, SMTP, no incluye opciones de autenticación, si bien existe una extensión (RFC 2554) que permite a un cliente SMTP negociar un nivel de seguridad con el servidor de correo.

SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SSL – SECURE SOCKETS LAYER : Aprobado como estándar por el Internet Engineering Task Force (IETF), es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL. Los navegadores Netscape y Explorer soportan SSL, y muchas páginas web emplean el protocolo para obtener información confidencial del usuario, como números de tarjeta de crédito, etc. Por convención, las URLs que precisen una conexión SSL comienzan con https, en lugar de http.

T

TARJETA DE RED INALÁMBRICA: Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: Compact Flash, PCI, PCMCIA, USB

TEXTO CODIFICADO (CIPHERTEXT): Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo.

TEXTO SIMPLE (PLAINTEXT): Se dice que un texto está escrito en plaintext cuando puede ser leído sin tener que realizar ninguna operación, es decir, no está codificado.

TKIP – PROTOCOLO DE INTEGRIDAD DE CLAVE TEMPORAL (TEMPORAL KEY INTEGRITY PROTOCOL): Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS – TRANSPORT LAYER SECURITY: Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS – situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el

TOKEN: En lenguaje de programación un elemento simple de un elemento de programación. Por ejemplo un token podría ser una palabra clave, un operador una marca de puntuación.
En redes, un token es una serie especial de bits que viajan a través de una red token-ring y a los cuales tiene acceso cualquier equipo perteneciente a esa red. El token actúa como un ticket, permitiendo a su propietario enviar un mensaje a través de la red. Existe sólo un token para cada red de modo que no sea posible que dos equipos intenten transmitir mensajes al mismo tiempo.
En sistemas de seguridad, un pequeño dispositivo del tamaño de una tarjeta de crédito que muestra un código ID que cambia constantemente (cada x minutos). El usuario primero introduce una clave y luego la tarjeta muestra un ID que puede ser utilizado para acceder a la red. Un mecanismo similar de generación de IDs son las smart card.

TRATAMIENTO DE DATOS(2): Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

TROYANO (TROJAN): Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

TTLS – TUNNELES TRANSPORT LAYER SECURITY: Protocolo de seguridad para redes inalámbricas del tipo EAP propiedad de la multinacional norteamericana Funk Software. Se trata de una extensión de EAP-TLS, protocolo utilizado por Windows XP en sistemas inalámbricos que proporciona los servicios de autenticación entre los usuarios y el servidor de la red basados en certificados. EAP-TTLS sólo requiere certificados al servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red

inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y encripta credenciales y password para garantizar la protección de la comunicación inalámbrica.

V

VARIANTE DE UN VIRUS: Se conoce como variante de un virus ya existente a otro virus básicamente igual al primero pero con algún pequeño cambio en su programación.

VIRUS: Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

VIRUS DE ARCHIVO: Virus que infecta los archivos ejecutables de los programas. Al abrir un programa infectado, primero se ejecuta el virus y luego se abre la aplicación. Cuando se ejecuta el virus se copia a sí mismo en otros archivos o en otro disco.

VIRUS DE COMPAÑÍA : Virus que crea un archivo para esconderse cuyo nombre es igual al de otro de extensión .EXE de algún programa legítimo y con extensión .COM. MS-DOS siempre lee primero los archivos con la extensión .COM, antes que los de extensión .EXE.

VIRUS DE INGENIERÍA SOCIAL (SOCIAL ENGINEERING): Este término es utilizado frecuentemente para describir los trucos utilizados por los virus de correo masivo para atraer a los receptores de los mensajes con archivos adjuntos infectados para ejecutarlos o visualizarlos.

VIRUS DE MACRO (MACRO VIRUS): Virus que infecta las macros de Word y Excel, principalmente, de modo que cuando se abre un archivo que tenga una macro infectada, infectará el sistema.

VIRUS DE SECTOR DE ARRANQUE Y DE PARTICIÓN (BOOT AND PARTITION SECTOR VIRUS): Los virus de esta categoría infectan el sector de arranque y sector de partición. La mayoría de las PCs están configurados para intentar arrancar de la unidad a: antes que del disco duro, por lo que si se ha introducido un disquete infectado en la disquetera en el momento de arrancar, el PC se infectará.

VIRUS DE SCRIPT (SCRIPT VIRUS): Estos virus son escritos en lenguajes de programación script, tales como Visual Basic Script o Java Script.

VIRUS DE SOBRE-ESCRITURA (OVERWRITTING VIRUS): Virus que sobrescribe cada archivo que infecta: el programa maligno copia su propio código sobre el archivo de modo que los programas dejan de funcionar. Aunque la desinfección es viable, no es posible recuperar la información de los archivos infectados.

VIRUS MULTIPARTITO (MULTIPARTITE VIRUS): Virus que utiliza una combinación de técnicas para expandirse infectando archivos ejecutables, de sector boot y de partición

VIRUS RESIDENTE EN MEMORIA (MEMORY-RESIDENT VIRUS): Virus que permanece en memoria después de que ha sido ejecutado e infecta otros objetos bajo determinadas circunstancias.

VLAN – RED DE ÁREA LOCAL VIRTUAL (VIRTUAL LOCAL AREA NETWORK): Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares

VPN – RED PRIVADA VIRTUAL (VPN – VIRTUAL PRIVATE NETWORK): Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

W

WPA – PROTOCOLO DE SEGURIDAD EN REDES INALÁMBRICAS (WIRELESS PROTECTED ACCESS): Protocolo de Seguridad para redes inalámbricas.
Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i.

WPA2 – PROTOCOLO DE SEGURIDAD WIFI PARA REDES INALÁMBRICAS (WIRELESS PROTECTED ACCESS): Protocolo de seguridad para redes wi-fi, definido en el estándar 802.11i.
Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.

WARCHALKING – ATAQUE A REDES INALÁMBRICAS: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.
Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

WARDRIVING – ATAQUE A REDES INALÁMBRICAS: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless.
Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.…

WARSPAMMING: Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

WI-FI(ALIANZA): Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado.

WEP – WIRED EQUIVALENT PRIVACY: Protocolo para la transmisión de datos “segura”.
La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red.

También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WI-FI – TECNOLOGÍA UTILIZADA EN REDES INALAMBRICAS: Abreviatura de Wireless Fidelity. Es el nombre “comercial” con el que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

WIMAX: Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

WLAN – RED DE ÁREA LOCAL INALÁMBRICA (WIRELESS LOCAL AREA NETWORK): También conocida como red wireless.
Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado.
Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA – ACCESO WI-FI PROTEGIDO (WI-FI PROTECTED ACCESS): Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WWWD – THE WORLDWIDE WARDRIVE: Evento internacional que durante una semana reúne a expertos de todo el mundo que buscan y catalogan nodos inalámbricos en sus ámbitos geográficos.