UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS
VERITATE SOLA NOBIS IMPONETUR VIRILIS TOGA. 1948

FACULTAD DE INGENIERÍA ELÉCTRICA

Departamento de Electrónica y Telecomunicaciones

TRABAJO DE DIPLOMA

Propuesta de un Procedimiento para la Realización de Pruebas de Seguridad a la Intranet de la UCLV.

Autor: Yudermys Morales Oramas

Tutor: Msc. Ramón Torres Rojas

Santa Clara

Curso 2006 – 2007

"Año 49 de la Revolución"

Universidad Central "Marta Abreu" de Las Villas
Facultad de Ingeniería Eléctrica
Departamento de Telecomunicaciones y Electrónica

Propuesta de un Procedimiento para la Realización de Pruebas de Seguridad a la Intranet de la UCLV.

TRABAJO DE DIPLOMA

Autor: *Yudermys Morales Oramas.*

Tutor: *Msc. Ramón Torres Rojas*.

Santa Clara
2007
"Año del 49 de la revolución"

Hago constar que el presente trabajo fue realizado en la Universidad Central “Marta Abreu” de las Villas como parte de la culminación de los estudios de la especialidad de Telecomunicaciones y Electrónica autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____
Firma del Autor

Los abajo firmantes, certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____
Firma del Tutor

_____
Firma del Jefe de Dpto.
Donde se defiende el trabajo

_____
Firma del Responsable de
Información Científico-Técnica

Pensamiento

Todos somos muy ignorantes. Lo que ocurre es que no todos ignoramos las mismas cosas.

Albert Einstein.

Dedicatoria

A mis padres, por su amor y comprensión, por guiarme siempre, por confiar en mí y por ser las personas que más quiero en el mundo.

A mi querida hermana, por lo mucho que la quiero.

A mi hermosa y única sobrina.

A mi pareja por acompañarme en todos estos momentos vividos.

A mis vecinos mas cercanos que siempre me tienen tan presente.

A mi familia toda.

A mi tutor Ramón, por estar siempre a mi lado, por su apoyo y dedicación.

A mi gran amigo Iván, por estar siempre ahí en los buenos y malos momentos y por tanto y tanto tiempo juntos.

A mis grandes amigas Nayibis, Maria de Lourdes, Irina, Csillag, Idileisy, Nerlyn y Rieni.

A mis amigas de grandes dificultades Juani y Maribel por su afecto y comprensión.

A mis amigas de secretaria por alegrarme la mayor parte de mis días.

A Amed por su espontaneidad y sabiduría.

A Osmany por toda ayuda prestada en esta recta final.

A mis amigos Yasiel, Yandy, Bullón, Darien, Yurky, Leo, Yanet, a los Ernesto, Ailicet, Sandor, Negruma, Ahmad, Fouad, Oscar, Saedy y en sentido general a todos mis compañeros de aula por haberme hecho sentir tan especial ,por ayudarme en todo lo que necesite y especialmente por todos los momentos que juntos compartimos.

A Hirám de Castillo, por su enseñanza y la genialidad de sus clases.

Al Cap. Ernesto por su preocupación constante

A Mario, por haberme guiado.

A Maria Esperanza, por sus consejos.

A Sarita, por su delicadeza y su entrega en clases.

A Taboada, por su conocimiento.

A todos mis profesores, por contribuir con mi formación.

A todas aquellas personas que de una forma u otra tuvieron que ver con mi vida durante estos cinco años.

A todos, Gracias.

A mis padres y familiares, con todo el cariño del mundo.

Tareas técnicas

- Realizar un estudio comparativo de las diferentes metodologías de seguridad existentes hasta el momento.
- Caracterizar las principales metodologías en cuanto a radio de acción, evaluación de riesgos y otros caracteres.
- Proponer una serie de procedimientos metodológicos que se adecue a la red de la UCLV.
- Evaluar los resultados parciales de los procedimientos propuestos anteriormente.

Resumen

Resumen:

Las redes de comunicaciones han experimentado un desarrollo vertiginoso en los últimos años, sin embargo continúan enfrentando el factor seguridad informática que puede afectar su eficiente aprovechamiento. Entre las alternativas existentes para hacerle frente a este problema, se han destacado los llamados Diagnósticos de Red. Esta Técnica es bastante nueva, sobre todo en el entorno informático cubano y específicamente en la red de la universidad “Marta Abreu de las Villas”.

En las redes de computadoras es importante el volumen de información confidencial que se maneja, el cual es necesario proteger a los ojos de intrusos, las perdidas económicas por concepto de la revelación de esta información confidencial pueden ser numerosas y a partir de este hecho las empresas dedicarán más o menos recursos en implementar una red segura.

Las auditorias de seguridad se han convertido en una herramienta muy importante para evaluar la seguridad de los sistemas en explotación., dando además información concisa de fallas y vulnerabilidades de los sistemas que pueden ser corregidos y de esta forma mejorar los niveles de seguridad ofrecidos y garantizar la estabilidad de los servicios en explotación.

Por este emotivo es que este trabajo, a través de un estudio de las principales metodologías existentes en el mundo, las herramientas de seguridad y las arquitecturas atípicas de las redes de datos internas de la red de la universidad, propone una serie de procedimientos a seguir que ayude a los especialistas novatos y a los más expertos a obtener resultados eficientes y confiables a la hora de realizar diagnósticos de seguridad a las redes, los servicios y las aplicaciones.

Índice

Índice

Propuesta de un Procedimiento para la Realización de Pruebas de Seguridad a la Intranet de la UCLV. 1
Introducción 1
Capítulo 1: Estado y desarrollo de los sistemas de auditoría de seguridad 4
1.1 Introducción 4
1.2 Actualidad de la Seguridad informática 5
1.3 Amenazas de los sistemas informáticos 5
1.3.1 Amenazas más comunes 6
1.3.2 Protección contra las principales amenazas 7
1.4 Seguridad de la información 8
1.5 Pruebas de seguridad 8
1.5.1 Clasificación de las Pruebas de Seguiridad 9
1.6 Prueba de penetración 10
1.6.1 Implementación de las Pruebas de Seguridad 12
1.6.2 Alcance de las Pruebas de Seguridad 13
1.6.3 Análisis de Costo 14
1.6.4 Resultados de la Prueba de Penetración 16
1.7 Metodologías para las Pruebas de Seguridad 16
1.7.1 Normas para Auditorias en Sistemas de Información 17
1.7.2 Proyecto Abierto de Seguridad de Aplicaciones Web 21
1.7.3 Sistema de Información para asentar una red de Trabajo 22
1.7.4 Manual de la Metodología Abierta de Testeo de Seguridad 23
1.8 Caracterización general 24
Capitulo 2: Diseño de los Procedimientos para la Realización de Pruebas de Seguridad a la Intranet de la UCLV 26
2.1 Mapa de Seguridad ..... **¡Error! Marcador no definido.**
2.1.1 Módulos del Mapa de Seguridad ..... **¡Error! Marcador no definido.**
2.2 Metodología ..... **¡Error! Marcador no definido.**
2.3 Seguridad de la información ..... **¡Error! Marcador no definido.**
2.3.1 Revisión de la Inteligencia Competitiva ..... **¡Error! Marcador no definido.**
2.3.2 Revisión de Privacidad ..... **¡Error! Marcador no definido.**
2.3.3 Recolección de Documentos ..... **¡Error! Marcador no definido.**
2.4 Seguridad de los procesos ..... **¡Error! Marcador no definido.**
2.4.1 Prueba de Solicitud ..... **¡Error! Marcador no definido.**
2.4.2 Prueba de Sugerencia Dirigida 33
2.4.3 Prueba de las Personas Confiables ..... **¡Error! Marcador no definido.**
2.5 Seguridad en las tecnologías de Internet ..... **¡Error! Marcador no definido.**
2.5.1 Logística y Controles ..... **¡Error! Marcador no definido.**
2.5.2 Sondeo de Red 35

2.5.3 Identificación de los Servicios de Sistemas ..... **¡Error! Marcador no definido.**
2.5.4 Revisión de Privacidad..... **¡Error! Marcador no definido.**
2.5.5 Búsqueda y Verificación de Vulnerabilidades.... **¡Error! Marcador no definido.**
2.5.6 Prueba de Aplicaciones de Internet..... 43
2.5.7 Enrutamiento..... 46
2.5.8 Prueba de Sistemas Confiados 47
2.5.9 Prueba de Control de Acceso ..... **¡Error! Marcador no definido.**
2.5.10 Prueba de Sistema de Detección de Intrusos 50
2.5.11 Prueba de Medidas de Contingencia..... **¡Error! Marcador no definido.**
2.5.12 Descifrado de Contraseñas..... **¡Error! Marcador no definido.**
2.5.13 Prueba de Denegación de Servicios 54
2.5.14 Evaluación de Políticas de Seguridad 55
2.6 Seguridad física..... 57
2.6.1 Revisión de Perímetro..... 57
2.6.2 Revisión de monitoreo ..... **¡Error! Marcador no definido.**
2.6.3 Evaluación de Controles de Acceso..... 58
Capitulo 3: Herramientas de Seguridad 60
3.1 Herramientas para la Exploración de la Red..... 60
3.2 Identificación de Servicios y Sistemas..... 60
3.2.1 Adquisión de blancos 60
3.3 Identificación de Sistemas Operativos..... 62
3.4 Identificación Pasiva de Sistemas 62
3.5 Barrido de Puertos..... 62
3.6 Identificación de Servicios..... 63
3.6.1 Amap 63
3.6.2 Nmap..... 64
3.7 Identificación de Servicios Web 65
3.7.1 DNS..... 66
3.8 Análisis de y verificación de vulnerabilidades 66
3.9 Inyección de paquetes 66
3.10 Evasión de Firewalls e IDSs 67
Conclusiones 68
Recomendaciones..... 69
Referencias Bibliográficas 70
Glosario..... 73
Anexos 75

Introducción

En la actualidad la mayoría de las empresas, organizaciones y países soportan su funcionamiento en los sistemas de información y comunicaciones. La seguridad de estos sistemas adquiere entonces una importancia vital. Es ya un hecho la migración de muchos de los servicios y tecnologías tradicionales, como la telefonía, al protocolo IP. Desafortunadamente, este desarrollo también es utilizado por piratas del ciberespacio, para obtener beneficios personales y causar daños a los sistemas.

La seguridad en redes de computadoras ha pasado de ser una simple preocupación de unos pocos a una difícil realidad en nuestros días. A cada momento crece el número de empresas que informatiza su trabajo de oficina y se va haciendo más dependiente de las nuevas tecnologías. Las redes de computadoras ganan terreno y su seguridad se convierte en una tarea de todos los profesionales del mundo de la informática.

En los sistemas informáticos es muy importante el volumen de información confidencial que se maneja, las pérdidas por concepto de la revelación de esta información confidencial pueden ser numerosas y a partir de esta consideración, las empresas dedicarán más o menos recursos a implementar una red segura.

Existen numerosas formas o técnicas de asegurar los sistemas, redes y aplicaciones, entre las que se encuentran los cortafuegos, programas detectores de intrusos, la criptografía, programas antivirus, zonas desmilitarizadas, entre otras. Una técnica menos conocida es el *Diagnóstico de Seguridad de las Redes,* la que poco a poco se ha convertido en una herramienta imprescindible en la evaluación de todos los sistemas de seguridad.

Hace algunos años el tema de la Seguridad era solo tema de científicos y profesionales especializados del área en cuestión. Este tema ha ido en constante evolución con el de cursar de los años. La responsabilidad de una red segura; o una Internet segura, ya no depende solo de profesionales de la seguridad, ahora, mucha más responsabilidad recae en los usuarios finales, usuarios de escritorio.

A partir de las características y elementos con que cuenta la red de la universidad se ha hecho imprescindible la realización de una guía a seguir para un reconocimiento general de la red. Para la solución de este problema surgen las siguientes interrogantes:

- ¿Cual es la situación actual que presenta el desarrollo de las auditorias de seguridad?
- ¿Que herramientas complementan las pruebas de intrusión de una metodología de seguridad?
- ¿Cuál sería la propuesta de procedimientos de seguridad adecuada para la Intranet de la UCLV?

Por ello, el objetivo general es presentar una guía de procedimientos para las pruebas de seguridad en la Intranet UCLV. Para lo cual se han propuesto las siguientes tareas específicas:

- Realizar un estudio comparativo de las diferentes metodologías de seguridad existentes hasta el momento.
- Caracterizar las principales metodologías en cuanto a radio de acción, evaluación de riesgos y otros caracteres.
- Proponer una serie de procedimientos metodológicos que se adecue a la red de la UCLV.
- Evaluar los resultados parciales de los procedimientos propuestos anteriormente.

Este trabajo se ha estructurado en: introducción, desarrollo, compuesto de tres capítulos, conclusiones, recomendaciones, referencias bibliográficas, glosario de términos y anexos. A continuación se describe brevemente el contenido de los diferentes capítulos.

CAPITULO I : Estado y desarrollo de los sistemas de auditorías de seguridad.

Este capítulo aborda el estado del arte de las distintas metodologías de seguridad existentes; teniendo en cuenta sus características, estándares aplicables y diferentes test de realización como el test de penetración y su costo. Así como lo relacionado con la seguridad informática y las amenazas más comunes presentadas en los sistemas de seguridad.

CAPITULO II: Diseño de los Procedimientos para la Realización de Pruebas de Seguridad a la Intranet de la UCLV.

El capitulo 2 trata sobre una propuesta de procedimientos para la realización de una auditoria de seguridad a la Intranet de la UCLV.

CAPITULO III: Herramientas de seguridad.

El capitulo 3 abarca las principales herramientas de seguridad que serán usadas en la realización de los procedimientos descritos para las auditorias de seguridad.

Capítulo 1: Estado y desarrollo de los sistemas de auditoría de seguridad

1.1 Introducción

El surgimiento de redes de comunicación, en particular de Internet, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario entonces, crear diferentes mecanismos, encaminados a garantizar la confidencialidad y autenticidad de los documentos electrónicos. (CERT, 2004)

Partiendo del criterio de que la seguridad se ocupa de la protección de los bienes, se pueden definir los bienes informáticos a proteger agrupándolos en tres grandes categorías que son, el software, el hardware y los datos, de todos los más expuestos, son los datos. Se devalúan rápidamente, su tiempo de vida útil suele ser corto y dependen del valor de la información que contienen. El hardware por su parte posee un tiempo de vida estimado de 2 ó 3 años, y el software depende básicamente del nivel de seguridad requerido para la información con la que opera.

Son varios los autores (Neyerber, 2005), (Nonaka, 2006) y (Hendel, 2004) que han descrito este proceso, teniendo en cuenta su naturaleza y el tipo de institución donde se aplica. Cada concepto es hijo de su tiempo y del contexto de aplicación donde se inserta como actividad por tal razón se determina como hilo teórico conceptual en esta investigación el postulado de Tanenbaum (2002) el que describe a la seguridad como un proceso continuo de reducción de riesgos donde sus problemas esenciales se dividen en las siguientes áreas: confidencialidad, validación de identificación, no repudio e integridad. Se hace un análisis de las características de la seguridad informática, donde no se limita a describir una situación práctica, si no que se abordan cuestiones como la confidencialidad: (se traduce en mantener la información fuera del alcance de usuarios no autorizados) Viéndose la apelación al uso de la validación de identificación como sustento que se encarga de determinar con quien se esta hablando antes de revelar información confidencial. El principio del no repudio tiene vital importancia en los procesos de seguridad informática, pues se encarga de garantizar la identidad del usuario de manera que no pueda negar la

participación en una transacción económica, siendo la integridad la que implica que los mensajes sólo sean modificados por usuarios autorizados. (Tanenbaum, 2002)

1.2 Actualidad de la Seguridad informática

Los recursos del sistema de información, que en ocasiones se les nombra Activos, son necesarios para que la organización funcione correctamente y alcance los objetivos propuestos. Por otra parte se cuenta con las Amenazas, un evento en el cual se puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, donde como consecuencia de la materialización de esta se observa el Impacto.

Se observa a su vez el Riesgo como una posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización. La Vulnerabilidad, se presenta como una posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo. Como otros recursos de los sistemas de información se presenta el Ataque, el cual se observa como un evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema. Y el desastre o Contingencia, interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio. (CERT, 2004)

1.3 Amenazas de los sistemas informáticos

Las amenazas sobre los sistemas informáticos presentan orígenes diversos. Así, el hardware puede ser físicamente dañado por la acción del agua, el fuego, los sabotajes, etcétera. Ellos también pueden dañar los medios magnéticos de almacenamiento externo. Pero, además, la información almacenada en estos últimos, también puede afectarse como resultado de la influencia de campos magnéticos intensos y, frecuentemente, por errores de operación. Las líneas de comunicación pueden interferirse o "pincharse". Otra clase de amenaza es la que representan usuarios o empleados infieles, que pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de una o más organizaciones. La ingeniería social es una manipulación verbal que en la mayoría de los

casos se lleva a cabo bajo identidad encubierta, ya sea por teléfono o a través de terceras personas y su alcance depende de la creatividad del atacante y de la ingenuidad de la víctima. Para ello el intruso se hacen pasar por el administrador o alguien importante, falseando la dirección de origen de un correo electrónico o mediante el teléfono para que el usuario le facilite su clave o le revele algún tipo de información que pueda necesitar. (Mclure, 2001)

Las amenazas más sutiles provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente. Una técnica fraudulenta muy utilizada consiste en transferir información de un programa a otro mediante canales ilícitos, no convencionales (canales ocultos). El análisis del comportamiento de las amenazas a la seguridad de la información revela que la mayoría de los hechos se cometen por intrusos individuales. Un por ciento menor corresponde a incidentes protagonizados por grupos organizados, y en la punta de la pirámide, se ubican los casos de espionaje (industrial, económico, militar...). (Ludwin,1996)

1.3.1 Amenazas más comunes

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento o transmisión de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias no informáticas que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia, en el caso de los datos y la descentralización mediante estructura de redes en el caso de las comunicaciones. (Ludwin,1996)

Estos fenómenos pueden ser causados por un operador el cual es causa del mayor problema ligado a la seguridad de un sistema informático. Programas maliciosos, programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano,

una bomba lógica o un programa espía o Spyware. Un intruso es aquella persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o *Script boy* y viruxer). Un siniestro (robo, incendio, por agua) tiene lugar cuando ocurre una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos. El último y no por ser el último el menos importante es el personal interno de Sistemas, pues las pugnas de poder que llevan a disociaciones entre los sectores traen consigo soluciones incompatibles para la seguridad informática. Por estas y otras razones, el tratamiento de los temas relacionados con la seguridad informática ha tomado un gran auge. CERT/CC (*Computer Emergency Response Team Coordination Center*) del *SEI* de la Carnegie Mellon University (grupo que se encarga de los problemas de seguridad)

1.3.2 Protección contra las principales amenazas

Muchas organizaciones gubernamentales y no gubernamentales han preparado documentos, dirigidos a orientar el uso adecuado de las tecnologías existentes y a evitar su uso indebido, pues los malos manejos de las referidas tecnologías ocasionan serios problemas en los bienes y servicios de las empresas en el mundo. Las medidas tomadas para enfrentar las amenazas informáticas pueden clasificarse en dos grupos:

- Seguridad física
- Seguridad técnica

El término seguridad física se emplea frecuentemente para referirse a las medidas de protección externas. Normalmente, se implementan mediante dispositivos electrónicos y mecánicos.

Definitivamente son las primeras que se introducen en todas las instalaciones informáticas. Su costo no es excesivo (con la excepción de los sistemas de continuidad eléctrica) y su mantenimiento no presenta dificultades especiales.

Las medidas de seguridad técnicas, pretenden proteger, tanto el software de aplicación

como los datos. Pueden implementarse en dispositivos hardware o en productos software.

Para el desarrollo de estas medidas, se ha hecho necesaria una investigación académica muy intensa, principalmente durante los últimos 15 años, lo que ha generado varios modelos teóricos de interés como: el control de accesos, el control del flujo de la información; así como el desarrollo de criptosistemas de clave privada y pública y de sistemas de firma digital y no repudio en la transmisión de datos. Cuando se recibe un mensaje no sólo es necesario poder identificar de forma unívoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que envía. En este sentido, es fundamental impedir que el emisor pueda rechazar o repudiar un mensaje, es decir, negar su autoría sobre la información que envía y sus posibles consecuencias. A esto se denomina no repudio en el contexto de la transmisión de datos.

1.4 Seguridad de la información

Como medidas de seguridad de la información en un sistema se tiene la Confidencialidad y la Autenticidad. La primera se refiere a la posibilidad de mantener un documento electrónico inaccesible a todos, excepto a una lista de individuos autorizados. La autenticidad, por su parte, es la capacidad de determinar si uno o varios individuos han reconocido como suyo y se han comprometido con el contenido del documento electrónico. El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa. Mediante su firma autógrafa, un individuo, o varios, manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, a cumplir con los compromisos que el documento establezca para con el individuo.

1.5 Pruebas de seguridad

En ocasiones se suele esperar para hacer pruebas o reportar los problemas y así se dilatan las soluciones de seguridad. Esperar hasta mañana para hace las comprobaciones requeriría también examinar el sistema para verificar que cosas faltan, o están dañadas, con lo cual se pierde un tiempo importante, teniendo en cuanta que una auditoria toma casi el mismo tiempo que una prueba de seguridad.

Cuando se realizan exámenes de seguridad se analizan los detalles, y muy a menudo los pequeños aspectos llevan a las más importantes fallas de seguridad. Es la acumulación de las cosas pequeñas, que individualmente no representan mucho riesgo, aunque sumadas, pueden llevar a una falla de seguridad importante.

Como regla general, los presupuestos de seguridad son bajos, por lo que el analista de seguridad necesita operar con eficiencia y creatividad para hacer más en menos tiempo. Si la prueba de seguridad es ineficiente el proceso se vuelve demasiado costoso, lo que hace que las organizaciones observen este proceso como un costo innecesario. Desafortunadamente este visión es errónea porque los riesgos asociados al no desarrollo de prueba de seguridad siguen siendo ignorados por las organizaciones. En consecuencia, cuando se hace un balance minucioso y eficiente en las exploraciones de seguridad, los resultados van a dar soluciones concretas lo que posibilita que la dirección de la organización vea el presupuesto de las pruebas de seguridad como un gasto justificado.

1.5.1 Clasificación de las Pruebas de Seguridad

Existen diversas formas para la realización de una prueba de seguridad, las cuales son muy útiles para chequear el funcionamiento de una red de trabajo. Primeramente es necesario conocer el significado de Tarea siendo esta la realización de las diversas pruebas de seguridad específicas en un módulo que se utilizan para alcanzar uno o más resultados esperados definidos, estos pueden ser clasificados como: Pruebas de aplicación, se realizan sobre cualquier aplicación, independientemente si es o no parte de la presencia en Internet. Pruebas de intrusión son realizadas con un objetivo definido que finaliza cuando el propósito es alcanzado o el tiempo ha terminado. Prueba automatizada; cualquier clase de prueba que también brinda análisis determinado.

Una Prueba con privilegios es realizada cuando las credenciales necesarias son suministradas al usuario y los permisos concedidos para la realización de la prueba con dichas credenciales. Prueba de seguridad, test donde existe presencia de seguridad pudiendo ser especificado por sección. Prueba de verificación realizada en una segunda

etapa luego que todos los parches han sido aplicados. Prueba de vulnerabilidad es un examen de servicio, donde son chequeados puertos abiertos y vulnerabilidades conocidas. Prueba manual, prueba que requiere que una persona ingrese datos durante el proceso de prueba y monitoree los resultados para efectuar análisis sobre ellos.

La Prueba de penetración es un conjunto de metodologías y técnicas de intrusión aplicadas sobre un sistema en un tiempo determinado con el objetivo de conocer el nivel de seguridad informática real del mismo, detectado y explotando vulnerabilidades. Formalmente prueba de penetración es una parte del proceso de seguridad informática de una organización.

La prueba metódica de seguridad se apoya en una combinación de creatividad y en extensas bases de conocimiento sobre las metodologías más adecuadas, cuestiones legales y las regulaciones inherentes al área de la industria del cliente. En otras palabras, se examinan todos los extremos de lo considerado como predecible, aprovechando al máximo las mejores prácticas para analizar los escenarios de los peores casos posibles que no son tan predecibles.

Los tipos de preguntas que debe hacer continuamente durante el proceso de prueba de seguridad son:

- ¿Qué bienes puedo acceder en qué momento para provocar el máximo riesgo de seguridad?
- ¿Bajo qué circunstancias encuentro la mayor parte de las vulnerabilidades?
- ¿Cuándo estoy más propenso a aplicar confidencialidad, integridad y accesibilidad a la prueba?

Manteniéndose sistemático y persistente, el efecto acumulativo de estas pruebas dará como resultado un panorama exacto de los riesgos, debilidades, filtraciones de información y vulnerabilidades. Esto servirá tremendamente con cualquier justificación de negocio de resguardo, como así también servirá para la satisfacción de los requisitos regulativos/legales a través de los debidos recaudos y la diligencia.

1.6 Prueba de penetración

La Prueba de penetración es muy completa pero no se puede decir que es una auditoria de seguridad completa y tampoco es un análisis de vulnerabilidades de seguridad informática. Según el FFIEC (2005) (Federal Financial Institutions Examination Council) las pruebas de penetración, auditorías de seguridad y análisis de vulnerabilidades pueden utilizar las mismas herramientas en sus metodologías, pero la naturaleza de los mismos es diferente. Este tuvo un nacimiento muy confuso, no se sabe exactamente donde nació, y se ubicó como una nueva rama dentro de la seguridad informática. Originalmente, los primeros examinaban redes x.25, conexiones dial-up, accesos remotos, servidores y servicios internos. Con el nuevo posicionamiento de la seguridad informática y auge de Internet, el examen de penetración fue evolucionando desde sus comienzos hasta llegar a ser algo muy completo y complejo, que incluye permanentemente nuevas técnicas.

En la actualidad las pruebas de penetración enfrentan una realidad muy compleja, debido a la desinformación que existe. Son muy pocas las organizaciones que tienen en claro ¿Para qué contratan este tipo de servicio? ¿Qué alcance le dan?, si están preparadas para recibir los resultados y si realmente valoran el trabajo realizado. Las recomendaciones que surgen en ellos en muchos casos no son implementadas. Existe un desconocimiento general sobre la “calidad” y sobre como “medir” en una prueba de este tipo, esto genera una amplia oferta que abarca desde estudiantes que corren una herramienta hasta equipos de expertos con una alta experiencia. Indiscutiblemente esto forma parte del proceso de la seguridad informática.

Su misión comienza una vez que las políticas de la organización han sido implementadas sobre los sistemas de información. Utilizando técnicas intrusivas se demuestran las vulnerabilidades que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información. Y nos da un punto de partida sobre el cual comenzar a ajustar las políticas de la organización.

Los exámenes de penetración generalmente se pueden dividir en dos grandes líneas, externos e internos. Los externos apuntan a analizar el nivel de seguridad real de una

organización desde el exterior y deberían incluir módems, centrales telefónicas, accesos remotos, Internet, conexión con sucursales, otras conexiones externas y redes wireless.

Los internos se destinan a analizar el nivel de seguridad real de una organización a nivel interno, incluyendo análisis de la infraestructura de la red, estaciones de trabajo, servidores, aplicaciones. Estos cada vez son más abarcativos e incluyen nuevos protocolos, equipos y tecnologías (aplicaciones web, software ERP, SAN.) También incluyen nuevas técnicas como: Cross-site-scripting, Sql-injection, Buffer-overflow, Formatstrings y técnicas anti-IDS entre otras

Las vulnerabilidades de seguridad informática tienen una relación directa con las pruebas de seguridad, pues mientras se sigan descubriendo nuevas vulnerabilidades, siempre será necesaria la realización de otras pruebas. Existen hoy en día más de 13.000 vulnerabilidades de seguridad informática y están apareciendo aproximadamente 4.000 más por año, esto implica que las organizaciones deben seguir una fuerte política de actualización y mantenimiento de sus sistemas informáticos. Las pruebas de seguridad brindan un gran aporte a la seguridad informática debido a que muchas vulnerabilidades son descubiertas durante la realización de los mismos. Normalmente las empresas de software realizan auditorías de seguridad sobre sus productos antes de lanzarlos al mercado.

1.6.1 Implementación de las Pruebas de Seguridad

Las principales características que se presentan Durante el "examen de penetración" se simula un atacante externo, se realizan varios scanners de debilidades y vulnerabilidades:

- Estudio de la red externa.
- Barrido de puertos: TCP y UDP
- Estudio de debilidades.
- Barrido de vulnerabilidades en componentes de red.
- Barrido de vulnerabilidades de sistemas operativos.
- Barrido de vulnerabilidades de aplicaciones de red.

- No se realiza la explotación de vulnerabilidades.

1.6.2 Alcance de las Pruebas de Seguridad

Es necesaria la realización de un test por varias razones, conocer la situación real de un sistema y mejorarlo, demostrar los riesgos existentes, justificar la obtención de más recursos económicos, verificar que los mecanismos de seguridad se encuentren funcionando correctamente, por regulaciones y/o obligación y como un seguro para poder cubrirse ante auditorias.

Las organizaciones esperan conocer los riesgos a los cuales se ven sometidos los sistemas informáticos. La experiencia demuestra que la mayoría de las veces, las empresas que piden exámenes de penetración están en un cierto grado de maduración en relación a la seguridad informática.

Las recomendaciones muchas veces son redactadas sin tener en cuenta el entorno operativo, esto provoca que incluso muchas recomendaciones sean técnicamente inviables. En las organizaciones suelen darse dos casos el área de seguridad informática es la que implementa los cambios o es la que supervisa al área de soporte técnico que es quien realiza los cambios.

En cualquiera de los dos casos, se definen las acciones a seguir y luego se comienza con el Plan de Implementación de las mismas. Sólo se aplican los cambios que implican un alto riesgo. Para esta problemática se ha propuesto una solución que radica en la clasificación de todos los problemas encontrados con dos variables nivel de riesgo y posibilidad de resolución.

Para saber la calidad de realización de una Prueba de Seguridad es un tanto complicada, ya que no existen estándares ni organismos controladores. La calidad puede diferir muchísimo entre un examen de una empresa y otra. Los factores principales que inciden sobre la calidad son el conocimiento del equipo que realiza los exámenes de penetración, la

experiencia en la realización del examen de penetración, la forma de redacción de los informes y la presentación e interacción con la organización.

Sin duda, el más importante es el nivel de conocimiento, ya que un examen contratado a una empresa puede dar como resultado que la organización está muy bien y la otra presente resultados negativos.

1.6.3 Análisis de Costo

Los exámenes de penetración cuestan mucho dinero. Existen muchas diferencias entre los costos que están basadas en disímiles aspectos. Es muy importante establecer el lugar donde se realice el examen, ya que el costo del realizado en Europa es muy parecido al que se realiza en Estados Unidos, pero muy diferente al costo en Latinoamérica. Cabe aclarar que el costo en este caso no implica nivel de calidad. Este factor se basa en el valor de obra de los miembros del equipo que realizan el prueba. Otro de los aspectos a resaltar son los recursos técnicos involucrados. La empresa que realiza los exámenes puede utilizar notebooks de última generación, licencias de software de seguridad informática que tienen un elevado costo y desarrollar aplicaciones propias.

Paralelamente a esto se puede ver el conocimiento y la experiencia del equipo humano que realiza el examen, si el equipo está compuesto por expertos con años de experiencia en el campo o si está formado por estudiantes con un nivel básico. Y el último factor que se debe tener en cuenta es la correcta definición del alcance. Este es uno de los factores clave para la determinación del costo, ya que en base al alcance se definirá el tiempo que durará el examen.

La suma de todos estos factores definirá el costo final del examen de seguridad y el mercado de ofertas de productos y servicios, mediante la ley de oferta/demanda también determina estos factores.

Un estudio que dimensiona la importancia de los diagnósticos es el publicado en el 2005

denominado “Ethical Hacking Survey”, en este caso por la compañía de consultoría de redes Internacional Network Service (INS). En ese estudio fueron encuestados 202 Instituciones y profesionales de seguridad de todo el mundo, reportándose que el 83 % de las instituciones realizan diagnósticos de seguridad con una frecuencia que oscila entre uno y cuatro veces al año (ver Fig.1). Por otra parte, se constata que el 68% de las entidades reservan parte del presupuesto de seguridad para la realización de los diagnósticos, que a veces puede a ascender hasta el 30 % del monto total.

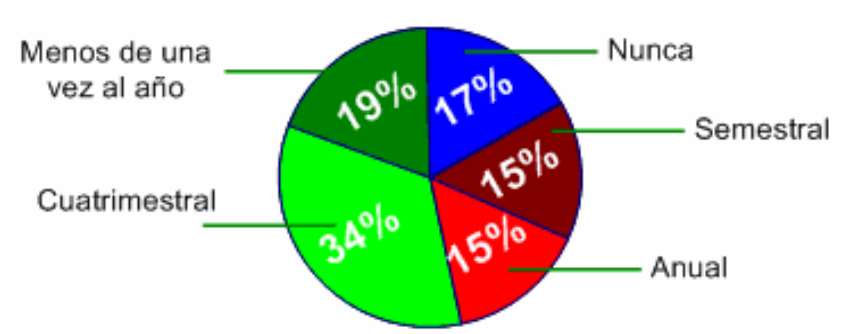

Fig.1 Frecuencia con que las entidades realizan diagnósticos de seguridad.

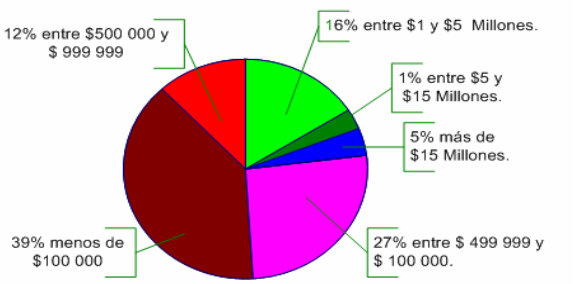

Fig.2 Monto de dinero presupuestado por las entidades para la seguridad.

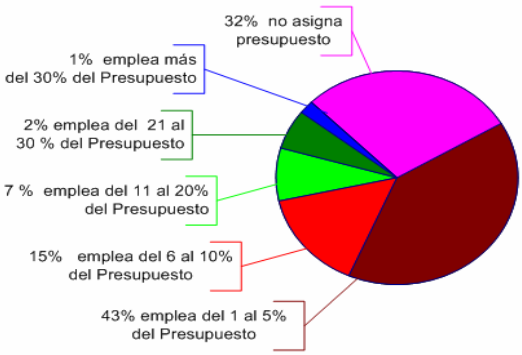

Fig.3 Por ciento del presupuesto de seguridad que es reservado para los diagnósticos de seguridad.

Internacionalmente el precio por la realización de un diagnóstico de seguridad a una red de datos suele estar entre los $10,000 y $100,000 dólares, en dependencia de la complejidad de la arquitectura de la red y de la cantidad de sistemas a analizar. Las empresas asumen este gasto debido a que las pérdidas a las que se exponen, si su red tiene brechas de seguridad no detectadas, son muy superiores llegando en ocasiones a millones de dólares.
El diagnóstico de seguridad, por la necesidad de su ejecución cíclica, debe convertirse en una herramienta de trabajo de los responsables de seguridad de cada entidad.

1.6.4 Resultados de la Prueba de Penetración

El resultado de la "prueba de penetración" mostrará una idea general del estado de la seguridad de los sistemas frente ataques externos:

- Pruebas de seguridad realizadas en el examen.
- Lista de vulnerabilidades y debilidades encontradas.
- Referencia técnica a estas vulnerabilidades y sus soluciones.
- Recomendaciones.

La mayoría de los especialistas de seguridad opinan que es imposible realizar un diagnóstico de seguridad con la calidad necesaria si no se tiene una metodología por la cual realizarlo. Muchas variables pueden influir en el resultado de un diagnóstico, incluyendo el estilo, la experiencia y predicciones del comprobador. Precisamente por todas estas variables es necesario definir el modo correcto de realizar los diagnósticos, qué pruebas se deben hacer, en qué orden, en qué tiempo y qué planillas e informes deben arrojar como resultado. Esta es una manera efectiva de reducir los falsos supuestos y evitar resultados mediocres.

1.7 Metodologías para las Pruebas de Seguridad

En la práctica, existen tantas metodologías como empresas de seguridad informática que presten este servicio. Los autores comprenden desde empresas privadas de seguridad e institutos nacionales de estándares para países determinados, hasta metodologías abiertas desarrolladas por institutos u organismos internacionales de investigación dedicados a la

definición de estándares. Estas metodologías abarcan desde las clásicas tres fases: identificación, scanning y explotación, hasta las de múltiples fases.

Existe una innumerable variedad de metodologías en todo el mundo unas más conocidas y aplicadas que otras. Algunas de las más populares se mencionan a continuación.

- Standards for Information Systems Auditing (ISACA)
- The CESG IT Health Check (CHECK)
- Application Security Project (OWASP)
- "Aplicación de la Prueba de penetración en organizaciones" del Instituto SANS.
- "Guía de Pruebas de Seguridad en RED" del Instituto Nacional de Estándares y Tecnología (NIST).
- The aim of The Open Source Security Testing Methodology Manual (OSSTMM).
- Proyecto ISSAF (Information System Security Assessment Framework).

El carácter especializado de la auditoría de los sistemas de información, y las habilidades necesarias para llevar a cabo dichas auditorías, requieren estándares aplicables globalmente que se adecuen específicamente a la auditoría de los sistemas de información. Una de las metas de la Asociación es adelantar los estándares para satisfacer esta necesidad. El desarrollo y la divulgación de los Estándares para la Auditoria de los Sistemas de Información es la piedra angular de la contribución profesional de la Asociación a la comunidad de auditores.

1.7.1 Normas para Auditorias en Sistemas de Información

Los objetivos de los Estándares de "Standards for Information Systems Auditing" (ISACA) o Auditoria de los Sistemas de Información son informar a los auditores de los sistemas de información sobre el nivel mínimo requerido de rendimiento aceptable pasa cumplir con las responsabilidades profesionales establecidas en el Código de Ética

Profesional para los Auditores de Sistemas de Información, a la Gerencia y a otros interesados sobre las expectativas de la profesión en relación con el trabajo de los auditores.

El marco de los Estándares de Auditoria de los Sistemas de Información de ISACA tiene múltiples niveles. Los Estándares definen los requisitos obligatorios para la auditoría y el informe de SI, mientras que las directrices brindan una guía para aplicar los estándares de auditoría de SI.

El auditor de SI debe considerarlas para determinar cómo llevar a cabo la implementación de los estándares citados anteriormente, usar su juicio profesional al aplicarlas y estar preparado para justificar cualquier desviación de las mismas.

Por su parte los procedimientos ofrecen ejemplos de los pasos a seguir por un auditor de SI en una Auditoría. Por otro lado los documentos de procedimiento brindan información sobre la manera de cumplir con los estándares cuando se está realizando un trabajo de auditoría de los sistemas de información, pero no fijan requisitos.

El Código de Ética Profesional de ISACA requiere que los miembros de ISACA y quienes cuentan con la designación CISA cumplan con los Estándares de Auditoría de Sistemas de Información adoptados por ISACA. El incumplimiento evidente de las mismas puede tener como consecuencia que ISACA o una junta o comité apropiado de ISACA, realicen una investigación de la conducta de los miembros o poseedores de la designación CISA Esto podría dar lugar a una medida disciplinaria.

1.7.1.1 Estándares aplicables

Dentro de los estándares aplicables a la auditoría de Sistemas de Información podemos encontrar los siguientes:

1 Estatuto de Auditoría

1.1 Responsabilidad y Autoridad

2 Independencia

2.1 Independencia Profesional

2.2Relación con la Organización

3 Ética Profesional y Estándares

3.1 Código de Ética Profesional

3.2 Debido Cuidado Profesional

4 Competencia

4.1 Destrezas y Conocimientos

4.2 Educación Profesional Continua

5 Planificación

5.1 Planificación de la Auditor

6 Realización del Trabajo de Auditoría

6.1 Supervisión

6.2 Evidencia

7 Informe

7.1 Contenido y Forma del Informe

8 Seguimiento de las Actividades

8.1 Seguimiento

La responsabilidad y la autoridad de las funciones de auditoría de los sistemas de información deben estar documentadas de una forma apropiada mediante un estatuto o carta de compromiso de auditoría. En todos los asuntos relacionados con auditoría, el auditor de sistemas de información debe ser independiente del auditado tanto en actitud y apariencia. La función de auditoria de sistemas de información debe ser lo suficientemente independiente del área que esté siendo auditada como para permitir que se logren los

objetivos de la auditoría. El auditor de sistemas de información debe acatar el Código de Ética Profesional de la Asociación.

Se debe ejercer el debido cuidado profesional y se deben observar los estándares aplicables de auditoría profesional en todos los aspectos del trabajo del auditor de sistemas de información. El auditor de sistemas de información debe ser competente desde el punto de vista técnico y debe tener las habilidades, destrezas y conocimientos necesarios para realizar el trabajo auditor. El auditor de sistemas de información debe mantener su competencia técnica por medio de una educación profesional continua apropiada.

El auditor de sistemas de información debe planificar el trabajo de auditoria de los sistemas de información para lograr los objetivos de la auditoría y para cumplir con los estándares aplicables de auditoria profesional. El personal de auditoria de sistemas de información debe estar debidamente supervisado para garantizar que se logren los objetivos de la auditoria y que se observen los estándares aplicables de auditoría profesional.

En el curso de la auditoria, el auditor de sistemas de información debe obtener evidencias suficientes, confiables, relevantes y útiles para lograr los objetivos de una forma efectiva. Los hallazgos y las conclusiones de la auditoría deben estar respaldados por análisis apropiados y por una interpretación correcta de esta evidencia.

El auditor de sistemas de información debe suministrar un informe, en una forma apropiada, a los destinatarios que corresponda al terminar el trabajo de auditoría. El informe de auditoría debe establecer el alcance, los objetivos, el período abarcado, la naturaleza y la envergadura del trabajo de auditoría que se realizó. El informe debe identificar la organización, los destinatarios y cualquier restricción sobre su circulación. El informe debe establecer los hallazgos, las conclusiones y las recomendaciones, así como también cualquier reserva o calificación según la opinión del auditor con relación a la auditoria.

El auditor de sistemas de información debe solicitar y evaluar la información pertinente sobre los hallazgos, conclusiones y recomendaciones anteriores relevantes para determinar

si se han implementado las medidas adecuadas de forma oportuna.

1.7.2 Proyecto Abierto de Seguridad de Aplicaciones Web

Otro de los estándares mas conocidos a nivel mundial es **OWASP** (Open Web Application Security Project) (Proyecto Abierto de Seguridad de Aplicaciones Web) Es una comunidad abierta dedicada a encontrar y combatir las causas de la inseguridad en el software. Todas las herramientas, foros y documentos son gratis y de código abierto para todo el mundo. Al ser una organización sin fines de lucro, le aporta al referido proyecto cualidades como: la imparcialidad y praxis (juicios pragmáticos o prácticos) sobre la información acerca de la seguridad. OWASP no está asociado con ninguna compañía tecnológica, a pesar que utiliza la información que ellos le suministran. La fundación provee servidores de banda ancha, facilidad para realizar proyectos. Una distinción que hace OWASP son los Amenazas, el uso de la palabra amenaza lo utiliza para describir un peligro potencial probable o riesgo de que algo salga mal. Para poder entender bien el concepto de seguridad y todo lo que lo rodea debemos poder distinguir entre riesgo, ataque, vulnerabilidad, impacto y otros términos de manejo de riesgos.

1.7.2.1 Categorías de amenazas

Hay tres tipos de categorías de amenazas:

- Naturales (Incendio, tornado, rayo).
- Humano No intencional (accidentes, descuidos).
- Humano Intencional (de adentro, de afuera).

1.7.2.2 Planes de contingencia

A su vez OWASP también propone entre sus proyectos planes y medidas de contingencia. Los planes o medidas de contingencia son tecnologías o módulos defensivos que pueden ser usados para detectar, detener o denegar un ataque. Hay planes necesarios en una aplicación que deben identificar amenazas, usando análisis de amenazas, para así, proteger a la aplicación en contra de cualquier tipo de ataque basado. Una debilidad o una falla en el

plan de contingencia, incluso la falta de un plan adecuado, puede resultar una vulnerabilidad que deja susceptible a la aplicación.

Ejemplos de planes de contingencia:

- Autentificación,
- Control de Acceso,
- Administrador de Sesión,
- Validación del ingreso,
- Manejo de errores,
- Logging,
- Criptografía.

El proyecto OWASP tiene varios principios; se entiende por principios de seguridad de aplicaciones a las reglas fundamentales de seguridad que describen el correcto comportamiento y/o diseño de una aplicación, las cuales se pueden mejorar cambiando las posturas sobre seguridad. Estos principios son generales, deben tomarse solo como una guía y no como una manual de procedimientos a seguir. Con esta herramienta que OWASP presenta se tiene una ayuda más; en los momentos de tomar decisiones en nuevas situaciones, usando estas ideas básicas.

1.7.3 Sistema de Información para asentar una red de Trabajo

El Proyecto ISSAF (Information System Security Assessment Framework). Esta es una metodología de pruebas de seguridad (muy orientada a Pruebas de penetración). ISSAF es un compendio procedimientos detallados, técnicos en muchos casos, para evaluaciones de seguridad de diversos tipos de dispositivos, procedimientos administrativos y software desde ruteadores hasta servidores Web pasando por sistemas operativos y procedimientos de control de cambios.

Debido a toda una serie de complicaciones y requisitos que tiene este proyecto aun no se encuentra en óptimas condiciones para su puesta en práctica, no por incompetencia sino por

profundizar en la perfección para trabajar con vulnerabilidades.

1.7.4 Manual de la Metodología Abierta de Testeo de Seguridad

Es extremadamente importante cuando se habla de seguridad referirse a la metodología para prueba de seguridad conocido por OSSTMM (The Open Source Security Testing Methodology Manual)

Este manual es un estándar profesional para el prueba de seguridad en cualquier entorno desde el exterior al interior. Este Manual como un estándar profesional, incluye los lineamientos de acción, la ética del auditor profesional, la legislación sobre el prueba de seguridad y un conjunto integral de pruebas. Su objetivo es crear un método aceptado para ejecutar un examen de seguridad minucioso y cabal intentando ser el manual de referencia del profesional.

El OSSTMM, frente a otras metodologías incluye el uso de "Valores de Evaluación del Riesgo". Estos valores se definen en cada módulo y tienen como objetivo principal medir la degradación de la seguridad respecto al tiempo.

La metodología esta dividida en secciones, módulos y tareas. Las secciones son puntos específicos en el mapa de seguridad que se sobreponen entre si y comienzan a descubrir un todo que es mucho mayor a la suma de sus partes. Los módulos son el flujo de la metodología desde un punto de presencia de seguridad hacia otro. Cada modulo tiene una salida y una entrada. La entrada es la información usada en el desarrollo de cada tarea. Las salidas es el resultado de las tareas completadas. La salida puede o no ser datos analizados (también conocido como inteligencia) para servir como entrada para otro modulo. Incluso puede ocurrir que la misma salida sirva como entrada para un modulo o sección.

Algunas tareas no brindan resultados, esto significa que existen módulos para los cuales no hay entrada. Los módulos que no tienen entrada pueden ser ignorados durante el análisis. El hecho de ignorar módulos no indica necesariamente un análisis inferior, al contrario indica un nivel de seguridad superior. Los módulos que no tienen salida como resultado, pueden

significar una de tres cosas: las tareas no fueron ejecutadas apropiadamente, no se aplicaban o revelaron niveles superiores de seguridad.

Es muy recomendable usar esta metodología por sus características donde sea descrito un análisis secuencial que permita realizar paso a paso todas las tareas necesarias de forma sistemática. Es una Metodología escalable, abierta y pública. Esto permite que los administradores de sistemas, responsables de Seguridad y empresas especializadas contribuyan a mejorar esta metodología que se ajusta a los estándares internacionales (ISO 17799).

Mucho antes de la existencia de esta Metodología, ya se podían encontrar en la red de redes algunos textos o materiales que detallaban este procedimiento, los cuales eran similares a este Manual o a sus Secciones. Y aunque al desarrollar la metodología, algunas tareas no brinden resultados esperados o no sean aplicables a una situación determinada, ello no implica un análisis inferior, pero tampoco resta importancia a la concepción de la Metodología como un todo.

1.8 Caracterización general

La mayoría de principales metodologías observadas hasta el momento no son iguales pero de una forma u otra todas coinciden en aplicar las siguientes fases:

1. Reconocimiento: Obtención de información, Análisis y planificación.
2. Búsqueda y Detección: Detección de vulnerabilidades.
3. Penetración: Explotación de vulnerabilidades, Escalada de privilegios.
4. Obtención de información
5. Informes: Análisis de los resultados, Desarrollo de informes, Presentación.
6. Limpieza.

Luego del estudio de las metodologías más importantes existentes, se analiza la posibilidad de la aplicación de una de las metodologías teniendo en cuenta las particularidades de la red de la universidad. Del resultado del estudio realizado se llega a las siguientes

conclusiones:

- Ninguna de las metodologías individualmente se adapta completamente al entorno y la arquitectura informática de la universidad

- Existen factores propios del entorno informático de la universidad que son imprescindibles considerar en el diseño de una metodología, pues podrían afectar la calidad de los resultados.

Capitulo 2: Diseño de los Procedimientos para la Realización de Pruebas de Seguridad a la Intranet de la UCLV

2.1 Mapa de Seguridad

El mapa de seguridad es una imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones. Las secciones se superponen entre si y contienen elementos de las restantes. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente.

Las secciones son:

1 Seguridad de la Información

2 Seguridad de los Procesos

3 Seguridad en las tecnologías de Internet

4 Seguridad en las Comunicaciones

5 Seguridad Inalámbrica

6 Seguridad Física

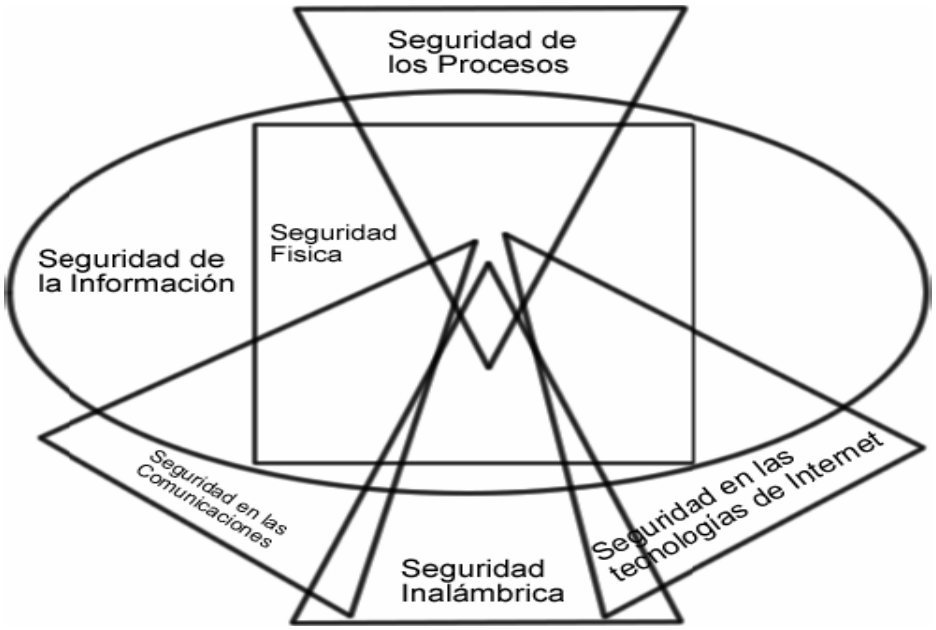

Fig.4 Mapa de seguridad

2.1.1 Módulos del Mapa de Seguridad

Los módulos del mapa de seguridad son los elementos primarios de cada sección. Cada módulo debe incluir todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas. Para desarrollar un análisis de seguridad de una sección particular, todos los módulos de la sección deben ser desarrollados.

1 Seguridad de la Información

1 Revisión de la Inteligencia Competitiva

2 Revisión de Privacidad

3 Recolección de Documentos

2 Seguridad de los Procesos

1 Prueba de Solicitud

2 Prueba de Sugerencia Dirigida

3 Prueba de las Personas Confiables

3 Seguridad en las tecnologías de Internet

1 Logística y Controles

2 Sondeo de Red

3 Identificación de los Servicios de Sistemas

4 Revisión de Privacidad

6 Prueba de Aplicaciones de Internet

7 Enrutamiento

8 Prueba de Sistemas Confiados

9 Prueba de Control de Acceso

10 Prueba de Sistema de Detección de Intrusos

11 Prueba de Medidas de Contingencia

12 Descifrado de Contraseña

13 Prueba de Denegación de Servicios

14 Evaluación de Políticas de Seguridad

4 Seguridad en las Comunicaciones

1 Prueba de PBX

2 Prueba del Correo de Voz

3 Revisión del FAX

4 Prueba del Modem

5 Seguridad Inalámbrica

1 Verificación de Radiación Electromagnética (EMR)

2 Verificación de Redes Inalámbricas [802.11]

3 Verificación de Redes Bluetooth

4 Verificación de Dispositivos de Entrada Inalámbricos

5 Verificación de Dispositivos de Mano Inalámbricos

6 Verificación de Comunicaciones sin Cable

7 Verificación de Dispositivos de Vigilancia Inalámbricos

8 Verificación de Dispositivos de Transacción Inalámbricos

9 Verficación de RFID

10 Verificación de Sistemas Infrarrojos

11 Revisión de Privacidad

6 Seguridad Física

1 Revisión de Perímetro

2 Revisión de monitoreo

3 Evaluación de Controles de Acceso

2.2 Metodología

La metodología fluye desde el módulo inicial hasta completar el módulo final. Permite a su vez la separación entre recolección de datos y tests de verificación de y sobre los datos recolectados. El flujo también determina los puntos precisos de cuando extraer e insertar estos datos.

Al definir la metodología de análisis, es importante no restringir la creatividad del analista introduciendo estándares excesivamente formales e inflexibles que la calidad de los tests sufra. Adicionalmente, es importante dejar tareas abiertas a alguna interpretación donde la definición exacta causará problemas a la metodología cuando una nueva tecnología sea introducida.

Cada módulo tiene una relación con el inmediatamente anterior y con el inmediatamente posterior. Cada sección tiene aspectos interrelacionados a otros módulos y algunos se interrelacionan con todas las otras secciones. Normalmente, los análisis de seguridad comienzan con una entrada que corresponde a las direcciones de los sistemas a ser analizados. El análisis de seguridad finaliza con el inicio de la fase de análisis y la construcción del informe final. Esta metodología no afecta la forma, tamaño, estilo o contenido del informe final ni especifica como los datos deben ser analizados.

Las secciones son el modelo total de seguridad dividido en porciones manejables y analizables. El módulo requiere una entrada para ejecutar las tareas del módulo y de otros módulos en otras secciones. Las tareas son los tests de seguridad a ejecutarse dependiendo de la entrada del módulo. Los resultados de las tareas pueden ser inmediatamente analizados para actuar como un resultado procesado o se pueden dejar sin analizar. De cualquier modo, estos son considerados la salida del modulo. Esta salida es a menudo la entrada para el siguiente módulo o en algunos casos, como equipos recién descubiertos; pueden ser la entrada para un módulo anterior.

El modelo de seguridad completo puede ser dividido en secciones administrables para las pruebas. Cada sección puede a su vez ser vista como una colección de módulos de test con cada módulo dividido en un conjunto de tareas.

2.3 Seguridad de la información

2.3.1 Revisión de la Inteligencia Competitiva

La IC es la información recolectada a partir de la presencia en Internet de la intranet de la UCLV. A diferencia del robo de propiedad intelectual encontrada en el hacking o el espionaje industrial, es que la IC tiende a no ser invasiva y mucho más discreta. Este es un buen ejemplo de cómo la presencia en Internet se extiende más allá de los hosts de la DMZ. Utilizar IC en un Test de Intrusión da valor de negocio a los componentes y puede ayudar a encontrar justificaciones de negocio para implementar distintos servicios.

1. Realizar un mapa y medir la estructura de directorio de los servidores web.

2. Realizar un mapa y medir la estructura de directorio de los servidores de FTP.

3. Determinar el costo de TI de la infraestructura de Internet basados en SO, Aplicaciones y Hardware.

4. Medir la respuesta de la organización basándose en grupos de noticias, tableros web, y los sitios de respuesta de la industria.

Resultados Esperados:

- Una medición de las justificaciones de negocio de la red de la organización
- Tamaño y alcance de la presencia en Internet
- Una medición de la política de seguridad a planes futuros de la red

2.3.2 Revisión de Privacidad

La revisión de privacidad es el punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad de los usuarios de la intranet UCLV. El uso de estos datos es la preocupación de muchas personas privadas y la legislación no da reglas específicas considerando la privacidad. La intranet de la UCLV es de carácter académica por lo que no puede ser usada con objetivos personales, lo cual esta debidamente referenciado en el reglamento de la UCLV. Con lo cual los usuarios tienen pleno conocimiento de que la información que tengan almacenados en los servidores puede ser auditada en cualquier momento.

1. Comparar públicamente la política accesible con la práctica actual

2. Comparar la practica actual con el fraude regional y las leyes de privacidad o cumplimiento

3. Identificar el tipo y tamaño de la base de datos para el almacenamiento de los datos

4. Identificar los datos conseguidos por la organización

5. Identificar la ubicación de almacenamiento de los datos

6. Identificar los tipos de cookies

7. Identificar las fechas de expiración de las cookies

8. Identificar la información almacenada en las cookies

9. Verificar los métodos de encripción de la cookie

10. Identificar la ubicación del servidor de error del web

11. Identificar web bug data gathered and returned to server

Resultados Esperados:

- Lista de cualquier revelación
- Lista de las fallas de conformidad entre la política publica y la practica actual
- Lista de los sistemas involucrados en la recolección de datos
- Lista de las técnicas de obtención de datos
- Lista de los datos obtenidos

2.3.3 Recolección de Documentos

En este modulo es importante la verificación de la información testeada y perteneciente a varios niveles de lo que se considera seguridad de la información. La cantidad de tiempo otorgado para la búsqueda y extracción de la información depende de la complejidad de la red de la UCLV y la longitud de tiempo planeado para el test. No obstante, mucho tiempo no siempre significa más información pero puede eventualmente llevar a partes claves del rompecabezas de la seguridad.

1. Examinar las bases de datos Web y los caches pertenecientes a objetivos y personal clave de la organización.

2. Investigar personas claves vía páginas personales, curriculums publicados, afiliaciones organizacionales, información de directorios, datos de compañías, y el registro electoral.

3. Recopilar direcciones de email de la organización y direcciones personales de personas claves.

4. Buscar en las bases de datos laborales por niveles tecnológicos requeridos necesarios que tiene la organización.

5. Buscar en los grupos de noticias referencias y publicaciones de la organización y personas claves.

6. Buscar en los documentos códigos ocultos o revisión de datos.

Resultados Esperados:

- Un perfil de la organización
- Un perfil de los empleados
- Un perfil de la red de la organización
- Un perfil de las tecnologías de la organización
- Un perfil de los socios, alianzas y estrategias de la organización

2.4 Seguridad de los procesos

2.4.1 Prueba de Solicitud

Este es un método de obtener privilegios de acceso a una organización y sus activos preguntando al personal de entrada usando las comunicaciones como un teléfono, e-mail, chat, boletines, desde una posición "privilegiada" fraudulenta. El personal de entrada son quienes tienen la autoridad para dar privilegios de acceso a otros. Conocido también como Ingenieria social es la técnica que se utiliza para obtener información confidencial o credenciales a partir de los medios antes mencionados, en este punto se pretende evaluar la cultura informática de los usuarios a fin de conocer los riesgos en este sentido.

1. Seleccionar una persona de entrada desde la información ya obtenida sobre el personal
2. Examinar los métodos de contacto con la persona de entrada desde el objetivo de la organización
3. Obtener información acerca de la persona de entrada (posición, hábitos, preferencias)
4. Contactar la persona de entrada y solicitar información desde una autoridad o posición privilegiada
5. Obtener información desde la persona de entrada
6. Enumerar cantidad de información privilegiada obtenida

Resultados Esperados:

- Lista de los métodos de código de acceso
- Lista de los códigos validos
- Nombres de las personas de entrada
- Métodos de obtención de esta información

- Lista de la información obtenida

2.4.2 Prueba de Sugerencia Dirigida

Este es un método de enumeración de puntos de acceso privilegiados a una organización y sus activos provocando a hablar mediante los medios de comunicaciones tal como: el teléfono, e-mail, chat, boletines a una ubicación fuera la organización desde una posición "privilegiada" fraudulenta. Esta técnica requiere una "ubicación" para la persona a provocar a hablar tal como una pagina web, una dirección de e-mail. Esta prueba puede realizarse a través de las técnicas de ingenieria social al personal con información sobre estos activos.

1. Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
2. Examinar los métodos de contacto a las personas de la organización objetivo
3. Invitar a las personas a usar / visitar una ubicación
4. Obtener información de los visitantes
5. Enumerar los tipos y cantidad de información privilegiada obtenida

Resultados Esperados:

- Lista de los puntos de acceso
- Lista de las direcciones IP internas
- Métodos de obtención de esta información
- Lista de la información obtenida

2.4.3 Prueba de las Personas Confiables

Este es un método de usar la posición de confianza tales como las de un estudiante, trabajador, amigo o hija de un usuario para inducir a la persona interna a la revelación de información concerniente a la organización objetivo.

Este modulo puede ser realizado mediante cualquier forma de comunicación o en persona.

1. Seleccionar una persona o personas a partir de la información ya obtenida sobre el personal
2. Examinar los métodos de contacto a las personas de la organización objetivo
3. Contactar a la persona interna desde una posición de confianza
4. Obtener información de la persona interna
5. Enumerar los tipos y cantidad de información privilegiada obtenida

Resultados Esperados:

- Lista de las personas de confianza
- Lista de las posiciones de confianza
- Métodos de obtención de esta información
- Lista de la información obtenida

2.5 Seguridad en las tecnologías de Internet

2.5.1 Logística y Controles

El propósito de este módulo es reducir los falsos positivos y negativos realizando los ajustes necesarios en las herramientas de análisis.

Comprobaciones de Error

1. Examinar la ruta a la red objetivo en busca de paquetes TCP perdidos.
2. Examinar la ruta a la red objetivo en busca de paquetes UDP perdidos.
3. Examinar la ruta a la red objetivo en busca de paquetes ICMP perdidos.
4. Medir el tiempo utilizado en el recorrido TCP de los paquetes.
5. Medir la latencia TCP a través de conexiones TCP.
6. Medir el porcentaje de paquetes aceptados y respondidos por la red objetivo.
7. Medir la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

Enrutamiento

8. Examinar el camino de enrutamiento al objetivo desde los sistemas de ataque.
9. Examinar el camino de enrutamiento para el ISP del objetivo.
10. Examinar el camino de enrutamiento para el Vendedor de Trafico Principal del ISP

objetivo

Resultados Esperados:

- Discrepancias por el Ancho de Banda usado en el Prueba
- Paquetes TCP perdidos
- Paquetes UDP perdidos
- Paquetes ICMP perdidos
- Problemas de enrutamiento
- Trafico de Enrutamiento del ISP y Vendedores de Tráfico

2.5.2 Sondeo de Red

El sondeo de red sirve como introducción a los sistemas a ser analizados. Se podría definir mejor como una combinación de recolección de datos, obtención de información y política de control. A pesar que a menudo es recomendable desde un punto de vista legal definir exactamente y contractualmente los sistemas a analizar, puede ser que no pueda empezar con los nombres de sistema o IPs en concreto. En ese caso es necesario sondear y analizar. La clave es encontrar el número de sistemas alcanzables que deben ser analizados, sin exceder los limites legales de lo que se quiere analizar. Por lo tanto, el sondeo de red es simplemente una forma de empezar un test; otra forma sería recibir el rango de direcciones IP a comprobar. En este módulo, no se realiza ningún tipo de intrusión directamente en los sistemas.

A pesar de no ser realmente un módulo en la metodología, el sondeo de red es un punto de partida. Muy a menudo se detectan más hosts durante el test. Hay que tener en cuenta que los hosts descubiertos posteriormente pueden ser añadidos en las pruebas como un subconjunto de los sistemas definidos y a menudo solamente con el permiso o colaboración del equipo de seguridad interna de la intranet de la UCLV.

Respuestas del Servidor de Nombres.

1. Examinar la información del registro de dominio en busca de servidores.
2. Encontrar el propietario del bloque de direcciones IP.

3. Consultar los servidores de nombres primario, secundario y del ISP en busca de hosts y subdominios.

Examinar la pared externa de la red.

4. Usar múltiples trazas a la puerta de enlace para definir los routers y segmentos externos de la red.

Examinar pistas de la organización a analizar.

5. Inspeccionar los logs del servidor web y los logs de intrusión en busca de eventos de los sistemas de la organización a analizar.

6. Inspeccionar mensajes de grupos de noticias y listas de distribución en busca de eventos de los sistemas de la organización a analizar.

Filtración de información

7. Examinar el código fuente y scripts del servidor web en busca de servidores de aplicación y enlaces internos.

8. Examinar las cabeceras de los correos electrónicos, los mensajes devueltos y los destinatarios de las alertas y eventos del sistema de los servidores.

9. Buscar información sobre la organización a analizar en los grupos de noticias.

Resultados esperados:

- Nombres de Dominio
- Nombres de Servidores
- Direcciones IP
- Mapa de Red
- Información ISP / ASP
- Propietarios del Sistema y del Servicio
- Posibles limitaciones de la prueba

2.5.3 Identificación de los Servicios de Sistemas

El escaneo de puertos es la prueba invasiva de los puertos del sistema en los niveles de transporte y red. También se incluye aquí la validación de la recepción del sistema a protocolos tunelizados, encapsulados o de enrutamiento. En este módulo se deben enumerar los servicios de Internet activos o accesibles en la intranet de la UCLV, así como

traspasar el cortafuego con el objetivo de encontrar más máquinas activas. La pequeña cantidad de protocolos empleados aquí tiene el objetivo de resultar en una definición clara de los objetivos. Es por esto que algunos de los protocolos no aparecen. La prueba de diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los mismos. En la sección Referencias de Prueba aparece una lista más completa de protocolos.

Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP posibles (incluido el Puerto 0). En cualquier caso, no siempre es necesario comprobar todos estos puertos en cada sistema. Los puertos que son importantes para la prueba según el servicio que ofrecen se listan con las tareas del módulo. Otros números de puertos empleados en los escaneos se deben obtener de bases de datos referenciadas en webs de proyectos de intrusión tales como www.dshield.org.

Una vez que los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. En algunos casos, más de una aplicación puede encontrarse detrás de un servicio donde una aplicación es la que realmente escucha en dicho puerto y las otras se consideran componentes de la aplicación que escucha.

Tras la identificación de los servicios de la red de la UCLV, el siguiente paso es identificar el sistema mediante las pruebas con el fin de obtener respuestas que puedan distinguir su sistema operativo y su versión.

Enumeración de sistemas

1. Recoger respuestas de broadcast desde la red
2. Intentar traspasar el cortafuego con valores estratégicos de TTLs (Firewalking) para todas las direcciones IP.
3. Emplear ICMP y resolución inversa de nombres con el objetivo de determinar la existencia de todos los sistemas en la red.
4. Emplear paquetes TCP con puerto origen 80 y el bit ACK activo en los puertos de

destino 3100-3150, 1001-10050, 33500-33550 y 50 puertos aleatorios por encima del 35000 para todos los sistemas de la red.

5. Emplear paquetes TCP fragmentados en orden inverso mediante escaneos FIN, NULL y XMAS en los puertos destino 21, 22, 25, 80 y 443 para todos los servidores de la red.

6. Usar escaneos TCP SYN sobre los puertos 21, 22, 25, 80 y 443 para todos los servidores de la red.

7. Emplear intentos de conexión a DNS para todos los servidores de la red.

8. Emplear FTP y Proxies para relanzar los escaneos al interior de la DMZ para los puertos 22, 81, 111, 132, 137 y 161 para todos los servidores de la red.

Enumeración de Puertos

9. Usar escaneos SYN TCP (Half-Open) para enumerar puertos abiertos, cerrados o filtrados para aquellos puertos TCP utilizados por defecto en el test, en todos los servidores de la red.

10. Usar scaneos TCP full connect para escanear todos los puertos por encima del 1024 en todos los servidores de la red.

11. Usar escaneos TCP fragmentados en orden inverso para enumerar puertos y servicios para el conjunto de puertos definidos en el Apéndice B por defecto para todos los servidores de la red.

12. Usar escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP por defecto si UDP no está siendo filtrado. [Recomendación: primero comprobar el sistema de filtrado para un subconjunto de puertos UDP.]

Verificación de Respuestas para Varios Protocolos

13. Verificar y examinar el uso de tráfico y protocolos de enrutamiento.

14. Verificar y examinar el uso de protocolos no estándar.

15. Verificar y examinar el uso de protocolos cifrados.

Verificación de Respuestas a Nivel de Paquete

16. Identificar la predictabilidad de las secuencias TCP.

17. Identificar la predictabilidad de los números de secuencia TCP ISN.

18. Identificar la predictabilidad de la Generación de Secuencia IPID.

19. Identificar el up-time del sistema.

Identificación de Servicios

20. Relacionar cada puerto abierto con un servicio y protocolo.

21. Identificar el nivel de parcheado del sistema a partir de su up-time.

22. Identificar la aplicación tras el servicio y su nivel de parcheado empleando los banners o la Identificación de huellas.

23. Verificar la aplicación y su versión en el sistema.

24. Localizar e identificar el remapeo de servicios o la redirección de sistemas.

25. Identificar los componentes de los servicios en escucha.

26. Usar peticiones propias de Troyanos y servicios UDP en todos los sistemas de la red.

Identificación de Sistemas

27. Examinar las respuestas de los sistemas para determinar el tipo de sistema operativo y su nivel de parcheado.

28. Examinar las respuestas de las aplicaciones para determinar su sistema operativo y su nivel de parcheado.

29. Verificar la predicción de secuencia TCP para todos los servidores de la red.

30. Busque ofertas de trabajo donde obtener información sobre los servidores y aplicaciones del objetivo.

31. Buscar en boletines técnicos y grupos de noticias información sobre los servidores y las aplicaciones del objetivo.

32. Relacionar la información recopilada con las respuestas de los sistemas para ajustar los resultados.

Resultados Esperados:

- Puertos abiertos, cerrados y filtrados
- Direcciones IP de los sistemas activos
- Direccionamiento de los sistemas de la red interna
- Lista de los protocolos descubiertos de tunelizado y encapsulado
- Lista de los protocolos descubiertos de enrutado soportados
- Servicios activos
- Tipos de Servicios

- Tipo y nivel de parcheado de las Aplicaciones de los Servicios
- Tipo de Sistema Operativo
- Nivel de parcheado
- Tipo de Sistema
- Lista de sistemas activos
- Mapa de la red

2.5.4 Revisión de Privacidad

La revisión de privacidad se centra en como se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a los usuarios de la red.

Para estas pruebas es necesario entender la diferencia entre información privada e información personal: por información privada entendemos aquella información que generalmente sólo es conocida por la persona a la que pertenece y la autoridad que ha recopilado dichos datos. Por otro lado, información personal es aquella información que describe una persona o su estilo de vida, como por ejemplo la fecha de nacimiento, color de pelo, ojos, nombre de los miembros de su familia, banco que utiliza, nombre de sus mascotas, preferencias sexuales, religión, o color favorito.

Adicionalmente, la información de identificación personal es aquella información que permite derivar la identidad de una persona por sí sola o en conjunto. Podría ser un nombre de persona o un número de identificación.

Política

1. Identificar la política de privacidad pública
2. Identificar los formularios web
3. Identificar el tipo y la localización de la base de datos donde se almacenan los datos recolectados
4. Identificar los datos recolectados por la organización
5. Identificar la localización de los datos almacenados

6. Identificar los tipos de cookies

7. Identificar el tiempo de expiración de las cookies

8. Identificar la información guardada en las cookies

9. Verificar los métodos de cifrado de las cookies

10. Identificar la claridad de la información relacionada con opt-out

11. Identificar la facilidad de usar opt-out

12. Identificar los gifs de publicidad y bugs web en los servicios web y en los correos electrónicos

13. Identificar la localización de los gifs de publicidad

14. Identificar los bugs de web recogidos y devueltos al servidor

Difamación y Falsa Divulgación

15. Identificar las personas, organizaciones e instituciones reales a las que corresponden realmente las ficticias.

16. Identificar personas u organizaciones retratadas de forma negativa.

Apropiación

17. Identificar personas, organizaciones o materiales que por ellos mismos o por similitud son utilizados comercialmente en sitios web o anuncios publicitarios.

Revelación de Datos Privados

18. Identificar información de empleados, organizaciones o materiales que contienen información privada.

Resultados Esperados:

- Listado de cualquier revelación
- Listado de las inconsistencias entre la política que se ha hecho
- pública y la práctica actual que se hace de ella
- Listado de los sistemas involucrados en la recolección de datos
- Listado de las técnicas de recolección de datos
- Listado de los datos recolectados

2.5.5 Búsqueda y Verificación de Vulnerabilidades

La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en los servidores de la Red de la UCLV o en la propia Red. La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe. Esta investigación incluye la búsqueda en bases de datos online y listas de correo relativas a los sistemas y redes que se están auditando. No se debe limitar la búsqueda a la web, también se debe considerar la utilización del IRC, grupos de noticias, y sitios FTP underground.

La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Aunque muchos escáneres automáticos están actualmente tanto en el mercado como en el mundo underground, es importante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen actualmente en el mundo underground. No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida de la red. La búsqueda manual de vulnerabilidades hace referencia a las personas que delante del ordenador utilizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo.

1. Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
2. Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.
3. Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
4. Intentar ajustar vulnerabilidades a servicios.
5. Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
6. Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.

7. Identificar todas las vulnerabilidades relativas a las aplicaciones.

8. Identificar todas las vulnerabilidades relativas a los sistemas operativos.

9. Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivos.

10. Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.

11. Verificar todos los positivos (Se debe tener en cuenta el contrato firmado con la organización objetivo en el caso de estar intentando penetrar o si se puede llegar a provocar una denegación de servicio).

Resultados Esperados:

- Tipo de aplicación o servicio por vulnerabilidad
- Niveles de parches de los sistemas y aplicaciones
- Listado de posibles vulnerabilidades de denegación de servicio
- Listado de áreas securizadas a través de ocultación o acceso visible
- Listado de vulnerabilidades actuales eliminando falsos positivos
- Listado de sistemas internos o en la DMZ
- Listado de convenciones para direcciones de e-mail y nombres de servidores
- Mapa de red

2.5.6 Prueba de Aplicaciones de Internet

Un test de Aplicaciones de Internet emplea diferentes Técnicas de prueba de Software para encontrar “fallos de seguridad” en aplicaciones cliente / servidor de un sistema desde Internet. En este módulo, se refiere a aplicaciones cliente / servidor que sean desarrolladas por los administradores de sistema con propósitos de la red de la UCLV y programadas con cualquier tecnología y lenguaje de programación. Como las Aplicaciones Web para el sistema de control docente, o el sistema de postgrado realizadas por el grupo de programadores de la dirección de informatización de la UCLV. Tests como "Caja Negra" y/o "Caja Blanca" pueden ser utilizados en este módulo.

Re-Ingeniería

1. Descomponer o Deconstruir los códigos binarios, si es posible.

2. Determinar las Especificaciones de Protocolo de la Aplicación Cliente / servidor

3. Adivinar la lógica del programa de los mensajes de error/debug en las salidas del programa y en el rendimiento y comportamiento del programa.

Autenticación

4. Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones.

5. A ser posible, buscar credenciales de cuentas válidas por fuerza bruta.

6. Saltarse el sistema de autenticación con una validación cambiada.

7. Saltarse el sistema de autenticación reproduciendo información de la autenticación

8. Determinar la lógica de la aplicación para mantener las sesiones de autenticación – número (consecutivo) de intentos fallidos, intentos fuera de tiempo, etc.

9. Determinar las limitaciones de control de acceso en las aplicaciones - permisos de acceso, duración de las sesiones, tiempo inactivo.

Administración de Sesiones

10. Determinar la Información de Administración de Sesiones – numero de sesiones concurrentes, Autenticaciones basadas en IP, Autenticación basada en roles, Autenticación basada en Identidad, uso de Cookies, ID de sesión dentro de las secuencias de codificación de la URL, ID de sesión en campos HTML ocultos.

11. Adivinar la secuencia y formato de la ID de sesión.

12. Determinar si la ID de sesión esta formada con información de direcciones IP; mirar si la misma información de sesión puede ser recuperada y reutilizada en otra máquina.

13. Determinar las limitaciones de mantenimiento de sesión - uso del ancho de banda, limitaciones de bajadas / subidas de archivos, limitaciones en transacciones.

14. Reunir bastante información con URL's exactas, instrucciones exactas, secuencias de acción / saltos de secuencia y/o omisiones de las páginas.

15. Reunir información sensible a partir de ataques Hombre-en-el-Medio.

16. Inyectar excesa/falsa información con técnicas de Hijacking.

17. Reproducir la información reunida para engañar a las aplicaciones.

Manipulación de la información de entrada.

18. Encontrar las limitaciones de las variables definidas y de los protocolos - longitud de datos, tipo de datos, formato de la estructura.

19. Usar cadenas largas de caracteres para encontrar vulnerabilidades de desbordamientos de memoria en las aplicaciones.

20. Concatenar comandos en las cadenas de entrada de las aplicaciones.

21. Inyectar comandos SQL en las entradas de cadenas de caracteres de aplicaciones Web basadas en bases de datos.

22. Examinar vulnerabilidades "Cross-Site Scripting" en las aplicaciones web del sistema.

23. Examinar accesos a directorios / ficheros no autorizados con directorios / rutas trasversales en las entradas de cadenas de caracteres de las aplicaciones.

24. Usar cadenas específicas de codificación URL y/o codificación Unicode para saltarse los mecanismos de validación de las aplicaciones.

25. Ejecutar comandos remotos a través de "Server Side Include".

26. Manipular el estado de las cookies (session/persistent) para tirar o modificar la lógica dentro de las aplicaciones web "server-side".

27. Manipular los campos variables (ocultos) en los formularios HTML para tirar o modificar la lógica en las aplicaciones web "server inside".

28. Manipular las variables "Referrer", "Host", etc. del protocolo HTTP para tirar o modificar la lógica en las aplicaciones web "server inside".

29. Usar información de entrada ilógica/ilegal para testear las rutinas de error de la aplicación y encontrar mensajes de error / depuración que sean útiles.

Manipulación de la Información de salida

30. Recuperar información importante / comprometedora guardadas en las cookies.

31. Recuperar información importante / comprometedora en la caché de la aplicación cliente.

32. Recuperar información importante / comprometedora guardada en los objetos con número de serie.

33. Recuperar información importante/comprometedora guardada en los archivos temporales y objetos.

Filtración de información

34. Buscar información utilizable en campos ocultos de variables en formularios HTML y comentarios en los documentos HTML.

35. Examinar la información contenida en los banners de la aplicación, instrucciones de uso, mensajes de bienvenida, mensajes de despedida, mensajes de ayuda y mensajes de error / depuración

Resultados Esperados:

- Lista de Aplicaciones
- Lista de los Componentes de las Aplicaciones
- Lista de las Vulnerabilidades de las Aplicaciones
- Lista de los Sistemas Confiados por las Aplicaciones

2.5.7 Enrutamiento

Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la intranet UCLV e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado. La protección también debe estar diseñada para restringir el flujo de salida de ciertos tipos de tráfico. Los Router están siendo cada vez más complejos y algunos tienen propiedades desconocidas para el auditor y en ocasiones para los propios especialistas de la red de la UCLV. En la universidad existe un backbone de fibra óptica soportada sobre dispositivos de conmutación de nivel 3 del propietario allied telesync los cuales constituyen los principales dispositivos de enrutamiento, además de dos router cisco para el enlace a Internet y para el acceso remoto.

El Router y sus características:

1. Verificar el tipo de router con información reunida de la obtención de Inteligencia.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
3. Verificar las intrusiones con opciones TTL estratégicas en los paquetes, (Firewalking) hecho en el módulo de escaneo de puertos. Verificar la configuración de las ACL's del router

4. Testear la ACL del router en contrade las políticas de seguridad y en contra de la regla "Deny All".

5. Verificar si el router está filtrando el tráfico de la red local hacia afuera.

6. Verificar que el router esté haciendo detección de direcciones falsas.

7. Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.

8. Testear las capacidades externas del router desde el interior.

9. Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.

10. Cuantificar la habilidad del router para manejar paquetes grandes.

11. Cuantificar la habilidad del router para manejar fragmentos coincidentes como los usados en ataques del tipo TEARDROP.

Resultados Esperados:

- Tipo de Router y Propiedades implementadas
- Información del router como servicio y como sistema
- Perfil de la política de seguridad de una red a partir de la ACL
- Lista de los tipos de paquetes que deben entrar en la red
- Mapa de las respuestas del router a varios tipos de tráfico
- Lista de los sistemas vivos encontrados

2.5.8 Prueba de Sistemas Confiados

El propósito de las pruebas de sistemas confiados es afectar la presencia en Internet planteándose como una entidad confiada en la red. El escenario de prueba es a veces más teoría que práctica, y en realidad mas que oscurecer la frontera entre un Test de Vulnerabilidad y un Prueba de Cortafuegos / ACLS, es dicha frontera.

1. Verificar las relaciones determinadas en la obtención de Inteligencia, Testo de Aplicaciones y Prueba de Servicios.

2. Testear las relaciones entre varios sistemas a través de provocación de eventos "event triggering" o engaño de origen.

3. Verificar que los sistemas puedan ser engañados.

4. Verificar qué aplicaciones pueden ser engañados.

Resultados Esperados:

- Mapa de los sistemas dependientes de otros sistemas
- Mapa de las aplicaciones con dependencias a otros sistemas
- Tipos de vulnerabilidades que afectan a los sistemas de confianzas y aplicaciones

2.5.9 Prueba de Control de Acceso

El cortafuego controla el flujo del tráfico de la intranet UCLV, la DMZ, e Internet. Opera en una política de seguridad y usa ACL's (Listas de Control de Acceso). Este módulo está diseñado para asegurar que solo lo que debe estar expresamente permitido puede ser aceptado dentro de la red, todo lo demás debe ser denegado. De manera adicional, el auditor debe entender la configuración cortafuego y cartografía que se provee entre los servidores y los servicios que hay detrás. Repasando los logs necesarios de los servidores para verificar los tests desempeñados en presencia de Internet, especialmente en casos donde los resultados de los tests no son inmediatamente evidentes para el auditor. Algunos que son desconocidos son destinados para el analista, quien no ha revisado los logs.

El Cortafuegos y sus características.

1. Verificar el tipo de router con información reunida de la Obtención de Inteligencia.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
3. Verificar las intrusiones con opciones TTL estratégicas en los paquetes, (Firewalking) hecho en el módulo de escaneo de puertos.

Verificación de la configuración de las ACL

4. Testear la ACL del cortafuego en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".
5. Verificar si el cortafuego está filtrando el tráfico de la red local hacia afuera.
6. Verificar que el cortafuego esté haciendo detección de direcciones orígenes falsas.
7. Verificar las intrusiones desde un escaneo inverso en el módulo de Escaneo de Puertos.
8. Testear las capacidades externas del cortafuego desde el interior.
9. Determinar el éxito de los métodos de identificación de cortafuegos a través de los

distintos paquetes de respuesta.

10. Verificar la posibilidad de escanear usando técnicas ocultas SYN para enumeración a través del cortafuego.

11. Verificar la posibilidad de escanear para enumeración usando puertos orígenes específicos.

12. Cuantificar la habilidad del cortafuego para manejar fragmentos superpuestos como los usados en ataques del tipo TEARDROP.

13. Cuantificar la habilidad del cortafuego para manejar fragmentos de paquetes diminutos.

14. Testear la habilidad del cortafuego para manejar series de paquetes SYN entrantes (inundación)

15. Testear la respuesta del cortafuego a paquetes con la bandera RST activada.

16. Testear el mantenimiento del cortafuego con paquetes UDP estándar.

17. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando paquetes ACK.

18. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando paquetes FIN.

19. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando paquetes NULL.

20. Verificar la habilidad del cortafuego para protegerse de varias técnicas midiendo el tamaño de ventana en el paquete (WIN).

21. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando todas las banderas activadas (XMAS).

22. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando IPIDs.

23. Verificar la habilidad del cortafuego para protegerse de varias técnicas usando protocolos encapsulados.

24. Cuantificar la robustez del cortafuego y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP ininterrumpidas.

25. Cuantificar la robustez del cortafuego y su susceptibilidad a los ataques de denegación de servicios con conexiones TCP temporales.

26. Cuantificar la robustez del cortafuego y su susceptibilidad a los ataques de denegación

de servicios con data gramas UDP.

27. Cuantificar la respuesta del cortafuego a todos los tipos de paquetes ICMP.

Revisión de Registros del Cortafuegos

28. Testear el proceso de registro del cortafuego.

29. Verificar escaneos TCP y UDP en los registros del servidor.

30. Verificar escaneos de vulnerabilidades automatizados.

31. Verificar deficiencias de registros de servicios.

Resultados Esperados:

- Información en el firewall como servicio y como sistema
- Información de las características implementadas en el firewall
- Perfil de la política de seguridad de la red a partir de la ACL
- Lista de los tipos de paquetes que deben entrar en la red
- Lista de tipos de protocolos con acceso dentro de la red
- Lista de los sistemas "vivos" encontrados
- Lista de paquetes, por número de puerto, que entran en la red
- Lista de protocolos que han entrado en la red
- Lista de rutas sin monitorizar dentro de la red

2.5.10 Prueba de Sistema de Detección de Intrusos

Este test está enfocado al rendimiento y susceptibilidad del IDS implementado en la Red UCLV. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunos de estos tests están relacionados con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos tests. Repasar los registros del servidor es necesario para verificar que los tests realizados en presencia en Internet, especialmente en los casos donde el resultado de éstos no es inmediatamente evidentes para el auditor. Algunos que son desconocidos son destinados para el analista, quien no ha revisado los registros y alertas.

El IDS y sus características

1. Verificar el tipo de IDS con información recogida de la Inteligencia de Información

2. Determinar la esfera de protección o influencia.

3. Testear los estados de alarma del IDS.

4. Testear los parámetros de sensibilidad de las firmas pasado 1 minuto, 5 minutos, 60 minutos, y 24 horas.

Prueba de configuración IDS

5. Testear la configuración del IDS para reacciones múltiples, ataques variados (inundación).

6. Testear la configuración del IDS para reacciones como URLs manipuladas y rutinas de explotación.

7. Testear la configuración del IDS para reacciones ante cambios de velocidad al enviar paquetes.

8. Testear la configuración del IDS para reacciones ante cambios aleatorios de velocidad durante un ataque.

9. Testear la configuración del IDS para reacciones ante cambios aleatorios de protocolos durante un ataque.

10. Testear la configuración del IDS para reacciones ante cambios aleatorios de origen durante un ataque.

11. Testear la configuración del IDS para reacciones ante cambios de puerto de origen.

12. Testear en el IDS, la habilidad de manejar paquetes fragmentados.

13. Testear en el IDS, la habilidad de manejar métodos de ataques de sistemas específicos.

14. Testear los efectos y reacciones del IDS. Una dirección IP contra varias direcciones.

15. Encontrar alertas de IDS sobre escaneos de vulnerabilidades.

16. Encontrar alertas de IDS sobre descifrado de contraseñas.

17. Encontrar alertas de IDS de pruebas de sistemas confiados.

Resultados Esperados:

- Tipo de IDS
- Nota del rendimiento de los IDS bajo una sobrecarga
- Tipo de paquetes eliminados o no barridos por el IDS
- Tipo de protocolos eliminados o no barridos por el IDS
- Nota del tiempo de reacción y tipo del IDS

- Nota de la susceptibilidad del IDS
- Mapa de reglas del IDS
- Lista de falsos positivos del IDS
- Lista de alarmas perdidas del IDS
- Lista de rutas no monitorizadas en la red

2.5.11 Prueba de Medidas de Contingencia

Las medidas de contingencia dictan el manejo de las catástrofes predecibles como programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados. Lo cual se traduce en un análisis exhaustivo del plan de contingencias aplicado a la intranet de la UCLV, el cual constituye un documento oficial de la red.

1. Medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas.
2. Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos están protegidos desde este subsistema.
3. Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.
4. Verificar recursos innecesarios.
5. Verificar las propiedades del sistema de contingencia.
6. Verificar la detección de medidas presentes para la detección de accesos 'no comunes' a los recursos 'necesarios'.
7. Medidas de respuestas y procesos contra el "sap 27"
8. Medidas de configuración del sistema.

Resultados Esperados:

- Definición de las capacidades Anti-Troyano
- Definición de las capacidades Anti-Virus
- Identificación de las Medidas de Contingencia de Escritorio
- Identificación de las Debilidades de Contingencia de Escritorio

- Lista de recursos de contingencia

2.5.12 Descifrado de Contraseñas

Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizadas, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos. Este módulo no debe ser confundido con el de recuperación de contraseñas vía escucha de texto por canales libres, es más sencillo de entender que un trastorno del sistema de seguridad, pero solo que tiene mecanismos de autenticación sin cifrar, nada de debilidades en contraseñas. Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que exploten los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos. Este puede ser un sistema para obtener acceso a un sistema inicialmente, quizá sea siempre con acceso de administrador o root, pero solo con fines educativos. Más allá de la predictibilidad manual de las contraseñas, a través de combinaciones por defecto o simples, se puede hacer fuerza bruta de contraseñas para aplicaciones como Telnet, usando scripts o programas personalizados, al menos no es viable por valores de espera agotados, siempre con aplicaciones de fuerza bruta con multiconexión (simulando el multihilo).

Una vez entrado con privilegios de root o administrador en un sistema el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales gracias a los usuarios cuyas contraseñas sean coincidentes en múltiples sistemas. Es una técnica válida que puede ser usada por influencia del sistema a través de un test de seguridad. L Descifrados de contraseñas minuciosos pueden ser realizados como un ejercicio de simple y debe ser subrayada la necesidad de algoritmos criptográficos fuertes para contraseñas de almacenamiento de sistemas de llave, también subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática, o módulos del tipo PAM.

1. Obtener el fichero de contraseñas desde el sistema que guarda nombres de usuario y

contraseña

1 Para sistemas Unix, ha de estar en /etc/passwd o/y /etc/shadow.

2 Para sistemas Unix que tienen que realizar autenticaciones SMB, puede encontrar las contraseñas de NT en /etc/smbpasswd.

3 Para sistemas NT, ha de estar en /winnt/repair/Sam._ (u otra, más difícil de obtener variantes)

2. Arranque un ataque automatizado de diccionario al fichero de contraseñas.

3. Arranque un ataque de fuerza bruta al fichero de contraseñas.

4. Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.

5. Arranque Programas automatizados de descifrado en ficheros cifrados que haya encontrado (como documentos PDF o Word) como intento de recopilar más datos y subrayar la necesidad de un cifrado del sistema o de documentos más fuerte.

6. Verificar la edad de las contraseñas.

Resultados Esperados:

- Ficheros de Contraseñas descifrados o no descifrados
- Lista de cuentas, con usuario o contraseña de sistema
- Lista de sistemas vulnerables a ataques de descifrado de contraseñas
- Lista de archivos o documentos vulnerables a ataques de descifrado de contraseñas
- Lista de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas

2.5.13 Prueba de Denegación de Servicios

La Denegación de Servicios (DoS) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos.

Es muy importante que los tests de DoS estén autorizados por los administradores de la UCLV y sea monitorizada a nivel privado. Inundación y ataques DoS Distribuidos (DDoS) que no estén específicamente comprobados pueden comprometer la estabilidad de los

sistemas. Los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo.

1. Verificar que las cuentas administrativas y los archivos y recursos del sistema están seguros apropiadamente y todos los accesos están concedidos con "Mínimo Privilegio".
2. Comprobar las restricciones de sistemas expuestas a redes sin confianza.
3. Verificar que los puntos de referencia están establecidos a partir de una actividad normal del sistema.
4. Verificar que los procedimientos están en un lugar que responde a una actividad irregular.
5. Verificar la respuesta a una información negativa SIMULADA (ataques propaganda)
6. Testear cargas de red y de servidor excesivas.

Resultados Esperados:

- Lista de puntos débiles en presencia de Internet incluidos los puntos individuales por averías
- Establecer un punto de referencia para un uso normal
- Lista de comportamientos de sistema por un uso excesivo
- Lista de sistemas vulnerables a DoS

2.5.14 Evaluación de Políticas de Seguridad

La política de seguridad descrita en este documento contiene políticas que delinean la reducción de riesgos en la Intranet UCLV con la utilización de tipos específicos de tecnologías. Esta estrategia puede ser también una forma de Listas de Controles de Acceso. Existen dos funciones a llevar a cabo: primero, la prueba de lo escrito contra el estado actual de las conexiones de la presencia en Internet y de otras conexiones no relacionadas a Internet; y segundo, asegurar que la política este incluida dentro de las justificaciones de la red UCLV.

Estas tareas exigen que las pruebas y verificación de vulnerabilidades sean hechas en su

totalidad y que todas las otras revisiones técnicas hayan sido llevadas a cabo. A menos que esto sea realizado, no es posible comparar los resultados con los lineamientos a lograr especificados por las políticas de seguridad, traducidos en medidas de protección del entorno operativo.

1. Comparar la política de seguridad contra el estado actual de la presencia en Internet.
2. *Aprobación de la Gerencia* – Busque cualquier signo que revele que la política está aprobada por la dirección de la institución. Sin esta aprobación, la política no tiene valor porque los usuarios no tienen la obligación de seguir las reglas establecidas en la política. Desde un punto de vista formal, se puede detener las investigaciones de la política de seguridad si ésta no es aprobada por la institución. Sin embargo, la prueba debería continuar para determinar cuán efectivas son las medidas de seguridad en el estado actual de la presencia en Internet.
3. Cerciórese de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos.
4. Identifique los procedimientos de manejo de incidentes para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada.
5. *Conexiones entrantes* – Verifique los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet -> DMZ, Internet -> red interna), y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos. Estos riesgos pueden ser permitidos en conexiones entrantes, típicamente SMTP, POP3, HTTP, HTTPS, FTP, VPNs y las correspondientes medidas como esquemas de autenticación, encriptación y Listas de Control de Acceso. Específicamente, las reglas que niegan el acceso con estado a la red interna generalmente no son alcanzadas por la implementación.
6. *Conexiones salientes* – Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet. Busque cualquier regla de conexiones salientes que no se corresponda con la implementación. Las conexiones salientes no pueden ser usadas para introducir código malicioso o revelar las

especificaciones de la red interna.

7. *Medidas de seguridad* – Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas. Aquellas pueden hacer uso de AVS, IDS, cortafuegos, DMZs, routers y las configuraciones / implementaciones adecuadas de acuerdo con los riesgos a contrarrestar.

8. Comprobar la política de seguridad contra el estado actual de las conexiones no relacionadas a Internet.

9. *Modems* – Debe existir una regla que indique que el uso de modems que no están especialmente asegurados está prohibido o al menos sólo permitido si los modems están desconectados cuando no se encuentran en uso, y configurados para no permitir el marcado. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

10. *Máquinas de Fax* – Debe existir una regla que indique que el uso de las máquinas de fax que pudiera permitir acceso desde el exterior a la memoria de las máquinas, está prohibido o al menos sólo permitido si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

11. *PBX* – Debe existir una regla que indique que la administración remota del sistema PBX está prohibida o al menos sólo permitida si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

12. Verifique que la política de seguridad establezca las medidas de contención y los tests de ingeniería social basados en el uso indebido de Internet por parte de los empleados, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad.

2.6 Seguridad física

2.6.1 Revisión de Perímetro

Este es un método para evaluar la seguridad física de la red UCLV y sus bienes, verificando las medidas de seguridad de su perímetro físico.

1. Trazar mapa del perímetro físico
2. Trazar mapa de las medidas de protección físicas (cercas, puertas, luces.)
3. Trazar mapa de las rutas de acceso y/o métodos físicos
4. Trazar mapa de las áreas no monitoreadas

Resultados Esperados:

- Mapa del perímetro físico
- Tipos de medidas de protección física
- Lista de áreas desprotegidas o insuficientemente protegidas

2.6.2 Revisión de monitoreo

Este es un método para descubrir puntos de acceso monitoreados, a la red UCLV y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico.

1. Enumerar los dispositivos de monitoreo
2. Trazar mapa de sitios protegidos y rutas recorridas
3. Trazar mapa de áreas monitoreadas y no monitoreadas
4. Examinar los dispositivos de monitoreo en búsqueda de limitaciones y vulnerabilidades
5. Examinar posibles ataques de denegación de servicio sobre los dispositivos de monitoreo

Resultados Esperados:

- Lista de puntos de acceso monitoreados
- Tipos de monitoreo
- Lista de puntos de acceso estándar y privilegiados, no monitoreados
- Lista de disparadores de alarmas

2.6.3 Evaluación de Controles de Acceso

Este es un método para evaluar los privilegios de acceso a la red UCLV y a sus bienes a través de puntos de acceso físicos.

1. Enumerar áreas de control de acceso
2. Examinar dispositivos y tipos de control de acceso

3. Examinar tipos de alarmas

4. Determinar el nivel de complejidad en un dispositivo de control de acceso

5. Determinar el nivel de privacidad en un dispositivo de control de acceso

6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades

7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

Resultados Esperados:

- Lista de puntos de acceso físicos
- Tipos de autenticación
- Tipos de sistemas de alarmas
- Lista de disparadores de alarmas

Capitulo 3: Herramientas de Seguridad

3.1 Herramientas para la Exploración de la Red

Puede realizarse búsquedas por DNS mediante los comandos del sistema nslookup o el más moderno dig; ambas utilidades originales del servidor de DNS bind. Las búsquedas pueden realizarse también desde Internet mediante un interfaz web: interfaz web para nslookup e interfaz web para dig. dnsdigger es un script en perl, diseñado para obtener el máximo posible de información de un servidor de DNS. Con NetCraft es posible realizar búsquedas de nombres de dominio similares , la cual cuenta con ofrecer protección anti-phishing y la posibilidad de ver quién es el dueño del bloque de red, lo cual es muy útil a la hora de elegir un hosting, al igual que con Whois Source.

El método más convencional es realizar las consultas desde web a las empresas de registro: Network Solutions para dominios internacionales, RIPE para Europa y NIC.es para España; así como interfaces Web de Whois como SamSpade.

Para la búsqueda de la ruta IP se utiliza traceroute o una interfaz visual como Visual Route o NeoTrace. IP-to-Country que permite averiguar el País a partir de la dirección IP, así como GeoBytes localiza el ISP. En el caso de Visual Route muestra la ruta de su conexión de internet, incluyendo la localización física de un servidor web, dirección IP o servidor de email en un Mapa Geográfico del Mundo, permitiendo obtener información acerca de un sitio web rápidamente a través de su navegador.

3.2 Identificación de Servicios y Sistemas

3.2.1 Adquisión de blancos

Una de las partes más costosas en tiempo para redes grandes es determinar los hosts que están vivos dentro del direccionamientos IP de tipo clases C o clases B. En estos casos se suele utilizar el nmap como un "bulk scanner", comprobando si un host está vivo o no mediante su respuesta a una solicitud icmp, o a una solicitud TCP por defecto al puerto 80 o a otros puertos. Nmap es una herramienta de código abierto para exploración de red y

auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan y qué tipo de filtros de paquetes o cortafuegos se están utilizando.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado.

El estado puede ser `open` (abierto), `filtered` (filtrado), `closed` (cerrado), o `unfiltered` (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. `Filtrado` indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra `abierto` o `cerrado`. Los puertos `cerrados` no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como `no filtrados` son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado `open|filtered` y `closed|filtered` cuando no puede determinar en cual de los dos estados está un puerto.

Sin embargo este tipo de escenarios no son tan fáciles: lo normal es que se trate de servidores con puertos abiertos en números de puerto no usuales, protegidos con un cortafuegos, con las respuestas de ICMP filtradas por las ACLs de los routers de acceso y con los accesos registrados IDS con posibilidades de bloqueo dinámico de IPs.

La herramienta más utilizada en este entorno es nmap. En este caso hay que optimizar los parámetros de nmap, para que evite la detección (envíos SYN) y se ajusten los puertos a comprobar; pues un escaneo completo de todos los puertos TCP y UDP puede llevar varias horas para una única máquina. Por ejemplo:

Nmap www.dvc.es -sS -SU -sV -O -p1-65535 -v -P0 -T4 -oN nmap-www.dvc.es

Total: 14350 segundos

Nmap www.ausejo.net -sS -SU -sV -O -p1-65535 -v -P0 -T4 -0oN nmap-www.ausejo.net

Sólo TCP: 1666 segundos

Total: 74509 segundos

3.3 Identificación de Sistemas Operativos

Las técnicas de detección remota de sistemas operativos se basan en analizar cómo ante determinadas solicitudes de red, documentadas o no en los estándares del protocolo, el sistema responde con una serie de características, frecuentemente valores en los campos del protocolo de red, en las cuales pueden ser utilizadas las herramientas nmap, hping2, SING.

También existen herramientas de detección remota para Windows. Entre las más conocidas se encuentran MingSweepr (que necesita modificar el parámetro TCP DisableUserTOSSetting), Winfingerprint y osfinger. Súper scanner v4.0 es un escaneador pequeño y sencillo de usar bajo Windows.

Actualmente, una de las herramientas más modernas es SYnscan, la cual se basa en la firma de todos y cada uno de los campos de la pila TCP/IP de las respuestas de red recibidas. Se ejecuta bajo linux y necesita de las librerías libdnet, libevent y libpcap.

3.4 Identificación Pasiva de Sistemas

Existe otra técnica denominada Passive OS Fingerprinting, basada en determinar el Sistema Operativo en base a la captura no intrusiva de paquetes. Dentro de las herramientas de detección pasiva de Sistemas se encuentran NeVO, RNA, Ettercap, ARCHAEOPTERYX, Prelude, pfprintd, K9, DISCO y p0f 2.0

3.5 Barrido de Puertos

Existe gran cantidad de escaneadores de puertos, siendo sin duda Nmap el escaneador Open Source por excelencia. Dispone de múltiples opciones, además de implementar el barrido de tipo idle mediante una máquina zombie. También existe una versión para Windows y

una modificación nmapsql que permite almacenar en base de datos para poder realizar escaneos distribuidos. Pero existen otros escaneadores como Angry IP Scanner es un escaneador interno para Windows que detecta la dirección MAC, el nombre del grupo y del usuario activo en ese momento.

Hay que tener en cuenta el cache-proxy de puertos abiertos cuando se realizan escaneos con routers ADSL, que puede generar falsos positivos; sobre todo en los puertos 80 (HTTP), 1755 (Streaming de Microsoft Windows Media) y 554 (Streaming de Real Networks y Quicktime).

3.6 Identificación de Servicios

Respecto a la identificación de servicios, lo normal es que el dispositivo a auditar esté atendiendo solicitudes de conexión en los puertos estándar, que aparecen listados en el directorio `/etc/services` en sistemas Unix o en `C:\WINDOWS\system32\drivers\etc\services` en sistemas Windows, en formato `< nombre de servicio > < tabulador > < número de puerto > / < protocolo > < [alias] > < [#comentario] >`. Se recomienda actualizar dicho fichero, incluso sobreescribirlo, con la última versión del fichero de asignaciones de números de puerto oficiales de la IANA la cual es la Agencia de Asignación de Números de Internet. Era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

3.6.1 Amap

También es posible que existan servicios con puertos abiertos escuchando con numeración no estándar. En este caso es muy útil la herramienta unix THC-Amap 4.5**,** esta es una herramienta que permite realizar una detección de protocolos de aplicación rápida y segura independientemente del puerto de destino TCP o UDP. Al escanear un host con amap, detectando que tipo de aplicaciones están escuchando en cada puerto aunque estas no estén en su puerto predeterminado. que comprueba servicios y aplicaciones independientemente de su número de puerto e identifica a qué servicio corresponde en base a la respuesta de una simulación de solicitudes. Funciona con servicios no ASCII (telnet, smtp y pop3.) al

basarse en triggers. Incluye la utilidad amapcrap para identificar servicios que no muestran ninguna salida aparente, mediante el envío de solicitudes aleatorias no estándares. Aunque no existe una versión Windows de AMAP y en el readme aparece que lo hará en fecha lejana, la versión 2.7 (la anterior a la 4.0) podía compilarse con Cygwin. La sintaxis es

Amap [Parámetros] IPOBJETIVO PUERTOINICIAL [-PUERTOFINAL]

Aunque pueden automatizarse las tareas de amap mediante ficheros de entrada de nmap:

Nmap -sS -oM entrada.nmap -p 1-65535 IPOBJETIVO
Amap -i entrada.nmap -o salida.amap -m

Algunos de los posibles parámetros son:

-u: comprueba sockets UDP (por defecto comprueba TCP)
-1: agiliza la ejecución de amap (recomendado)
-b: muestra el banner de aquellos servicios con salida ASCII
-q: no muestra los mensajes relativos a puertos cerrados
-v: el "famoso modo verboso" ;-)
-t y -T para opciones de timeout

Amap también puede utilizarse como un escaneador y capturador de banners, perdiendo sus ventajas de identificación de aplicaciones; algo muy útil para los scripts de escaneos bulk de grandes redes que tengan filtrado de icmp y se quiera saber cuales son los hosts existentes antes de pasar a identificar los servicios.

Amap -qbp http TARGET 1-65535

3.6.2 Nmap

Nmap ha incluido en sus últimas versiones la identificación de servicios. Un ejemplo de este:

Nmap -A -T4 -F www.insecure.org

Starting nmap 3.40PVT16 (http://www.insecure.org/nmap/) at 2003-09-06 19:49 PDT

Interesting ports on www.insecure.org (205.217.153.53):

(The 1206 ports scanned but not shown below are in state: filtered)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 3.1p1 (protocol 1.99)

25/tcp open smtp Qmail smtpd

53/tcp open domain ISC Bind 9.2.1

80/tcp open http Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)

113/tcp-closed auth

Device type: general purpose

Running: Linux 2.4.X|2.5.X

OS details: Linux Kernel 2.4.0 - 2.5.20

Uptime 108.307 days (since Wed May 21 12:27:44 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 34.962 seconds

Un ejemplo a lo bruto de escaneo bulk de todos los puertos TCP y UDP para comprobar las versiones:

Nmap -sS -sV -P0 -v -p 1, 65535 -n 192.168.1.1

Nmap -sU -sV -P0 -v -p 1,65535 -n 192.168.1.1

3.7 Identificación de Servicios Web

Para la identificación remota de servidores web. La herramienta netcat es muy útil en este sentido:

nc -v -n 192.168.1.1 80

Aunque existen herramientas que detectan la versión del servidor web a través de su banner como WotWeb, hmap y httprint v200, con un whitepaper sobre HTTP Fingerprinting.

En caso de que la conexión sea http; pueden comprobarse solicitudes HTTP mediante

OpenSSL:

$ Openssl s_client -connect localhost: 443 -state -debug GET / HTTP/1.0

Es posible utilizar el interfaz web de navegación SamSpade para recopilar datos desde un direccionamiento seguro.

NetCraft realiza periódicamente un estudio de los sistemas utilizados en Servidores Web, tanto para http como para https mediante detección remota.

3.7.1 DNS

Un mecanismo para identificar la versión de DNS es:

Nslookup -q=txt -class=chaos version.bind ns0.example.com
dig CHAOS TXT version.bind @IP.ADD.RE.SS

3.8 Análisis de y verificación de vulnerabilidades

COPS, TITAN y SATAN, fueron las primeras herramientas de análisis de vulnerabilidades internas en servidores Unix. SARA y SAINT son una evolución de SATAN, permitiendo análisis remotos de vulnerabilidades. También se tiene a Nessus siendo este el escaneador de vulnerabilidades OpenSource más conocido, para el cual están comenzando a surgir varios interfaces web como por ejemplo Inprotect y OSSIM (Open Source Security Information Management).

Existen varias herramientas específicas para buscar vulnerabilidades en Servidores de Web (URLs, CGIs.), como por ejemplo Twwwscan, VoidEYE, HTTPush, Nikto y Gherkin siendo esta ultima una herramienta gratuita vía web que centraliza los escaneos de Nessus, resolución de dns, y fingerprint de nmap con una salida normalizada en una base de datos Postgres.

3.9 Inyección de paquetes

La inyección de tramas puede ser muy compleja dependiendo de lo que se quiera hacer. El

portal más conocido en este entorno es PacketFactory, que aloja los proyectos Nemesis (una herramienta para la inyección de paquetes desde línea de comandos o desde un script; ISIC (IP Stack Integrity Checker, que comprueba la DitónDidad de una pila IP) y PackIt (una herramienta para auditoría de red); además de la API Libnet. packETH es una herramienta reciente basado en un GUI de Linux que genera paquetes IP en una LAN, útil para simular ataques DoS locales.

Otras APIS para construir tramas de red, además de Libnet son Net::RawIP en PERL e Impacket, de Core Security, en lenguaje Ditón.Derivado de Nemesis y basado en libnet para Win32 se encuentra Engage Packet BuilderHping también puede ser utilizado para lo que se denomina Packet Crafting

ARP0c Connection Interceptor permiten ataques de tipo Man-in-the-middle mediante la inyección de respuestas falsas de arp spoofing en un entorno de switching

3.10 Evasión de Firewalls e IDSs

Datatpipe permite encapsular a través de un proxy cualquier conexión que permita connect.. Otro método de saltarse un cortafuego es mediante un SOCKS Proxy local, como por ejemplo hopster o httptunnel.

Conclusiones

Como conclusiones del trabajo se tienen:

- Se caracterizaron las principales metodologías en cuanto a radio de acción, evaluación de riesgos y requerimientos necesarios para su aplicación práctica en procesos de auditoría, para junto con la experiencia de varios especialistas conformar la propuesta adecuada

- Existen factores propios del entorno informático de la universidad que son imprescindibles considerar en el diseño de una metodología, pues podrían afectar la calidad de los resultados, constándose que ninguna de las metodologías individualmente se adapta completamente al entorno y la arquitectura informática de la universidad

- Se propuso una serie de procedimientos para la realización de una auditoria de seguridad que se adecue a la red de la UCLV tenido en cuenta las condiciones tecnológicas y las características propias de los Sistemas de Información y las Redes de la Universidad Central de las Villas.

- Se evaluaron los resultados parciales de los procedimientos llevados a cabo lo que facilitó el desarrollo de un procedimiento contentivo de una serie de acciones de probada eficacia que pueden ser implementados en los procesos de auditoria de seguridad en la UCLV

Recomendaciones

Como recomendaciones se propone:

- Analizar con regularidad las vulnerabilidades de los servicios ofrecidos a partir de auditorías de seguridad siguiendo las recomendaciones propuestas en este trabajo.

- Continuar el estudio de los protocolos de seguridad haciendo énfasis principalmente en IPv6, el cual será implementado próximamente en la UCLV.

- Realizar un estudio de las diferentes secciones que fueron abordadas con poca profundidad en este trabajo como la Seguridad en las Comunicaciones y la Seguridad Inalámbrica, así como sus módulos correspondientes.

- Crear un grupo de auditores informáticos en la UCLV para acometer exámenes sistemáticos de seguridad en la UCLV.

Referencias Bibliográficas

- **AD – *Active Directory***. En línea Disponible en: http://www.microsoft.com/windows/technologies/directory/ad/default.asp [Accesado el 20 de marzo del 2007]
- American National Standards Institute (1981). *ANSI X3.92 American National Standard- Data Encryption Algorithm*, American National Standards Institute,
- American National Standards Institute (1983). ***AN**SI X3.106 American National Standard - Data Encryption Algorithm Modes of Operation, American.* Washington National Standards Institute.
- Aneiro Rodríguez L. (2000) *Elementos de arquitectura y seguridad informática*, La Habana. Instituto Superior Politécnico "Eduardo García Delgado",
- Ángel J. Criptografía para principiantes. En Línea. Disponible en: http://www.htmlweb.net/seguridad/cripto_p/cripto_princ_1.html [Acceso: 15 de enero del 2006].
- Asaka, Midori (1999). Local Attack Detection and Intrusion Route Tracing. ***IEICE Transactions on Communications*** .E82-B(11): 1826-1833
- Bradanovic T. Algo sobre Criptografía. En Línea. Disponible en http://www.vcd.cl/tombrad/pcasual/ayuda5.html [Accesado 20 de enero del 2006.]
- ***Building Open Source Network Security Tools: Components and Techniques (2000), Willey, Washington, DC.***
- Calrkson, D. (2000). *Vulnerability Assessments: Finding holes without digging your own.* Omaha. Willey.
- Canavan, John E. (2000). *Fundamentals of Network Security*. Boston, Artech House
- CERT - **Computer Emergency Response Team** (2004) [En Línea] Disponible en: http://www.CERT.org [Consultado 12/02/2004]
- Chandra, Pravir; Messier, Matt; Viega, John (2002) **Network Security with OpenSSL**. Sebastopol, CA, O'Reilly
- Cisco System Inc (2000) **Designing Network Security**. USA, Cisco Press publication

- Doraswamy, N. (2003). *IPSec: The new Security Standard for the Internet, Intranets and Virtual Private Networks.* 2da ed., Prentice-Hall PTR, Upper Saddle River.
- Federal Information Processing Standards. Data Encryption Standard (FIPS 46-2). En línea. Disponible en: http://www.itl.nist.gov/fipspubs/fip46-2.htm [Acceado el 20 de febrero del 2007].
- Federal Information Processing Standards. FIPS 81. DES modes of operation. En Línea. Disponible en: http://www.itl.nist.gov/fipspubs/fip81.htm [Accesado el: 24 de febrero del 2007].
- Govanus, G. y King, R. (2000) *MCSE: Windows 2000 Network Security Design.* Alameda, CA, SYBEX .
- Hada, S. "A Formal Treatment of Non-repudiation Protocols". en: *IEICE Transactions on Communications*, Vol. 87, n.2, 2004, pp. 461-470
- Hanaoka, G. *"Efficient Unconditionally Secure Digital Signaturas"*. en ***IEICE Transactions on Communications,*** Vol. 87, n.1,2004 pp. 120-130
- Hazeyama, O., Masafumi Y. *"A Layer-2 Extension to Hash-Based IP Traceback"*. En ***IEICE Transactions on Communications***, Vol. 86, n. 11, 2004, pp. 2325-2333
- Herzog, P (2003). *OSSTMM: Open Source Testing Methodology Manual.* Washington, Institute for Security and Open Methodologies.
- Hispasec En línea Disponible en http://www.hispasec.com/ [Accesado el 10 de febrero del 2007]
- Hispasec Sistemas. PGP Enterprise: Componentes de PGP Enterprise Security. Seguridad de comunicación mundial con PGP. En Línea. Disponible en: http://www.hispasec.com/directorio/laboratorio/articulos/PGPEnterprise/03.html [Accesado el: 6 de febrero del 2007].
- Horng, G. *"Cryptanalysis of a Key Management Scheme for Secure Multicast Communications"*. ***IEICE Transactions on Communications***, Vol. 85, n.5,2002 pp. 1050-1051
- ISO. ISO 8372 *Information processing - Modes of operation for a 64-bit block cipher algorithm.* Geneva: ISO, 1997.

- Kornack, Vince (2006). *Arming Linux With Penetration Testing Tools*, Massachusetts Pretice-Hall.
- Lachniet, M. (2004) *Performing a Network Vulnerability Assessment*, New York MacgrawHill,
- Mendvil I. El ABC de los documentos electrónicos seguros. En Línea. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m163a.htm [Accesado: 20 de enero del 2007].
- McBride, G (2004) . *The Art of Penetration Testing.* The Penetration Test. Attentort, Nebraska.
- Menezes A., Oorschot P. y Vanstone S. Handbook of applied Cryptography. En Línea. Disponible en: http://www.cacr.math.uwaterloo.ca/hac/ [Accesado 10 de febrero del 2007]
- Mehta, Puneet Guide to penetration testing, Part 5: Testing methodology and standards. en linea. Disponible en http://www.ackstorm.es/security_index.cfm [Accesado el 28 de febrero del 2007]
- National Institute of Standard and Technology (1996). *General Principles for Information Systems Security Policies*, New York Mc Graw Hill.
- Organization for Economic Cooperation and Development (1992). *Guidelines for security of information systems*. New York Lippincott.
- Ruiz, O. (2007) *Tests of Penetration in a Data Network*. Nebraska System Editions.

Glosario

ACK	*Acuse de Recibo*
ACL	*Access Control Lists*
CERT/CC	*Computer Emergency Response Team Coordination Center*
CHECK	*The CESG IT Health Check*
CISA	*CERTified Information Systems Auditor*
DMZ	*Demilitarized zone*
DNS	*Domain Name System*
DoS	*Denegación de Servicios*
EMR	*Radiación Electromagnética*
ERP	*Enterprise Resource Planning*
FFIEC	*Federal Financial Institutions Examination Council*
FTP	*File Transfer Protocol*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
IBM	*International Business Machines*
IC	*Inteligencia Competitiva*
ICMP	*Internet Control Message Protocol*
ID	*International design*
IDS	*Intrusion Detection System*
INS	*Internacional Network Service*
IRC	*Internet Relay Chat*
ISACA	*Standards for Information Systems Auditing*
ISP	*Internet service provider*
ISSAF	*Information System Security Assessment Framework*
NAT	*Network Address Translation*
NIST	*Instituto Nacional de Estándares y Tecnología*
OSSTMM	*The Open Source Security Testing Methodology*
OWASP	*Application Security Project*

POP3	*Post Office Protocol*
RFID	*Radio Frequency IDentification*
RST	*Rhetorical Structure Theory*
SAN	*Storage Area Network*
SEI	*Solfwart engineering Institute*
SMTP	*Simple Mail Transfer Protocol*
SQL	*Structured Query Language*
SYN	*Estudent Youth Network*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*

Anexos

La sintaxis básica de nmap es:

Nmap [tipo de scan] [opciones]

Por ejemplo si tenemos un host en nuestra red, con dirección ip 192.168.0.1 y deseamos conocer que puertos tiene abiertos, ejecutamos:

Nmap 192.168.0.1

Nmap mostrara en pantalla:

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/n
)
Interesting ports on localhost (192.168.0.1):
(The 1545 ports scanned but not shown below are
Port State Service
22/tcp open ssh
25/tcp open smtp
111/tcp open sunrpc
6000/tcp open X11
```

Este resultado puede variar, dependiendo de las opciones que se le pasen a nmap o de la cantidad de puertos, que se encuentren abiertos en el host, que esta siendo "scaneado".

Si queremos, conocer que tipo de sistema operativo, esta corriendo el host al que le realizamos el scaneo, sólo basta agregar el parámetro -O a el comando nmap.

Nmap -O 192.168.0.1

Mostrando un resultado como este:

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/n
)
Interesting ports on localhost (192.168.0.1):
(The 1545 ports scanned but not shown below are

      Port State Service
      22/tcp open ssh
      25/tcp open smtp
      111/tcp open sunrpc
      6000/tcp open X11

No exact OS matches for host (If you know what O

TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i386-suse-linux%D=7/20%Time
TSeq(Class=RI%gcd=1%SI=1B445E%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=2E12CD%IPID=Z)
T1(Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTN
T1(Resp=Y%DF=Y%W=7FFF%ACK=O%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTN
T3(Resp=Y%DF=Y%W=7FFF%ACK=O%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
```

Este es el resultado que mostró el comando, al realizar un scaneo a una pc con Linux, distribución SuSE Linux.

Pero que significan esas cadenas de caracteres en la salida de nmap?

```
TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i386-suse-linux%D=7/20%Time=
TSeq(Class=RI%gcd=1%SI=1B445E%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=2E12CD%IPID=Z)
T1(Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW
T1(Resp=Y%DF=Y%W=7FFF%ACK=O%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
```

Pues, todo esto es la "huella" TCP/IP

(TCP/IP fingerprint) que posee cada Sistema Operativo en particular.

Nmap nos muestra esto cada vez que no logra identificar con exactitud que Sistema Operativo se esta corriendo en el Host destino.

Y como hace nmap, para reconocer el sistema operativo, que se esta ejecutando en el host destino?

Básicamente, cada sistema operativo, responde diferente, cuando se le envían paquetes tcp específicos (en realidad no tan específicos, mas bien incoherentes) , así se logra determinar con una buena exactitud, que sistema operativo se esta ejecutando.

Al ejecutar nmap, contra un host con sistema operativo Windows XP, se produjo este resultado:

```
# nmap -O 192.168.0.1

Starting nmap V. 2.54BETA30 ( www.insecure.org/nm
Interesting ports on (192.168.0.2):
(The 1544 ports scanned but not shown below are
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open listen
5000/tcp open fics

Remote OS guesses: Windows Me or Windows 2000 RC
release, Windows Millenium Edition v4.90.3000
```

Instalación en Linux (amap)

Descargar el fichero de amap para Linux y ejecutar los siguientes comandos como **root**:

```
tar -zxvf amap-?.?.tar.gz
cd amap-?.?
./configure
make
make install
```

La sintaxis básica de amap es la siguiente

```
amap [host] [puerto]
```

Un ejemplo de uso; va a identificar que programa está corriendo en el host *pop.gmail.com* en el puerto *995*:

```
#amap pop.gmail.com 995

amap v5.2 (www.thc.org/thc-amap) started at 2006-12-13 09:02:41 - MAPPING mode

Protocol on 64.233.183.109:587/tcp matches smtp
Protocol on 64.233.183.109:587/tcp matches nntp

Unidentified ports: none.

amap v5.2 finished at 2006-12-13 09:02:42
```