INSTITUTO TECNOLÒGICO Y DE ESTUDIOS

SUPERIORES DE MONTERREY

CAMPUS CIUDAD DE MÈXICO

ESCUELA DE GRADUADOS EN ARQUITECTURA E INGENIERÌA

"SEGURIDAD COMPUTACIONAL EN INSTITUCIONES ACADÉMICAS "

TESIS

QUE PARA OBTENER EL GRADO DE

MAESTRO EN ADMINISTRACIÒN DE LAS TELECOMUNICACIONES

P R E S E N T A :

ERICK RENÉ VALENCIA RODRÍGUEZ

BAJO LA DIRECCIÒN DE:

DR. GUILLERMO ALFONSO PARRA RODRÌGUEZ

DR. JOSÉ RAMÓN ÁLVAREZ BADA

JULIO, 2004

MÉXICO, D.F.

RESUMEN

La privacidad y la confidencialidad de la información que poseen los profesores, así como las bases de datos de calificaciones, alumnos, registros, etc. comúnmente se ven perturbados por estudiantes que debido a su exceso de tiempo y actividad, buscan fracturar los dispositivos de seguridad que una institución académica posee.

Para la elaboración del presente trabajo, es necesario tener en cuenta todos los aspectos que influyen en el comportamiento de los intrusos en las instituciones académicas. Esto se puede obtener, creando escenarios posibles de comportamiento del intruso; tomando en cuenta, los orígenes, la educación, la formación, los estudios, las aspiraciones, los anhelos, los valores, la compañía, los amigos, las influencias, etc.

Una forma de lograr obtener los escenarios posibles, es haciendo uso de la investigación. Misma que puede ser documental, bibliográfica, de campo, etc.

Por lo indicado, el siguiente trabajo busca crear una hipótesis sobre las diferentes razones, posibilidades de ataque, sistemas de seguridad, tipos de ataque y otro tipo de actividades a las que se afronta una institución académica. Tomando en cuenta toda la información que se pueda reunir, se podrá obtener una serie de resultados que bien nos servirán para una toma de decisiones apegada a la realidad y certera respecto a los planes y acciones a seguir para poder mejorar e incrementar la seguridad del sistema, reconociendo las vulnerabilidades con las que cuenta dicho sistema.

CONTENIDO

Página

LISTA DE FIGURAS

Capítulo 1

Introducción

1.1 Antecedentes

El presente trabajo pretende crear una perspectiva sobre la tesis que se refiere a la Seguridad Computacional en Instituciones Académicas. Para esto, se buscará analizar dicho problema desde distintos puntos que ofrece para el análisis el tema en cuestión, logrando así un sistema integral multidisciplinario que nos proporcione todos los elementos necesarios. Para ello tomaremos las distintas perspectivas, tales como la psicológica, la social, la legal, la económica y la tecnológica; un análisis de los orígenes, el impacto, el desarrollo, la evolución; para lograr de una forma íntegra propuestas de solución.

Para comprender el proceso de infiltración de los "Piratas Cibernéticos", mejor conocidos en el argot como "Hackers", se requiere estudiar las causas por las cuales se despierta el interés en corromper con los dispositivos de Seguridad con los que puede contar un sistema informático. Sin embargo no podemos olvidar que este tipo de infiltraciones se encuentran en un marco globalizado a nivel internacional, el cuál no muestra limitantes para que el ilícito no se lleve a cabo a través de las fronteras. Sin

embargo en lo que se refiere al marco regulativo, habrá de ser estudiado y analizado por personas con la capacidad, los conocimientos, la experiencia y la visión suficiente para lograr el Objetivo señalado en el presente trabajo.

El impacto económico que representa la existencia de los "Piratas Cibernéticos" es afectado desde la inversión que generan las diferentes empresas en Dispositivos de Seguridad integrales, hasta el fraude a través de la Internet.

El pilar y herramienta que hay que tomar en cuenta en esta temática sin duda alguna, se encuentra caracterizado por la tecnología. Ya que en ésta, se encuentra el elemento o factor principal de tentación: "La Información". El principal interés en ella, se debe a que alguna u otra forma, el "Pirata Cibernético" desea infiltrarse en los sistemas de información para alterar, sustraer, eliminar, o simplemente observar la información de alguien más.

El último elemento a tomar en cuenta y sin duda alguna el "Talón de Aquiles" de los Sistemas de Seguridad Computacional lo podemos encontrar en "El Usuario". Esto debido al desinterés e irresponsabilidad muchas veces para llevar a cabo las distintas políticas de comportamiento y operatividad para el uso de los recursos Tecnológicos.

1.2 Definición del problema

La situación a la que nos afrontamos, se ocupa de distintas problemáticas para que se lleve a cabo su investigación. Uno de los principales problemas lo encontramos en el

estudio de campo. Se deben hacer participes distintos factores como la confidencialidad de las fuentes de información, ya que sin ellas, este trabajo no puede ser posible.

El presente trabajo se realizó de acuerdo a un plan cronológico de trabajo. Su estructura fue conformada (dependiendo del área de investigación) por investigaciones bibliográficas, de campo, prácticas, muestreos, encuestas y otros métodos. Así se podrá mantener un mayor control, eliminando todos aquellos obstáculos que puedan resultar de una mala planeación.

Los resultados deberán ser compatibles con cualquier institución académica que tenga sistemas informáticos, ya que la finalidad de este proyecto, es principalmente reducir los ataques al sistema, así como una reducción de los daños que estos pudieran acarrear. También debemos tomar en cuenta las disminuciones de las afecciones a la sección económica, así como los problemas legales en los que pudiera incurrir el "Hacker.

1.3 Objetivo

Llevar los ataques al mínimo mediante un estudio integral de la problemática de infiltración a los sistemas informáticos, a través de una participación conjunta de las áreas involucradas; tales como estudiantes, directivos, proveedores, personal docente, administrativo y de seguridad. Reduciendo así costos y elevando la productividad y disponibilidad de los recursos.

1.4 Hipótesis

El problema radica en que la cantidad de ataques que se llevan a cabo tienen una raíz psicológica, por lo que la hipótesis radica en una influencia del entorno sobre el individuo. Se confirmarán los diferentes elementos que influyen al individuo para llevar a cabo las actividades de piratería cibernética, así como la identificación de las herramientas, con que disponen los piratas cibernéticos. Una vez identificados y aislados dichos elementos, verificará la presente hipótesis para proceder con lo indicado en los objetivos.

Para disminuir los ataques a los sistemas informáticos en instituciones académicas, encontraremos la fortaleza en la prevención; analizando el comportamiento del futuro infractor y motivándolo a no cometer los actos ilegales. Logrando esto a través de sistemas tecnológicos y procedimientos que puedan difundir una cultura de seguridad computacional.

1.5 Justificación

Debido a las constantes amenazas y atentados por perpetrar en los sistemas informáticos de la Institución Académica, surge la inquietud por crear un esquema Integral de seguridad que ofrezca la suficiente seguridad de la información.

Dichas amenazas principalmente son:

- La alteración de calificaciones es una de las principales amenazas a las que se afronta el personal docente, así como las bases de datos de la institución.
- La modificación de datos o eliminación de estos por simple gusto o reto.
- El acceso a las redes inalámbricas desde las residencias cercanas a la institución académica.
- El acceso a los equipos de los compañeros con fines de diversión o extracción de tareas.
- El acceso a la información del personal docente para la extracción de exámenes.

Todo esto tendrá un fin de posible aplicación para permitir un nicho de mercado con resultados efectivos que ofrezca seguridad a la información de las instituciones académicas.

1.6 Conclusiones del Capítulo

En este capitulo se indican las bases para el desarrollo la tesis. De esta forma se define el enfoque que va a percibir aquella persona que consulte o utilice como referencia esta tesis.

La intención de la tesis es plasmada desde los antecedentes que buscan dar un semblante de la inquietud por emitir un documento que sirva de base para la implementación de un sistema genérico de seguridad computacional. Además se a través de la definición del problema, se puede percibir la situación actual por la que los usuarios de Internet cruzan a grandes rasgos.

A través del objetivo se delimitan los alcances del proyecto, permitiendo así descubrir las intenciones reales y su posible aplicación en el campo de las telecomunicaciones.

También en este capitulo se proporciona una hipótesis de lo que se quiere lograr con la investigación realizada y analizada para que sea empatada con los resultados.

Así mismo encontramos la razón por la cuál se justifica la realización del proyecto en donde se reconoce que la inseguridad informática como un problema que nos abarca a todos como usuarios del sistema y de la red de telecomunicaciones.

Capítulo 2

Marco teórico

2.1 La dependencia de la informática

2.1.1 El valor de la información

La manejamos y vemos día con día nos hemos acostumbrado a llevarla en nuestras vidas como una herramienta mas, y no es sino hasta que sufre algún percance cuando reconocemos su valor: "La información".

Comúnmente escuchamos en el medio de la informática expresiones tales como: "Un virus me borró la información", "Se metieron a mi computadora y me borraron archivos", "Me hackearon y ahora no se que voy a hacer con esa información, era demasiado importante", "Por accidente borré el archivo de mi tesis" o "Me robaron la Lap Top y allí iba toda mi información". Es en estos casos, cuando nos damos cuenta de cuanto valen las cosas y nos lamentamos no haber recurrido a las recomendaciones que los especialistas nos sugirieron.

Sin embargo muchas otras veces, por mas que se procure proteger la información, seguir las recomendaciones de los especialistas o inclusive respaldar la información: el resultado es negativo.

Tal es el caso de la "Piratería Informática" en las instituciones académicas. Las escuelas invierten grandes recursos para crear redes lo suficientemente inmunes a los ataques de los estudiantes, pero a pesar de la paranoia que se genera, los estudiantes terminan penetrando dichos sistemas de seguridad.

Es en ese momento cuando nos preguntamos: "¿Por qué hacen esto?", "¿Cuál es su motivación?", "Si se invierte tanto en equipos, ¿porqué es insuficiente?", "¿Estarán haciendo mal su trabajo los especialistas en seguridad informática?".

Entonces, ¿Cuál es el valor de la información? Una nota informativa emitida por Microasist nos hace ver lo siguiente: ¿qué pasaría si me roban la computadora de la oficina o de mi hogar? Y por lo general nos contestamos "No lo se", nos llega a la mente que si el equipo esta asegurado, recuperaremos parte del costo, sin embargo, en cuanto a la información nadie nos lo paga y no tiene precio y de verdad que se tiene una sensación en el estómago poco agradable, nos quedamos callados y nos formulamos cualquier cantidad de preguntas.[1]

De lo indicado en el párrafo anterior, podemos llegar a la conclusión de que la información tiene el valor que representa para cada persona. Posiblemente la tesis de maestría en administración de las Telecomunicaciones, no tenga un verdadero valor para un Teólogo, para un vendedor ambulante o para un asaltante; sin embargo el valor que le

puede asignar un Ingeniero en Telecomunicaciones, puede ser altísimo. Todo depende del cristal donde se mire.

2.1.2 Problemática de la inseguridad.

Una vez que se ha reconocido el valor de la información, habrá que cuantificar y asignarle de alguna forma, valor a la información que se posee. Esto se debe de realizar, para poder mantener una visión mayor de la seguridad que se le debe asignar a cada tipo de información. Si tenemos información que consideremos de alto valor, seguramente, alguien mas pueda tenerla valorada de igual o mayor valor. Inclusive puede existir información que depreciemos, y que sin embargo pueda tener un valor elevado para alguna persona ajena a nosotros. Es en este momento en donde surge el interés por explotar dicha información y utilizarla para beneficiarse otras personas.

La paranoia que exista respecto a la clasificación de la información, depende directamente de la información que se maneje, o en su defecto, de las políticas de la empresa. Esta es una parte muy importante, porque si no se realiza una clasificación adecuada, se pude incurrir en algunos problemas. Estos problemas pueden recaer en diversos escenarios.

- Si la información que clasificamos como de alto valor, no lo es, nadie va a querer modificarla, borrarla o robarla. Por lo tanto, estaríamos invirtiendo recursos innecesarios en sistemas de seguridad para información que no requiere tener un alto grado de seguridad.

- Si la información que clasificamos como de bajo valor, no lo es, estaríamos poniendo a disposición de cualquiera, la información que realmente puede serle de utilidad a un tercero. Nuevamente, estaríamos asignando recursos de una forma equívoca, lo que nos lleva a tener desperdicio de los mismos.
- Si la información que poseemos, la clasificamos en un valor demasiado alto, podríamos generar una inaccesibilidad a la misma, lo que nos estaría provocando un efecto negativo. Una analogía la podríamos encontrar cuando compramos una caja fuerte demasiada segura, que al guardar joyas en ella, perdemos la combinación, no quedaría disponible la información.

En nuestro caso de estudio, que es la seguridad computacional en instituciones académicas, debemos diferenciar la información que es confidencial (secreto) así como la que debe de recibir un tratamiento de privacidad (reservado) de la de dominio público. Esto, para evitar el fácil acceso a la información por cualquiera, limitando el número de atentados en contra de la información.

Pero para lograr todo esto, tenemos distintos problemas que los originan. Sin embargo, tal y como lo indica la hipótesis del presente proyecto, creemos que podemos encontrar la solución en la prevención. Disminuyendo los altos costos que generan los equipos de alta tecnología (porque como es bien sabido de todos, la seguridad es costosa), y por lo tanto, se pueden reasignar dichos recursos, o inclusive menores, a actividades de mayor impacto en la seguridad informática. Analizando las razones por las cuales los

alumnos se ven motivados a sustraer, modificar o simplemente observar la información que no les concierne.

Al mismo tiempo, descubriremos otras fugas de información, como lo pueden ser los empleados, personal de seguridad, intendencia, profesores o simplemente intrusos que puedan acceder desde el exterior de las instalaciones a través de la red inalámbrica. Inclusive analizar y categorizar aquellos intrusos que al ingresar a la institución (sin tener relación alguna a esta) pudieran infiltrarse a la información de la institución.

2.1.3 Informática, ¿necesidad o lujo?

Comúnmente observamos oficinas de gobierno, en las que el control lo mantienen mediante el uso de fichas de papel, formas llenas a mano, manejo de documentos en papel, entre otros. Igualmente podemos observar que instituciones académicas de recursos limitados utilizan mecanismos administrativos rudimentarios. Y a pesar de esto estas instituciones siguen produciendo y trabajando.

El método de enseñanza tradicional de educación primaria, secundaria, preparatoria y algunas materias de Universidad, que se utiliza en nuestro país, se basa en el uso casi nulo de tecnologías de la información, excluyendo clases tales como las de computación. Y aun así, han surgido profesionistas altamente capacitados, grandes investigadores, técnicos competentes, médicos de clase mundial, etc.

Pese a todo lo anterior, hay quienes argumentan que se puede lograr aumentar el rendimiento del estudiante mediante el uso de herramientas tecnológicas. ¿Será esto cierto?

Según un artículo de FMM Educación [2], nos dice que "Los alumnos se entusiasman con las infinitas posibilidades que ofrecen las herramientas de autor para que ellos desarrollen sus propios proyectos y, a la vez, se crea la necesidad de tener que aprender a utilizar los utilitarios para crear textos, imágenes, sonidos y animaciones que compondrán su trabajo". A la vez que nos señala: "se ven en la necesidad de tener que aprender a utilizar otros programas utilitarios y la informática en general, tanto en software como en hardware. La necesidad surge de su propia motivación interna y, por ello, su aprendizaje será ameno y divertido. Aprenderán porque quieren hacerlo, tienen el deseo de hacerlo".

Por lo tanto, se tiene la teoría de que el alumnado estará dispuesto a trabajar con un mayor rendimiento y con mayor interés cuando posee herramientas que le hacen mas sencillo el aprendizaje. Tal es el caso de los simuladores de vuelo para los pilotos, que ayudan a mejorar la técnica de estos sin arriesgar al piloto, disminuyendo costos, y dándole la oportunidad de acercarse de una forma dinámica al vuelo. Otro caso, lo podemos encontrar en los simuladores virtuales de rodillas; que son programas de computadoras que le brindan la oportunidad al estudiante de poder conocer mas de cerca como es la rodilla humana, sin la necesidad de intervenir cadáveres o rodillas de cerdos. De esta forma, el estudiante se acerca a la realidad pudiendo, inclusive, "intervenir quirúrgicamente virtualmente" a una rodilla en estos programas, permitiendo conocer más de cerca las características que posee la rodilla.

En electrónica, podemos encontrar simuladores de circuitos. Mismos que sirven para realizar circuitos electrónicos y así poder obtener los resultados, sin la necesidad de llevar a las *tablillas prototipo*, el circuito. Se disminuyen costos, se eleva el rendimiento y se acerca a mayor velocidad al estudiante.

Por ello, hay que colocar en una balanza al lujo contra la necesidad. Si los recursos asignados a cierto proyecto de implementación de tecnologías de la información, van a ser considerados una inversión o un gasto. Todo dependerá de la eficiencia en los métodos utilizados para inducir al alumnado al uso de estas tecnologías, además de la disponibilidad que se tengan de estas para los alumnos.

En conclusión, la tecnología poco a poco, va desplazándose de ser un lujo a ser una necesidad, ya que aunque se puede subsistir sin ella, los beneficios que nos provee, son verdaderamente altos. Pero en el momento de aplicar las tecnologías de la información al alumnado, no debemos olvidar que la capacitación del personal docente encargado de guiar al alumnado a través de la senda del conocimiento mediante el uso de dichos recursos, deberá ser altamente capacitado con técnicas de enseñanza revolucionarias que posean la capacidad de transmitir los conocimientos de una forma eficiente y dinámica.

2.2 Conceptos Generales de Seguridad

2.2.1 Principios Básicos

Para podernos relacionar de una manera un tanto más completa a lo que se refiere con la Seguridad Computacional, debemos de tener claros algunos conceptos y definiciones, de tal suerte que no exista confusión al tratar algún tema en específico.

A continuación, enunciaremos algunos elementos que definen la seguridad en la Tecnología de la Información [3]:

- Seguridad
    - ¿Qué Proteger? Antes que nada, debemos de estar concientes de cuál es nuestro objetivo a proteger.
        - Hardware. Debemos saber que tipo de herramientas utilizaremos para proteger nuestro equipo. Esto se refiere a los sistemas de protección físicos. Mismos que pueden ir desde Sistemas Antiincendios, hasta cerraduras.
        - Software. Posiblemente lo que queramos proteger, son programas que puedan ser alterados o perturbados para lograr distintos objetivos. Es por eso que se debe de proteger.
        - Datos. Deberán ser clasificados según su nivel de importancia y valor, a partir de esta clasificación, podremos obtener su ubicación.
    - ¿De qué proteger? Para poder proteger, debemos de aislar las amenazas y clasificarlas, de esta manera sabremos como protegernos con mayor eficiencia.

- Personas. Es aquí en donde encontramos a los usuarios que no siguen las políticas de seguridad computacional, ya que descuidan las bases para evitar ataques, aumentando la vulnerabilidad del sistema.
- Amenazas Lógicas. Todos aquellos programas maliciosos que puedan interferir o dañar nuestra información, o que la puedan dañar.
- Problemas Físicos. Aquellos problemas que pueden ser ocasionados por maltrato de los equipos, mantenimiento inadecuado, uso de elementos o partes ilegítimas, entre otras.
- Catástrofes. Todos aquellas amenazas que se pudieran ocasionar de sismos, incendios, inundaciones, entre otros. Que nos pudieran dañar o eliminar la información. Habrá que tomarlos en cuenta para tener planes de contingencia.

- ¿Cómo proteger?
  - Prevención. Sin duda alguna uno de nuestros elementos pilares de la hipótesis planteada en este proyecto.
  - Detección. Cuando la prevención no es suficiente, se procede a detectar el ataque, el rastro que quedó, y los distintos movimientos y/o alteraciones que se ocasionaron.

- Recuperación. Busca recuperar las afecciones realizadas al sistema, mediante el uso de respaldos de información, programas de recuperación, etc.
- Auditoría. Para determinar, las causas del siniestro, los daños que éste ocasionó y aislar los motivos de la intervención, para proteger en un futuro esos accesos.

o ¿Qué conseguir? Mediante los sistemas de seguridad, se desea obtener cierto control, mismo que se obtendrá mediante lo siguiente.

- Autenticación. Comprobar que el usuario que desea ingresar a los datos, es realmente quien dice ser.
- Autorización. Que aquel usuario que desee acceder a los datos esté autorizado para acceder a ellos.
- Disponibilidad. Que la información se encuentre disponible y no sea limitada por los dispositivos de seguridad.
- Confidencialidad. Que se garantice que la persona que sea asignada, sea la autorizada de observar la información. Y que no podrá ser vista por nadie más.
- Integridad. Que la información se encuentre tal y como fue elaborada y que no sufra alteraciones por los dispositivos de seguridad.

- No repudio. Aquellos usuarios que tienen la autorización de ver cierta información, ésta no les sea negada.

Para tener una visión íntegra de lo descrito arriba, ver figura 2.1.

A continuación, los capítulos que se indican son los que serán investigados y completados mediante la investigación bibliográfica, de campo y la documental.

2.2.2 Arquitectura

Como parte de la arquitectura, debemos conocer cuáles son los pasos que sigue un *hacker* para poder realizar sus ataques y sus metas, por ello, es que se requiere conocer cual es la arquitectura del *modus operandi* del pirata cibernético. Para lograrlo, se rige de cierto procedimiento característico (ver figura 2.2). La realización de dicho procedimiento, es consecutivo y puede alterarse, según lo indicado en el mismo.

a) Encontrar huellas. Consiste en identificar el objetivo, las direcciones y toda la información que se pueda obtener del objetivo a ser atacado.

b) Explorar. En este paso, debemos de conocer el entorno en el que nos ubicamos, reconocer cuales son los puertos, las redes, subredes así como en las que se encuentra nuestro objetivo.

c) Enumerar. En este punto es en el que vamos a encontrar los diferentes medios de acceso que pudieran ser débiles a un ataque, estos pueden ser cuentas de correo, sesiones de inicio, carpetas compartidas, archivos compartidos, programas de chateo, entre otros.

d) Obtener acceso. Ya debemos de tener la suficiente información, para saber cual puede ser su principal debilidad de la víctima, por lo que podemos usar herramientas para capturar las claves de usuario que pasen a través de la red, captura de archivos con claves de usuario, ataque de fuerza bruta a archivos o carpetas compartidas, entre otras. En este punto, posiblemente nos sea negado el acceso y tengamos que comenzar el procedimiento una vez mas, buscando nuevas debilidades en el sistema.

e) Escalar. Posiblemente el acceso obtenido, no nos brinde el nivel jerárquico suficiente para obtener los resultados que queremos, por lo que será necesario que busquemos la forma de avanzar y lograr terreno en otro nivel de usuario.

f) Saquear. Podemos sustraer la información, pero si esta es muy importante, seguramente posea dispositivos de seguridad mas avanzados, por lo que deberemos regresar al paso de enumeración.

g) Limpiar. Ya que el objetivo se encuentra asegurado, debemos de cubrir cualquier pista que pudiéramos haber dejado de nuestra intrusión, de igual forma, esconder las utilerías que necesitemos.

h) Creando Puertas Traseras. En este paso debemos dejar accesos para que en el futuro podamos entrar en el sistema si lo requerimos. De esta forma no será necesario cruzar por todo el procedimiento.

i) Negación del Servicio. Si no se logró el acceso, deberemos de reiniciar desde el proceso y lograr el acceso.

Con este proceso, podremos comprender de una forma mas efectiva el método por el cual se llevan a cabo los ataques a un sistema, una vez identificándolos, lograremos tener un desempeño mas efectivo para poder aislar los diferentes puntos de acceso.

2.2.3 Riesgos

Para poder determinar cuales son los riesgos a los que se enfrenta una institución académica a sufrir incendios, inundaciones y sismos; se debe de realizar una valoración de la ubicación geográfica, orográfica, hidrográfica, así como una identificación de las zonas sísmica más cercanas al inmueble. Así mismo, se debe de realizar un estudio de los materiales, con los que se encuentra elaborado el inmueble de tal manera que soporte algún siniestro. De esta forma, se podrán considerar algunos aspectos fundamentales de protección civil, así como de seguridad.

Para entender de una manera más amplia lo descrito en el párrafo anterior, podemos tomar en cuenta el siguiente texto en lo que se refiere a sismos:

El promedio de muertes producidas por los sismos excedió las 15,000 personas por año los últimos 40 años, por lo que es primordial la predicción de sismos para menguar sus daños, por lo menos en la pérdida de vidas.

Desde luego que los 3 países que más han avanzado en los estudios relacionados son circumpacíficos: Estados Unidos, Japón y China, que son quienes más han sufrido los terremotos y están en más peligro.

Los métodos empleados son variables: Desde el más lógico, que es midiendo los tiempos que transcurren entre un sismo grande y el siguiente para calcular lo que toma a las placas involucradas para vencer la fricción que impide que se desplacen lenta y continuamente con mínimas destrucciones.

También se apela a la expulsión de gas radón, que se supone aumenta al comenzar los esfuerzos deformantes que resultan en terremotos.

Otros métodos recurren a las modificaciones de los campos magnéticos, los micro sismos previos, los cambios de los niveles freáticos del agua subterránea y hasta al comportamiento de los animales, ya que algunos modifican sus hábitos porque "sienten" la proximidad de las placas deslizándose para producir mortales terremotos.

Algunas personas han apelado a las alineaciones planetarias para predecir los sismos, pero su influencia es tan insignificante que nada han indicado.

Desde luego que se ha encontrado una relación estrecha entre las mareas y los sismos, porque las placas continentales se abomban por el paso del Sol y la Luna, como lo hacen los mares.

Los sismos son más intensos cuando las influencias de los dos astros coinciden y las mareas "sólidas" son más fuertes. También la declinación solar debe estar entre los 17 grados norte y sur.

Se ha encontrado también que los cambios sobre la corteza promueven sismos. Una nueva presa construida en una región conocida como tectónicamente inestable aumenta por lo menos temporalmente la sismicidad.

El equilibrio de la corteza está delicadamente ajustado a los pesos "ligeros" de los continentes (con peso específico de 2.7) y las cortezas oceánicas (con 3.0 de peso específico).

También las extracciones de petróleo, agua y hasta rocas acarrean cambios llamados isostáticos (de igual equilibrio) promueven mayor sismicidad.

Durante la ya superada "guerra fría" se instalaron gran cantidad de sismógrafos en todo el mundo. Por medio de estos aparatos y por triangulación se podían localizar los puntos donde los contrincantes producían sus explosiones atómicas experimentales.

Desde luego que los sismos originados por las explosiones son fácilmente distinguibles de los producidos por los movimientos tectónicos y vulcanismo en nuestra litosfera [6].

De igual forma, debemos de considerar algunos elementos que son importantes, para proteger nuestros inmuebles de una inundación, tomando en cuenta la localización, el sistema de desagüe, diques, presas, etc. Por lo anterior, se sugiere seguir las recomendaciones de la FEMA (*Federal Emergency Management Agency*, Agencia Federal de Administración de Emergencias en los Estados Unidos de Norteamérica).

De igual manera no debemos descartar los posibles incendios que se pueden producir en nuestro inmueble, para evitar daños en el mismo, debemos de saber cuando se inicia uno, y poder actuar mediante los dispositivos adecuados. Por ello, se recomiendan unos de los mas sensibles detectores que son los detectores iónicos de fuego. Según un informe del Senado de España, estos detectores son utilizados con mayor frecuencia por su efectividad, de tal forma que se instalaron en el año 1998 en el estado 198.000 unidades.

Básicamente, estos detectores están fabricados con Americio 241. Este elemento tiene una actividad por debajo de 0,09 microcurios, o 33,3 kbq (kilobequereles). Las emisiones radiactivas que emiten son de tipo alfa (pesadas) y, su intensidad hace que a 5 centímetros de la fuente pierdan la suficiente potencia como para dejar de ser perjudiciales para la salud. También emiten partículas gamma que son despreciables. En los casos de detectores muy antiguos los hay con Radio 226. [7]

2.3 Naturaleza del Pirata Cibernético

Para poder atacar el problema de la piratería cibernética, es necesario conocer la raíz del mismo, de otra manera únicamente estaríamos ejerciendo paliativos que no nos servirían para solucionar el problema en su totalidad. Por lo que será necesario que hagamos un análisis de las razones que motivan a un pirata cibernético a realizar los distintos ataques.

Para poder comprender de una manera más amplia dicho comportamiento, se requiere de investigación documental, así como investigación de campo. Una vez reunida la información, podremos empatarla y determinar cuáles son las causas que afectan y que influyen en nuestro entorno, así como la influencia que puede tenerla idiosincrasia mexicana sobre el estudiante.

2.3.1 El entorno

Uno de los elementos a estudiar, es el entorno de un pirata cibernético. La siguiente es una visión del entorno que tiene el pirata cibernético sobre su entorno:

"Ser un pirata cibernético brinda mucha diversión, pero es una diversión que cuesta mucho trabajo. El esfuerzo requiere motivación. Los atletas exitosos obtienen su motivación de algún tipo de actividad física que permita la mejora de sus cuerpos, empujándolos sobrepasar sus propios límites. Similar, para ser un pirata cibernético se debe de tener cierta habilidad para resolver problemas, agilizar las habilidades y ejercitar la inteligencia" [5].

Dentro de las pláticas sostenidas con un joven pirata cibernético de alias "©hµch¤", reconoce al entorno como un momento y un lugar en el que encuentra amenazas y retos. Los retos son todas aquellas metas que demuestran cierta dificultad para ser violadas. Tal es el ejemplo de diversos ataques fructuosos efectuados a la Universidad X. En la cuál, después de realizar diversos análisis y estudios de la red y de los usuarios, se logró obtener claves de acceso de diversos usuarios, llegando a obtener las claves de acceso de los diversos servidores de la red, permitiendo de esta manera acceder

a todos los equipos conectados a la red, así como a sus diversos archivos y calificaciones. Otros retos que van surgiendo en el transcurso del desarrollo del pirata cibernético, corresponde al análisis de dispositivos electrónicos como los teléfonos celulares para modificar los ESN (*Electrónic Serial Number*, Número de Serie Electrónico); actividad que hasta la fecha, se encuentra en proceso de desarrollo y muy pronto se esperan resultados.

©hμch□ reconoce como amenaza, a las leyes y reglamentos que rigen a las instituciones académicas, así como su comportamiento dentro y fuera de estas. También ubica como amenaza, a los dispositivos de detección de intrusos, los cuáles, día con día se van convirtiendo en una nueva amenaza debido a su alto desarrollo tecnológico en tan poco tiempo. Otros tipos de amenazas, los podemos ubicar en otros piratas cibernéticos, los cuáles en la búsqueda por lograr fines similares o personales, generan guerras de poderes entre los mismos.

2.3.2 Situación Actual Global

Para lograr comprender la magnitud del problema que ofrecen los ataques cibernéticos, es necesario conocer cuál es la situación actual en los ataques que se tienen en los diferentes países. Desde ataques famosos, hasta aquellos que pasan por inadvertidos.

Se pueden encontrar innumerables casos. Pero algunos serán históricos. Tal es el caso del primer joven "Hacker", Wang Qun de 19 años, capturado por el gobierno de

China el 19 de Septiembre del 2001. Quien pese a su corta edad, ya poseía los cargos en su contra por haber violado más de 30 sitios de Internet del gobierno bajo el alias de "Playgirl". [8]

Pero no siempre es malo ver con malos ojos a un "Hacker". ¿Porque no auxiliarnos de ellos mismos, para protegernos? Esa es la innovación que el Profesor Walter Chieng, director de informática de la Universidad Saint Kentigern en Auckland (Nueva Zelanda), aprovechó para mejorar la seguridad de la informática en el colegio. El imparte clases de seguridad en redes inalámbricas a unos 1,100 alumnos y profesores utilizando computadoras portátiles para conectarse a la red inalámbrica del colegio. De esta forma, se pueden encontrar los agujeros de seguridad que se puedan localizar en la red, permitiéndoles a los alumnos y profesores realizar distintos ataques para poder descubrir las vulnerabilidades y de esta forma poderlas eliminar posteriormente.

Otro aspecto a considerar, son las estadísticas que publican diversas organizaciones y/o compañías que se encargan de registrar los ataques, parar emitir estadísticas y poder determinar planes de acción. Prueba de ello, se encuentra en las estadísticas de ataques de incidentes de seguridad de Tecnologías de la información publicadas por la CERT (Equipo de Respuesta a Emergencias Informáticas) de Carniege Mellon, mismas que nos indican que en año 2000, se registraron 21,756 incidentes; en el 2001, se registraron 52,658; en el 2002, 82,094; y tan solo del primer al tercer trimestre del 2003, 114,000 incidentes. Esta es una muestra del crecimiento de los ataques informáticos. Cabe mencionar que un incidente puede envolver un sitio o cientos (en

algunos casos hasta miles) de sitios. También algunos incidentes pueden envolver actividades por largos periodos. Ver gráfica anexa figura 2.3 [9]

Así mismo la CERT publica las estadísticas de las vulnerabilidades reportadas a esta institución para el 2000 mostró 1,090 vulnerabilidades; para el 2001, 2437 vulnerabilidades; para el 2002, 4129 vulnerabilidades; para el periodo que comprende el primero al tercer trimestre del 2003, 2982 vulnerabilidades. Ver gráfica anexa figura 2.4 [9]

En lo que a publicaciones de alertas de seguridad se refiere, la CERT reportó en el 2000, 22 avisos y 4 resúmenes de alertas; en el 2001, 37 avisos y 4 resúmenes de alertas; en el 2002, 37 de avisos y 4 de resúmenes; y en el periodo que comprende del primero al tercer trimestre del 2003, 25 avisos y 3 de resúmenes. Ver gráfica anexa figura 2.5 [9]

La CERT cuenta con un registro de los correos electrónicos manipulados y estos van del año 2000 con un registro de 56,365; en el 2001, con un registro de 118,907; en el 2002, con un registro de 204,841; y en el periodo que comprende del primero al tercer trimestre del 2003 con un registro de 468,825. Ver gráfica anexa figura 2.6 [9]

2.3.3 Herramientas de Ataque

Dentro de las amenazas a las que se enfrentan las instituciones académicas, podemos encontrar que los "hackers" hacen uso de diversas herramientas de atque. Estas herramientas son utilizadas de acuerdo a las necesidades (es decir, a la etapa en la que se encuentren en el desarrollo del ataque) que tengan los "hackers" para lograr sus objetivos, ya sea infiltración, espionaje, alteración, plagio o cualquier otra actividad ilícita.

Para lograr dichos ataques, existe un esquema de ataque que se encuentra descrito de acuerdo a la figura 2.2. Mismo que se describe en los siguientes subcapítulos.

2.3.3.1 Encontrar Huellas

Sin duda alguna este es el paso en cuál nos enfrentamos a la misión de encontrar la información necesaria del objetivo o víctima a ser atacado, en esta etapa del análisis, se hace uso de técnicas para investigar la dirección como "whois". Con esta herramienta podemos ubicar en los distintos sistemas operativos a los equipos que deseamos atacar. Una herramienta de búsqueda del tipo "whois", es la que podemos localizar en la dirección http://www.arin.net/whois/. En esta dirección, se ubica una base de datos en donde se tiene el registro de los contactos y la información registrada para recursos registrados en ARIN (American Registry for Internet Numbers).

2.3.3.2 Explorar

Esta etapa comprende la identificación del objetivo y sus direcciones a través de herramientas que permitan encontrar las distintas rutas o vías de acceso. En esta etapa se contemplan una serie de actividades que arrojen una información con mayor precisión de nuestro objetivo final. Las herramientas utilizadas son el barrido por envío de paquetes "ping" con programas tales como f_ping, WS_Ping Pro pack. Una herramienta muy versátil y que basa su funcionamiento en envío de paquetes "ping" para trazar la ruta por la cual tiene que pasar el incluyendo los ruteadores, switches y equipos; esta herramienta se llama "Visual Route".

Otra herramienta que sirve para detectar los puertos que son vulnerables es la de exploración de puertos TCP/UDP. Mediante esta herramienta, podemos detectar cuales son los puertos disponibles y que permitan el acceso a un hacker. Algunos ejemplos de estas herramientas, son los siguientes: nmap, scan.exe. Otra herramienta que es utilizada comúnmente, es el "Back Orifice 2000". Este programa es muy completo, ya que tiene la capacidad de realizar árboles de redes, detecta los puertos vulnerables, instala troyanos e inclusive permite manipular la información, el ratón, los periféricos y otros dispositivos.

2.3.3.3 Enumerar

Para comprender el funcionamiento de esta etapa, es necesario comprender que aquí encontraremos los diferentes medios de acceso que puedes ser débiles a un ataque, estos pueden ser a través de cuentas de correo, sesiones de inicio, carpetas compartidas, programas de chateo, programas de intercambio de archivos, entre otros.

Para lograr esta etapa, podemos utilizar programas como el ya antes mencionado "Back Orifice 2000". Programa que traza un mapa de todos los equipos que se encuentran en la red. A su vez, analiza cuales son las carpetas que se encuentran compartidas en cada equipo, así mismo, detecta cuáles son los permisos que tienen los usuarios para cada carpeta.

De esta forma, se crea un árbol de posibilidades para poder determinar cuales son las diferentes vías para desplazarse por la red, una vez que se ha logrado el acceso a algún usuario de la red, sin importar los privilegios con los que cuente el usuario.

2.3.3.4 Obteniendo Acceso

La finalidad de esta etapa es que una vez obtenida la información necesaria, obtener las claves de acceso para poder ingresar al sistema del usuario. Esto lo a través de diferentes posibilidades de capturar las claves de usuario o rutas de acceso.

Sin duda alguna es una de las etapas con mayor variedad de medios que van desde la ingeniería social hasta complejos programas de decodificación de claves. Estos ataques se pueden clasificar de acuerdo a la siguiente lista

"Key loggers"

Los *key loggers* son programas que capturan todo lo que se escribe en el teclado, para lograr esto, se puede:

- Instalar el programa directamente al equipo (cuando el usuario no se encuentre en el).
- Se puede enviar por correo como un archivo adjunto.
- A través de alguna macro de un programa como Excel [36].
- Usando como medio de acceso, programas de chateo.

Existen diversos *key loggers,* uno de los mas sencillos que podemos encontrar es el de Sister Spy. Este programa, se instala en algún subdirectorio, después se corre y una vez activo en memoria, se puede ocultar y cuando se requiere sustraer la información, únicamente se presiona la tecla F12 y se puede visualizar la ventana de donde se copian

todas las teclas capturadas. Se comporta como un virus troyano. Actualmente ya es detectable por programas de antivirus. Ver figura 2.7

También podemos encontrar programas más complejos como el "Back Orifice 2000". El cuál tiene una serie de beneficios que mantiene abiertos ciertos puertos y vulnerabilidades del sistema.

"Sniffers"

Estos programas tienen la peculiaridad de poder analizar el tráfico que se encuentra circulando por la red. De esta forma podemos controlar y determinar todo el tipo de información que circula por la red. La capacidad que puede ser explotada por los piratas cibernéticos consiste en que al estar analizando la red, podemos ver circular el inicio de las sesiones que normalmente no se encuentran encriptados y que además se muestran en texto plano. Así al capturar las tramas, podemos analizarla y encontrar diferentes claves de acceso.

Para ello, tenemos programas como *"Ethereal"*, programa de sencilla manipulación que permite el análisis de la red, de sus usuarios y de las tramas que circulan por este. Ver figura 2.8 y 2.9.

Ataque por Fuerza Bruta

Este ataque consiste en ingresar a través de programas de repetición o de iteraciones, combinaciones de palabras, para lograr determinar la clave del usuario. Los hay de 2 tipos:

- El primero es un proceso por el cuál se ingresan combinaciones aleatorias de números y letras, hasta que coincide la combinación adecuada con la del usuario. El problema de este proceso es que es demasiado lento debido al elevado número de combinaciones.
- El segundo es un proceso que copia de una lista llamada "diccionario" las palabras y las ingresa una por una hasta que coinciden con la clave del usuario.

Ingeniería Social

Consiste en tener la capacidad psicológica y habilidad para lograr convencer a las personas de que nos permitan realizar ciertas intervenciones, obteniendo así claves o el acceso para dejar residentes puertas traseras (*back door*). De esta manera, lograremos acceder al sistema a través de medios no informáticos.

Un ejemplo podría ser el siguiente. Uno puede llegar ante alguna secretaria bajo el argumento de querer corregir algún error que tiene el sistema de su jefe. Si no existen políticas de seguridad correctas, la secretaria puede permitir el acceso al que pretende ejecutar un ataque y obtener así alguna clave de acceso, necesaria o en su defecto, instalar algún programa que lo permita.

2.3.3.5 Escalar

Este se logra una vez que se han obtenido los datos necesarios o las claves para poder ingresar a la cuenta del usuario objetivo. Si este usuario no tiene las cualidades necesarias para alterar la información que necesitamos o efectuar los movimientos que queremos, será necesario aumentar el nivel de privilegios.

En esta etapa es donde aplicamos lo utilizado en la enumeración, ya que conocemos todas las vulnerabilidades de los equipos que se encuentran alrededor nuestro. Una vez conociendo cuál puede ser el equipo adecuado, podemos hacer uso de programas o aplicaciones que nos permitan romper con claves de usuarios superiores. También podemos aprovechar que ya estamos dentro del sistema, para ingresar a los servidores de correos, de usuarios o alguna otra vulnerabilidad que podamos encontrar en este sistema.

Se pueden utilizar herramientas similares a las mencionadas en la sección denominada "Obteniendo Acceso" o inclusive las mismas herramientas. Todo esto se puede lograr a través de las distintas capas del modelo OSI. No hay que olvidar que existen diferentes rutas para llegar a un mismo fin.

2.3.3.6 Saqueo

Podríamos definirla como la etapa objetivo. En esta etapa es en la que nos encontramos ante la misión de realizar la sustracción, alteración o cualquiera que sea nuestro deseo y objetivo de acceder a la información NO permitida para el pirata Cibernético. Al realizar estas operaciones, debemos de saber en cuál de los 2 escenarios posibles nos vamos a ubicar.

El primer escenario contempla un comportamiento por parte del atacante en el cuál no desea darse a conocer ante los demás. Es decir, prefiere el anonimato. En este caso, es de suma importancia no efectuar operaciones que puedan poner en riesgo la evidencia, es decir, no debemos de dejar registros de entrada y salida de información.

En algunas ocasiones, la intención de un pirata cibernético es que nos conozcan, que sepan que existimos, que efectuamos operaciones. En este caso el pirata cibernético puede dejar rastro de identificación, en el cual muestre o dé a conocer al pirata. Esto se puede dar a conocer mediante un *banner*, algún programa ejecutable, o simplemente un recado en *Notepad* que lo de a conocer.

Cabe mencionar que es un buen momento para poder localizar algunas claves que se puedan encontrar en texto plano, esto con la finalidad de que si existe alguna necesidad de corromper algún otro sistema o que queramos ingresar que se encuentre relacionado con el objetivo.

2.3.3.7 Limpiar

Una vez que hayamos realizado nuestro objetivo, es necesario que no dejemos registros que nos puedan incriminar del ataque que se realizó, esto lo podemos lograr procurando eliminar cualquier registro de bitácoras o algún otro dispositivo que pueda evidenciar la dirección del *host* origen. Sin embargo, también podemos hacer uso de "trucos" cibernéticos.

Uno de los trucos que podemos emplear en este punto, es el tan controversial y conocido *IP Spoofing*.

"IP Spoofing"

El *IP Spoofing* [10] consiste en enviar un paquete IP con la dirección de origen falseada, de forma que el destinatario crea que proviene de otra localización. Esta técnica puede emplearse para muchas cosas, entre otras para un ataque *DoS* (Denial of Service, Negación del Servicio).

El *IP spoofing* no es una técnica cuyo éxito dependa única y exclusivamente de quién emite el paquete. Es decir, nosotros podemos mandar un paquete con una dirección de origen falseada, pero ese paquete no llegar nunca a su destino.

En redes grandes (como Internet) existen muchos dispositivos de red que pueden realizar filtrados al tráfico que gestionan. Uno de esos filtros es precisamente la comprobación de la IP de origen. Estos dispositivos, pueden ser

- *Firewalls*
- *Routers*
- *Switches*
- *Proxy Servers*

Evidentemente, el *IP spoofing* funciona en una Red de Área Local (LAN, Local Área Network), en especial si esta no es dinámica. Sin embargo, en Internet no podemos suponer por adelantado que puede funcionar. Los *ISP's* (*Internet Service Provider*, Proveedor de Servicios de Internet) aplican (o deberían aplicar; Caso que en México no se

aplica) filtros en los servidores de acceso y en sus *routers* para contra atacar este problema. En el peor de los casos, si no lo hace el ISP, lo debería de hacer el *carrier*, así que estamos en una situación parecida.

Por tanto, para que un ataque *DoS + IP spoofing* tenga éxito desde una enlace PPP (Point to Point Protocol) *dial-up* convencional (conexión vía módem telefónico), tanto el *carrier* como el *ISP* tendrían que ser muy descuidados.

"Smurf"

El éxito de un ataque tipo smurf se basa en dos principios que tienen que darse "simultáneamente"[10]:

- *IP Source address spoofing*
- La transformación de tráfico *broadcast* nivel 3 en *broadcast* nivel 2. Por ejemplo, que la multidifusión IP se transforme en multidifusión Ethernet.

Sobre el primer punto ya hemos hablado en el primer punto. Sobre el segundo, comentar que casi todos los *routers* (sobre todo los modernos) vienen configurados con esta opción deshabilitada por defecto.

En cualquier caso, puede, nuevamente, filtrarse en el *router* y evitar que usen nuestra red como amplificador de tráfico. De hecho, la mayoría de las redes tienen esta protección activada.

Es cierto que existen listas de redes grandes que continúan mal configuradas y que pueden usarse como amplificadores. Sin embargo, para que *smurf* tenga éxito, deben tenerse en cuanta las consideraciones de sobre *spoofing* mencionadas anteriormente.[10]

2.3.3.8 Creando Puertas Traseras

La creación de puertas traseras, es un elemento que puedes ser utilizado para continuar con las intrusiones a las victimas. Esto se puede lograr por el uso o instalación de programas similares a los ya antes mencionados: *key loggers*, "Back Orifice 2000", entre otros.

También se pueden sustituir ciertas aplicaciones comunes, por troyanos. De esta forma cuando se ejecuten, se mantendrá o se podrá volver a obtener la información de la victima.

Un ejemplo de los programas de troyanos, lo podemos encontrar en aplicaciones como la que a continuación se describe:

Supongamos que se desea obtener alguna información de un usuario. Si la víctima tiene algún programa de chateo como Hotmail Messenger, se le puede enviar un archivo, ya sea a su correo o a través de la transferencia de archivos, haciendo uso de la ingeniería social, para convencerle de que el programa es inofensivo o que es una fotografía. Este programa al ser recibido y/o activado inmediatamente envía a un correo electrónico indicando la dirección IP del *host* victima. De esta forma, cada que se conecte el usuario, se enviará la dirección a ese correo electrónico, permitiendo así a través de un programa controlar algunas funciones del equipo remoto incluyendo opciones como las de *key logger*.

2.4 Virus

Sin duda alguna, estos se han vuelto uno de los elementos de propagación y daño en las redes de telecomunicaciones de gran temor. Pero para poder comprenderlos y lograr así una defensa efectiva, es necesario reconocerlos, clasificarlos y en su debido momento aislarlos.

Los virus han sido definidos como un pequeño programa creado para alterar la forma en que funciona un equipo sin el permiso o conocimiento del usuario [11]. Sin embargo para que estos programas sean considerados como virus, deben presentar 2 características:

- Debe ser capaz de ejecutarse a sí mismo. A menudo coloca su propio código en la ruta de ejecución de otro programa.
- Capaz de replicarse. Esto quiere decir que puede reemplazar otros archivos ejecutables con una copia del archivo infectado.

El virus puede estar facultado para atacar al equipo infectado dañando programas, eliminando archivos, reformateando el disco duro o modificando la información. Otros no están creados para causar algún daño, simplemente se dan a conocer enviando mensajes de texto, video o sonido. Sin embargo debido a la naturaleza de los virus, algunas veces pueden causar errores ocasionando perdidas de datos y bloqueos del sistema.

2.4.1 Tipos de Virus

Con la finalidad de tener una mayor protección de los diversos virus que nos podemos encontrar, es recomendable conocer el comportamiento de los mismos y así podemos defender de ellos con mayor efectividad de acuerdo a su comportamiento y medio de distribución. Es por eso que los clasificaremos de acuerdo a su comportamiento.

2.4.1.1 Virus que Infectan Archivos

Estos virus poseen la característica de atacar a los archivos de programa. Normalmente atacan archivos ejecutables directamente a su código. Los archivos que son infectados con mayor frecuencia, son los que tienen extensión .exe y .com. El equipo se puede infectar desde un disquete, un disco duro o a través de una red.

2.4.1.2 Virus del Sector de Arranque

Como su nombre lo indica, estos virus tienen la peculiaridad de auto instalarse en el área de sistema de un disco, en otras palabras, infectan el registro de arranque de los discos duros, así como de los disquetes. Tienen la peculiaridad de copiarse en esta parte del disco infectado, posteriormente se activan cuando el usuario reinicia el sistema desde el disco infectado. Su ubicación dentro del equipo para efectuar la propagación e infección, es dentro de la memoria por naturaleza. La mayoría de estos virus fueron utilizados para DOS, pero todos los equipos, independientemente del sistema podrán ser infectados mediante el uso de los discos de inicio infectados.

2.4.1.3 Virus del Sector de Arranque Maestro

Su comportamiento para la infección de los equipos, es de la misma forma que los virus del sector de arranque. Lo que los diferencia, es la ubicación del código vírico. Los virus del sector de arranque maestro normalmente guardan una copia legítima del sector de arranque maestro en otra ubicación. Si un virus del sector de arranque maestro infecta a un equipo con sistema operativo Windows NT®, este no podrá arrancar. Si el disco duro de arranque se encuentra formateado con particiones del tipo FAT, se puede eliminar el virus arrancando desde DOS y utilizando un programa antivirus. Si la partición de arranque es del tipo NTFS se deberá de reinstalar el sistema operativo a través de los discos de instalación de Windows NT.

2.4.1.4 Virus Múltiples

Tienen la característica de infectar los registros de arranque, así como los archivos de programa. Presentan un grado de complejidad para su inhabilitación con cierta dificultad, ya que en ocasiones cuando se limpia el área de arranque, los archivos aún contienen el código vírico, lo que nos lleva a que el área de arranque se vuelva a infectar. Esto también sucede en sentido opuesto. Es por eso que se debe reconocer perfectamente este tipo de archivos, para poder inhabilitarlos y eliminarlos en ambas partes de los equipos.

2.4.1.5 Virus de Macro

Su área de infección de estos virus, son los archivos de datos. Son los más comunes debido a que no requieren de complicados métodos o conocimientos demasiado elevados en programación para poder realizarlos. Infectan archivos de Microsoft Office; Word, Excel, PowerPoint y Access. Se pueden crear virus de macro que infecten archivos de datos y desde que surgió Office 97, también infectan otros archivos. Su modo de operación consiste en automatizar ciertas tareas dentro del programa.

2.4.2 Caballo de Troya

Evocando a la Mitología Griega y en especial al libro de la Iliada (escrito por el historiador y filósofo Homero, aproximadamente 700 A.C.), surge el término de Caballo de Troya dentro del argot del cómputo por programas que tienen un comportamiento aparentemente loable o benigno y que al ser ejecutados (al igual que el caballo de Troya al ser ingresado a la ciudad de Troya) ataca al sistema. Su principal característica que puede diferenciar al comportamiento tradicional de un virus, es que NO se replican a si mismos, estos se ejecutan cuando se abre algún archivo adjunto de correo o ejecutando algún archivo. Estos son altamente utilizados como herramientas de *Hackeo*. Un ejemplo de uso es el programa mencionado en la sección 2.3.3.4 de la presente Tesis, en donde se incluyen los *Key Loggers*, Puertas Traseras, entre otros.

2.4.3 Gusanos

La principal característica de este tipo de programas es que se replican a sí mismos de sistema a sistema o de equipo a equipo sin la necesidad de utilizar un archivo para hacerlo. En esto radica la diferencia de los virus, que necesitan extenderse mediante un archivo infectado y se encuentran ocultos principalmente dentro de otros archivos. Los archivos mas comunes son documentos de Word® o Excel ®. Es de importante reconocer la diferencia entre virus y gusanos; esta radica en la forma en que los gusanos y los virus utilizan el archivo que los alberga. Normalmente el gusano generará un documento que ya contendrá la macro del gusano dentro. Así, el documento completo viajará de un equipo a otro, de forma que el documento completo debe ser considerado como gusano.

2.4.4 *HOAX*... Una Falsa Alarma

Los *HOAX* son falsas alarmas de virus que normalmente son enviados con mensajes por correo electrónico. Tal y como las famosas y en algunas ocasiones molestas "cadenas", son enviados y reenviados a través de la red.

De acuerdo a un listado de la empresa Symantec® [11], algunas de las expresiones mas utilizadas en Latinoamérica son las siguientes:

- Si recibe un mensaje de correo electrónico titulado (nombre de la falsa alarma de virus), no lo abra.
- Bórrelo inmediatamente.
- Contiene el virus (nombre de la falsa alarma).
- Borrará el contenido del disco duro y (aquí se especifica un peligro extremo e improbable).
- (Nombre de una empresa famosa) ha informado hoy de la existencia de este virus.
- Remita este aviso a todos sus conocidos

En algunas ocasiones existen falsas alarmas que invitan al usuario a eliminar algún archivo argumentando que dicho archivo es un virus "peligroso" que puede eliminar o dañar información. Sin embargo estos archivos a eliminar son archivos que requiere el sistema para operar de manera adecuada.

2.4.4.1 Errores en Equipo que No Son Virus

En ocasiones algunos problemas en un equipo, es mal interpretado y algunos usuarios culpan a los virus de ellos. A continuación se presenta un listado con los problemas que normalmente no son provocados por virus ni por otro código dañino [11].

- Problemas de hardware. No existen virus que puedan dañar físicamente el hardware. En otras palabras un virus no tiene la capacidad de dañar una tarjeta, chip, monitor o cualquier dispositivo y periférico.
- El equipo no registra 640 kb de memoria convencional. Aunque esto puede ser causado por un virus, no es el único problema por el cual se presenta este problema, algunos controladores del hardware pueden usar esta sección de memoria.
- Se tienen dos programas antivirus instalados en el mismo equipo y uno de ellos informa la existencia de un virus. En ocasiones uno de los antivirus detecta la firma del otro programa residente en memoria. Además existen problemas de compatibilidad entre antivirus, una razón mas para generar conflictos. No hay que olvidar que un antivirus ejecuta instrucciones para revisar archivos, carpetas o inclusive algunos se mantienen activos

revisando las carpetas mientras uno trabaja, razón por la cual el sistema se puede volver mas lento, esto debido a que se duplica el trabajo. Ejemplo, cuando se abre un archivo de Word®, el antivirus analiza que ese archivo no tenga virus, al tener dos antivirus, los 2 revisarán el archivo, duplicando el trabajo y disminuyendo los recursos del sistema.

- Cuando se ejecuta un programa como Word® o Excel® y aparezca un aviso de que el archivo contiene macros, no precisamente quiere decir que sea un virus, en algunas ocasiones se utilizan macros para automatizar algunas funciones de las hojas de cálculo o de algún formulario que se requiera de Word®, es por eso que se utilizan macros.
- No puede abrir un documento. Puede no estar infectado, para comprobarlo, se puede intentar abrir otro documento o una copia de respaldo del documento. Si otros documentos abren sin problemas, posiblemente el documento esté dañado.

2.5 Marco Regulativo

Para poderle dar una atención al problema de la piratería cibernética, es necesario que se conozca la legislación y el marco regulativo a nivel nacional e internacional. Así podremos emitir recomendaciones de operación en un sistema informático académico sin faltar a la legislación vigente y operar dentro de un marco de estado de derecho. Logrando así la posibilidad de poder actuar legalmente en caso de ser necesario.

2.5.1 Delitos informáticos

Ante las diferentes acciones ilegales que en diversas ocasiones se llevan a cabo por los piratas cibernéticos, se busca emitir diversas leyes o reglamentos para poder llevar a cabo acción penal y así mismo controlar este ámbito.

Entiéndase como delito a toda acción penada por las leyes por realizarse en perjuicio de alguien o por ser contraria a lo establecido por aquéllas [12].

2.5.2 Código Penal Federal

En el Código Penal Federal Titulo Noveno, Capitulo II "Acceso ilícito a sistemas y equipos de informática" se encuentra lo referente a la piratería cibernética. En el artículo 211 bis encontramos los diferentes casos en los que podemos contemplar como delito el acceso, modificación y otras actividades a sistemas informáticos. Estos son algunos de los delitos contemplados:

- Modificar, destruir o provocar perdida de información sin la autorización correspondiente en sistemas informáticos que cuenten con sistemas de seguridad. Esto contempla para sistemas privados y del Estado.
- Modificar, destruir o provocar perdida de información aunque cuente con la autorización correspondiente para acceder al sistema informáticos que cuenten con sistemas de seguridad. Esto contempla para sistemas del estado.

- Modificar, destruir o provocar perdida de información sin la autorización correspondiente en sistemas informáticos que cuenten con sistemas de seguridad. Esto contempla para sistemas financieros.
- Modificar, destruir o provocar perdida de información aunque cuente con la autorización correspondiente para acceder al sistema informáticos que cuenten con sistemas de seguridad. Esto contempla para sistemas del financieros.

De esta manera se cuenta con un parámetro efectivo para poder determinar cuales son las penas en las que puede incurrir un pirata cibernético en la institución académica. Y tenemos las herramientas para poder proceder con la acción penal correspondiente en caso de encontrarse frente a un caso de los antes mencionados.

2.5.3 Ley Federal de Derechos de Autor

En ocasiones existe dentro de la Piratería Cibernética el plagio de la información y en ocasiones es de vital importancia que se encuentre regulado. Supongamos que alguien tiene acceso a un artículo o publicación y que sea difundida antes de tiempo a través de medios electrónicos [14]. Si un fabricante de software descubre que su software está siendo distribuido ilegalmente, tendrá la capacidad de poder reconocer en que momento están incurriendo en un delito en contra de los derechos de autor.

La Ley Federal de los Derechos de Autor, protege al autor de programas y a los poseedores de información.

- Los programas de Cómputo poseen la misma protección que los libros (obras literarias). Se extiende a programas operativos y aplicativos, ya sea en código fuente o código objeto. Algo interesante es que se exceptúan de protección de derechos de autor a todos aquellos programas que busquen dañar a otros programas o equipos. (art. 103, [14])
- Las Bases de datos o de otros materiales, quedan protegidos como compilaciones, siempre y cuando la disposición de contenido constituya creación intelectual. (art. 107, [14])
- Sin embargo las bases de datos que no son originales , de acuerdo a la LFDA, son para uso exclusivo por quien las haya elaborado, durante un lapso de 5 años. (art. 108, [14])
- Es común que nuestra información personal sea publicada mediante la común venta de bases de datos de correos electrónicos o de nuestras direcciones, es por eso que el artículo 109 [14] que protege la información de carácter privado relativa a las personas, contenida en las bases de datos que indica el artículo 108 de la publicación, divulgación, comunicación y transmisión sin la autorización previa de las personas que se trate. Este tipo de actividades son permitidas únicamente para fines de investigación, las autoridades competentes mediante los procedimientos adecuados.

2.5.4 Acuerdos Internacionales

Debido a que para la Internet no existen fronteras, debe de existir un organismo regulador para que sean reguladas todas actividades y lograr así un control de las jurisdicciones, así como de las distintas actividades y transacciones internacionales. Supongamos que alguna persona en México contrata a un pirata cibernético que se encuentra en Brasil y que desean afectar a un usuario que se encuentra en Inglaterra. Sin los acuerdos internacionales, sería muy fácil que los agresores salieran ilesos y sin problema alguno, o talvez los cargos serían muy limitados.

Décimo Congreso de las Naciones Unidas sobre la Prevención del Delito y Tratamiento del Delincuente

Derivado de este congreso, surgen distintos acuerdos materia del delito informático. Para ello, se requiere que existan sanciones para los infractores de la ley. Por lo tanto existe un apartado en el cual nos habla del tratamiento de los delincuentes. Sin embargo hay que conocer como visualiza el congreso algunos términos que son de uso común.

En su tema 5 referente a la "Prevención eficaz del delito: adaptación a las nuevas situaciones", en su apartado de "Delitos relacionados con las redes informáticas". Mismo que contemplados categorías de delitos cibernéticos:

a) Delito cibernético en sentido estricto ("delito informático"): todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos;

b) Delito cibernético en sentido lato ("delito relacionado con computadoras"): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos.

De acuerdo a la definición del párrafo anterior, el delito informático está en relación con todo comportamiento ilegal que atente contra la seguridad de sistemas y datos mediante operaciones electrónicas. La seguridad de los sistemas y datos informáticos puede determinarse en función de tres principios: garantía de confidencialidad, integridad o disponibilidad de los datos y funciones de procesamiento. De conformidad con la lista de la Organización de Cooperación y Desarrollo Económicos, de 1985 y la Recomendación formulada en 1989 por el Consejo de Europa, que es más detallada, los delitos contra la confidencialidad, la integridad o la disponibilidad incluyen:

a) El acceso no autorizado, es decir, el acceso sin derecho a un sistema o una red informáticos violando medidas de seguridad.
b) El daño a los datos o a los programas informáticos, es decir, borrado, la descomposición, el deterioro o la supresión de datos o de programas informáticos sin derecho a ello.
c) El sabotaje informático, es decir, la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, o la interferencia en sistemas

informáticos, con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones.

d) La interceptación no autorizada, es decir, la interceptación, realizada sin autorización y por medios técnicos, de comunicaciones destinadas a un sistema o a una red informáticos, provenientes de ese sistema o esa red o efectuadas dentro de dichos sistema y red.

e) El espionaje informático, es decir, la adquisición, la revelación, la transferencia o la utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona.

2.5.5 Entidades Nacionales Gubernamentales Encargadas de la Supervisión

Para velar por el cumplimiento de lo indicado en las leyes mexicanas, es importante que existan entidades gubernamentales que integren en su organigrama áreas de inteligencia y seguridad informática para que hacer cumplir la ley.

2.5.5.1 Secretaría de Seguridad Pública Federal

El poder ejecutivo habilitó a través de la Secretaría de Seguridad Pública Federal, un área de especialización dependiente de la Policía Federal Preventiva, que a través de las atribuciones legales y con la finalidad de garantizar la presencia de la autoridad en la supercarretera de la información, estableció la Unidad de Policía Cibernética.

La Unidad de Policía Cibernética posee una estructura orgánica que le permite atender 2 problemáticas principales. La primera de ellas, realiza actividades de acciones preventivas en materia de delitos cometidos por la Internet, así como aquellos que hayan usado medios informáticos. La segunda y que es sin duda alguna una gran noticia que se destinen recursos del erario para esta finalidad, tiene que ver con la materia de prevención y atención a denuncias de delitos contra menores; un esquema utilizado en países de primer mundo.

Estas son algunas de las principales actividades que desempeña la Unidad de Policía Cibernética:

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de paidofilia, así como de redes de prostitución infantil.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos utilizando computadoras.
- Realización de operaciones de patrullaje anti-hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

- Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve una cultura de legalidad, respeto y seguridad en la red.

2.6 Impacto Económico

El impacto económico que ha generado y producido la actividad de los piratas cibernéticos se ve reflejada directamente en los usuarios de la Internet. Los principales fraudes cometidos por los piratas cibernéticos, son los de fraudes a usuarios finales. Eso lo podemos constatar en las cifras estadísticas que obtenidas por la IFCC (Internet Fraud Complaint Center, Centro de Quejas sobre fraudes de Internet).

De acuerdo a la IFCC [16] en el 2002, el fraude por la Internet, supero a otros fraudes como la mayor ofensiva en este aspecto, estando integrado por el 46.1% de los fraudes. Esto representa un incremento del 7.7% con respecto al 2001 (42.8%); mientras que las quejas por productos no entregados disminuyo del 2001 al 2002 del 54.2 % al 31.3% y las quejas sobre tarjetas de crédito y débito disminuyeron del 23.4% al 11.6%.

En números son 48,252 el total de las quejas por fraudes procesadas por la IFCC durante el año, 36,332 fueron victimas de pérdidas económicas. El total de pérdidas económicas en los casos indicados durante el 2002 fue de $54 millones, comparándolo con lo del 2001 que fue una pérdida registrada de 17 millones.

La IFCC también nos entrega un resultado de el género de los perpetradores, y nos arroja un 21.3% mujeres y el 78.7%; esto es que aproximadamente 4 de cada 5 víctimas. La mitad del los hombres viven en California, Florida, New York, Texas, Illinois y Pensilvania.

2.7 Conclusiones del Capítulo

Es interesante comprender el valor que la información puede llegar a tener. No solo por el valor económico, sino por el valor estimativo. Cuando una persona tiene cierto valor por la información puede ser muchísimo mayor el valor que tiene al valor que le puede tener la persona número 2. Sin embargo muchas veces no hacemos lo necesario o lo suficiente para resguardarla. Se cree que jamás nos va a pasar.

Es por eso que surge la piratería cibernética, por el interés por obtener la información a como de lugar. Esto es un efecto que comúnmente se da en las escuelas por los alumnos, entre ellos y contra los profesores. En algunas ocasiones para robar información como calificaciones, exámenes, alteración de la información e inclusive la negación del servicio. En resumen, la información tiene el valor que representa para cada persona.

En ocasiones y dependiendo de la situaciones y necesidad, la información es una necesidad en la actualidad para muchas ramas de trabajo.

Uno de los principales elementos que hay que conocer, es la arquitectura de comportamiento de un pirata cibernético para atacar e ingresar a las áreas de seguridad. Su *modus operandi*.

También hay que tomar en cuenta los riesgos físicos para poder proteger a nuestro sistema como los incendios, inundaciones, sismos, seguridad y otros fenómenos naturales y sociales que pudieran poner en riesgo nuestra información.

Se concluye que para poder reconocer los puntos débiles del hacker, hay que conocerlo, no solo como un ente que nos pueda afectar, sino también como un ser humano con inquietudes por obtener mayor información.

Se conocieron las diferentes herramientas que utilizan los hackers para ir perpetrando a través de la red de acuerdo a la arquitectura de comportamiento de un pirata cibernético, que va desde la investigación, pasando por el uso de ingeniería social e instalación de programas de hackeo.

Además de las amenazas humanas existen los virus, que aunque son producto de la programación de hackers, merecen ser tratados con su debido cuidado para evitar la infección y pérdida de información.

El marco regulativo es un punto muy importante que no hay que olvidar, porque en ocasiones somos atacados y de acuerdo al marco regulativo, podremos saber como proceder. Sin embargo también nos sirve para no diseñar nuestras políticas de seguridad fuera de un marco regulativo y así evitar caer en ilegalidades a nivel nacional e internacional.

Figura 2.1. Conceptos de Seguridad [3]

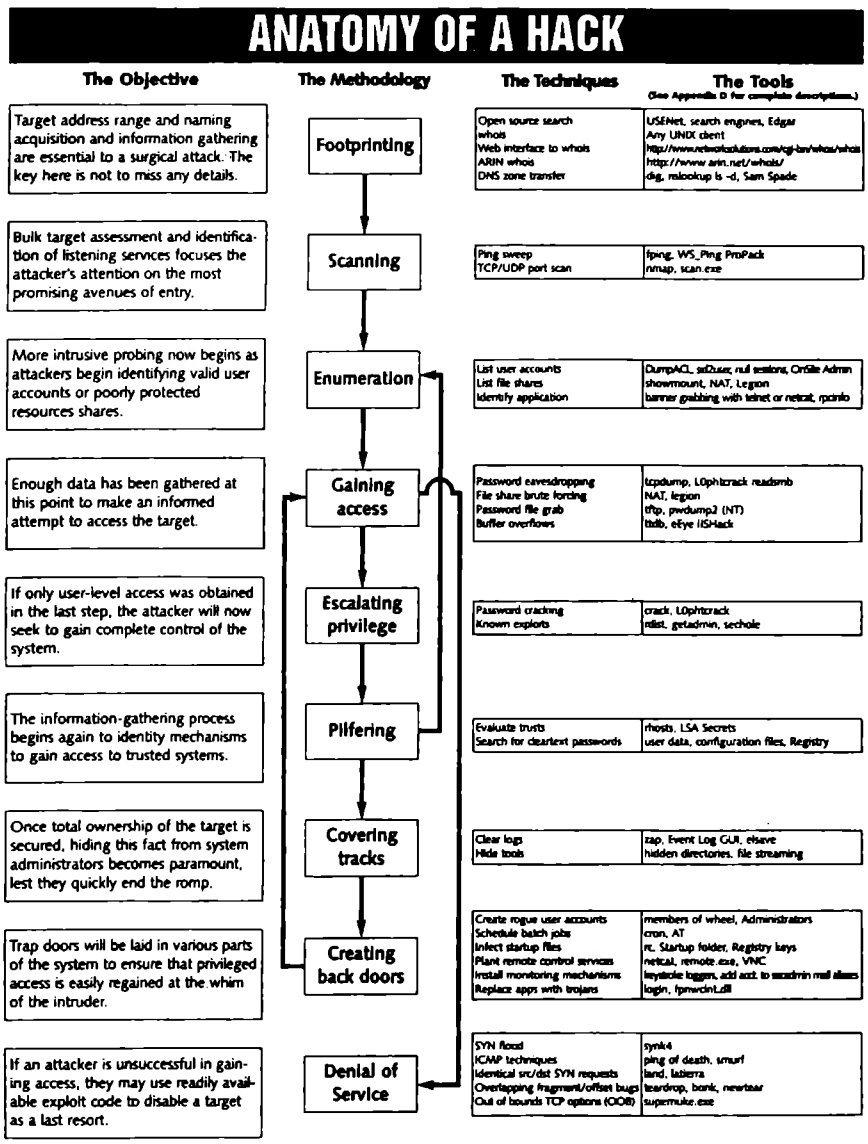

Figura 2.2 Arquitectura de un ataque [4]

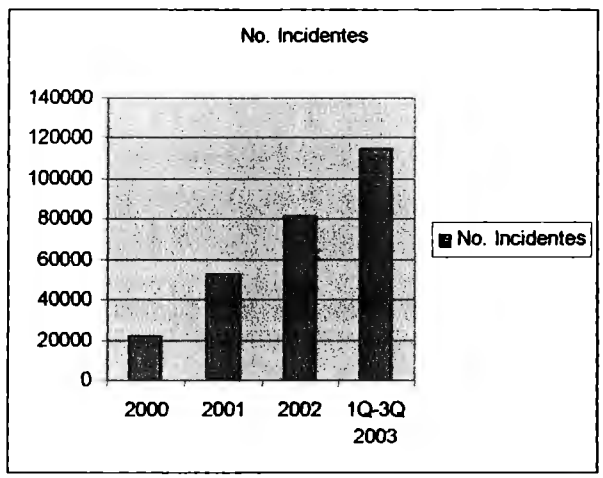

Figura 2.3 Número de Incidentes [9]

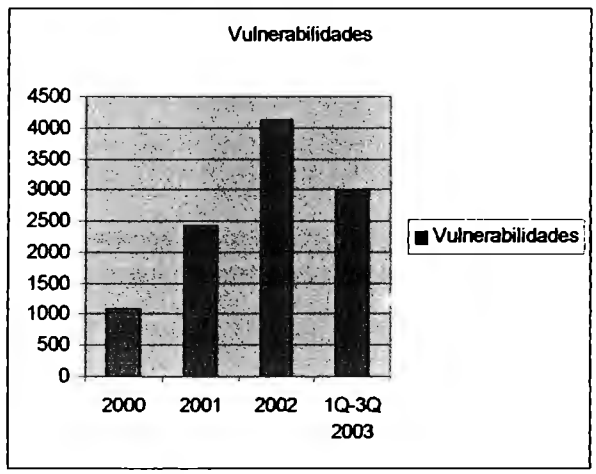

Figura 2.4 Vulnerabilidades [9]

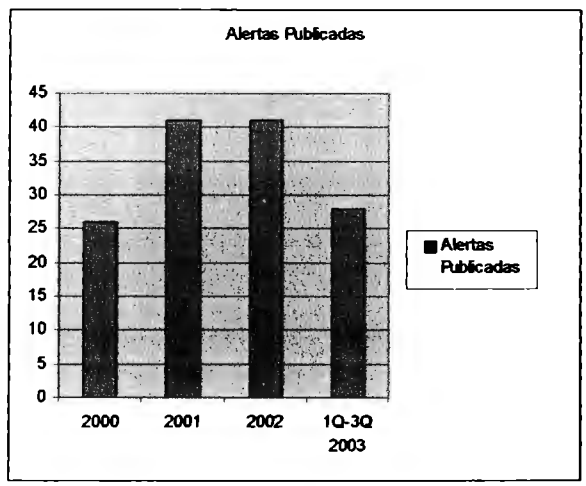

Figura 2.5 Alertas Publicadas [9]

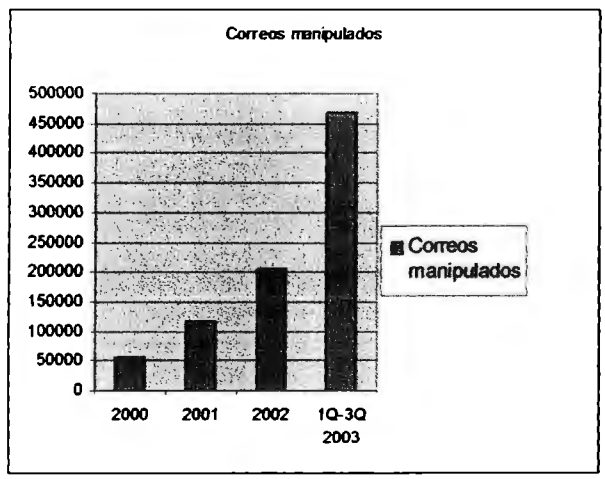

Figura 2.6 Correos Manipulados [9]

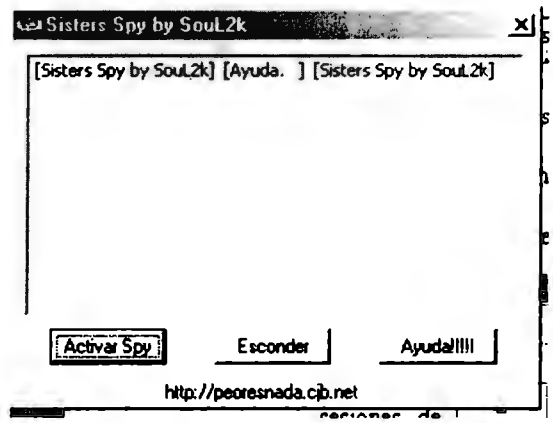

Figura 2.7 Pantalla de Programa "Sister Spy"

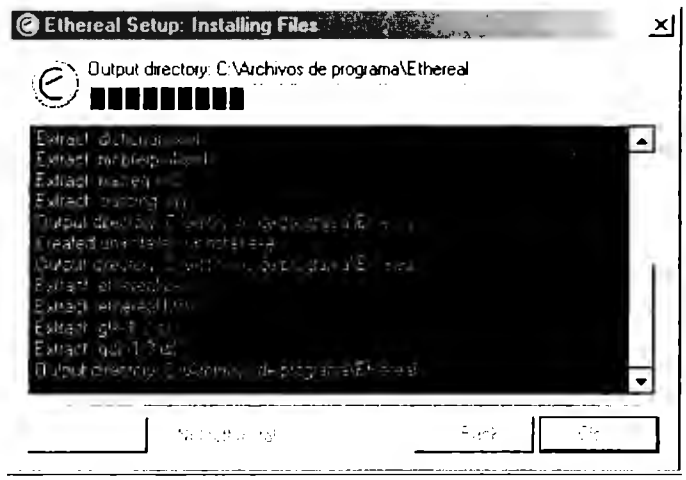

Figura 2.8 Ethereal Setup

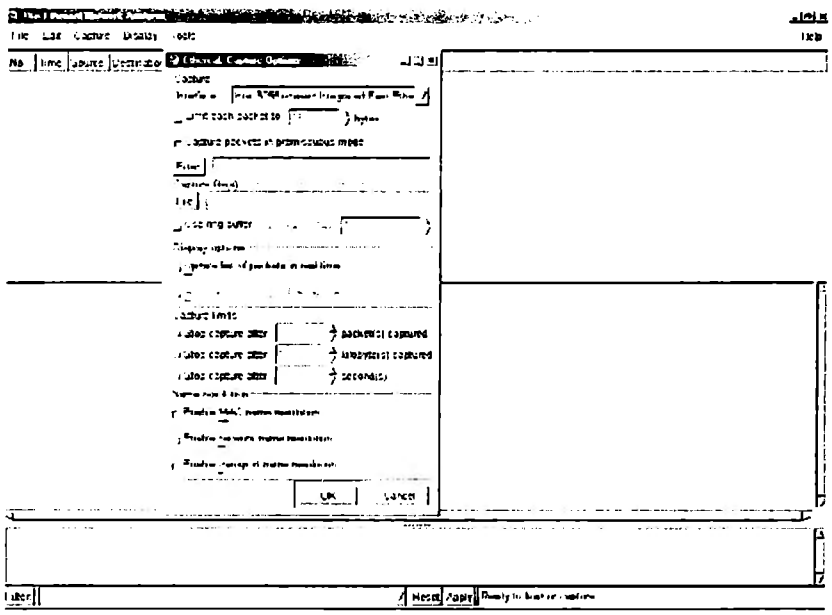

Figura 2.9 Ethereal

Referencias

[1] Microasist. http://microasist.com.mx/noticias/en/mpeen0803.shtml, artículo. Artículo Obtenido el 28 de Marzo del 2003.

[2] Entrada a FMM Educación, http://www.fmmeducacion.com.ar/Informatica/infoeduc.htm, artículo, 20 de marzo de 1999, Federico Martín Maglio, Buenos Aires, Argentina. Artículo Obtenido el 30 de Marzo del 2003.

[3] Conceptos de Seguridad, http://www.unap.cl/~setcheve/ac/AsignaturaAC2002-16.htm, artículo; imagen, ©2002, Sergio Etcheverry G. Artículo e imagen tomados el día 27 de Marzo del 2003.

[4] Seguridad computacional, Arturo García, Trimestre Ene-Mar 2003

[5] How to become a hacker, http://www.catb.org/~esr/faqs/hacker-howto.html, artículo, ©2001, Eric Steven Raymond, artículo tomado el día 5 de julio de 2003.

[6] http://www.online.com.mx/el_heraldo/reportajes/20030309/2.html, El Heraldo de Chihuahua Domingo 09 de Marzo del 2003

[7] Domótica, http://www.domotica.net/Sistemas_contra_incendios.htm, 9 Marzo 2003

[8] VIRUSPROT, http://www.virusprot.com/Curiosid4.html, tomado el día 20 Octubre 2003

[9] CERT/CC Statistics 1998-2003, http://www.cert.org/stats/cert_stats.html#incidents, 17 Octubre 2003, Carniege Mellon CERT Coordination Center, artículo tomado el día 17 de octubre de 2003.

[10] Mitos Sobre ICMP, http://www.idg.es/iworld/articulo.asp?id=113039&n=31&sec=iworld, artículo, Copyright © 1997-2000 Gonzalo Álvarez Marañón, CSIC, artículo tomado el jueves 27 de marzo de 2003.

[11] "Diferencias entre virus, gusanos y caballos de troya", http://service1.symantec.com/SUPPORT/INTER/navintl.nsf/la_docid/pf/2001092109524 8905, 21-09-2001, Symantec, artículo tomado el 2 de Mayo de 2004.

[12] "María Moliner: Diccionario de uso del español", Anne Jarraud Milbeau, Silvia Ramón Jarraud, Fabián Ramón Jarraud, Helena Ramón Jarraud; Segunda Edición, Editorial Gredos, S.A. Madrid 1998.

[13] "Código Penal Federal" H Congreso de la Unión, cámara de Diputados, Última Reforma DOF, 26-05-04.

[14] "Ley Federal del Derecho de Autor" H Congreso de la Unión, cámara de Diputados, Última Reforma DOF, 23-07-03.

[15] "Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente", ONU, Abril 2000, Tema 5 "Prevención eficaz del delito: adaptación a las nuevas situaciones".

[16] IFCC 2002 Internet Fraud Report, January 1, 2002 – Dec. 31 2002; Prepared by The National White Collar Crime Center and the FBI.

Capítulo 3

Pruebas y Aplicaciones

3.1 Vulnerabilidades de acceso al sistema

Existen diversos medios de acceso al sistema que pueden ser buenos medios para que un "hacker" ejecute sus fechorías. Estos puntos de acceso o medios de acceso, son los siguientes:

- Red Alambrada
- Red Inalámbrica

Estos medios de acceso, al ser normalmente públicos para el acceso a los estudiantes, son excelentes para propagar virus, analizar archivos, revisión de datos, intercambios de archivos, intrusión a las redes personales.

3.1.1 Acceso inalámbrico

La tendencia de las redes de área local se basan en el uso de las redes inalámbricas, debido a su versatilidad , facilidad, movilidad y otros beneficios que hacen de esta tecnología una tecnología noble que tiene muy buena aplicación para usuarios que no requieren de una alta demanda en anchos de banda.

Sin embargo existe un aspecto que en el cual hay que pensar antes de instalar una red inalámbrica y ese es la seguridad informática. Las amenazas son las mismas a las de

las redes alambradas. Pero difieren en que las redes inalámbricas tienen mayores puntos de acceso (ya que en estas no se requiere de un punto en específico para que conectarse como en las alambradas).

Al ser tan versátiles y móviles las redes inalámbricas, es por eso que podemos acceder a ellas desde puntos donde nadie se podría imaginar. Si un nodo no se encuentra bien configurado con la potencia adecuada, podríamos estar llegando con el nodo a lugares de acceso no controlado. Es decir, muchos podrían estarse conectando a la red de la escuela estando físicamente afuera de la barda que divide el predio de la escuela de la calle. Inclusive, pueden estar utilizando los recursos si alguien vive junto a la escuela.

3.1.2 Pruebas y Vulnerabilidades del Acceso inalámbrico

Una prueba de la facilidad que se tiene para la captura de datos a través de programas como "IP Scanners" (ver figura 3.1), "Sniffers" (ver figura 3.2). La adquisición de estos programas es relativamente sencilla, ya que son del tipo libre. Por esta razón, únicamente se requiere tener conocimientos básicos y se podrán analizar los paquetes con relativa facilidad, ya que se puede conocer la IP de los equipos en red, el nombre de los equipos y el tráfico de datos de estos equipos.

Una desventaja de acceso a los recursos de una red inalámbrica de institución académica es que en algunas escuelas se puede acceder a las redes inalámbricas desde fuera, esta es una de las pruebas que se realizaron a algunas escuelas.

Para poder disminuir el riesgo de que la información sea analizada por personas no aceptadas o deseadas en una red inalámbrica, se puede hacer uso de la Privacidad

Equivalente Alámbrica (WEP), una tecnología que forma parte de la norma 802.11b que se encarga de cifrar los paquetes transmitidos. El problema de la WEP, es que hace uso de claves estáticas como parte de su metodología de encriptación, que en cierta forma facilitaban la intercepción de los paquetes suficientes para descubrir la clave y por lo tanto se puede descifrar el tráfico codificado[3]. Por esta razón, es que inicialmente los "Hacker" experimentados descubrieron diversas formas de hacer uso de los distintos medios y herramientas para analizar la información en tráfico. El problema es que los "Hackers" desarrollaron herramientas de uso sencillo para los piratas cibernéticos de poca experiencia y que fácilmente se pueden usar en estos medios. Dejando así abierta la posibilidad de inclusive sustituir los paquetes enviados por un usuario.

3.1.3 Acceso a Redes Alámbricas

A diferencia de las inalámbricas, estas nos brindan la seguridad de acceso a la red a través de un punto de red, esto obliga a que cualquier usuario a tener que estar dentro del campus (siempre y cuando no existan conexiones clandestinas a través de módems o dispositivos similares). Las aplicaciones para ataques en las distintas plataformas y para este medio, son las mismas que para los de red inalámbrica.

3.1.4 Otros dispositivos inalámbricos

Tarde o temprano el uso de dispositivos inalámbricos tales como los teléfonos celulares y PDA's (Personal Digital Assistant; Asistente Digital Personal), podrán abarcar el mercado de las telecomunicaciones inalámbricas para fines académicos. Por el

momento no tienen mucha función o aplicación académica otorgada por las instituciones académicas, pero di lo tienen por los estudiantes. Por experiencia propia, recuerdo que un compañero en la carrera utilizaba un teléfono celular y el cable para manos libres (ambos escondidos), para realizar una llamada telefónica a algún compañero y dictarle las preguntas del examen, quien a su vez hacía uso de los apuntes para darle las respuestas. Ese tipo de comportamiento se ha detectado en diversas escuelas del mundo. Es por eso que se han buscado soluciones a ese tipo de actividades.

Al norte de Italia en el Enrico Tosi Technical Institute, encontraron una forma mas efectiva de solucionar este tipo de problemas [1]. En lugar de hacer uso del método convencional de recoger los equipos celulares antes de entrar a clases, se instalaron unos dispositivos llamados C-Guard, fueron desarrollados por expertos militares y en la industria de defensa para Netline Copmmunications Technologies. Estos dispositivos bloquean la señal de los celulares en un radio de aproximadamente 80 metros en espacios cerrados.

En México existe una compañía que comercializa este tipo de productos, es la compañía UNICOM con el producto Restrict-O-Cel LP. También tienen aplicaciones para usar en cines, teatros, hospitales, iglesias, restaurantes exclusivos, centros deportivos, entre otros lugares.

3.1.5 Puertos Disponibles

Para poder tener un mejor control del acceso a los diferentes recursos de las instituciones académicas a través de un servidor proxy, se deben conocer los puertos

disponibles y mas comunes, de manera que los estudiantes y piratas cibernéticos no dispongan de los puertos abiertos. Ver anexo 1[2]

También es conveniente tener una referencia de los puertos que algunos virus troyanos abren para permitir el tránsito de datos de acuerdo a lo configurado por los creadores de los virus. Ver anexo 2 [2]

3.1.6 Pruebas a Redes

Una prueba realizada dentro de una red empresarial con la finalidad de encontrar la vulnerabilidad de los diferentes equipos conectados a esta red para protegerse del tan conocido y altamente propagado virus del tipo gusano, W32.Sasser.B.Worm (conocido así por la empresa Symantec®).

Antes de describir los resultados, es importante conocer al virus, así como su comportamiento.

3.1.6.1 W32.Sassser.B.Worm [4]

El gusano Sasser B, es una variante del gusano W32.Sasser.Worm. Mismo que explota la vulnerabilidad del LSASS. Su medio de propagación se caracteriza por realizar un escaneo aleatorio los puertos previamente seleccionados. Una vez detectado el puerto abierto, se propaga a través del mismo.

Se dice que es una variante al gusano W32.Sasser.Worm, porque opera de igual manera, pero utiliza un diferente "mutex" y tiene un nombre de archivo diferente:

"avserve2.exe". Tiene un código diferente: MD5. Y crea un diferente valor en el registro: "avserve2.exe".

Este gusano también es conocido por varios nombres dependiendo de la empresa: WORM_SASSER.B (Trend), W32/Sasser.worm.b (McAfee), Worm.Win32.Sasser.b (Kaspersky), W32/Sasser-B (Sophos), Win32.Sasser.B (Computer Associates), Sasser.B (F-Secure), W32/Sasser.B.worm (Panda), Win32/Sasser.B.worm (RAV), W32/Sasser.B (F-Prot).

Su número de infecciones, fue mayor a los 1000 equipos, 10 sitios, con una alta distribución geográfica.

3.1.6.2 Prueba de vulnerabilidad de puertos realizada

Las pruebas realizadas a este equipo, se realizaron 2 semanas después del surgimiento del virus W32.Sasser.B.Worm y se realizó escaneando el puerto 5554 de las distintas IP's de una red informática empresarial.

Para la realización de esta prueba, se utilizaron herramientas que recurren al envío de pings y trazar de rutas. El primer utilizado es el fping, sin embargo por lo lento del programa, se recurrió a "IP scanner" para detectar los equipos conectados y a través de "visual route" se determinaron los distintos equipos y puertos disponibles.

El resultado de las pruebas realizadas, se puede encontrar en el Anexo 3.

Se analizaron 99 equipos de cómputo, de los cuales, el 54,55% de los equipos, presentaron vulnerabilidad ante el puerto 5554, lo que significa que no se habían aplicado los parches correspondientes a la vulnerabilidad descrita en el boletín de seguridad de

Microsoft® No. MS04-011. Tomando en cuenta que esto fue solo un muestreo de lo que puede darse en un sistema o red informática, podremos determinar concluir que no han sido seguidas las políticas de seguridad informática establecidas, ya que existen ciertas labores que a través de las áreas de informática y con los dispositivos remotos, no es posible cubrir.

3.2 Conclusiones del Capítulo

Es importante que la teoría se vea representada en la práctica, y si algunas herramientas demuestran la fragilidad de las redes, es importante conocer cuales son las acciones en vivo que se pueden correr o desarrollar.

Tal es el caso de las redes inalámbricas, las cuales muestran una fragilidad a diferentes herramientas, tales como los sniffers, IP Scanner's y programas diversos. Además la desventaja es que cuando existe algún tipo de ataque, es mas difícil reconocer el punto exacto del ataque e inclusive se puede llegar a dar desde zonas externas de las instalaciones.

Las redes alámbricas padecen de herramientas similares a las de las inalámbricas, pero brinda la ventaja de seguridad que requiere de un nodo cercano para conectarse y físicamente tiene que estar presente el usuario.

Existen otros dispositivos inalámbricos que proveen problemas en las instituciones académicas por la deshonestidad académica en la que pueden recaer los estudiantes . Como pasar las respuestas entre los compañeros en los exámenes o

simplemente la interrupción de las clases. Para ello ya existen dispositivos que trabajan en contra de este tipo de comportamiento.

Interesante que se tengan los puertos que son disponibles, así como algunos que son atacados por los virus, para poder prevenir cualquier ataque y además reconocer la utilidad de muchos que en ocasiones no se dejan abiertos sin saber que pueden ser elementos de inseguridad.

La prueba realizada a la empresa, demuestra como en ocasiones aún cuando se poseen políticas empresariales de seguridad informática, existen deficiencias. Es por eso que se debe de tener una mentalidad mas proactiva tanto por las empresas, instituciones académicas, personal y estudiantes.

Figura 3.1. "IP Scanner"

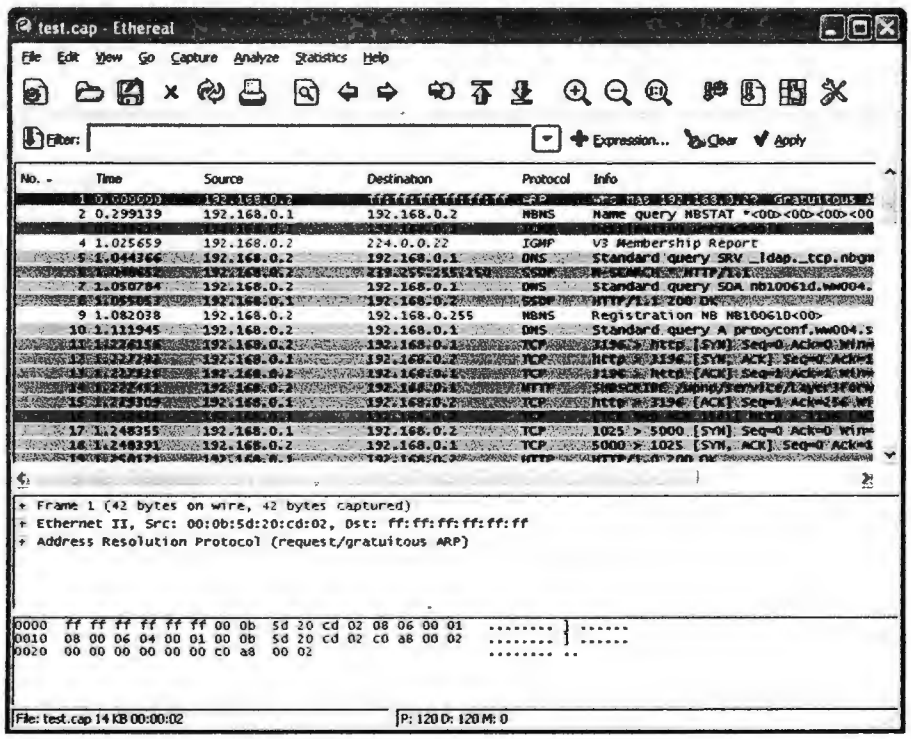

Figura 3.2. "Sniffer Ethereal"

Referencias

[1] "Las escuelas instalan un dispositivo para anular la señal de los móviles" Fuente: Europa Press, 21/06/2004.

[2] "Delitos informáticos-puertos" by ripper, última actualización 15 de marzo 2001 http://www.delitosinformaticos.com/hacking/puertos.shtml

[3] "Como reformar la seguridad inalámbrica LAN" Publicado en EEUU 20 de enero de 2004, publicado en LAM 18 de Febrero de 2004, Thomas Schmidt.

[4] Symantec Security Response – W32.Sasser.B.Worm, W32.Sasser.B.Worm, http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.sasser.b.worm.html , reporte; ©2004.

Capítulo 4

Propuesta de Procedimientos

La principal aportación que se genera de esta tesis parte de la recopilación integral de los distintos capítulos que abarcan la tesis. Una vez retomados todos los capítulos se analizan y se descubren aquellos puntos de falla que existen en una institución académica. Lo importante es que estos procedimientos se encuentran enmarcados en un concepto genérico para poder ser aplicado en diversas instituciones académicas.

4.1 Aspectos Generales

4.1.1 Limites

Con la finalidad de mantener un estrecho y efectivo control sobre los recursos de la red, es importante delimitar los alcances y el objeto de los recursos.

Con el crecimiento de la Internet, esta se ha convertido en una fuente inagotable de información y recursos para los estudiantes. Tomando en cuenta que las instituciones académicas cada vez se entrelazan con otras a través del intercambio de conocimientos, es una buena idea el crear políticas que contemplen el uso de la "RED DE REDES"

En primer lugar, debemos de definir la aplicación de la Internet.

- Describir lo que se considera aceptable para uso de Internet. Como ejemplo, los servicios de mensajería instantánea pueden ser aceptados para usos académicos, intercambio de información integración de equipos de trabajo, disminución de costos, comunicación. Pero posiblemente no se acepte este tipo de recursos, ya que pueden ser usados para distraerse en clase, intercambio de archivos no deseados y otros usos no deseables. En esta etapa debemos definir programas de intercambio de archivos, y de "transferencia" de archivos de música.
- Fines académicos. Se tiene que marcar la pauta para indicar los fines académicos, es decir, se tiene que indicar la razón por la cuál los recursos son académicos e indicar su aplicación. Por ejemplo, se indica que existe el correo electrónico y se señala que el correo electrónico es un recurso de comunicación entre equipos de trabajo, para que el personal docente se comunique con los estudiantes, entre otros.
- Pueden existir estrategias institucionales para apoyar el acceso a Internet como una herramienta para estudiantes. En este caso se puede recurrir a estrategias como las siguientes:
    - El profesor puede motivar el uso de foros públicos para la aportación de ideas o para publicación de trabajos; o en caso de que las instituciones cuenten con foros dedicados a esos fines, se puede fomentar el uso de esos recursos.

- Fomentar el uso en clases (si existe el medio para realizarlo) de bibliotecas digitales.

- Recurrir a prácticas seguras y responsables del manejo de la Internet por los profesores, estudiantes y en algunos casos, padres de familia. Esto se refiere a no hacer publicas las contraseñas personales, porque como se indicó en el inciso 2.5.2 de este documento, el uso indebido de recursos (aún cuando existe autorización) puede incurrir en delito.

- Compromiso de los usuarios de consentimiento y exención por cumplir y respetar las políticas establecidas.

4.1.2 Actividades Escolares

Dentro de la problemática que deriva de lo indicado en el inciso 2.3.1 el joven pirata cibernético tiene inquietudes por el exceso de tiempo. Por lo que al tener un exceso de tiempo, el joven estudiante, busca romper con esas barreras que el sistema le ha creado e impuesto. Sin embargo si su tiempo libre se puede reducir, el riesgo en el que estaríamos incurriendo sería menor, ya que dispondrían de menor tiempo para realizar los análisis con los que comúnmente hacen los atentados los "piratas cibernéticos" esto se puede lograr mediante una carga efectiva de actividades curriculares y extracurriculares. Que permitan al estudiante enfocar su energía en actividades mas productivas. Hay que aclarar que esta sección es únicamente preventiva e inclusive no garantiza que el estudiante no haga uso inadecuado de los recursos.

4.1.3 Actualización

Así como la informática se va desarrollando día con día, debemos de recordar que los "hacker" buscan también nuevas estrategias de ataque. Por lo tanto debemos de mantener actualizadas de acuerdo a los cambios de los sistemas nuestra red, con el objeto de esconder el mayor tiempo posible la estrategia empleada por las políticas de seguridad emitidas por la institución académica.

4.2 Seguridad Informática (nivel lógico)

La seguridad contenida en esta rama, debe de cumplir con los principios básicos de la seguridad informática descrita en el capitulo 2.2.1 de este documento. Para lograr esta seguridad podemos ir clasificando cada uno de los elementos que nos brinden seguridad a nivel de software. Así mismo, para tendríamos que clasificar de acuerdo a las necesidades de escuela de acuerdo a los siguientes subtemas

4.2.1 Protección antivirus

El primer paso por el que podemos cubrir y proteger nuestra red, es la protección antivirus de los equipos que se encuentran en la red. Para lograr esto, se debe asegurar que todos los equipos que se encuentren conectados en la red, posean un antivirus que proteja la información contra posibles ataques de virus. Esto se puede obtener mediante la adquisición de una licencia corporativa que permita a los usuarios de la red, el uso del antivirus.

Se deben de mantener actualizados los antivirus de los equipos conectados a la red. Para lograr esto, existen 2 posibilidades de operación.

- La primer posibilidad es mediante la difusión y promoción entre los usuarios, mediante correos electrónicos programados para enviar a los usuarios, invitándolos a actualizar su antivirus. indicar dentro de las políticas y/o reglamento para el uso de la red.
- La segunda posibilidad requiere de un programa de antivirus que se configura para que el equipo al encontrarse conectado en la red, se comunique a un servidor (dentro de la red) quien este a su vez envía la instrucción de actualización de las definiciones de virus.

Se debe restringir el uso de programas "piratas", ya que la mayoría de las veces, estos programas no poseen una política antivirus.

Otra fuente de riesgo para la difusión de los virus, es a través del correo electrónico. Por lo tanto se deben adoptar políticas restrictivas que contemplen recomendaciones a los usuarios del correo electrónico para que efectúen las siguientes recomendaciones:

- Evitar el reenvío de las "cadenas" de correos electrónicos, ya que estas normalmente poseen códigos maliciosos.
- Evitar abrir correos electrónicos cuando no conozcan al remitente del mismo.

- Configurar los programas de antivirus (en el caso de que se utilice correo electrónico por POP3, SMTP o un servidor dominó), para que revisen los correos automáticamente al momento de su recepción y/o envío.

Un factor muy importante y que en ocasiones se descuida, es el intercambio de archivos con medios magnéticos. Este intercambio de archivos a través de disquetes, discos compactos, memorias USB; propicia a la difusión de diversos virus, tales como los virus de sector de arranque y los virus del sector de arranque maestro.

Otra recomendación, aunque en ocasiones no es muy respetada, propone no acceder a páginas de pornografía, hackeo y de origen desconocido, ya que muchas de estas páginas utilizan los pop-ups para instalar programas de hackeo o programas de auto marcado vía telefónica a través del módem (y por lo regular estas llamadas son de larga distancia).

4.2.2 Seguridad en Transmisión de Datos

En algunas ocasiones, nos podríamos encontrar en la necesidad de enviar archivos importantes a través de la red. Pero como enviarlos sin que sean alterados o violados los datos.

Dependiendo de la aplicación y la necesidad del usuario para el envío de información privada, se puede decidir que aplicaciones utilizar. Supongamos que existe un profesor que desea enviar información con calificaciones y en ocasiones podría ser información valiosa para un pirata cibernético. Que mejor que enviar la información codificada.

Existe una solución que inclusive es de aplicación pública: PGP[1].

4.2.2.1 PGP [1]

PGP es el acrónimo de "Pretty Good Privacy". Su creación data del año 1991, por Phil Zimmerman (PZ). Originalmente surgió como un programa que utilizaba algoritmos conocidos, tales como IDEA, MD4, MD5, RSA. Por esta razón, RSA trató de demandar a Pgil Zimmerman por el uso de licencias sin la autorización correspondiente, así mismo, EUA determino que la exportación de PGP era ilegal, ya que este producto comenzó a ser exportado debido a su popularización. Posteriormente se realizó un fondo común para la defensa de Phil Zimmerman. Actualmente existe una parte de software comercial y otra de software libre.

Lo que se puede hacer con este correo es codificar la información de un correo electrónico para poderlo enviar de una forma segura, así si es interceptado, no lo podrán abrir si no es el destinatario autorizado, ya que hace uso de llaves de seguridad.

4.2.2.2 VPN [2]

VPN es el acrónimo de "Virtrual Private Network" y tiene como función la interconexión de los componentes y recursos de una red con los de otra, de una forma segura. Las VPN's logran esto permitiendo que el usuario haga un "túnel" a través del Internet o de otra red pública de una manera que deje a participantes del túnel gozar de la misma seguridad y características antes disponibles solamente en redes privadas.

La VPN permite conectar sucursales de una manera segura realizando una conexión punto a punto, esto puede ser utilizado para interconectar un equipo con un servidor de datos para iniciar sesiones y modificar datos o calificaciones de una forma segura. Ver figura 4.1.

4.2.3 Control de Accesos

Para algunas aplicaciones hay que tener los accesos controlados a los distintos recursos del sistema. Si tenemos que acceder a los correos electrónicos, es importante contar con un mecanismo de recomendación para crear claves de acceso. Estos procedimientos se basan en estudios estadísticos de tal manera que sean las combinaciones mas difíciles de descubrir por un hacker.

Estas son algunas de las recomendaciones que Symantec® recomienda para la elaboración de claves de usuario:

- Use una combinación de letras mayúsculas y minúsculas, símbolos y números.
- Asegúrese de que sus contraseñas tengan por lo menos ocho caracteres. Si tienen más caracteres, será más difícil adivinarlas.
- Trate en lo posible de que sus contraseñas no tengan sentido y sean escogidas al azar.
- Use diferentes contraseñas por cada cuenta.

- Cambie sus contraseñas con frecuencia. Establezca una rutina para cambiarlas, como el primer día de cada mes o cada dos meses el día de pago del salario.
- Nunca anote sus contraseñas ni las entregue a nadie.

4.2.4 Configuración de equipos

Es conveniente realizar una estandarización de la configuración que se tiene en los equipos conectados a la red, de esta forma, se puede detectar cuando un equipo que no corresponde a la red, se encuentra conectado, ya que tendrá características que lo harán diferente de los demás. Esto se puede lograr manteniendo una base de datos de las direcciones IP asignadas (para las estáticas) y las direcciones IP para los servidores DHCP (Dinámicas). De esta forma, se conocerá el estándar generado por la institución académica, así que si se conecta algún otro equipo fuera de ese estándar, estaría afectando y fallando.

4.2.5 Mantenimientos Programados

Se debe de fijar un calendario de mantenimiento vía software, en el cuál se deben realizar auditorias de la red y auditorias de configuración. Con esto comprobaremos que los usuarios no estén haciendo mal uso de los recursos de configuración. Es decir, en ocasiones existe un servidor proxy para cierto grupo de usuarios que tienen ciertos privilegios, y otro servidor proxy para otro grupo que puede tener mas privilegios. Si los del primer grupo tienen la configuración del segundo grupo (ejemplo, los alumnos tienen

privilegios de los profesores) entonces se tendrán que volver a reconfigurar los servidores proxy, así como de los equipos para evitar los accesos no autorizados o transferencias de datos y/o archivos de carácter privado.

Dentro de la seguridad, es de suprema importancia mantener al día las actualizaciones a los parches de seguridad de los diversos sistemas operativos, disminuyendo así la posibilidad de que nuevas herramientas, virus o hackers puedan entrar a nuestro sistema a través de las múltiples vulnerabilidades del sistema.

Como elemento sencillo de protección, se puede recomendar el uso de protectores de pantalla que posean claves de acceso, con esto se puede disminuir el riesgo de que usuarios no deseados accedan al sistema y de esta forma realicen operaciones supliendo al usuario principal.

4.3 Seguridad Informática (nivel físico)

Al referirnos como nivel físico, se considera a los dispositivos de "hardware" que se utilizan para el resguardo de la red y de su seguridad. Es aquí donde vamos a dar un nivel de seguridad con la capacidad de proteger a los sistemas de acuerdo a las características de nuestra red. Esta seguridad la vamos a lograr desarrollando etapas de protección de acuerdo a las aplicaciones dentro de nuestra estructura.

En una primera etapa de protección, es conveniente recurrir a equipos como los "firewall". Estos equipos se encargan de crear una "barrera" para mantener elementos dañinos alejados de nuestra red. Esto lo logra filtrando la información que viene de la

Internet hacia nuestra red privada. Si cierta información está marcada por los filtros, simplemente no se le permite el acceso. Esto lo hace por 3 métodos diferentes:

- Filtrado de paquetes. Los paquetes son analizados por los filtros previamente configurados y si estos filtros lo aprueban, permiten el paso, de lo contrario lo niegan.
- Servicio de Proxy. La información de Internet es almacenada por el firewall y después es enviada por el usuario cuando este la requiera y viceversa.
- Inspección de facto. Este procedimiento consiste en realizar un análisis comparativo de ciertas partes clave de los paquetes con una base de datos de información confiable. La información que viaja del interior de la red, al exterior, es examinada y comparada con aquella que viaja hacia el interior, si esta es similar se le permite el paso, de lo contrario se le negará.

Es muy importante el no olvidar que se debe de tener los conocimientos necesarios de la red para realizar una correcta configuración del firewall. De lo contrario pueden quedar sin configurar algunos parámetros que podrían permitir el paso de información no deseada e inclusive permitiría el acceso no autorizado de usuarios indeseables.

Otra ventaja que nos ofrecen los firewall's, es que al actualizar sus parámetros, y registros, también posee un filtro para eliminar virus. Es por eso que cuando un virus quiere pasar a través de un firewall, este lo detiene y le niega el paso.

La siguiente etapa de protección física puede encontrarse con un concentrador de VPN's. Así como se recomendó el uso de VPN's a nivel lógico, tambien se puede utilizar VPN's que hagan uso de un concentrador de VPN's. La función de este equipo es concentrar todas las VPN's que pueden existir en un sistema o red con un servidor en específico.

Ya que el uso de los Hub's es casi nulo para aplicaciones de redes de alta velocidad (esto debido a la reducción de la velocidad de transmisión de datos), el uso de recursos tales como los "switches" es un recursos bastante efectivo. Los "switches" permiten que diferentes nodos se comuniquen directamente con otro de una manera suave y eficiente.

Una ventaja de los "switches" es que pueden ser utilizados para crear VLAN's (Virtual Local Area Network; Redes de área local virtual). Esto consiste en realizar una agrupación de nodos ubicados en el mismo servidor de dominio. Las ventajas que nos ofrecen son las siguientes:

- Seguridad. Separan sistemas que poseen información confidencial o sensible, del resto de la red, de esta forma se reduce la posibilidad de que un usuario invada una zona que no tiene autorizado.

- Asignación de recursos. Supongamos que dentro de la universidad, se tiene un grupo de investigación que requiere un ancho de banda amplio, y existe otro grupo que no requiere tanto ancho de banda, ya que hacen uso de recursos como Internet, Messenger, entre otros. Esto nos permitiría una asignación optima de los recursos.

En las redes inalámbricas se puede recurrir en algunas ocasiones a recursos de identificación de usuario como el WEP (Privacidad Equivalente Inalámbrica). Con esto se puede obtener un mayor control de los accesos a la red y además se tiene un mayor nivel de seguridad en la transmisión de la información. Permitiendo a los administradores de red, mantener un mayor control de los registros, conociendo el usuario que se está conectando y en algunos casos se les puede asignar privilegios. Hay que considerar los niveles de disponibilidad de acuerdo a la política de la institución académica. Ya que este recurso, limitaría mas los accesos a los servicios.

En ocasiones es recomendable el uso de sistemas que protejan la red de ser espiada. Estos equipos se les llama "anti-sniffers". Es recomendable el uso, para evitar que los piratas cibernéticos capturen la información personal de los usuarios. En ocasiones es re

4.4 Seguridad Física

En muchas ocasiones estamos preocupados por los ataques a través de la red que puedan recibir nuestros sistemas y que podamos perder información, sin embargo también podemos perder información por factores físicos.

Se debe de tener una política de mantenimiento continuo en el área eléctrica. La red eléctrica debe de estar diseñada con todos los parámetros necesarios.

- Toda la instalación eléctrica deberá de estar aterrizada para protección del sistema en caso de alguna descarga.
- Si es posible, y el diseño lo amerita, es de importancia la instalación de un apartarrayos para la protección de los sistemas.
- Se debe de contar con las protecciones suficientes tales como interruptores térmicos y fusibles.
- Los contactos deben estar en buen estado para evitar corto circuitos.
- La instalación de equipos supresores de picos y reguladores de voltaje.
- Una herramienta excelente para evitar la pérdida de la información, es el uso de energía alterna:
    - Se puede tener un banco de baterías como respaldo en caso de la suspensión del servicio energético.
    - Se puede tener una planta de generación eléctrica de dimensiones adecuadas a los equipos a interconectar.

Como parte de la protección de la integridad física de los sistemas, también se debe contar con un sistema antiincendios que nos indique desde el momento en que un incendio se inicia, así como equipos para la extinción del fuego (extinguidores, aspersores, arena). Estos equipos deben estar funcionando y deben ser los adecuados de acuerdo al lugar donde nos encontremos. Por ejemplo, si existe equipo electrónico, podemos utilizar extinguidores con CO2 en lugar de agua o polvos que pudieran dañar la circuitería de los equipos. Los detectores de humo indicados en el inciso 2.2.3, son una buena opción para proteger y anticipar cualquier contingencia que se tenga.

Un elemento en el que siempre nos preocupamos, es la seguridad física. Debido al problema de inseguridad en el país, es de gran importancia que tomemos medidas necesarias para disminuir el riesgo de robo de los elementos de nuestro sistema. El primero que podemos tomar en cuenta, es el uso de alarmas que se interconecten a alguna central de la policía. También debemos de localizar los equipos en un inmueble que tenga ciertos recursos que dificulten la entrada a los delincuentes. Sin embargo aunque tengamos muchos recursos de este tipo, siempre existe una probabilidad de que un robo se pueda concluir. El para lo cuál es buena idea proteger nuestra información respaldándola (concepto que se tomará mas adelante). También debe de tener seguridad contra revueltas, para que la información no se accesible a los agentes dañinos.

Los fenómenos meteorológicos, también son un riesgo. Es importante no hacer caso omiso de los diferentes estudios de recomendación que se indican en la sección

2.2.3, de esta forma podremos tomar medidas preventivas para proteger los equipos en caso de inundaciones, huracanes, tormentas o riesgos derivados de los meteorológicos.

Debido a la situación geográfica de nuestro país, existen muchos puntos donde pueden ocurrir sismos. Es por eso que se deben tener construcciones que deriven de los análisis de la zona en donde se encuentra localizado nuestro equipo y que de esta forma la construcción garantice mayor seguridad a nuestro equipo, inclusive cuando haya existido un siniestro.

4.5 Respaldo

Dependiendo de los recursos con los que cuenten las instituciones académicas, se pueden instalar diferentes sistemas de respaldo como lo siguientes:

- Unidades de grabación de Disco Compacto. Es un sistema de grabación económico aunque actualmente es limitado debido a su capacidad de grabación de máximo 720 MB.
- Unidades de grabación ZIP®. Esta es una de las marcas que se encarga de realizar equipos de almacenamiento como respaldo en unidades magnéticas y ópticas.
- Unidades de grabación de DVD. Una ventaja de los sistemas de grabación de DVD es que la capacidad de grabación es de 4.7 GB
- En el mercado podemos encontrar algunos discos duros externos que sirven para realizar backup's de los sistemas, ya que poseen capacidades

superiores a los 50 GB, siendo esta una solución para una red no muy amplia.

- Sistemas de Respaldo. Este tipo de sistemas de respaldo de información utiliza bancos de discos para respaldar toda la información que pueda tener el sistema y los va almacenando.

4.6 Ingeniería Social

Sin duda alguna una de las herramientas de mayor riesgo para los usuarios, ya que es un elemento que hoy en día es comúnmente utilizado para obtener información por parte de los piratas cibernéticos.

Como recomendaciones, es importante mantener pláticas con el personal operativo y usuarios; ya que en muchas ocasiones debido a la falta de conocimiento, por los usuarios, son excesivamente fáciles de convencer. Por ejemplo, si un gerente recibe la visita de un supuesto ingeniero de soporte, argumentando que existe algún problema, seguramente debido a la ignorancia del gerente, este puede permitir el acceso al supuesto ingeniero de soporte. Sin saber que le pueden instalar programas de keyloggers, virus, robarle información, entre otras.

Este problema también radica en los mandos bajos. Si una secretaria recibe una llamada de urgencia, en la cuál le soliciten que mande cierta información de su jefe con la finalidad de arreglar algún problema, seguramente la secretaria dará esa información

pretendiendo ser proactiva y liberando de carga de trabajo a su jefe, sin darse cuenta que le está haciendo un mal.

Esta política radicará en el grado de paranoia que tenga la empresa, ya que puede ser muy restrictiva por algunos jefes y por otros lo sería mas ligera y suave.

4.7 Conclusiones del Capítulo

La integración de los recursos es algo muy importante para lograr un ambiente seguro que brinde niveles mayores de seguridad. Es aquí donde podemos hablar de que la unión hace la fuerza. Integrando todos los conocimientos que se han plasmado en la presente tesis, se puede obtener una política de seguridad computacional efectiva y de interesantes resultados.

En primera instancia se recomienda delimitarlos fines de nuestras recomendaciones de políticas de seguridad. Esto sirve para conocer los alcances que tendrá nuestra estructura, así como las limitantes; permitiendo así una estructura sólida y confiable con una filosofía definida. A través de este procedimiento, la institución orienta los fines académicos que tienen los recursos.

Así mismo apoya la educación a través de actividades formativas que limitan e impulsan a realizar proyectos de vida integrales a través de la recomendación de actividades escolares que también se pueden prolongar a extraescolares. De esta forma se mantiene una visión mas objetiva y efectiva del estudio lo que conlleva a tener profesionistas que mantengan un sentido de la responsabilidad sólido.

Sin duda alguna la actualización juega un papel básico en la seguridad informática. La evolución y desarrollo de la tecnología requiere una atención estrecha y de gran visión para mantenerse activo en el ámbito de la seguridad informática. De otra forma los ataques nos podrán tomar por sorpresa, dejándonos atrás en esta carrera de la información.

En ocasiones creemos que por instalar un antivirus, ya es suficiente, aquí encontramos las posibilidades que tenemos para la protección de nuestra red a través de un antivirus y su comportamiento. Los antivirus son elementos importantes en nuestro sistema que al ser combinados con un firewall, la seguridad se eleva y nos otorga grandes beneficios como una gran barrera (aunque no inmune) a los ataques.

El uso de programas de encriptación para envío y recepción de archivos nos permite tener un mejor control de la información y aumenta la certeza de que la información llegue en buen estado.

Los procedimientos de seguridad ayudan a estandarizar y organizar mejor las redes, lo que nos brinda un sistema limpio y seguro que sea de características bastante aceptables. Así los mantenimientos serán mas rápidos y confiables; permitiendo en caso de auditoría tener a la mano los resultados.

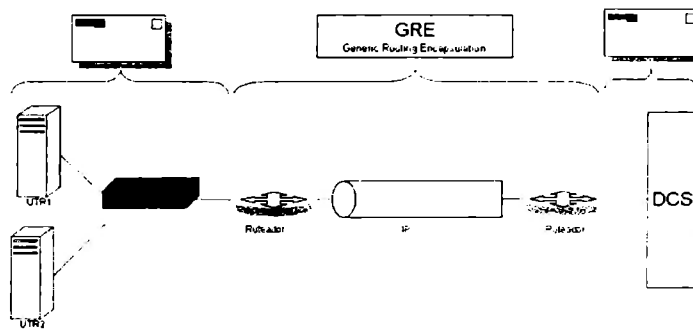

Figura 4.1 Red Privada Virtual

Referencias

[1] Seguridad computacional, Arturo García, Trimestre Ene-Mar 2003

[2] "Enlace de telecomunicaciones entre una central de generación y el Área de Control a través de una VPN". Erick René Valencia Rodríguez; Ponencia; Reunión de Verano de Potencia IEEE Julio- 2004.

Capítulo 5

Conclusiones Generales

La seguridad informática en las instituciones académicas es un elemento muy interesante debido a su complejidad multidisciplinaria que abarca ramas extremas e inclusive encontradas. Lo interesante es que partiendo de una premisa y una necesidad, se descubrieron elementos que en ocasiones despreciamos para realizar la defensa de nuestros sistemas. Como pudimos observar en el Capitulo 1, se identifica a la inseguridad informática partiendo de una premisa de protección de la información que los piratas cibernéticos podrían perturbar, con el objetivo de llevar los ataques al mínimo para lograr un sistema confiable, seguro y que esté basado en un marco regulativo vigente, apegado a las políticas de la institución académica y que pueda ser implantado en cualquier institución gracias a su modelo genérico.

El soporte técnico que recibe este modelo, se encuentra altamente identificado y brinda la capacidad de reconocer cada uno de los elementos que abarcan la protección y la seguridad informática. Identifica al pirata cibernético desde su comportamiento y respaldo técnico con un fuerte reconocimiento de los hechos, basado en estadísticas publicadas por entidades como la CERT, historias publicadas en diversos diarios y experiencias de distintos "Hackers". Asimismo se encuentra plenamente identificado y aislado el proceso por el cual los Piratas Cibernéticos analizan y atacan a sus víctimas a través de un

esquema plenamente identificado que evoca a diversos programas de hackeo. De esta forma se aísla el problema paso a paso y se pueden tomar decisiones sobre las acciones a tomar para prevenir la afectación de la red.

De igual forma se hace alusión a diversos agentes como los fenómenos naturales que pueden dañar la integridad de nuestro sistema. Incluyendo los casos en los que se pueden dar accidentes que van desde los incendios, cortos circuitos y abarcando las afecciones climatológicas como la lluvia, inundaciones y tormentas.

Se analizan los conocidos y temibles virus de acuerdo a su modo de operación , para poder prevenir el contagio de ellos y asegurándonos de evitar cualquier contacto con este tipo de archivos maliciosos. Con esta información se pueden repeler de una manera ágil y precisa para subsanar el daño que estos pudieran causar a nuestro sistema.

Pero no debemos olvidar que como disciplina interdisciplinaria, existe la etapa de análisis legal. Es aquí en donde se reconocen las leyes y los acuerdos internacionales para saber que posición adoptar ante la situación actual global. No hay que olvidar que antes de emitir cualquier recomendación o procedimiento de seguridad, este debe pasar al departamento o área responsable del derecho en la institución académica (por un abogado), para que conforme a derecho se definan las bases que rigen nuestros procedimientos.

Por último, a través de las pruebas, se puede apreciar la aplicación de la teoría y el proceder para los casos mencionados, sin olvidar que deben ser tomados para la realización de los procedimientos. Estos últimos diseñados para la creación de una

empresa de consultoría en seguridad informática en instituciones académicas gracias a su modelo genérico que puede aplicarse de acuerdo a los recursos de cada red informática. Abarcando los niveles de software, los de hardware, la seguridad física, el comportamiento del hacker y la protección antivirus.

El desarrollo del presente trabajo conformó un reto único e interesante que me brindó la posibilidad de implementar los conocimientos adquiridos en la maestría e inclusive adquirir nuevos a través de la investigación e inclusive de la experiencia.

Anexo 1

Puertos Mas Comunes

9
11
13
15
17/tcp
19
21
22/tcp
23
25
37
38/tcp
39
42/tcp
43
49/tcp
50/tcp
53
63/tcP
69/tcp
70
79
80
88/tcp
107
109/tcp
110
111/tcp

113/tcp
115/tcp
117/tcp
119
133/tcp
136/tcp
137/tcp
137/udp
138/tcp
138/udp
139/tcp
139/udp
143/tcp
144/tcp
161/tcp
194/tcp
213/tcp
220/tcp
443
512/udp
513/tcp
513/udp
514/tcp
514/udp
515/tcp
520
529/tc

Anexo 2

Puertos que abren los Troyanos

puerto 21 - Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash
puerto 23 - Tiny Telnet Server
puerto 25 - Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy
puerto 31 - Hackers Paradise
puerto 80 - Executor
puerto 456 - Hackers Paradise
puerto 555 - Ini-Killer, Phase Zero, Stealth Spy
puerto 666 - Satanz Backdoor
puerto 1001 - Silencer, WebEx
puerto 1011 - Doly Trojan
puerto 1170 - Psyber Stream Server, Voice
puerto 1234 - Ultors Trojan
puerto 1245 - VooDoo Doll
puerto 1492 - FTP99CMP
puerto 1600 - Shivka-Burka
puerto 1807 - SpySender
puerto 1981 - Shockrave
puerto 1999 - BackDoor
puerto 2001 - Trojan Cow
puerto 2023 - Ripper
puerto 2115 - Bugs
puerto 2140 - Deep Throat, The Invasor
puerto 2801 - Phineas Phucker
puerto 3024 - WinCrash
puerto 3129 - Masters Paradise
puerto 3150 - Deep Throat, The Invasor
puerto 3700 - Portal of Doom
puerto 4092 - WinCrash
puerto 4590 - ICQTrojan

puerto 5000 - Sockets de Troie
puerto 5001 - Sockets de Troie
puerto 5321 - Firehotcker
puerto 5400 - Blade Runner
puerto 5401 - Blade Runner
puerto 5402 - Blade Runner
puerto 5569 - Robo-Hack
puerto 5742 - WinCrash
puerto 6670 - DeepThroat
puerto 6771 - DeepThroat
puerto 6969 - GateCrasher, Priority
puerto 7000 - Remote Grab
puerto 7300 - NetMonitor
puerto 7301 - NetMonitor
puerto 7306 - NetMonitor
puerto 7307 - NetMonitor
puerto 7308 - NetMonitor
puerto 7789 - ICKiller
puerto 9872 - Portal of Doom
puerto 9873 - Portal of Doom
puerto 9874 - Portal of Doom
puerto 9875 - Portal of Doom
puerto 9989 - iNi-Killer
puerto 10067 - Portal of Doom
puerto 10167 - Portal of Doom
puerto 11000 - Senna Spy
puerto 11223 - Progenic trojan
puerto 12223 - Hack´99 KeyLogger
puerto 12345 - GabanBus, NetBus
puerto 12346 - GabanBus, NetBus
puerto 12361 - Whack-a-mole

puerto 12362 - Whack-a-mole
puerto 16969 - Priority
puerto 20001 - Millennium
puerto 20034 - NetBus 2 Pro
puerto 21544 - GirlFriend
puerto 22222 - Prosiak
puerto 23456 - Evil FTP, Ugly FTP
puerto 26274 - Delta
puerto 30100 - NetSphere
puerto 30101 - NetSphere
puerto 30102 - NetSphere
puerto 31337 - Back Orifice
puerto 31338 - Back Orifice, DeepBO
puerto 31339 - NetSpy DK
puerto 31666 - BOWhack
puerto 33333 - Prosiak
puerto 34324 - BigGluck, TN
puerto 40412 - The Spy
puerto 40421 - Masters Paradise
puerto 40422 - Masters Paradise
puerto 40423 - Masters Paradise
puerto 40426 - Masters Paradise
puerto 47262 - Delta
puerto 50505 - Sockets de Troie
puerto 50766 - Fore
puerto 53001 - Remote Windows Shutdown
puerto 54320 - Back Orifice 2000
puerto 54321 - Back Orifice 2000
puerto 61466 - Telecommando
puerto 65000 – Devil

Anexo 3

	IP	Vulnerable
1	159 . 16 . 10 . 21	NO
2	159 . 16 . 10 . 74	SI
3	159 . 16 . 11 . 65	NO
4	159 . 16 . 11 . 19	SI
5	159 . 16 . 12 . 48	SI
6	159 . 16 . 13 . 79	SI
7	159 . 16 . 14 . 48	NO
8	159 . 16 . 15 . 74	NO
9	159 . 16 . 17 . 9	NO
10	159 . 16 . 17 . 77	NO
11	159 . 16 . 18 . 82	SI
12	159 . 16 . 18 . 13	NO
13	159 . 16 . 19 . 33	SI
14	159 . 16 . 20 . 42	NO
15	159 . 16 . 20 . 82	SI
16	159 . 16 . 21 . 90	SI
17	159 . 16 . 22 . 81	SI
18	159 . 16 . 22 . 47	SI
19	159 . 16 . 22 . 19	NO
20	159 . 16 . 23 . 46	NO
21	159 . 16 . 23 . 57	SI
22	159 . 16 . 23 . 70	NO
23	159 . 16 . 24 . 34	SI
24	159 . 16 . 24 . 30	SI
25	159 . 16 . 25 . 63	NO
26	159 . 16 . 26 . 74	NO
27	159 . 16 . 26 . 42	NO
28	159 . 16 . 26 . 34	SI
29	159 . 16 . 26 . 97	SI
30	159 . 16 . 27 . 95	SI
31	159 . 16 . 29 . 89	NO
32	159 . 16 . 31 . 39	SI
33	159 . 16 . 32 . 3	NO
34	159 . 16 . 32 . 45	SI
35	159 . 16 . 33 . 39	NO
36	159 . 16 . 34 . 15	SI
37	159 . 16 . 34 . 45	SI
38	159 . 16 . 34 . 77	SI
39	159 . 16 . 34 . 80	SI
40	159 . 16 . 35 . 58	SI
41	159 . 16 . 40 . 95	SI
42	159 . 16 . 43 . 75	SI
43	159 . 16 . 45 . 8	NO
44	159 . 16 . 45 . 22	SI
45	159 . 16 . 45 . 27	SI
46	159 . 16 . 45 . 63	NO
47	159 . 16 . 45 . 90	SI
48	159 . 16 . 45 . 89	NO
49	159 . 16 . 46 . 61	NO
50	159 . 16 . 47 . 25	SI
51	159 . 16 . 48 . 64	SI
52	159 . 16 . 48 . 94	SI
53	159 . 16 . 49 . 45	SI
54	159 . 16 . 49 . 9	SI
55	159 . 16 . 50 . 51	NO
56	159 . 16 . 52 . 65	SI
57	159 . 16 . 53 . 55	NO
58	159 . 16 . 54 . 49	NO
59	159 . 16 . 54 . 55	SI
60	159 . 16 . 54 . 34	SI
61	159 . 16 . 55 . 8	SI
62	159 . 16 . 56 . 34	NO
63	159 . 16 . 56 . 13	NO
64	159 . 16 . 56 . 16	SI
65	159 . 16 . 57 . 9	SI
66	159 . 16 . 58 . 49	SI
67	159 . 16 . 58 . 33	NO
68	159 . 16 . 59 . 63	SI
69	159 . 16 . 59 . 99	NO
70	159 . 16 . 59 . 81	NO
71	159 . 16 . 60 . 75	NO
72	159 . 16 . 61 . 78	SI
73	159 . 16 . 62 . 62	NO
74	159 . 16 . 63 . 6	NO
75	159 . 16 . 64 . 26	NO

76	159 . 16 . 67 . 21	SI
77	159 . 16 . 67 . 10	SI
78	159 . 16 . 68 . 41	SI
79	159 . 16 . 71 . 62	SI
80	159 . 16 . 72 . 98	SI
81	159 . 16 . 73 . 84	NO
82	159 . 16 . 73 . 38	SI
83	159 . 16 . 76 . 82	SI
84	159 . 16 . 76 . 15	NO
85	159 . 16 . 77 . 23	SI
86	159 . 16 . 78 . 22	NO
87	159 . 16 . 78 . 17	NO
88	159 . 16 . 82 . 91	NO

89	159 . 16 . 82 . 85	SI
90	159 . 16 . 82 . 94	NO
91	159 . 16 . 85 . 32	NO
92	159 . 16 . 85 . 45	NO
93	159 . 16 . 85 . 10	NO
94	159 . 16 . 86 . 71	NO
95	159 . 16 . 87 . 52	NO
96	159 . 16 . 87 . 46	SI
97	159 . 16 . 87 . 90	SI
98	159 . 16 . 89 . 54	SI
99	159 . 16 . 89 . 84	NO

Síntesis Biográfica

Erick René Valencia Rodríguez nació en la Ciudad de México el 24 de febrero de 1981. Sus padres son Fausto Valencia Rosales y María Luisa del Rocío Rodríguez Rojas. Su hermano es Juan José Valencia Rodríguez. Realizó sus estudios de Primaria y Secundaria en el Colegio Panamericano de Texcoco, cursó sus estudios preparatorios en el Instituto Francisco Ferreira y Arreola de Texcoco y realizó sus estudios profesionales en la Universidad Tecnológica de México, Campus Sur, donde obtuvo el título de Ingeniero en Electrónica y Comunicaciones. Estudió un diplomado en Telecomunicaciones en la Alcatel University. Estudió la Maestría en Administración de las Telecomunicaciones en el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Ciudad de México y se encuentra laborando en la Comisión Federal de Electricidad en la Coordinación de Proyectos Termoeléctricos en la supervisión de la Ingeniería en Proyectos de Centrales Termoeléctricas.