Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA

José Vladimiro Rivera Ramos
Asesorado por el Ing. Gerson Ottoniel Villatoro Pérez

Guatemala, noviembre de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JOSÉ VLADIMIRO RIVERA RAMOS
ASESORADO POR EL ING. GERSON OTTONIEL VILLATORO PÉREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2011

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

CICLO DE VIDA DE UNA PRUEBA
DE PENETRACIÓN FÍSICA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha noviembre de 2010.

José Vladimiro Rivera Ramos

Guatemala, 25 de Abril de 2011

Ingeniero
Carlos Alfredo Azurdia Morales
Revisor de trabajos de Graduación
Escuela de Ciencias y Sistemas

Estimado Ingeniero:

Por medio de la presente, me permito informarle que he asesorado el trabajo de graduación titulado: **CICLO DE VIDA DE UNA PRUEBA DE PENETRACION FÍSICA** elaborado por el estudiante José Vladimiro Rivera Ramos, y a mi juicio el mismo cumple con los objetivos propuestos para su desarrollo.

Agradeciéndole de antemano la atención que le preste a la presente, me suscribo de usted.

Atentamente,

Ing. Gerson Ottoniel Villatoro Pérez

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 11 de Mayo de 2011

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JOSÉ VLADIMIRO RIVERA RAMOS**, carné **1993-12475**, titulado: **"CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA - INGENIERÍA EN CIENCIAS Y SISTEMAS - COORDINACIÓN

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA"****, presentado por el estudiante JOSÉ VLADIMIRO RIVERA RAMOS, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería Ciencias y Sistemas

Guatemala, 17 de noviembre 2011

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.527.2011

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA,** presentado por el estudiante universitario **José Vladimiro Rivera Ramos,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, noviembre de 2011

/cc

ACTO QUE DEDICO A:

Dios	Por ser el creador de todo.
Mis padres	Edna Doris Ramos y Vladimiro Rivera (q.e.p.d.) por todo el cariño, amor, esfuerzo, apoyo y dedicación, que me brindaron.
Mi esposa	Mónica Paulette, por ser mi complemento y demostrarme cada día, todo ese amor incondicional que me tiene.
Mi abuela	María Concepción (q.e.p.d.) por haberme querido tanto.
Mis hermanos	Sigfrido y Paris, por ser un ejemplo de disciplina, constancia, dedicación y apoyarme siempre.
Mi sobrino	Patrick Jesús, que desde pequeño está demostrando ser un gran guerrero.

AGRADECIMIENTOS A:

Dios y la Virgen Santísima	Por todo lo maravilloso que me ha dado.
La Universidad de San Carlos	Por darme todo el conocimiento
Ing. Carlos Azurdia	Por su orientación profesional.
Compañeros de Promoción	Por compartir conmigo largas noches de desvelo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Acceso remoto Acceso a la red interna a través de la red telefónica conmutada u otra red de acceso público.

Activo Cualquier cosa que tenga valor para la organización. Más concretamente, recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Algoritmo Conjunto de sentencias o instrucciones en lenguaje nativo, los cuales expresan la lógica de un programa.

Amenaza Cualquier circunstancia o evento capaz de causar daño a un sistema en la forma de denegación de servicio o destrucción, revelación no autorizada o modificación de datos.

Análisis de riesgos Evaluación del posible impacto y probabilidad de materialización de las amenazas de seguridad a las que se encuentra expuesta una organización.

Antivirus Programas informáticos que permiten analizar memoria, unidades de disco, mensajes o transmisiones en busca de virus.

Backdoor También conocido como troyano o puerta trasera, es un defecto en un *software* o página *web* que permite ingresar a un recurso que usualmente está restringida a un usuario ajeno.

Backtrack Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

Bluetooth Es una especificación industrial para redes inalámbricas de área personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.

Cifrado Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Cracker Es una persona que mediante ingeniería inversa realiza: seriales, *keygens* y *cracks*, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del *software* o *hardware* original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

Crimeware	Es un tipo de *software* que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El término fue creado por Peter Cassidy, Secretario General del *Anti-Phishing Working Group* para diferenciarlo de otros tipos de *software* malicioso.
Descifrado	Operación que obtiene un texto original a partir de un texto cifrado.
Encriptar	Es la acción de proteger información para que no pueda ser leída sin una clave.
Exploits	*Exploit* (del inglés *to exploit*, explotar o aprovechar) es una pieza de *software*, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, *hardware*, o componente.
Externalización	Situación en la que un proceso de la organización ha sido delegado en otra organización, normalmente a través de un acuerdo de nivel de servicio.
Fake	*F*also en inglés se refiere en general a una falsificación, montaje fotográfico, o anuncio falso, etc.

Firewall	Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas
Gadgets	Es un dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso. Los *gadgets* suelen tener un diseño más ingenioso que el de la tecnología corriente.
Google	Google Inc. es la empresa propietaria de la marca Google, cuyo principal producto es el motor de búsqueda del mismo nombre.
GPS	El GPS (*Global Positioning System*: sistema de posicionamiento global) o NAVSTAR-GPS es un sistema global de navegación por satélite (GNSS) que permite determinar en todo el mundo la posición de un objeto, una persona o un vehículo con una precisión hasta de centímetros.
Hacker	Es un experto en informática que utiliza su conocimiento y habilidades para irrumpir en sistemas y tecnologías para demostrar fallas en los sistemas de protección.

Hardware	Corresponde a todas las partes tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
Hito	Es una tarea de duración cero que simboliza el haber conseguido un logro importante en el proyecto. Los hitos son una forma de conocer el avance del proyecto.
Honeypot	Se denomina al *software* o conjunto de computadoras cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas.
ISO/IEC 27002:2005	Conjunto de controles que comprende las mejores prácticas en seguridad de la información. Es el resultado de la estandarización de la primera parte del BS7799.
IT	La Tecnología Informática (IT), es “el estudio, diseño, desarrollo, puesta en práctica, ayuda o gerencia de los sistemas informáticos computarizados, particularmente usos del *software* y *hardware*.”

Keylogger	Es un tipo de *software* que se encarga de registrar las pulsaciones que se realizan en el teclado, para memorizarlas en un fichero y/o enviarlas a través de *internet*.
LiveCD	Una distribución *live* o LiveCD o LiveDVD, es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD, que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro.
MAC *Address*	En las redes de computadoras, la dirección MAC es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.
Malware	Del inglés *malicious software*, también llamado *badware*, *software* malicioso o *software* malintencionado. Es un tipo de *software* que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
Modo promiscuo	En informática, es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los *sniffers* que se basan en este modo para realizar su tarea.

Parche — En informática, consiste en los cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

Pendrive — Es un dispositivo USB de almacenamiento que utiliza memoria *flash* para guardar la información que puede requerir y no necesita baterías (pilas).

Phishing — *E*s un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Scam — Es un término anglosajón que se emplea para designar el intento de estafa a través de un correo electrónico fraudulento (o páginas *web* fraudulentas).

SMS — El servicio de mensajes cortos o SMS (*Short Message Service*) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre teléfonos móviles.

Sniffer — En informática, es un *software* destinado para detectar y capturar todo el tráfico que viaja por la red.

Software	Programas, procedimientos, reglas y documentación posible asociada con la computación, así como los datos pertenecientes a la operación de un sistema de cómputo.
Spyware	Un programa espía, es un programa, que se instala furtivamente en una computadora para recopilar información sobre las actividades realizadas en éste.
SSID	El SSID (*Service Set Identifier*) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
Switches	Un conmutador o *switch* es un dispositivo digital de lógica de interconexión que su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.
Virus	Un virus informático es un *malware* que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora.

RESUMEN

La proliferación de sistemas conectados a *internet* ha hecho más frecuentes los casos de ingresos no autorizados, robo de información confidencial y mal uso de los recursos informáticos. Esto ha hecho evidente, para las organizaciones que basan su operación en estos sistemas, la necesidad de contar con equipos de respuesta, integrados con personal altamente calificado, que tenga las habilidades necesarias para descubrir las deficiencias relativas a la seguridad de sus sistemas antes que lo haga otro.

Una forma efectiva para desarrollar estas habilidades es simulando un ataque tal y cómo lo haría un *hacker*, citando lo que decía Sun Tzu en su libro el Arte de la Guerra[1], "Si conoce a su enemigo y se conoce a sí mismo; en cien batallas, nunca saldrá derrotado. Si es ignorante de su enemigo pero se conoce a sí mismo, sus oportunidades de ganar o perder son las mismas. Si es ignorante de su enemigo y de sí mismo, puede estar seguro de ser derrotado en cada batalla".

Si se conocen las técnicas más habituales, con las que los *hackers* realizan accesos no autorizados, cómo burlan los mecanismos de seguridad, cómo utilizan la ingeniería social, se podrá asegurar de una forma más efectiva todos los recursos de una empresa.

[1] Sun Tzu, El arte de la guerra, traducción directa del chino antiguo a cargo de Albert Galvany, coautor de la primera traducción directa y completa del Yijing del chino al castellano. Incluye texto original chino; Editorial Trotta: Madrid, 2001 [7ª edición 2010]

OBJETIVOS

General

Dar a conocer la metodología Ciclo de Vida de una Prueba de Penetración Física.

Específicos

1. Conocer los fundamentos de una prueba de penetración física.

2. Conocer los riesgos a los que se puede enfrentar un equipo de penetración.

3. Dar a conocer las técnicas que utilizan los *hackers y* ponerlas en práctica para evaluar la seguridad.

4. Dar a conocer las técnicas utilizadas para vulnerar los mecanismos de seguridad físicos.

5. Proporcionar los mecanismos más comunes de ataque de ingeniería social, para tener la capacidad y habilidad para detectar un ataque y contraatacar.

6. Proporcionar una guía para la construcción de un plan de seguridad basado en ISO/IEC 27002:2005.

INTRODUCCIÓN

Las pruebas de penetración son un método para evaluar la seguridad por medio de la simulación de un ataque, tal y como lo haría un *hacker*; involucran un análisis activo de los sistemas en búsqueda de debilidades, fallas conocidas o desconocidas y potenciales vulnerabilidades que podrían ser el resultado, de configuraciones defectuosas de *software* o malas instalaciones de *hardware*. El Instituto en Seguridad Computacional CSI (*Computer Security Institute*), anualmente pública un informe estadístico sobre delitos informáticos y encuestas de seguridad.

En su edición 15 correspondiente al año 2009, describe qué tipos de ataque son victimas las organizaciones *y* presenta resultados a sus encuestas relacionadas a tecnologías utilizadas por las empresas para protegerse y para evaluar su seguridad (ver Tabla I). El estudio refleja que la mayoría de ataques provienen de virus y *malware* (gusanos, troyanos*, rootkits, spyware, crimeware*), en segundo lugar aparecen todas aquellas computadoras que son utilizadas para realizar actividades ilegales, sin que el usuario se dé cuenta, comúnmente llamados *bots* o *zombies*, en tercero están los fraudes y la suplantación de identidad.

El estudio refleja un preocupante incremento en los ataques a todo nivel, incluso se han creado nuevas categorías para su clasificación, es evidente que ya no funciona solo instalar un antivirus y un *firewall* para contener los ataques (ver figura 1).

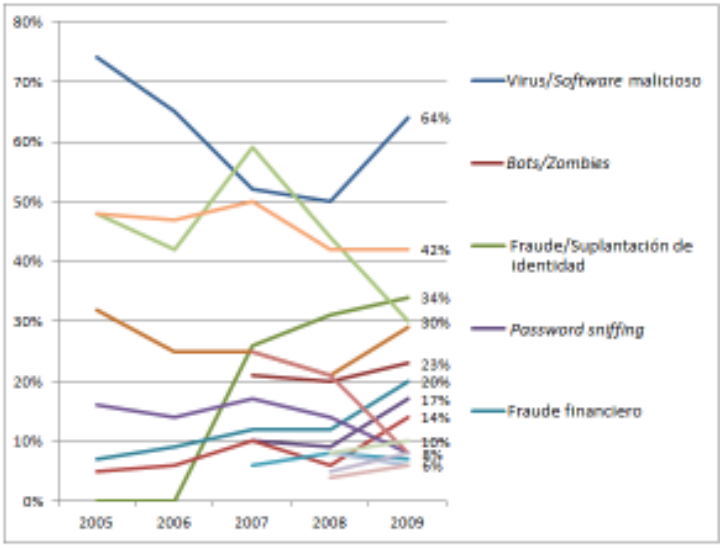
Tabla I. **Tipos de ataques experimentados por las organizaciones**

Tipo	2005	2006	2007	2008	2009
Virus/*Malware*	74%	65%	52%	50%	64%
Bots / *zombies*			21%	20%	23%
Fraude /Suplantación de identidad			26%	31%	34%
Password sniffing			10%	9%	17%
Fraude financiero	7%	9%	12%	12%	20%
Negación de servicio	32%	25%	25%	21%	29%
Extorsión					3%
Desfiguración de *websites*	5%	6%	10%	6%	14%
Otros tipos de desfiguración					6%
Ataque a redes inalámbricas	16%	14%	17%	14%	8%
Ataques de DNS			6%	8%	7%
Ataques a clientes *web*					11%
Ataques a redes sociales					7%
Ataques a mensajería instantánea			25%	21%	8%
Abuso de información privilegiada	48%	42%	59%	44%	30%
Autorización no autorizada					15%
Penetración a los sistemas por extraños					14%
Robo de *laptops* o dispositivos móviles	48%	47%	50%	42%	42%
Acceso no autorizado debido a pérdida o robo de dispositivos móviles				8%	6%
Acceso no autorizado a propiedad intelectual debido a pérdida o robo de dispositivos móviles.				4%	6%
Acceso no autorizado debido a otras causas.				8%	10%
Robo de propiedad intelectual debido a otras causas				5%	8%

Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2009.pdf. 11/11/2010.

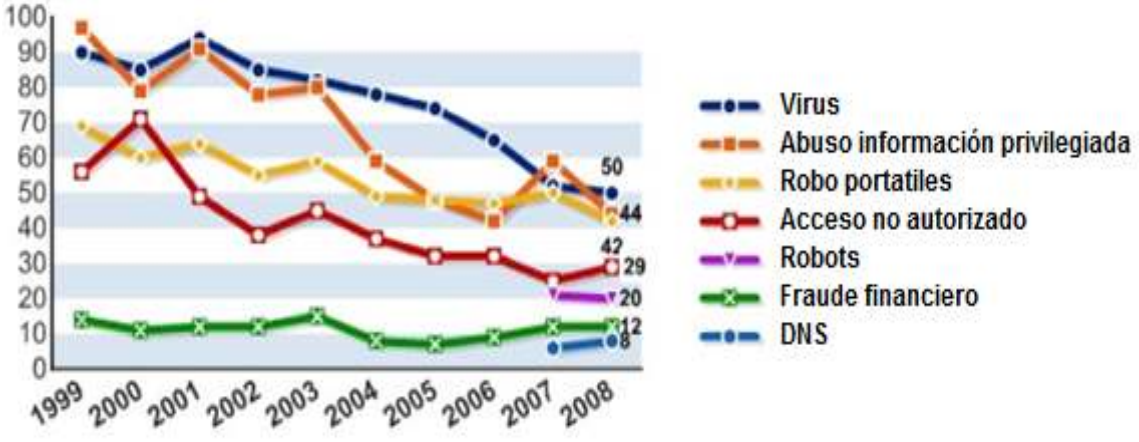
Si se compara este mismo estudio con el del año 2008, es notorio que la mayoría de ataques se centraba antes en virus, en abuso de información privilegiada y robo de portátiles (ver figura 2).

Figura 1. **Ataques más frecuentes a las empresas año 2009**



Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2009.pdf. 11/11/2010.

Figura 2. **Ataques más frecuentes a las empresas año 2008**



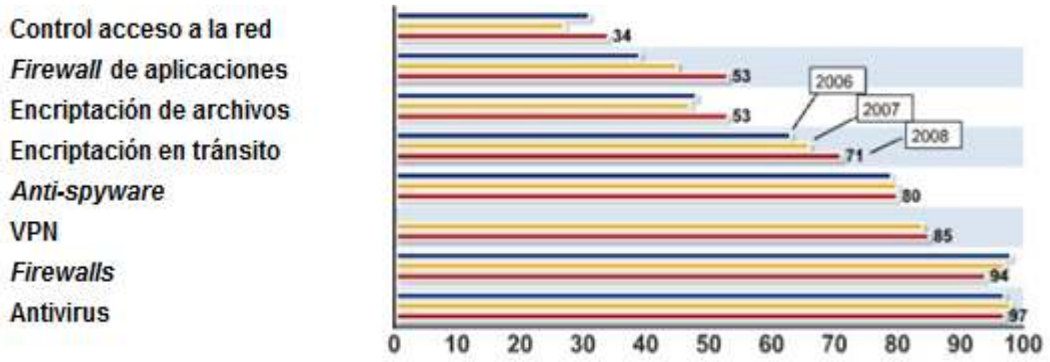
Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf. 11/11/2010.

El término abuso de información privilegiada, se refiere a una amplia gama de actividades de los, funcionarios, directores, empleados, accionistas principales, agentes y otras personas en instituciones financieras, que intentan

beneficiarse realizando acciones fraudulentas aprovechando su posición. En la edición 14 de su informe correspondiente al año 2008, sobre delitos informáticos, los encargados de los departamentos de IT, fueron encuestados sobre el tema “Tecnologías de protección y evaluación de seguridad”.

Al ser cuestionados sobre ¿Qué tipo de tecnología utilizan para proteger sus sistemas?, la mayoría descansa su seguridad en el uso de antivirus, *firewalls* y redes privadas virtuales, (ver figura 3). Algo interesante es que el 97% dice utilizar antivirus pero según las estadísticas de ese año, los virus fueron la mayor causa de ataque. Y algo más preocupante es que sobre el abuso interno y el robo de portátiles no se ve, que utilicen ninguna tecnología.

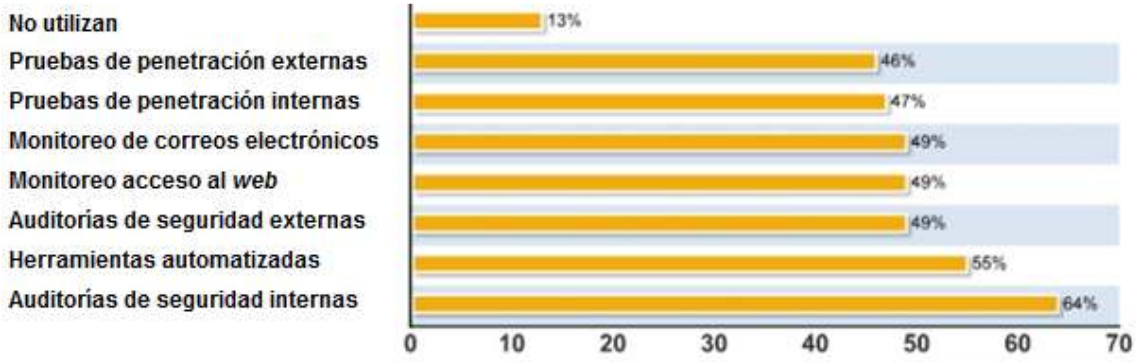
Figura 3. **Tecnologías utilizadas para proteger sus sistemas año 2008**



Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf. 11/11/2010.

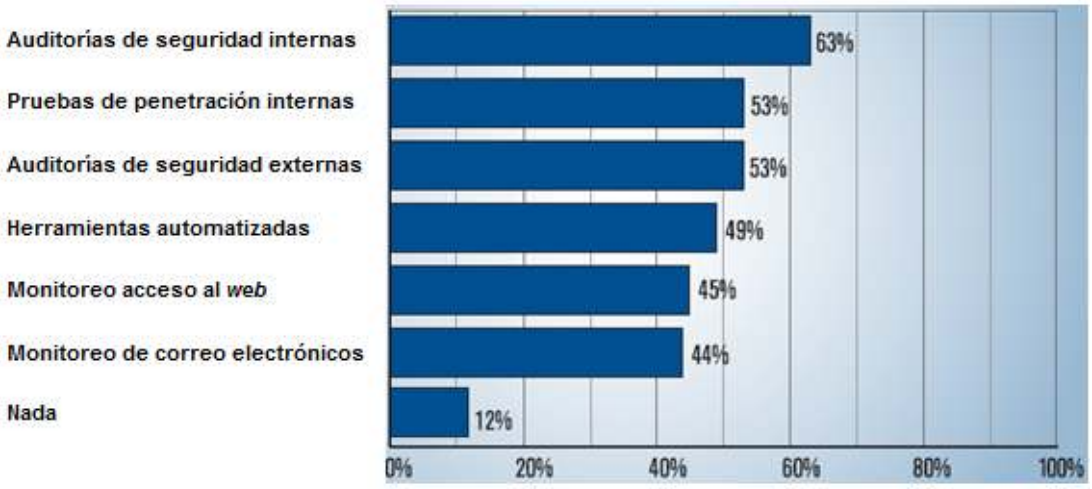
Al ser cuestionados los encargados de IT, ¿Qué técnicas utilizan para evaluar su seguridad?, se puede observar que las auditorías internas y externas así como el uso de herramientas automatizadas, son las preferidas. Algo interesante es que ya existe una conciencia en la importancia de las pruebas de penetración internas y externas y se ve al comparar los resultados con la misma encuesta del año 2007.

Figura 4. **Tecnologías de seguridad utilizadas año 2008**



Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf. 11/11/2010.

Figura 5. **Tecnologías de seguridad utilizadas año 2007**

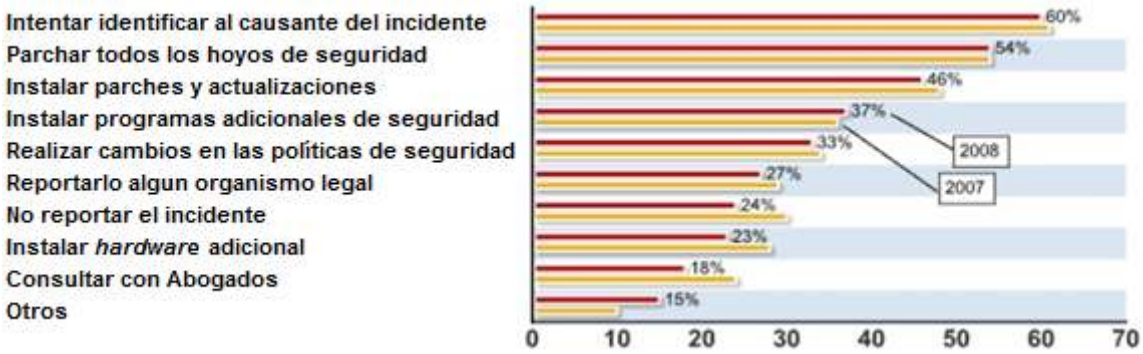


Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2007.pdf. 11/11/2010.

Se observa una disminución en las pruebas de penetración internas pero se ve compensada con el surgimiento en la utilización de pruebas de penetración externas. Al ser cuestionados los encargados de IT, ¿Cómo responden ante un ataque? La mayoría indicó, intentar identificar al causante del incidente, en segundo lugar parchar todos los hoyos de seguridad y en

tercer lugar aplicación de parches y actualizaciones, en cuarto instalar programas adicionales de seguridad y en quinto lugar aparece algo que debería estar entre los primeros lugares y es la de realizar cambios en las políticas de seguridad.

Figura 6. **Respuesta ante un ataque año 2008**



Fuente: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf. 11/11/2010.

Al analizar la evolución de los ataques informáticos *y* la forma en que se defienden las empresas, se puede ver que los ataques están evolucionando más rápido y que las defensas siguen siendo las mismas, no se puede esperar resultados distintos si se siguen haciendo las mismas cosas. La seguridad no es solo instalar antivirus, *firewalls*, sistemas de detección de intrusos, hay que poner énfasis en otros mecanismos e implementarlos. Este estudio también muestra que las organizaciones ponen muy poco énfasis en su seguridad física. Los expertos en seguridad informática están conscientes que una vez el acceso físico a las red se obtiene, uno a uno estos mecanismos de seguridad son eliminados.

Los atacantes saben que después de varios intentos fallidos remotamente, tienen la opción de ir ellos mismos hasta los sistemas y vulnerarlos, teniendo únicamente que librar la seguridad estándar existente en

las empresas. Adicionalmente de los ataques que pueden ocurrir desde el exterior, intentando tener acceso no autorizado al sistema, están todos aquellos empleados que ya tienen acceso y que son potencialmente vulnerables a ataques de ingeniería social. Hay un viejo dicho que dice, “la seguridad es tan fuerte como el eslabón más débil de la cadena y generalmente el eslabón más débil lo constituyen las personas. Esto porque las personas cometen errores y pueden ser manipulados.

Es necesario conocer, como piensa un atacante, que tácticas utiliza *y* así poder implementar contramedidas activas. Es mucho más valioso entender que hace un atacante, que instalar un parche que solucione alguna vulnerabilidad. La práctica hace al maestro y es por ello que si se quiere ser más efectivo en la seguridad se deben conocer las metodologías que permitan preparar escenarios donde se pueda poner a prueba todas las técnicas y habilidades de ataque. Una de esas metodologías es la Prueba de Penetración Física, conocida también como *hacking* ético o prueba de intrusión, con esta prueba el equipo demuestra la vulnerabilidad a través de una intrusión física en las instalaciones del cliente, utilizando técnicas que utilizaría un atacante real.

La información es recopilada a través de espionaje, engaño, por ingeniería social e incluso de la misma basura que desecha la empresa. A lo largo del tiempo ha ido creciendo la conciencia de las organizaciones de las amenazas que enfrentan, al tratar de mantener sus datos confidenciales seguros, apoyándose en nuevas tecnologías que van surgiendo, instalando mejores *firewalls*, teniendo mejores políticas de seguridad, incorporando sistemas de detección de intrusos, revisando el código fuente en busca de código malicioso, programando auditorías eventuales, etc.

Todos estos enfoques están bien, si se hacen periódicamente y bien hechos pueden dar un buen resultado, sin embargo si un atacante puede tener acceso físicamente a las instalaciones de una empresa y logra llegar hasta donde están los servidores y tiene acceso al sistema, las estrategias anteriores no la protegerán. Es una falsa sensación de seguridad y no hay nada peor que creer que se tiene un traje antibalas, que resulta ser un mosquitero. Prueba de ello en la actualidad es lo que le ocurrió a la diplomacia estadounidense, cuando fueron difundidos más de 250 mil documentos, en un sitio llamado Wikileaks, donde información secreta fue revelada.

Siempre se ha advertido por los expertos en seguridad, la amenaza que plantean los trabajadores disgustados y las políticas de seguridad vulnerables que dan demasiado acceso a datos confidenciales. Y no hay nada en la difusión de estos documentos diplomáticos norteamericanos que no pueda ser emulado por un trabajador descontento *y* que lo haga revelar los secretos de la organización. Urge reforzar la seguridad física en las organizaciones, ya que corren riesgo de perder sus secretos empresariales, correos electrónicos, documentos, bases de datos, o sufrir la publicación no autorizada de sus *chats*, tomas de decisiones, estrategias, lanzamientos, planes, cronogramas, etc.

Pese a que tecnológicamente es fácil limitar en cada compañía quién deberá tener acceso a determinado tipo de información, muchas organizaciones dejan ese acceso demasiado abierto. Y pese a la mejor de las intenciones, los errores son inevitables a medida que las redes se tornan más complicadas con reorganizaciones y adquisiciones. Aun cuando la seguridad sea eficaz, es muy difícil detener a alguien que tenga acceso legítimo y que se haya tornado rebelde.

Un ex analista de la compañía de préstamos hipotecarios *Countrywide Financial*, ahora propiedad del *Bank of America*, está imputado de haber descargado datos de 2 millones de clientes a lo largo de dos años, cobrando US$ 500,00 por cada tanda de 20 000 archivos. La fiscalía dice que el acusado trabajaba secretamente los domingos utilizando una computadora de *Countrywide* que no tenía resguardos de seguridad y que le permitía cargar información en *pendrive*s. Otras compañías de préstamos compraron los archivos, incluso números de seguridad social, como pistas para nuevas ventas, según las autoridades.

No es necesario ser un experto en informática para vulnerar un sistema de seguridad, vasta a veces un poco de codicia e ingenio. No se hablado de crear negaciones de servicio, de desbordar *buffers*, de aplicar fuerza bruta a las pantallas de autenticación, que por supuesto son técnicas que se puede usar, si no que se va más allá, el escenario es que el atacante puede llegar a tener acceso, hasta el servidor donde esta esa aplicación que le está pidiendo que se autentique.

1. FUNDAMENTOS DE UNA PRUEBA DE PENETRACIÓN FÍSICA

1.1. ¿Qué es una prueba de penetración física?

Una prueba de penetración física (en adelante, *pentest* física), es el proceso por medio del cual se somete a un ataque controlado, la seguridad física de una empresa, buscando identificar, las debilidades que pueda tener, antes que un atacante real lo haga. La seguridad física, son todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso de una organización, estos recursos, incluyen el personal, las instalaciones donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan.

Consiste en introducirse en las instalaciones de una organización tratar de burlar toda la seguridad que esta pueda tener y recopilar toda la información valiosa y confidencial, durante el proceso, utilizando para ello todos los mecanismos, métodos y herramientas que un agente malicioso utilizaría. Se sabrá si una penetración física fue exitosa si:

- Se logra violar la seguridad perimetral, es decir llegar a un área restringida
- Se obtiene acceso físico a la red de computadoras
- Se logra fotografiar algún activo determinado
- Adquirir un activo determinado
- Obtener acceso a personal predeterminado
- Adquirir información valiosa
- Plantar evidencia física de la presencia

1.2. ¿Porqué realizar *pentest* físicas?

- Identifica vulnerabilidades conocidas o desconocidas, antes que lo haga un atacante mal intencionado.
- Permite evaluar cual es el impacto real de una vulnerabilidad, mediante la realización de pruebas controladas.
- Pone a prueba las políticas existentes de seguridad.
- Determina que tan susceptibles son los empleados a los ataques de ingeniería social.
- Es importante estar preparado para ataques en todas escalas y construir planes de respuesta adecuados.
- Es importante capacitar al personal para que sean capaces de detectar cuando están siendo atacados con ingeniería social y saber cómo contraatacar.

1.3. ¿Quiénes realizan las pruebas?

Profesionales de seguridad, o *hackers* que han dejado sus actividades delictivas y que utilizan todo su conocimiento y habilidades para atacar de forma controlada dependiendo de la naturaleza de la prueba un sistema o una instalación física. Sin tomar ventaja de las brechas de seguridad, a cambio documentan la falla, para después entregarla en un informe. Al grupo de profesionales destinados a una prueba de penetración física, se les conoce como equipo de penetración.

1.4. ¿Qué hacen los profesionales en pruebas de penetración?

Un profesional en pruebas de penetración (en adelante *penetration tester,* por ser el nombre como es identificado en el ámbito de seguridad), es el

encargado de comprometer la seguridad de una organización con el fin de demostrar una vulnerabilidad. Son también conocidos como "*hackers* éticos" *y* la razón es porque al momento de realizar una prueba de penetración utilizan su amplio conocimiento y experiencia en métodos y técnicas *hacker*, con el propósito principal de buscar y resolver vulnerabilidades de seguridad.

Para demostrar fallas en la seguridad informática, utiliza ingeniería inversa, vence protocolos y explota vulnerabilidades conocidas para demostrar fallas en la seguridad física. Lo hace a través de la intrusión física en las instalaciones esto a menudo se logra a través de la recopilación de inteligencia encubierta, del engaño en general y la ingeniería social, también puede implicar un enfoque más directo, como una intrusión nocturna, venciendo cerraduras, pero todo esto depende de lo que se haya establecido en los términos del contrato, conocido como reglas de enfrentamiento.

1.5. El rol de una *pentest* física, en un programa de seguridad

Las pruebas de penetración por sí solas no pueden proporcionar una protección adecuada para la seguridad de la red, sin embargo, son un componente muy importante en un programa de seguridad. Las mejores prácticas sugieren implementar las siguientes medidas clave para asegurar un nivel óptimo de protección:

- Evaluación de riesgos de seguridad
- Fuertes políticas de seguridad de la información
- Capacitación en políticas y procedimientos
- Pruebas de penetración de *software*
- Evaluación de vulnerabilidades
- Pruebas de penetración física periódicas

1.6. ¿Qué es *hacking* ético?

Es el arte y ciencia de determinar las vulnerabilidades de una infraestructura de información para mejorarla, simulando un ataque tal y como lo haría un *hacker*. La idea detrás del *hacking* ético es colocarse en los zapatos de los *hackers*, ver lo que ellos ven, hacer lo que ellos hacen y aprender con esto, medidas defensivas ante un posible ataque.

La historia ha demostrado que los *hackers* siempre van algunos pasos por delante de los especialistas en seguridad. Es el caso de una firma de seguridad HBGary que fue brutalmente atacada y a consecuencia de ello el contenido de los correos de algunos de sus directivos fueron filtrados al mundo entero, después de que uno de sus ejecutivos Aaron Barr afirmara que se había infiltrado en un grupo *hacker*, llamado anonymous y que conocía el nombre de algunos de sus líderes.

Es claro que si una firma de seguridad es fácilmente vulnerada donde el conocimiento sobre aspectos de seguridad es superior a la media del conocimiento que tienen las empresas que no se dedican a ello, da un claro panorama del riesgo que correría una organización si algún grupo de estos la emprendiera en su contra.

1.7. Procedimientos Legales

Antes de contratar los servicios de un equipo de penetración es necesario asegurarse, que todos los integrantes del equipo de penetración están asegurados, las aseguradoras son muy exigentes al momento de firmar una póliza de seguro *y* por lo general exigen antecedentes penales, policíacos y

médicos, antes de firmar. Resultaría contraproducente contratar a alguien que ha tenido problemas con la ley.

1.7.1 Autorizaciones de seguridad

Cuando se realicen pruebas de penetración de cualquier tipo, los equipos necesitan tener autorizaciones de seguridad. Las autorizaciones de seguridad dependen de la naturaleza del trabajo que se realizará y la sensibilidad del objetivo. Todas las autorizaciones deberán estar firmadas y debidamente selladas.

1.7.2 Investigación de antecedentes

Es importante exigir que se entreguen los antecedentes penales y policíacos de los miembros del equipo de penetración, que participaran durante la prueba y que estén actualizados.

1.7.3 Actuar apegado a la ley

Es importante no olvidar y tener presente en todo momento de la prueba, las repercusiones legales que pudieran llegar a tener las acciones que realice un equipo de penetración, estas repercusiones por lo general se dan por violación de privacidad o por haber cometido un delito informático.

En el primer caso según la Declaración Universal de los Derechos Humanos en su artículo 12 dice “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

Este artículo claramente se refiere a la privacidad, si un equipo de penetración, en el ejercicio de sus funciones, accidentalmente o deliberadamente intercepta el contenido de un correo electrónico, habrá cometido una violación de privacidad.

En este otro caso, un *hacker* logra penetrar la seguridad de un departamento gubernamental, o al menos eso cree. En realidad, es una violación a una *honeypot*, que fue creada con el objetivo de estudiar el comportamiento de los atacantes informáticos y sus técnicas, interceptando todo lo que hagan estando dentro y revisa su correo electrónico, este correo es privado y mediante la captura, lectura y el almacenamiento de este ya se ha cometido una violación de privacidad. Todos los integrantes del equipo de penetración deben estar conscientes de que pueden hacer y que no. Ejemplo:

Un equipo de pruebas de penetración puede tener permiso para dirigirse a un equipo específico dentro de la red, pero no las adyacentes a ella. Puede ser autorizado para atacar a un determinado servidor, pero no las aplicaciones que se ejecutan sobre él.

Por lo que sí, ataca alguna aplicación, o accede a otra máquina para llegar al objetivo, habrá cometido un delito.

1.8 ¿Cómo contratar una *pentest* física?

Los departamentos de IT en muchas organizaciones son los más indicados para realizar un determinado grado de pruebas de penetración, pero la mayoría de los departamentos carecen de los conocimientos y la experiencia para llevar a cabo una prueba completa y exacta. Es por ello que las empresas deberán contar con los servicios de una empresa especializada que pueda

realizar pruebas de penetración periódicas así como otras auditorías y evaluaciones de protección.

Las pruebas de penetración son generalmente realizadas por un proveedor de servicios de seguridad, que cuenta con gran experiencia en el campo y conoce las mejoras prácticas. Un método para evaluar que proveedor es el más indicado, consiste en elaborar un cuestionario con una serie de preguntas que han sido ponderadas por la importancia que percibe la organización sobre ese punto y responderlo para cada empresa seleccionada de tal manera que la empresa que saque el punteo más alto debiera ser la elegida.

- ¿Cuenta con una metodología para realizar las pruebas?
- ¿Cuenta con profesionales capacitados?
- ¿Tiene seguro para su equipo?
- ¿Puede un representante de la compañía estar presente para supervisar la prueba de la penetración?
- ¿Presentó las referencias pertinentes?
- ¿Brinda una muestra de los reportes que entregará?
- ¿Ofrece una solución de *software* para gestionar el proceso?
- ¿Hay una manera fácil de convertir los resultados en un informe de lectura?
- ¿Cuáles son las credenciales del proveedor de seguridad?
- ¿Utilizar técnicas manuales o automatizadas para descubrir vulnerabilidades?
- ¿El proveedor notificará de inmediato si las vulnerabilidades de alto riesgo se encuentran durante la prueba, o deberá esperar e informarlo en el informe final?

2. ARMANDO EL EQUIPO DE PENETRACIÓN

2.1. ¿Cómo armar el equipo que hará la prueba?

El equipo operativo es el que llevará a cabo la penetración física y los miembros pueden dividirse en diferentes roles con diferentes responsabilidades y áreas de experiencia. Es normal que la composición del equipo varíe de una prueba a otra.

2.1.1 Operador

Este término se utiliza para referirse a todos los miembros del equipo, independientemente de sus especialidades o funciones. Por lo general son las personas que participan directamente en las pruebas y no en un papel de apoyo.

2.1.2 Líder del equipo

Este miembro del equipo tiene la responsabilidad final de entregar la asignación, administrar el proyecto y a los miembros del equipo, la coordinación con la cliente. Este papel no debe ser permanente, si no cíclico. Esto le dará experiencia de liderazgo a cada miembro y alienta a nuevos enfoques. El líder del equipo por lo general dirige al equipo en el campo, pero a veces esto tiene que hacerse desde el centro de control, donde toma el papel de coordinador.

2.1.3 Coordinador

El coordinador dirige y asiste a los miembros del equipo desde el centro de control o de otra ubicación fuera de las instalaciones. Este miembro del equipo asegura que la asistencia fuera de la oficina (técnicos, jurídicos, de referencia, la ingeniería social, etc.) siempre esté disponible.

2.1.4 Ingeniero social

Este miembro tiene habilidades naturales para el engaño y la manipulación humana, es el encargado de atacar el eslabón más débil de la cadena, el usuario final.

2.1.5 Especialista en intrusión en computadoras

También conocido como "*hacker* ético", se encarga del acceso a las computadoras y redes, dentro de una prueba de penetración el objetivo son los sistemas de información.

2.1.6 Especialista en seguridad física

Este miembro del equipo debe ser experto en abrir cerraduras *y* experto en derrotar los mecanismos de seguridad físicos. Debe ser hábil en la utilización de herramientas manuales así como electrónicas, debe estar siempre practicando para que al momento de ser requerido resuelva eficientemente.

2.1.7 Especialista en vigilancia

Este miembro del equipo es el encargado de documentar fotográficamente las instalaciones, personal, gafetes, insignias, contenedores de basura y seguridad perimetral. Debe ser capaz de recopilar toda la información posible de forma encubierta, esto significa que debe introducirse dentro de la empresa y fotografiar todo sin ser descubierto. Toda la información recopilada es luego trasladada al coordinador del equipo de penetración, para que pueda establecer bien su estrategia de ataque.

3. CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA

3.1. Introducción

Por ciclo de vida de una prueba de penetración física se entiende la sucesión de fases por las que pasa la prueba desde que inicia hasta que finaliza. Cada fase tendrá un documento de salida, que formará parte del documento final que será entregado al cliente. El ciclo de vida de una prueba de penetración consta de 7 fases:

- Contratación
- Negociación de las reglas del enfrentamiento
- Investigación preliminar
- Determinación de riesgos
- Escribir plan de pruebas
- Ejecutar plan de pruebas
- Presentar resultados

3.2. Contratación

Es la etapa formal en la que comienza una prueba de penetración física, es el momento donde se asigna la responsabilidad de la prueba a un equipo de penetración, la salida por lo general en esta etapa son los contratos firmados por el cliente y el equipo que hará la prueba. Generalmente algunos clientes quieren negociar las reglas de enfrentamiento (ROE) y las incluyen como una sección del contrato antes de firmar.

3.3. Negociación de las reglas del enfrentamiento

Las reglas de enfrentamiento ("*Rules Of Engagement*, ROE") en el contexto de una prueba de penetración física, son los parámetros de operación dentro de los cuales los miembros del equipo de penetración trabajarán, se guiarán y se restringirán durante todo el ciclo de vida de la prueba. La importancia de estas reglas, es proteger al equipo de penetración de malentendidos con los clientes y consecuencias jurídicas que estas puedan generar *y* deberán ser acordados entre los encargados de las pruebas y el cliente. Aquí está una lista de las consideraciones mínimas:

- Determinar qué áreas de la seguridad el cliente considera débil y quiere probar, por ejemplo, el perímetro de seguridad física.
- Determinar qué áreas de las pruebas el cliente desea evitar por razones legales, porque ya fueron revisadas recientemente o porque son confidenciales.
- Cuanto es el tiempo máximo permitido para la prueba.
- Determinar si se irá notificando al cliente cada vez que se encuentre una vulnerabilidad o si se presentará todo al final.
- Deberá indicarse si será prueba de caja blanca o prueba de caja negra.

Una prueba en la que el equipo obtiene información importante por adelantado (con el fin de ahorrar tiempo y concentrarse en un área en particular) se llama "prueba de caja blanca". Cuando no se proporciona información la prueba se conoce como "prueba de caja negra". Y una mezcla entre los dos es llamada una "prueba de caja gris". Se deberá dejar claras las circunstancias para que la prueba sea considerada un éxito, un fracaso o sea abortada.

Deberá estar de acuerdo sobre las medidas que deben tomarse inmediatamente después que la prueba sea un éxito, un fracaso o haya sido abortada. Se debe establecer un calendario para la presentación y entrega del informe final. Una vez el encargado de la prueba y el cliente estén de acuerdo acerca de estos detalles, el documento ROE estará completo para su inclusión en la documentación del proyecto. La salida por lo general en esta etapa es el documento ROE firmado por el cliente y encargado de la prueba.

3.4. Investigación preliminar

El objetivo de esta etapa es conocer con el mayor detalle posible toda la información necesaria acerca del objetivo. En esta etapa no se requiere por el momento una especialización y ya que esta es un área común, cualquiera de los miembros del equipo está en la capacidad de realizarla. Estas funciones preliminares conforme vaya avanzando el proyecto irán siendo reevaluadas *y* los miembros del equipo irán poco a poco desempeñándose en su área de especialización.

El líder debe tener la habilidad necesaria para establecer esta reevaluación de funciones para no malgastar los recursos, por ejemplo: tener un experto en intrusión de red haciendo ingeniería social. En esta fase se realizan las siguientes actividades.

- Recopilación de información de inteligencia
- Vigilancia fotográfica
- Ingeniería social

3.4.1 Recopilación de información de inteligencia

La información de inteligencia puede ser obtenida de diferentes fuentes que pueden ser clasificadas en:

- Inteligencia humana (HUMINT)
- Señales de inteligencia (SIGINT)
- Fuentes de inteligencia abiertas (OSINT)
- Inteligencia de imágenes (IMINT)

3.4.1.1 Inteligencia humana (HUMINT)

HUMINT es un acrónimo en inglés (*Human Intelligence*), se refiere a cualquier información recogida de una fuente humana. La OTAN define inteligencia humana como “una categoría de la inteligencia derivada de la información recogida y proporcionada por fuentes humanas”. Las personas que proporcionan la información podrían ser neutrales, amistosas u hostiles, de buena o baja confianza.

El acto de recolección de información se conoce como ingeniería social. El uso experto de la inteligencia humana le dará al equipo de operación una ventaja considerable al penetrar en cualquier organización.

3.4.1.2 Señales de inteligencia (SIGNT)

SIGINT es un acrónimo en inglés (*Signals Intelligence*), es una rama de la inteligencia que se basa en la utilización de diferentes medios de comunicación. La inteligencia de señales engloba diferentes recursos.

3.4.1.2.1 COMINT

COMINT es un acrónimo en inglés (*Communications Intelligence*) supone la utilización de toda clase de comunicaciones conocidas, como el teléfono, la radio, televisión, etc.

3.4.1.2.2 ELINT

ELINT es un acrónimo en inglés (*Electronic Intelligence*) y significa adquisición de información por medios electrónicos.

3.4.1.3 Fuentes de inteligencia abiertas (OSINT)

OSINT es un acrónimo en inglés (*Open Source Intelligence*), se refiere a la obtención de información de inteligencia que se obtiene de fuentes públicas. Es información relevante derivada de una recolección, procesamiento y análisis sistemático de la información disponible, en respuesta a un requerimiento de inteligencia, puede provenir de *internet*, periódicos, noticias, etc.

3.4.1.4 Inteligencia de imágenes (IMINT)

IMINT es un acrónimo en inglés (*Imagery Intelligence*) es una rama de la inteligencia derivada de la información obtenida mediante imágenes proporcionadas a través de satélites o medios aéreos. Existen varias aplicaciones de *software* que pueden ser utilizados para adquirir inteligencia de imágenes, sin embargo Google con su producto Google *Earth* es el líder actual.

Google *Earth*, es un programa informático similar a un Sistema de Información Geográfica (SIG), creado por la empresa Keyhole Inc., que permite visualizar imágenes en 3D del planeta, combinando imágenes de satélite, mapas y el motor de búsqueda de Google que permite ver imágenes a escala de un lugar específico del planeta. Otras alternativas podrían ser:

- Marble, aplicación geográfica liberada bajo la licencia libre LGPL y desarrollada por KDE y la comunidad del *software* libre.

- *World Wind*, editado por la NASA es un programa similar. Este programa y las imágenes que muestra son de licencia libre.

3.5. Determinación de riesgos

Es responsabilidad del líder del equipo determinar qué constituye un nivel aceptable de riesgo. Si el líder del equipo considera que el nivel de riesgo es demasiado alto, entonces las ROE deben ser reevaluadas o la prueba no debe llevarse a cabo. Los riesgos en las pruebas de penetración física pueden clasificarse en las siguientes áreas:

- Riesgos contractuales
- Riesgos operacionales
- Riesgos legales
- Riesgos ambientales

En el ámbito de las *pentest* físicas para referirse a estos riesgos en conjunto se hace por su acrónimo en inglés COLE (*Contractual, Operational, Legal and Environment*) y así será referido en adelante.

3.5.1 Riesgos contractuales

Por lo general se producen cuando la compañía de pruebas ha subestimado la capacidad del equipo para complementar cierta tarea, por lo que no está a la altura de sus obligaciones contractuales. El hecho de que un equipo no logre completar una tarea, puede dar la idea de que el cliente está seguro *y* la razón puede ser otra, por ejemplo que el equipo de pruebas este mal entrenado.

3.5.2 Riesgos operacionales

Son accidentes o imprevistos durante la ejecución de una prueba de penetración, en el mejor de los casos puede ocasionar un atraso o no lograr completar una tarea *y* en el peor de los casos abortar la prueba. Entre estos riesgos están la mala interpretación de una instrucción, una falla técnica, una mala evaluación de la dificultad de una tarea.

3.5.3 Riesgos legales

Un proyecto puede incurrir en el riesgo legal directa o indirectamente. Los miembros del equipo se pueden colocar en una posición que podría llevar directamente a su arresto. Esto puede suceder cuando un guardia de seguridad evita el procedimiento e involucra directamente a la policía, cuando cree que un miembro del equipo está actuando sospechosamente o cuando los miembros del equipo son directamente aprehendidos por la policía, por ejemplo: durante un ejercicio de penetración nocturno.

Durante una prueba de caja negra, el alcance puede ser operativamente superado y a veces desastroso. Un ejemplo de esto es penetrar en la

instalación incorrecta. Por lo menos, esto puede implicar explicar a un juez que accidentalmente se irrumpió en el edificio equivocado, tales errores son siempre costosos.

3.5.4 Riesgos ambientales

Estos son los riesgos físicos que un equipo puede encontrar durante las pruebas que pueden afectar directamente la salud y la seguridad de los miembros del equipo. Algunos de los riesgos son:

- Trabajar por la noche o en la oscuridad
- Trabajar cerca de grandes concentraciones de agua
- Trabajo en presencia de máquinas o de alta tensión
- Escalar y descender
- Ser atacado por perros guardianes
- Trabajar en condiciones extremas de calor o frío
- Atravesar alambres espigados o con púas
- Confrontar seguridad armada

Muchas organizaciones hacen uso de seguridad armada, en tales circunstancias, existe un riesgo inherente de lesión o muerte a cualquier miembro del personal asignado al equipo de operación. La responsabilidad de todas las partes involucradas es enorme, se debe prestar mucha atención al evaluar los riesgos ambientales porque es seguro que un cliente no estará dispuesto a firmar si percibe que hay mucha probabilidad que uno de los miembros llegue a salir herido.

3.6. Escribir el plan de pruebas

Está compuesto a su vez por un Plan Estratégico, un Plan Táctico y un Plan Operacional.

3.6.1 Plan estratégico

Es una visión de muy alto nivel del proyecto, que detalla el objetivo, activos físicos, miembros del equipo, riesgos COLE potenciales, equipamiento necesario, así como un resumen de los antecedentes del proyecto.

3.6.2 Plan táctico

Dado el objetivo estratégico, en esta sección se crea una lista de los hitos y el orden en el cual deben ser entregados.

3.6.3 Plan operacional

Esta sección define en detalle que es requerido completar en cada hito y como su finalización afectará la *pentest* física.

3.6.4 Ejemplo de un plan de pruebas

Líder del Equipo: Vladimir Herbinsky
Fecha: 4 de Junio 2011
Cliente: Proveedora de Mariscos S.A. (PROMASA)

- Plan estratégico

PROMASA, es una empresa dedicada a la comercialización de productos marítimos, se encuentra ubicada en Escuintla y sus oficinas centrales, en Villa Nueva. Ha solicitado nuestros servicios de penetración física porque está interesado en evaluar su seguridad interna y está particularmente interesado en:

- Si es posible sacar producto de las instalaciones
- Introducir dispositivos a las instalaciones
- Evaluar el tiempo de respuesta al incidente
- Descubrir donde se encuentra la bóveda
- Introducir dentro de la bóveda todos los activos que puedan tomar durante la incursión

El cliente ha tomado la decisión de negociar las reglas del enfrentamiento. A continuación se detallan todas las reglas:

- ROE

Se tienen cinco días (empezando el 20 de marzo, 2011) para completar el trabajo en el sitio. Ya se está llevando a cabo una investigación preliminar. La asignación será en caja negra y los objetivos no están conscientes de la prueba (Jefaturas y personal operativo no han sido informados de la prueba). Ha sido habilitada una sala de juntas para servir como punto de contacto, aprovechando que ha habido auditorías externas recientemente y que son instalados en esa sala, nadie sospechará. Toda la prueba estará restringida al horario laboral, empezando a las 8:00 am y finalizando a las 17:00 pm.

- Riesgos COLE

La instalación cuenta con varios guardias de seguridad pero en la investigación preliminar se determinó que hay un acceso no cubierto desde un barranco donde colinda la empresa. El personal de seguridad se encuentra armado dentro y fuera de las instalaciones, pero generalmente cuando es medio día salen almorzar y quedan pocos realizando vigilancia. No existen patrullajes y el personal de seguridad es rotado constantemente y hay muchos que no conocen a los empleados de alto rango.

Por lo que se puede aprovechar el hecho de que no saben si algún miembro del equipo es o no un empleado. Hay que actuar con tranquilidad y seguridad. Se ha determinado también en la investigación preliminar que cuentan con 2 cámaras *web*, una ubicada en gerencia y la otra en un pasillo que lleva al departamento de compras.

- Miembros del equipo

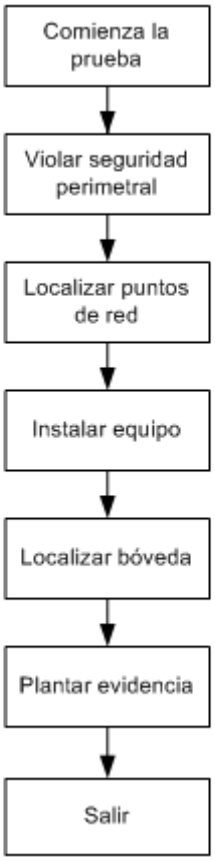
    - CJ – Ingeniero social
    - VL – Especialista en intrusión de computadoras
    - DF – Especialista en vigilancia y fotografía
    - Yo – Coordinador del equipo desde la oficina de control
    - MR – Llevara a cabo cualquier apertura de cerradura
    - *Extractor One* – Equipo encargados de extraer activos de las instalaciones
    - Alfa – Encargado de la penetración física

- Equipamiento

    - Herramientas para abrir cerraduras
    - *Laptops* y accesorios
    - El vestuario deberá ser camisa blanco y pantalón azul

- Plan táctico

Figura 7. **Diagrama de flujo de plan táctico**



Fuente: elaboración propia.

- Plan operacional

    - Violar seguridad perimetral – Lograr entrar desde la puerta principal.

    - Violar seguridad interna – Lograr pasar más allá de recepción.

    - Extraer activos de la empresa – Deberán ser activos pequeños como engrapadoras, plumas, reglas, esto será llevado a cabo por el equipo "*Extractor one*".

    - Localizar puntos de red – Buscar dentro de las instalaciones puntos de acceso a la red, descuidados y conectar *Access Point* y dispositivos de escucha electrónicos.

    - Adquirir contraseñas – Proceder con cautela y a discreción. Este es trabajo de *cypher.*

    - Buscar la bóveda – Se desconoce la ubicación física de la bóveda por lo que requerirá trabajo en conjunto con los ingenieros sociales. Será necesario entrar al edificio principal que a su vez requiere pasar por dos puntos de control, antes de llegar a recepción.

    - Plantar evidencia – Introducir los activos a los que se ha logrado tener acceso dentro de la bóveda, estos activos podrán ser celulares, portátiles, armas de fuego (Se considera un bono extra por cada arma de algún agente colocada dentro).

    - Salir – Salir de las instalaciones.

3.7. Ejecutar el plan de pruebas

En términos generales existen tres enfoques para conducir una prueba de penetración física y escoger el más viable dependerá de la investigación preliminar que se haya realizado.

- Enfoque al descubierto
- Enfoque encubierto
- Enfoque invisible

3.7.1 Enfoque al descubierto

En este el *penetration tester* no hace ningún intento por ocultar su presencia, tampoco por evitar los controles de seguridad y o guardias, esto no significa que quiera dar a conocer sus intenciones, lo que intenta es mezclarse tanto como sea en el sistema. Cuando se trabaja abiertamente el *penetration tester* confía en las fallas humanas utilizando para ello ingeniería social. Es probable que un operador de una cámara de seguridad no note nada sospechoso en un *penetration tester* que se comporta como parte del medio ambiente.

Un ejemplo de esto podría ser que un *penetration tester* llegue a recepción y ofrezca información falsa y reciba una tarjeta de visitante legítima, ya que se ha logrado vencer esta barrera. El *penetration tester* se convierte en parte del sistema y ya no tiene nada que temer. Este tipo de enfoque requiere mucho más tiempo de planificación, para lograr que el *penetration tester* obtenga un buen grado de confianza.

3.7.2 Enfoque encubierto

En este el *penetration tester* realiza actividades similares al anterior, solo que en este enfoque evita tener contacto con personal que este en posición de autoridad. No ingresa por la puerta principal a menos que cuente con llaves, tarjetas de acceso, prefiere hacerlo por puertas alternas o pegarse lo más que pueda a un grupo que este ingresando para así aprovechar el acceso que el grupo ha logrado.

Un ejemplo de esto podría ser que un *penetration tester* simule estar atendiendo una llamada mientras se acerca alguien con acceso legítimo a la puerta de acceso y en el instante que el empleado entra este termina la plática y simular estar apurado y se le pega al otro empleado, por lo general esto es muy común en grandes organizaciones con este tipo de restricción de entrada, procurando nunca hacer contacto visual.

3.7.3 Enfoque invisible

En este enfoque el *penetration tester* actúa en sigilo nunca hace contacto con nadie dentro de las instalaciones, generalmente son incursiones nocturnas. Está más orientado a eludir guardias y cámaras de seguridad, el *penetration tester* tiene grandes habilidades en abrir cerraduras y nervios de acero. Los peligros en este tipo de pruebas es que si lo detecta un guardia de seguridad lo tomarán como un agente hostil y es muy probable que no tenga oportunidad de explicar que hace dentro de las instalaciones. Este tipo de pruebas es más recomendable para evaluar específicamente la seguridad interna y externa.

3.7.4 Como conducir la exploración del lugar

Mientras el *penetration tester* se encuentra dentro de las instalaciones el riesgo de ser descubierto crece exponencialmente mientras más tiempo transcurra adentro. Esto no quiere decir que debe ser rápido, ya que apresurarse es también muy arriesgado, es por ello que el *penetration tester* debe saber que está buscando, no ir a tratar de improvisar, debe estar totalmente apegado a su plan. Eso sí, este debe ser flexible para darle un pequeño margen para decidir qué hacer en el momento que se le presente una complicación, generalmente las organizaciones están divididas en áreas como las siguientes.

- Recepción: esta área tiene como función principal dar la bienvenida a los visitantes, es la cara de la organización. Por lo general los visitantes dependerán de la naturaleza de la organización pero se puede identificar como: clientes, contratistas, vendedores, compradores, visitantes o delegados de instituciones de gobierno. Los cuales son tratados de diferentes maneras, aquí ya se tiene una pista y como dice el dicho popular "así como lo ven será tratado".

  No hay que mezclar recepción con seguridad y este es un gran error, ya que son cosas totalmente distintas y que no son compatibles entre sí. El hecho de que una recepcionista no deje pasar a alguien no significa que hay seguridad en ese punto de acceso, es más, crea el sentimiento de falsa seguridad, es muy frecuente que los protocolos de seguridad sean rotos más en recepción que en otra parte, porque a veces queda a discreción de la recepcionista el hacer firmar a un visitante o pedir su identificación y más si considera que es una persona muy importante y que la puede ofender al

hacerle firmar o pedirle su cédula o licencia para asegurarse de que es la persona que dice ser.

- Sala de juntas: estas áreas son usadas eventualmente por algunas horas para discutir temas de interés en las compañías, para atender clientes o contactos importantes, por lo que generalmente se encuentran vacías, siempre vale la pena explorarlas ya que generalmente cuentan con puntos de red que no son supervisados y no hay cámaras de seguridad por lo mismo que a veces se discuten temas de confidenciales. Este sería un buen punto para introducir un dispositivo de escucha o plantar un *Access Point* en algún punto de red disponible.

- Oficina de gerencia: una prueba no se limita únicamente a tener acceso físico a las instalaciones o sustraer un activo, también puede estar dirigida a tener acceso a una persona importante. Cuando una prueba está dirigida a un directivo, se pretende evaluar que tan expuesto esta un ejecutivo de una amenaza externa, esto significa que estar dentro de unas instalaciones no significa que esté seguro, estos ataques podrían ser empleados descontentos, espías corporativos, periodistas, etc.

- Cuarto de servidores: es una de las zonas que debiera estar más seguras dentro de cualquier organización y su incumplimiento es el blanco de muchas pruebas de penetración física. Una gran organización puede tener más de un cuarto de servidores y, ciertamente, disponer de una infraestructura de red tales como *routers* y *switch*es en cada piso.

  Obtener acceso directo a los servidores físicos significa que se puede pasar por alto muchos mecanismos de seguridad tales como *firewalls* y sistemas de detección de intrusos. Sólo demostrando que se

puede acceder al cuarto de servidores sin autoridad, es un problema extremadamente grave de seguridad.

- Bodegas: es una de las áreas más atractivas por los ladrones por lo tanto un objetivo excelente para una prueba de penetración. Generalmente los almacenes tienen varias entradas que están bien custodiadas. En muchas organizaciones basta con portar un carnet para lograr el acceso. La investigación preliminar deberá suministrar este tipo de información, para que al momento de llegar el *penetration tester* lleve todo lo necesario. Es aconsejable ir con el uniforme de la empresa para no levantar sospechas.

- Garitas de seguridad o dormitorios: en grandes organizaciones los empleados de seguridad cuentan con áreas de descanso o dormitorios por lo que podría ser un objetivo interesante, ya que es muy probable encontrar llaves de acceso, uniformes, armas, balas, dispositivos de radio comunicación, programación de turnos, información relacionada a áreas de vigilancia, manual de procedimientos, etc.

3.7.5 Enfoques tácticos

3.7.5.1 Seguir de cerca (*Tailgating*)

Es un ataque que se puede utilizar en cualquier entorno que haga uso de proximidad, como puertas de control. En principio, el concepto es bastante simple pero en la práctica, se requiere un poco de previsión para la ejecución exitosa. Está claro que un intruso no puede abrir una puerta sin una llave o tarjeta magnética, por lo que para superar esta limitación el intruso esperará que alguien con acceso legítimo abra la puerta y luego el intruso se deslizará detrás.

Es importante hacer esto sin levantar sospechas. Un acercamiento clásico es hablar por teléfono próximo a una puerta y concluir la llamada justo cuando alguien pase y abra la puerta. Lo sigue y da la impresión que salió únicamente atender una llamada, la cual usted ha concluido y que ahora regresa, no deberá realizar contacto visual si es posible deberá verse preocupado, frustrado.

Ya que estas son emociones comunes en un ambiente corporativo. Hay que tener cuidado de no seguir muy de cerca a una misma persona a lo largo de varios puntos de acceso, esto podría levantar sospechas, no debe involucrar a la persona que sigue de cerca en la conversación, ya que pude abordarlo y preguntarle a donde se dirige.

3.7.5.2 Vestimenta adecuada

“Así como lo ven lo tratan”, es un hecho que la gente juzga por la apariencia. En una prueba, es exactamente lo que se desea que hagan. Es posible adoptar varios personajes para la prueba particularmente si se lleva a cabo en fases. La investigación preliminar deberá de ayudar a determinar que vestimenta es la más adecuada, poniendo atención a los detalles, es decir colores, tarjetas de identificación, etc. Por ejemplo: si todos los trabajadores usan camisa blanca y el *penetration tester* lleva roja es obvio que de inmediato se darán cuenta de la diferencia.

3.8. Presentar resultados

En esta fase se presentan los resultados al cliente, el documento deberá contener todos los documentos que fueron generados durante el ciclo de vida de la prueba. Estos documentos son:

- Contrato firmados
- ROE
- Plan de pruebas
- Copia de identificación de cada miembro del equipo
- Antecedentes policíacos y penales de los miembros del equipo
- Copia de las pólizas de seguro de los miembros del equipo
- Copia de autorización para realizar la prueba

4. MECANISMOS DE SEGURIDAD FÍSICA

4.1. Mecanismos de seguridad física

Son todos aquellos elementos que impiden el acceso físico de personas no autorizadas a las instalaciones de una organización, con el objetivo de resguardar y proteger a sus individuos o bienes. Entre los mecanismos más comunes están:

- Uso de gafetes
- *Token* de proximidad
- Guardias
- Cámaras de vigilancia
- Controles biométricos

4.1.1 Gafetes de identificación

Gafetes se refiere a un término para definir las insignias que se ponen en la ropa, para identificar al portador y permitirle acceso a edificios. Está compuesto por dos elementos, el soporte, que es donde los datos de la persona son colocados y la sujeción que complementa el soporte para fijarlo en determinado lugar (ver figura 8). El tipo de sujeción que generalmente se utiliza es el alfiler de gancho o el pin, también pueden utilizarse otros sistemas, tales como, cintas (colgantes), velcro, pinzas, etc.

Existe gran variedad, siendo lo más utilizados los siguientes:

- Gafetes de papel
- Gafetes acrílicos y PVC
- Gafetes metálicos

Figura 8. **Gafete con cinta colgante**

Fuente: http://www.pcdomino.com/page/PROD/USBVUME2GBOR.html. 05/01/2011

4.1.1.1 Anulando el control por gafetes

Una empresa dentro de sus políticas de seguridad puede establecer que los empleados y visitantes deben portar gafete de identificación mientras están dentro de las instalaciones y quien no las use podrá ser amonestado (ver figura 9). En un escenario como el anterior es mucho más seguro que alguien note que una persona no porta su gafete de identificación a que note que el gafete no es el correcto, o que no lo lleva derecho. En estos casos lo ven más como parte de su indumentaria, esto también crea una falsa seguridad porque el hecho de que alguien tenga gafete no significa que realmente ha sido identificado o que deba estar donde está.

Figura 9. **Gafetes para personal interno y visitantes**

Fuente: http://www.vitro.com/miv/ext/espanol/medios.htm. 05/01/2011

En la investigación preliminar se deberá documentar la forma en que los empleados o visitantes son identificados dentro de las instalaciones, se deberá conocer en detalle todas las características del gafete de identificación así como establecer si el gafete cuenta con alguna marca o color que establezca algún permiso especial o que denote jerarquía.

Con esta información el equipo de penetración será capaz de fabricar una credencial que permita a los miembros del equipo movilizarse libremente dentro de las instalaciones. Un elemento que se tiene a favor es que la naturaleza humana de las personas no es confrontativa por lo que es muy poco probable que alguien detenga a un miembro del equipo y cuestione alguna característica de un gafete.

Otro elemento a favor es la vergüenza, muchos gafetes por lo general portan una fotografía del empleado, pero si alguno de ellos tiene la idea que se ve mal es muy probable que siempre utilice el gafete al revés *y* como esto es tan común es muy poco probable alguien sospeche de un miembro del equipo de penetración que lleve el gafete al revés.

Fabricar un gafete es una de las mejoras formas de burlar este tipo de seguridad basta contar con un *software* y con todas las características que se obtuvieron en la investigación preliminar y reproducirlo. Uno de los mejores programas para realizarlo es *ID Flow Photo ID Badge Maker Software*, ya que brinda todo lo necesario para diseñar e imprimir tarjetas de identificación.

4.1.2 Tarjetas de proximidad

Son tarjetas utilizadas para abrir puertas, son elementos pasivos, es decir, no tienen fuente de poder propia y sólo se activan cuando se encuentren en la proximidad del lector. Aparte de la seguridad básica, estos dispositivos tienen la ventaja que pueden ser configurados con diferentes niveles de acceso, por lo que el personal que la porte solo podrá ingresar en donde su nivel de acceso le permita.

Figura 10. **Tarjetas de proximidad**

Fuente: http://www.contractorstools.com/keri_ct.html. 17/01/2011

4.1.2.1 Anulando las tarjetas de proximidad

Una forma fácil de anular este mecanismo de seguridad es obtener la tarjeta de un empleado mientras este se encuentre ocupado realizando sus

labores diarias o extrayendo alguna tarjeta de alguna oficina cercana. Se puede también por medio de ingeniería social lograr que un empleado preste su tarjeta de proximidad, esto requerirá una gran habilidad del miembro del equipo que realice el engaño.

4.1.3 Llaves de proximidad

Son dispositivos que contienen medios electrónicos de control lo que los hace muy difícil de replicar. Cada dispositivo tiene un identificador único el cual es asociado a un empleado con un determinado nivel de acceso (ver figura 11). Una ventaja de estos dispositivos es que pueden ser integrados con otros mecanismos de seguridad, como por ejemplo alarmas contra incendio, al momento de activarse la alarma el sistema de forma automática desactiva el verificador de acceso y abre las puertas, hasta que la alarma sea desactivada, el sistema se activará de forma automática de nuevo.

Figura 11. **Llaves de proximidad**

Fuente: http://www.contractorstools.com/keri_ct.html. 17/01/2011

4.1.3.1 Anulando una llave de proximidad

Aunque si existen los dispositivos que son capaces de clonar las llaves son demasiado caros. Hay dos formas posibles para anularlos, una es

utilizando ingeniería social con el encargado de la administración de la base de datos de control de accesos y la otra es activando la alarma contra incendios.

4.1.4 Guardias de seguridad

Son las personas encargadas de proteger la integridad física de las personas y los bienes materiales de la empresa donde labora, teniendo a su disposición recursos técnicos (su experiencia) y tecnológicos (cámaras de video, radios de comunicación, detectores de metales o dispositivos electrónicos biométricos de control de acceso: huella e iris del ojo, entre otros). También pueden utilizar otros medios como perros amaestrados.

En muchos lugares también les es permitido portar armas de fuego y usarlas en defensa propia o cuando el objetivo que intentan proteger está bajo amenaza.

4.1.4.1 Anulando los guardias de seguridad

Un guardia es un elemento que se puede explotar de una manera que no se pueden explotar las contramedidas electrónicas y es utilizando ingeniería social. Los guardias pueden llegar a ser muy útiles para un ingeniero social, ya que ellos más que nadie están familiarizados con todos los puntos de control, con las instalaciones, etc. También se puede explotar el hecho que los guardias también son entrenados en relaciones humanas y se espera que sean amables y que den un buen servicio al cliente.

4.1.5 Circuito cerrado de televisión

Circuito cerrado de televisión o CCTV (siglas en inglés de *closed circuit television*) es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores de vídeo o televisores. Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control donde se puede configurar su panorámica, enfoque, inclinación y *zoom*.

Figura 12. **Circuito cerrado de televisión**

Fuente: http://identitronics.blogspot.com/. 17/01/2011

Estos sistemas incluyen visión nocturna, operaciones asistidas por computadora y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros.

4.1.6 Controles biométricos

Los controles biométricos se refiere al conjunto de tecnologías destinas a medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación. Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas).

4.1.7 Control de acceso

El control de accesos ha evolucionado considerablemente a lo largo de estos años, actualmente se puede identificar como un sistema integrado de políticas y procesos organizacionales que pretende facilitar y controlar el acceso a los sistemas de información y a las instalaciones. Mediante la implantación de un sistema de control de accesos se puede gestionar y monitorizar no solo las entradas y salidas a determinados edificios o instalaciones, también se puede hacer un seguimiento pormenorizado de la ubicación de las señales que se reciban de los dispositivos de identificación.

Figura 13. **Tipos de reconocimiento biométrico**

Reconocimiento dactilar	Reconocimiento del iris	Reconocimiento facial

Fuente: http://clasipar.paraguay.com/control_de_acceso_de_personal_biometrico_668371.html. 17/01/2011

Figura 14. **Sistema de acceso RFID**

Fuente: http://www.diytrade.com/china/4/products/5448642/RFID_access_control.html. 17/01/2011

Dependiendo de cuál sea el objetivo buscado con la implantación de un sistema de estas características se podrá saber por ejemplo, en qué zona se encuentra una persona en caso de emergencia. Las tecnologías más usadas son radio frecuencia y las tarjetas magnéticas.

Figura 15. **Tarjeta magnética**

Fuente: http://www.mmlocksmith.com/ACC1.Html. 17/01/2011

4.1.8 Perros de seguridad

La función de estos perros es actuar como elemento disuasorio de posibles malhechores. Se clasifican en dos tipos guarda y seguridad personal. Los perros de guarda se encargan de proteger un espacio cerrado, como un carro o un terreno. Su uso está generalizado en empresas que tienen amplias aéreas circundantes a los edificios, donde se pueda dificultar la vigilancia humana. Los perros de protección se encargan de proteger al dueño o guía en situaciones en las que se vea comprometida su seguridad. Principalmente, son utilizados como defensa personal para evitar agresiones. Estos perros siempre deben ser activados por el guía o dueño, actuando sólo cuando este lo cree conveniente.

5. INGENIERÍA SOCIAL

5.1. ¿Qué es la ingeniería social?

Significa la obtención de información confidencial privilegiada mediante la manipulación de las fuentes legítimas o titulares de esa información, generalmente implica la obtención de contraseñas o información personal. En palabras de Kevin Mitnick, uno de los personajes más famosos del mundo por delitos utilizando la ingeniería social como principal arma: “usted puede tener la mejor tecnología, *firewalls*, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresar sin más. Tienen todo en sus manos”.

El principio que sustenta la ingeniería social es el que en cualquier sistema “los usuarios son el eslabón débil”. En la práctica, un ingeniero social usará comúnmente el teléfono o *internet* para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía *internet* o la *web* se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas *web* o memos falsos que solicitan respuestas e incluso las famosas “cadenas”, llevando así a revelar información sensible o a violar las políticas de seguridad típicas.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, por ejemplo: proporcionando detalles financieros a un aparente funcionario de un banco, en lugar de tener que encontrar agujeros de seguridad en los

sistemas informáticos. Cuando se realizan pruebas de penetración a sistemas informáticos o redes, las técnicas utilizadas y los resultados obtenidos se pueden medir y es mucho más fácil recomendar y presentar los hallazgos y algo que es importante también son repetibles.

Esto significa que si se realiza una prueba de penetración en unos meses es muy probable que ya no sean los mismos resultados, sin embargo cuando se atacan personas no importa el tiempo que transcurra los resultados pueden llegar a ser los mismos ya que las técnicas y acercamientos pueden ser diferentes.

5.2. Guerrilla psicológica

Hay varias facetas de la psicología humana que pueden ser explotados para obtener información, predecir y controlar el comportamiento. Todas las personas responden de forma diferente a estímulos y lo hacen de acuerdo a su carácter. Sin embargo personas con el mismo carácter generalmente se encuentra en roles similares, por lo que es posible predecir con cierto grado de precisión que técnica es más efectiva a determinado tipo de persona.

Toda persona padece las mismas debilidades dentro y fuera del sistema informático o de la red de trabajo. En este sentido, las técnicas de engaño conocidas mundialmente y vigentes desde los inicios de la humanidad, sólo deben ser adaptadas al nuevo medio por el cual las personas maliciosas apuntan a concretar sus ataques. La efectividad de tal adaptación es complementaria con el aprovechamiento, para su explotación, de cualidades propias del ser humano como, por ejemplo:

- Confianza
- Ignorancia
- Credulidad
- Codicia
- Deseo de ayudar
- Deseo de ser querido

5.2.1 Explotando la confianza

Es la parte medular del ataque de ingeniería social, se centra en lograr la confianza de las personas para luego engañarlas y manipularlas para el beneficio propio de quien la implementa. La gente confía en lo familiar y por naturaleza los seres humanos son más confiados en su propio clan o en su círculo social y menos fuera de ellos. La persuasión es una habilidad clave, ya que el secreto no está en preguntar sino en la forma de realizar la pregunta

Una técnica comúnmente usada es la de “soltar nombres”, durante una conversación se pueden mencionar nombres de personas o amigos en puestos prominentes, con tal de impresionar y de esta forma hacer pensar a la otra persona que es alguien conocido y además importante. Esta técnica trabaja directamente en el subconsciente de la víctima ya que al darle mucha información esta asumirá de inmediato que la persona que le habla es de confianza y a medida que se le suministre más información, este grado de confianza irá creciendo.

Hay un principio que dice “si usted le da un poco de conocimiento a las personas, ellas asumirán que usted tiene mucho” y es el principio principal detrás de la técnica llamada pretexto. Pretexto es el acto de crear y utilizar un escenario inventado (el pretexto) para enfrentar una víctima específica de una

manera que aumenta la posibilidad de que la víctima divulgue información o realice acciones que no haría en circunstancias normales.

Es más que una simple mentira, ya que a menudo implica una investigación previa y el uso de información previa para la suplantación (por ejemplo, fecha de nacimiento, número de seguro social, la cantidad último recibo) para establecer la legitimidad en la mente de la víctima.

5.2.2 Explotando la ignorancia

La ignorancia no es lo mismo que falta de inteligencia. Esto significa que al hablar de ignorancia se refiere a que hay ciertas áreas donde las personas son más competentes y otras donde no. Las personas tienen una tendencia natural de someterse a la autoridad de otras personas en situaciones donde se sienten menos competentes. Informática es un área en la que la mayoría de la gente se siente ignorante en gran o menor medida, sobre todo cuando se habla con alguien que da la impresión de que sabe demasiado.

La explotación de la ignorancia de las personas en los sistemas informáticos es una poderosa herramienta de ingeniería social cuando se junta con el hecho de que la gente no les gusta sentirse ignorante. Una actitud de “por supuesto que sé lo que estoy haciendo, solo necesito que me digas qué hacer” es una combinación peligrosa entre orgullo e ignorancia que se puede explotar.

La mayoría de las personas se ven obligados a utilizar sistemas informáticos, pero no es lo mismo saber cómo utilizarlo a saber cómo funciona *y* esto se puede explotar transmitiendo instrucciones técnicas a la victima porque es muy probable que no comprenda las consecuencias de lo que está haciendo,

sin embargo la victima tendrá la percepción de que uso a la perfección el sistema y que resolvió eficientemente a la solicitud técnica.

5.2.3 Explotando la credulidad

El nivel de credulidad de una persona es cuan predispuesta es a creer en algo sin alguna evidencia que soporte la verdad o existencia. Cuando la naturaleza de la verdad no tiene ningún impacto en el día a día de una persona, esta se convierte en una verdad subjetiva y la verdad subjetiva es más susceptible a la manipulación. Es evidente que una persona crédula es más útil a un ingeniero social. Una manera interesante de aumentar la credulidad de una persona es mediante la explotación de su codicia.

La codicia y la credulidad van de la mano y la gente parece dispuesta a creer en cosas realmente absurdas si se presiona su codicia al límite. Un ejemplo clásico es la estafa nigeriana, timo nigeriano o timo 419. Se lleva a cabo principalmente por correo electrónico no solicitado. Adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país.

Esta estafa consiste en ilusionar a la víctima con una gran fortuna, que en realidad es inexistente, con objeto de persuadirla luego para que pague una suma de dinero por adelantado como condición para acceder a la supuesta fortuna. Es decir, se le promete a la víctima el todo o parte de una inexistente cantidad millonaria de dinero, para luego convencerla – mediante excusas muy elementales inventadas – a adelantar cierta cantidad de dinero propio al estafador.

5.2.4 Explotando la codicia

La explotación de la codicia es un poderoso vector de ataque. Incluso las personas que no se consideran a sí mismos codiciosos son susceptibles a esta forma de manipulación, porque el deseo de querer más de lo que se tiene es un impulso humano. La explotación de la codicia es saber lo que la gente quiere, lo que necesitan (o creen que necesitar) y proporcionárselos, aunque no de la manera que ellos esperan. Este constituye la base de uno de los posibles ataques más devastadores, los troyanos.

Un troyano es un *software* malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo y en la mayoría de las veces como un regalo, pero al ejecutarlo ocasiona daños. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés *backdoor*) que permite la administración remota a un usuario no autorizado. Recuerden nada es gratis y nadie regala nada, cuando alguien regala algo lo mejor es dudar.

5.2.5 Explotando el deseo de ayudar

Ser útil es algo que se requiere de todo el personal en una empresa, sobre todo a los recién llegados y los clientes. Por ello, las nuevas contrataciones y clientes visitando son disfraces muy populares para los ingenieros sociales. Alguien nuevo en la compañía se espera que haga preguntas ya que no saben. Un cliente es una fuente de ingresos y la mayoría de las empresas harán lo imposible para asegurarse de que son felices. Pretender ser un nuevo empleado es el más fácil de explotar.

Todo el mundo recuerda su primer día en el trabajo y la forma en que puede ser intimidante, por lo que es una tendencia natural entre el personal existente echar una mano al nuevo. El ser un nuevo empleado también le permite realizar una serie de preguntas difíciles sin levantar sospecha. Por ejemplo: pedir instrucciones, pedir ayuda para entrar en la red, pedir que lo dejen entrar con el pretexto que todavía no tiene tarjeta magnética, etc.

5.2.6 Explotando el deseo de ser adulado

Prácticamente todo el mundo le gusta sentirse adulado. Un ataque clásico de ingeniería social es inducir a este sentimiento en los que están manipulando. Esto es sorprendentemente fácil y, a pesar de las apariencias, la persona más fría puede llegar a ser la más fácil de manipular *y* esto se debe a que la mayoría de personas que son frías están acostumbradas a que los traten con indiferencia o que los vean de reojo.

5.2.7 Ingeniería social inversa

Ocurre cuando el *penetration tester* crea un personaje que parece estar en una posición de autoridad de tal modo que le pedirán información a él, en vez de que él la requiera. Las tres fases de los ataques son: sabotaje, promoción y asistencia. El atacante sabotea una red o sistema, ocasionando un problema, luego promueve que él es el contacto apropiado para solucionar el problema. Cuando comienza a dar asistencia en el arreglo el problema, va requiriendo información poco a poco de los empleados y de esa manera obtiene lo que realmente quería cuando llegó. Los empleados nunca supieron que estaban siendo atacados, porque su problema quedo resuelto.

5.3. Enfoques tácticos útiles de ingeniería social

5.3.1 Actuar impacientemente

Actuar con impaciencia cuando alguien se está moviendo demasiado despacio o que parezca que esta validando su historia puede ser eficaz en lograr distraerlo y desenfocarlo del procedimiento de control de seguridad. Se pueden esperar al menos tres respuestas a este enfoque, poner nervioso al objetivo, un objetivo más colaborador o que el objetivo lo ignore.

5.3.2 Ser cortés

La cortesía es un comportamiento humano de buena costumbre, es el uso práctico de las buenas costumbres o las normas de etiqueta.

5.3.3 Inducir miedo

Esta es una táctica muy desagradable, pero eficaz y es utilizada muy a menudo por ingenieros sociales criminales. En esencia, se crea un problema (o la creencia de que existe un problema) y se convence a un destino de que él o ella es la causa. Esto crea temor, un sentimiento de culpa, si se puede mantener a la gente con miedo es más fácil manipularlos.

5.3.4 Realizar una falsa suplica

Esta es una técnica eficaz para obtener ayuda (en particular si el atacante es bueno en fingir emociones fuertes) porque no es algo que mucha gente sepa cómo tratar.

5.3.5 Utilizar poder

Esta técnica consiste en aprovechar que los mandos medios nunca van a cuestionar las órdenes de un superior, es más solo las acatarán, es muy parecida a la táctica de miedo, a diferencia que esto es implícito cualquiera sabe que si desobedece a una autoridad puede quedar despedido.

5.3.6 Manipulación sexual

Otra de las técnicas comunes de ingeniería social empleada es la manipulación sexual. Es más común que en esta área los hombres sean los más susceptibles y esto se debe a que al momento de que una dama le pide ayuda, esto alimenta poderosamente el ego y querrá quedar bien y lo que menos está pensando es que la dama sea un atacante. Las armas pueden ser sonrisas, guiños de ojos e incluso un beso de agradecimiento.

5.4. Arte del engaño

Este “arte de engañar” puede ser utilizado por cualquiera, desde un vendedor que se interesa en averiguar las necesidades de sus compradores para ofrecerles un servicio, hasta creadores de *malware* y atacantes que buscan que un usuario revele su contraseña de acceso a un determinado sistema. Más allá de las coincidencias, o no, en el límite de lo éticamente correcto, todo intento de obtener información confidencial para un uso inapropiado, resulta una actividad altamente cuestionable.

En el mundo de la seguridad de la información, el “arte del engaño” es utilizado para dos fines específicos:

- El usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema: esto ocurre cuando el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto, abrir la página *web* recomendada o visualizar un supuesto video. Un caso de "éxito" de este tipo de infecciones es el gusano Sober que, mediante un sencillo mensaje, logró ser el de mayor propagación del año 2005. Este *malware* alcanzó una distribución masiva con asuntos de correos tales como "*Re:Your Password*" o "*Re:Your email was blocked*".

- El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del *scam* y el *phishing*, en los que el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza o con un pretexto de que obtendrá algo a cambio, generalmente un "gran premio".

Estos casos evidencian otra importante característica de la ingeniería social: la excelente relación costo beneficio obtenida con su aplicación. La convierte en una técnica de lo más seductora, con sólo una llamada telefónica, un correo electrónico o un mensaje de texto vía SMS el atacante puede obtener acceso a información valiosa del usuario, la empresa o incluso acceder a una red de sistemas. No hay tecnología capaz de proteger contra la ingeniería social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque.

La ingeniería social no pasa de moda, se perfecciona y sólo tiene la imaginación como límite. Así mismo, existe una única y efectiva forma de estar prevenido contra ella: la educación. Que consiste en una concientización social que permita al usuario estar prevenido y alerta para evitar ser un blanco fácil de este tipo de ataques.

6. CERRADURAS

6.1. Como abrir cerraduras

Conocido como *lock picking*, se refiere a todas las técnicas de apertura de cerraduras sin el medio original, por lo general llaves. Abrir cerraduras es una habilidad que se obtiene únicamente estando en la práctica, requiere bastante entrenamiento para dominar la técnica. Es claro que cualquier mecanismo físico de seguridad puede ser pasado de forma destructiva, sin embargo es muy probable que una prueba de penetración en las reglas de enfrentamiento se haya establecido que no se puede dañar físicamente ninguna cerradura.

Por esta razón es necesario tener una idea general de cómo está compuesta una cerradura, como funciona y como se puede vulnerar.

6.1.1 Partes de una cerradura

Las expresiones utilizadas para describir las cerraduras y sus partes, varían entre fabricantes, a continuación las formas más comunes:

- Tambor (*Hull*): esta es la parte de la cerradura que no gira
- Cilindro (*Plug*): este girará cuando la llave correcta sea insertada
- Canal de la llave (*Keway*): es donde se inserta la llave

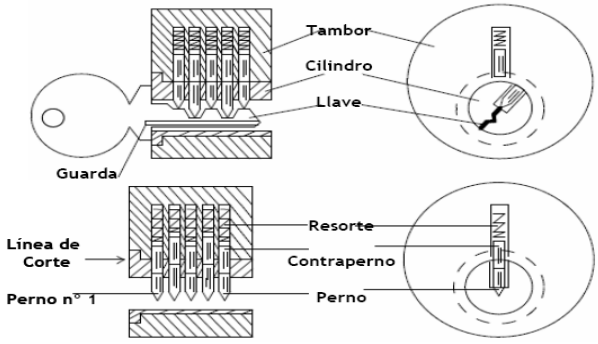
- Guarda (*Ward*): son las salientes que están en la bocallave que sólo permiten que llaves de un corte adecuado, puedan ser insertadas en la ranura.

- Contrapernos (*Driver pins*): son las clavijas que se asientan sobre la llave y son empujados por resortes.

- Perno (*Key pins)*: Son los pines que son empujados por la llave hacia arriba.

- Línea de corte (*Sheer line*): cuando la llave correcta se introduce en una cerradura, los pernos y contrapernos quedan alineados y allí es cuando permite que la cerradura pueda ser abierta. Cuando una llave incorrecta es insertada, los pernos no quedan alineados y es allí donde no permiten la rotación y por ende la cerradura no es abierta.

Figura 16. **Cámara de pernos**



Fuente: MIT *Guide to Lock picking*. p. 6.

6.1.2 Funcionamiento de una cerradura

La llave correcta levanta cada perno hasta que el plano de separación entre éste y el contraperno alcanza la línea de corte. Cuando todos los pernos

están en esta posición, el cilindro puede rotar *y* la cerradura se abre (ver figura 17).

Figura 17. **Funcionamiento de una cerradura de pernos**

Los pernos están alineados y alcanzan la línea de corte.

Permite la rotación del cilindro

Fuente: http://en.wikipedia.org/wiki/Pin_tumbler_lock. 17/01/2011

Hay dos condiciones en las cuales los pernos impiden la rotación del cilindro la primera es cuando no hay llave, ya que los resortes empujan los pernos contra el tambor e impiden que este rote (ver Figura 18.a), *y* la segunda es cuando se inserta una llave incorrecta, ya que dejará algunos pernos trabados entre el cilindro y el tambor, e impiden que este gire (ver Figura 18.b).

Figura 18. **Pernos no alineados**

(a) (b)

Cuando no hay llave

Cuando la llave es incorrecta

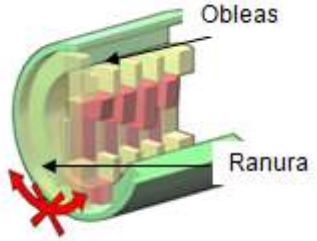
Fuente: http://en.wikipedia.org/wiki/Pin_tumbler_lock. 17/01/2011

6.1.3 Cerradura de oblea

Una cerradura de oblea es un tipo de bloqueo que utiliza un conjunto de obleas planas para evitar la apertura a menos que la llave correcta sea insertada (ver la figura 19). Este tipo de bloqueo es similar a la cerradura de pines y funciona en un principio similar. Sin embargo, a diferencia de la cerradura de pines, la oblea es una sola pieza. Sin la llave correcta, las obleas son empujadas por resortes a ranuras en la superficie del cilindro previniendo así la rotación.

Cuando la llave correcta es ingresada las obleas son levantadas lo necesario para permitir la rotación.

Figura 19. **Cerradura de oblea**



Fuente: http://www.bondedlockservice.com/pages/wafer-tumbler-lock%20.htm. 17/01/2011

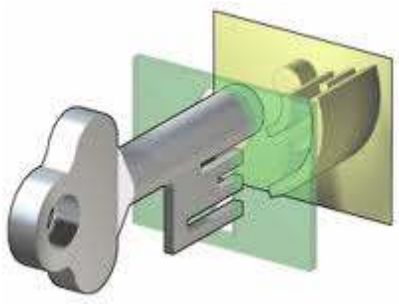
Figura 20. **Cerradura de oblea con la llave correcta**

Fuente: http://www.bondedlockservice.com/pages/wafer-tumbler-lock%20.htm. 17/01/2011

6.1.4 Llave de guarda

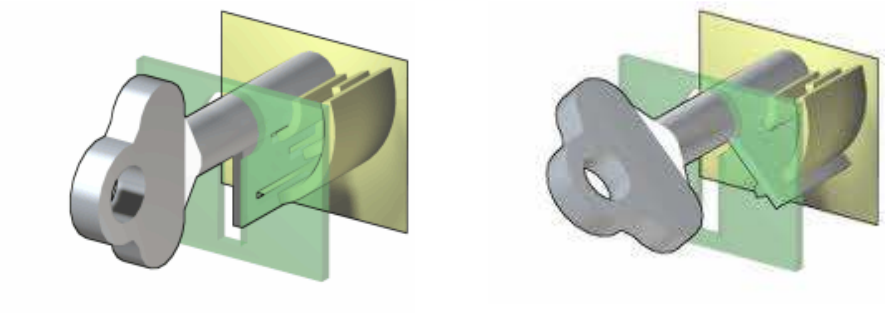
Es un tipo de cerradura que utiliza un conjunto de obstáculos, para bloquear la apertura a menos que la llave correcta se insertada. La llave correcta tiene muescas o ranuras que se corresponden a las obstrucciones en la cerradura permitiendo de esa manera que gire libremente. La llave es insertada por el ojo de la cerradura. Si la llave es la correcta se corresponderán las ranuras que tiene la llave con los obstáculos que tiene la cerradura, la llave rotará.

Figura 21. **Cerradura de llave de guarda**



Fuente: http://uk.ask.com/wiki/*Ward*ed_lock?qsrc=3044. 17/01/2011

Figura 22. **Llave de guarda correcta**

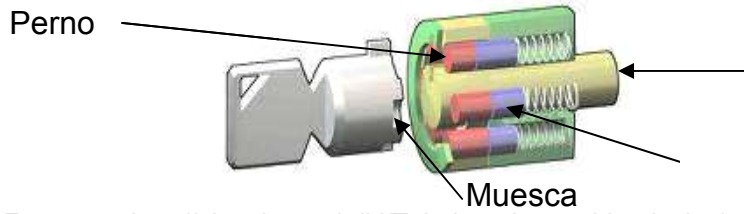


Fuente: http://uk.ask.com/wiki/*Ward*ed_lock?qsrc=3044. 17/01/2011

6.1.5 Cerradura tubular

Es una variación de las cerraduras de pernos, que consisten en que los pernos están dispuestos en una forma circular, que se corresponde a la forma cilíndrica de la llave. Cuando la llave no ha sido insertada los pernos y los contrapernos son empujados hacia la parte delantera de la cerradura, evitando que el tambor gire. La llave tubular tiene varias muescas en el cilindro para alinearse con los pasadores.

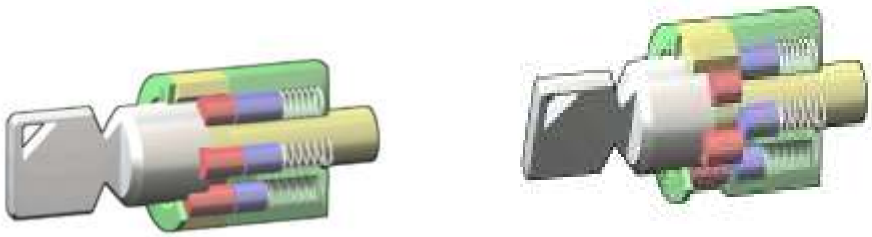
Figura 23. **Cerradura tubular**



Fuente: http://uk.ask.com/wiki/Tubular_pin_tumbler_lock. 17/01/2011

La protuberancia en la parte superior de la llave encaja en el hueco rectangular en la cerradura, haciendo que las muescas se alineen correctamente con los pasadores *y* permitan la rotación.

Figura 24. **Llave correcta cerradura tubular**

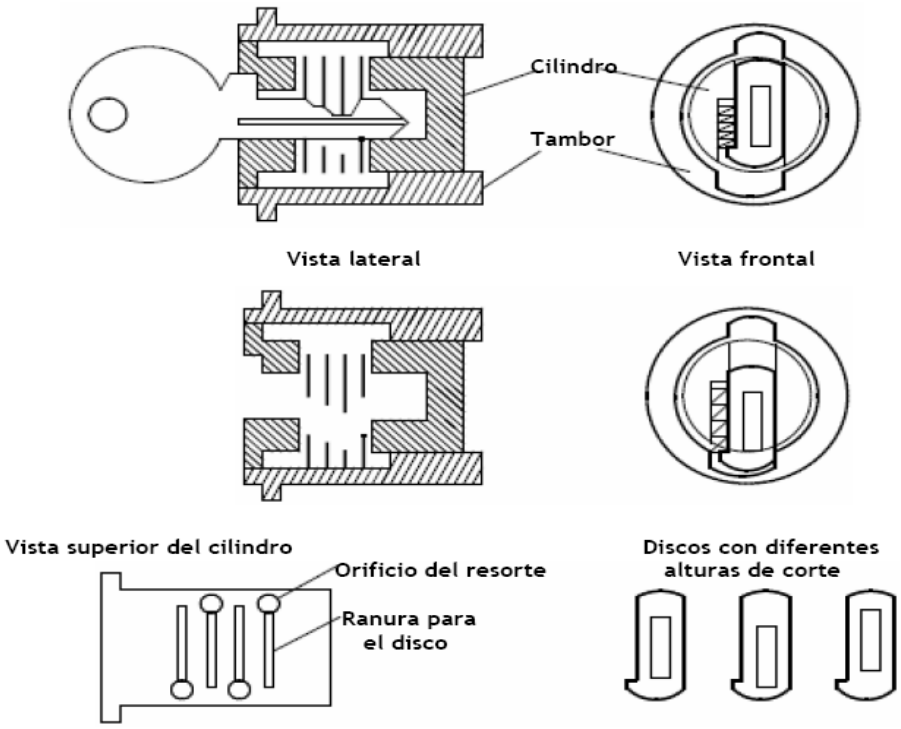


Fuente: http://uk.ask.com/wiki/Tubular_pin_tumbler_lock. 17/01/2011

6.1.6 Cerradura de cilindros de discos

Estas son cerraduras económicas que emplean discos de metal en vez de pernos. Los discos tienen la misma forma por fuera pero distinta altura del corte rectangular interior.

Figura 25. **Cerradura de cilindro de discos**



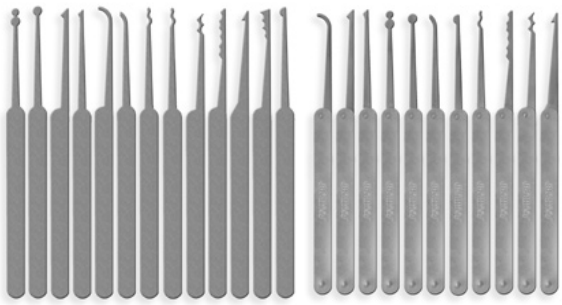
Fuente: MIT Guía del *Lock picking*. p. 41.

6.1.7 Herramientas para abrir cerraduras

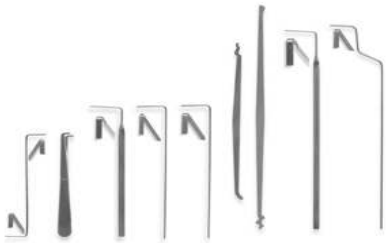
Para abrir una cerradura es necesario colocar los pernos y contrapernos en su línea de corte tal y como lo haría la llave correcta. Las herramientas ideales para esta tarea son las ganzúas, hay de dos tipos ganzúas manuales (Ver. figura 26) y ganzúas eléctricas. (ver Figura 27).

Figura 26. **Ganzúas manuales**

Ganzúas



Pinzas de tensión



Snap Gun

Fuente: http://www.ganzuas-picks.es/products_new.php?page=3. 17/01/2011

Figura 27. **Ganzúas eléctricas**

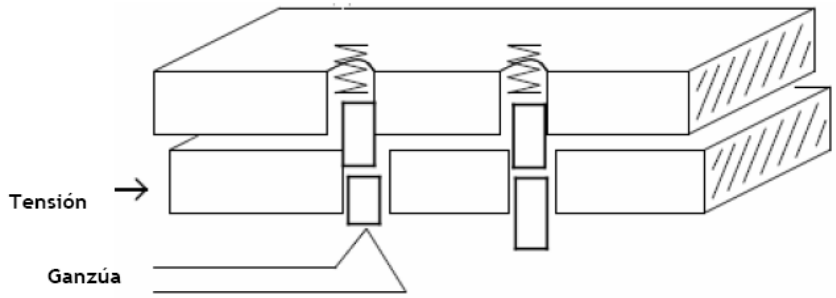
Fuente: http://www.elespia.es/ganzuas-22/ganzuas-electricas-60/. 17/01/2011

6.1.8 Utilizando las ganzúas manuales

El defecto básico que hace posible el ganzuado es ir levantando los pernos uno a uno, sin necesidad de una llave que los levante todos a la vez. (ver figura 28). El primer paso del procedimiento es aplicar tensión a la cerradura presionando en la placa inferior. Esta fuerza hace que uno o más contrapernos queden trabados entre las placas superior e inferior. (ver figura 29).

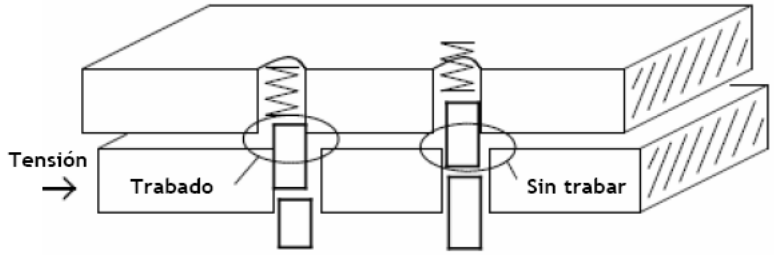
El defecto más común es que sólo se trabe uno a la vez. Un perno puede ser empujado hacia arriba con una ganzúa incluso si está trabado. Cuando la parte superior del perno llegue a la línea de corte, la placa inferior se deslizará ligeramente. Si se retira la ganzúa, el contraperno quedará sujeto por la placa inferior, atrapado sobre esta *y* el perno caerá hasta su posición inicial. Y el ligero movimiento de la placa inferior provocará que otro contraperno se trabe. (ver figura 30).

Figura 28. **Ganzuando perno a perno**



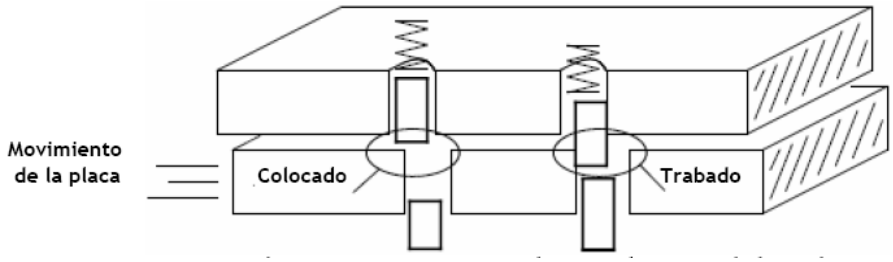
Fuente: MIT Guía del *Lock picking*. p. 5.

Figura 29. **Aplicando tensión**



Fuente: MIT Guía del *Lock picking*- p. 5.

Figura 30. **Perno colocado y perno trabado**



Fuente: MIT Guía del *Lock picking*. p. 5.

Se puede usar el mismo procedimiento para colocar este nuevo contraperno. Por tanto el procedimiento para ganzuar una cerradura perno a perno es aplicar tensión, encontrar el contraperno que más roza y levantarlo.

Cuando la parte superior del perno alcance la línea de corte, la parte móvil de la cerradura girará ligeramente *y* el contraperno quedará atrapado por encima de la línea de corte. A esto se le llama colocar un contraperno.

Pasos necesarios:

- Aplicar tensión
- Encontrar el contraperno trabado que más roce
- Empujar ese perno hacia arriba hasta sentir que se ha colocado en la línea de corte
- Volver al paso 2

6.1.9 Rastrillado básico

- Inserte la ganzúa y la herramienta de tensión. Sin aplicar tensión tire de la ganzúa hacia fuera para sentir los resortes de la cerradura.
- Aplique una ligera tensión. Inserte la ganzúa sin tocar los pernos. Al tirar hacia afuera la ganzúa haga presión a los pernos. La presión debe ser ligeramente superior que la mínima requerida para vencer la tensión de los resortes.
- Aumente gradualmente la tensión con cada rastrillada de la ganzúa hasta que los pernos se coloquen.
- Manteniendo la tensión prefijada, rastrille adelante y atrás sobre los pernos que no se han colocado. Si los pernos restantes no se colocan, afloje la tensión y reinicie el proceso comenzando con la tensión adecuada del último paso.
- Una vez que la mayoría de los pernos estén colocados, incremente la tensión y rastrille con algo más de presión; esto hará que se coloquen los pernos que no lo han hecho debido al biselado, rebabas, etc.

6.1.10 Utilizando ganzúas eléctricas

Las ganzúas eléctricas funcionan según el principio de percusión, básicamente consiste en golpes fuertes sobre los pernos de un cilindro. Por estos golpes, los pernos internos del rotor (también llamados guardas) golpean los pernos externos del cuerpo del cilindro. Así se crea el "efecto de billar" que mueve los pernos externos. Si la ganzúa eléctrica golpea los pernos en el ángulo correcto, los pernos internos y externos se separan y durante menos de un segundo se crea una abertura entre los dos.

Si esta abertura está a la altura del borde del rotor, el rotor gira (para ello, tiene que estar puesto bajo tensión con una herramienta de tensión). Entonces ahí se puede usar un pequeño destornillador para girar el rotor. Al mismo tiempo que se realiza este proceso, la leva que controla el mecanismo de cierre de la cerradura hace su actuación. El rotor puede ser girado solamente una vuelta entera antes de que los pernos cargados al resorte vuelvan a juntarse bloqueando el rotor de nuevo.

Para evitar que el cilindro tenga que ser manipulado después de cada vuelta entera, existe la herramienta "*Flipper*" (girador de rotores). Los "*Flipper*" tienen un resorte integrado y aceleran el rotor. El rotor pasa así el punto crítico tan rápidamente que los pernos pueden juntarse y el rotor mismo no puede bloquearse. Para poder usar las ganzúas eléctricas efectivamente se requiere algo de práctica. El secreto del éxito es el uso sensible de la ganzúa y la aplicación de tensión apropiada simultáneamente.

Como esta técnica de manipulación no es muy nueva, los productores de cilindros de alta calidad tomaron medidas preventivas. Por un lado, las ranuras son más angostas y paracéntricas, previniendo así que la ganzúa eléctrica

pueda tocar o golpear los pernos directamente. En caso de que la ranura sea angosta, la ganzúa eléctrica muchas veces puede hasta bloquearse. Por otro lado, la integración de pernos anti ganzúa (distintos canales mecanizados en el pitón) complica la manipulación o la hace imposible.

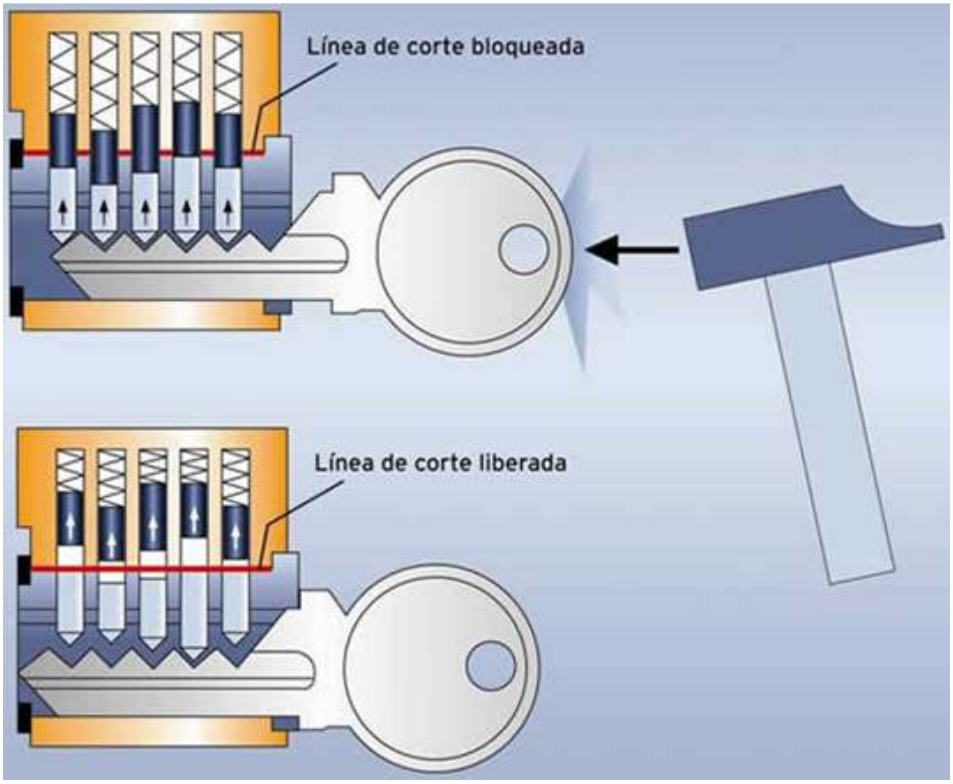
En este caso, cuchillas de formas especiales pueden lograr el éxito. Estas cuchillas se deberían pedir junto a la ganzúa eléctrica.

6.1.11 Llaves de percusión

La llave de percusión se inserta en la ranura del cilindro como una llave común. La diferencia es que no se inserta por completo, sino solamente hasta el último perno. De esta manera los cortes de la llave de percusión quedan posicionados directamente adelante de los pernos. Golpeando la llave con un objeto adecuado, como por ejemplo: un *Tomahawk*, la llave se inserta en la ranura completamente y las paredes de los cortes golpean contra los pernos (ver figura 31).

Mediante estos golpes los pernos se mueven rápidamente en sus canales y se produce el efecto de percusión: los pernos golpean los contrapernos y se crea una abertura entre los dos. Aplicando una tensión suave con la llave en ese mismo momento, el rotor puede girarse y el cilindro se deja abrir.

Figura 31. **Llave de percusión**



Fuente: http://syswoody.com/curiosidades/llaves-bumping. 17/01/2011

Es importante encontrar y practicar la fuerza óptima del golpe, así como el momento exacto en que se aplica la tensión (básicamente al mismo tiempo en que se golpea la llave), respecto al *Tomahawk.* El nombre o la forma puede variar entre fabricantes.(ver figura 32).

Figura 32. ***Tomahawk* para martillar llaves de percusión**

Fuente: http://www.multipickservice.com/htdocs/es/werkzeug/361bump_keys_intro.php. 17/01/2011

Normalmente se necesitan varios golpes hasta que el rotor deja girarse (después de cada golpe la llave de percusión se debe retirar un poco de la ranura nuevamente). Para aclarar la técnica de nuevo: los golpes deben ser rápidos, cortos y no demasiado suaves ni fuertes. La tensión, a su vez, debe ser un movimiento suave en la dirección deseada. La técnica de llaves no causa ningún daño y tampoco es muy ruidosa. Con suficiente práctica y experiencia, la probabilidad de una apertura exitosa es muy alta.

6.2 Técnicas avanzadas

Cualquiera puede aprender el ganzuado básico. Sin embargo las técnicas avanzadas es un arte que requiere de sensibilidad mecánica, destreza física, concentración visual y mente analítica. Si se esfuerza en mejorar el ganzuado, progresará por estos caminos.

6.2.1 Habilidades mecánicas

Aprender a deslizar la ganzúa sobre los pernos es sorprendentemente difícil. La traba radica en que las habilidades aprendidas con anterioridad implican mantener una posición prefijada de sus manos, independientemente de la magnitud de fuerza requerida. En el ganzuado, debe aprender a aplicar una fuerza predeterminada sin importar la posición de sus manos. Al tirar de la ganzúa hacia fuera de la cerradura, tiene que aplicar una determinada presión sobre los pernos.

La ganzúa debe traquetear arriba y abajo a lo largo del recorrido de la llave de acuerdo a la resistencia presentada por cada perno. Al ganzuar una cerradura observe la reacción a sus maniobras. Para sentir la reacción debe tratar de ser sensible al sonido y al tacto de la ganzúa pasando sobre los

pernos. Esta destreza mecánica solo puede ser aprendida con la práctica. Solo la práctica lo ayudará a interpretar la valiosa información proveniente de sus dedos.

6.2.2 Análisis espacial

Para progresar en el ganzuado, debe aprender a visualizarlo mentalmente. La idea es que emplee la información de sus sentidos para elaborar una imagen sobre lo que está ocurriendo dentro de la cerradura en el momento de ganzuarla. Básicamente tiene que proyectar sus sentidos dentro de la cerradura para recibir una imagen completa de cómo está respondiendo a sus manipulaciones. Una vez que haya aprendido a construir esta imagen, será fácil elegir las maniobras que abrirán la cerradura.

Todos sus sentidos le proporcionan información sobre la cerradura. El tacto y el oído dan la mayor parte, pero los otros sentidos pueden revelar información adicional. Por ejemplo, su olfato podrá decirle cuándo una cerradura ha sido lubricada recientemente. Como novato necesitará usar la vista, para coordinarla con el tacto, pero una vez avance en el ganzuado se dará cuenta que es innecesario mirar la cerradura. Por lo tanto es mejor no mirar *y* construir una imagen mental basada en la información que recibe de sus dedos y oídos.

La meta de esta habilidad mental es la de adquirir una concentración adecuada. No fuerce la concentración, trate de evitar las sensaciones y pensamientos que no estén relacionados con la cerradura. Trate de concentrarse solo en la cerradura.

6.2.3 Pensamiento analítico

Cada cerradura tiene sus propias características especiales que hacen fácil o difícil su ganzuado. Si aprende a reconocer y explotar las peculiaridades de cada una, el ganzuado será mucho más fácil. Básicamente necesita analizar y diagnosticar dichas características y, usando su experiencia, decidir un método u otro para la apertura. Muchas personas menosprecian las habilidades analíticas en el ganzuado.

Piensan que las ganzúas son las que abren las cerraduras *y* que la llave de tensión es solo una herramienta pasiva que somete a la cerradura a una tensión determinada. Permítanme otra forma de ver la situación. Con la ganzúa moviéndose sobre los pernos para obtener información acerca de la cerradura *y* basándonos en el análisis de esa información, la tensión es ajustada para hacer que los pernos se coloquen en la línea de corte.

¡Es el tensor el que abre la cerradura! variar la tensión a la vez que se mueve la ganzúa es un truco que puede ser usado para algunos problemas de ganzuado. Por ejemplo, si los pernos de la mitad se colocan pero no los del final, puede incrementar la tensión a la vez que la ganzúa pasa sobre los pernos de la mitad. Esto reduce la posibilidad de alterar los pernos colocados. Si algún perno parece no levantarse lo suficiente al paso de la ganzúa sobre él, trate de disminuir la tensión en la siguiente pasada.

La destreza de ir ajustando la tensión a la vez que la ganzúa se mueve requiere de una cuidadosa coordinación entre sus manos, pero una vez que mejore en la visualización del proceso de ganzuado, empezará a mejorar esta destreza.

6.3 Atacando otros mecanismos

6.3.1 Candados

Un candado es un dispositivo de seguridad que se utiliza como cerradura portátil. También son usados para cerrar puertas con cadenas. Aunque los candados están basados en tambor de pines no cuentan con toda la seguridad como las cerraduras, lo que los hace fáciles de atacar con ganzúa, aunque no es necesario por las deficiencias adicionales que el mecanismo en si tiene y es que expone una parte vital del mecanismo que es el arco, el cual puede ser cortado (ver figura 33).

Sin embargo, esto tampoco es necesario. Internamente, sin importar si él candado está basado en pines o en una cerradura de combinación, la relación entre el grillete y el mecanismo de bloqueo es muy simple. Solo se necesita de herramientas especiales llamadas cuñas. Las cuñas son pequeñas piezas finas de metal que se puede insertar entre el grillete y el casco para desconectar el mecanismo de bloqueo (ver Figura 34).

Figura 33. **Cizalla para cortar metal**

Fuente: http://www.construmatica.com/construpedia/Cizalla. 17/01/2011

.

Figura 34. **Cuñas (*Shims*)**

Fuente: http://www.lockpicks.com/padlock-shims-sps-20.aspx. 17/01/2011

Las cuñas también pueden ser fabricadas con latas de bebidas, ya que el grosor de la lámina es el indicado.

6.3.2 Cerraduras tubulares

Figura 35. **Cerraduras tubulares**

Fuente: http://www.spyemporium.com/locksmith_tubular_lock_picks.html. 17/01/2011

Para abrir este tipo de cerraduras es necesario contar con ganzúas circulares, las cuales se pueden configurar según el número de pines que tenga la cerradura. Así como la profundidad de la ranura.

Figura 36. **Ganzúa circular**

Fuente: http://www.spyemporium.com/locksmith_tubular_lock_picks.html. 17/01/2011

7. RECOPILACIÓN DE INFORMACIÓN

7.1. Buscando en la basura

Generalmente conocido como buceo en la basura, consiste en buscar dentro de los contenedores de basura información valiosa y sensible de la empresa o empleados, que posteriormente puede ser utilizada, para realizar una prueba de penetración. Por lo general los basureros carecen de guardias o cámaras de vigilancia *y* es muy raro que una empresa, emplee algún recurso para protegerla.

Que puede ser útil y que no dependerá del perfil del objetivo, generalmente el valor de la información recopilada no tiene valor hasta que se usa, por lo que mientras más información se tenga mucho mejor, sin embargo hay que utilizar criterios y sentido común para saber que puede llegar a ser útil y que no. Por lo general la información valiosa puede ser:

- Listados telefónicos
- Organigramas
- Memorandos internos
- Manuales de políticas de la compañía
- Agendas en papel de ejecutivos con eventos y vacaciones
- Manuales de sistemas
- Impresiones de datos sensibles y confidenciales
- "*Login*", "*Logon*" y a veces contraseñas
- Listados de programas (código fuente)
- Cintas

- Papel membretado y formatos varios
- *Hardware* obsoleto
- Impresión de correos electrónicos
- Recibos, facturas, notas de crédito, etc.
- Firmas
- Sellos deteriorados

7.1.1 Aspectos legales

Generalmente los contenedores de basura se encuentran dentro de las instalaciones por lo que se debe ser cuidadoso, de ser descubierto puede ser acusado de violación de propiedad. Por lo que se recomienda tomar en serio esta actividad tal y como lo haría dentro de las instalaciones, entrar y salir lo más pronto posible, no clasificar la información dentro del contenedor, es mejor tomar lo que se puede y posteriormente, analizar si es útil o no, en un entorno seguro.

7.2. Técnicas de observación directa

La observación directa es el acto de observar a alguien, para obtener información, es eficaz en lugares muy concurridos, ya que es relativamente sencillo y no se levanta sospecha. Puede ser llevada a cabo a distancia con el uso de binoculares o cerca del objetivo, la información puede llegar a ser variada pero por lo general se buscan contraseñas, códigos, información personal al momento de llenar formularios, etc.

Las técnicas dependerán del tipo de acercamiento que se desee, por ejemplo el acercarse a alguien que está ingresando su clave en un cajero puede ser diferente al acercamiento que se haría a alguien que se encuentre

llenando un cheque en una cola. Por lo general se pueden utilizar lentes obscuros, gorras, periódicos o cualquier otro elemento distractor que bloquee el contacto visual o incluso se puede utilizar ingeniería social, para acercarse simulando tener una duda en el llenado de un documento o para pedir prestada una pluma.

7.3. Recopilación fotográfica

Antes de iniciar una prueba de penetración física es necesario estar familiarizado con las instalaciones, por lo que la utilización de fotografías es muy útil, ya que permite al equipo de penetración conocer el entorno donde estarán trabajando. La recopilación fotográfica deberá incluir lo siguiente:

- Fotos de las instalaciones en todos los ángulos posibles
- Fotos de puntos de ingreso y egreso
- Fotos de puntos de acceso
- Fotos de gafetes
- Fotos de los contenedores de basura
- Fotos del personal de seguridad
- Fotos de los mecanismos físicos de seguridad
- Fotos de la ubicación de las cámaras de vigilancia
- Fotos de las cerraduras o candados utilizados

7.4. Buscando información en fuentes públicas e *internet*

7.4.1 Medios sociales

Los medios sociales son medios de comunicación para la interacción social, utilizando técnicas de edición accesibles y escalables. Los medios de

comunicación social utilizan tecnologías basadas en *internet* para transformar los medios de comunicación y difusión monólogos en diálogos medios de comunicación social. Apoyan la democratización del conocimiento y la información y transforman a las personas de consumidores de contenido a productores de contenidos. Por lo general se puede:

- Publicar
- Compartir
- Discutir
- Redes sociales
- *Microblogs*
- *LiveStream*
- Mundos virtuales
- Juegos sociales
- Juegos en línea

Los medios sociales, junto con ingeniería social, son el mejor medio para obtener información (ver Figura 37).

Figura 37. **Medios sociales**

Fuente: http://mktactivo.files.wordpress.com/2010/09/social.jpg. 17/01/2011

.

7.4.2 Sitio de *web* de la empresa

No está de más revisar la pagina *web* de la empresa donde se hará la prueba de penetración, ya que incluso allí se revela información como directorios, contactos, números de empleados, direcciones de otras sucursales, fotografías, etc.

7.4.3 Buscadores

Por lo fácil y rápido y la capacidad de filtrado entre las búsquedas Google es el mejor para esta tarea, el éxito en la utilización queda en la habilidad que tenga la persona en buscar la información.

7.5. Usando imágenes satelitales

Aunque hay varios programas que permiten ver imágenes satelitales, entre ellos *Marble*, *World Wind*, *Live Search Maps*, el mejor es Google *Earth*, ya que permite volar a cualquier lugar para ver imágenes de satélite, mapas, imágenes del relieve, edificios 3D, galaxias lejanas o las profundidades del océano.

- Explora el detallado contenido geográfico
- Permite buscar la ubicación de las empresas
- Permite observa los edificios en 3D
- Visualiza los seguimientos GPS

La información obtenida le permitirá al equipo conocer de antemano la distribución física de la empresa, podrán identificar posibles puntos de entrada, podrán marcar aquellos que sean peligrosos, etc.

7.6. Vigilancia electrónica

El monitoreo electrónico encubierto es uno de los mayores peligros para las organizaciones por el riesgo de espionaje. Es por esta razón que los equipos de penetración física, buscan colocar dispositivos de escucha en zonas sensibles, para dejar en evidencia el peligro potencial que pudiera tener una organización, si fuera real. Entre los dispositivos más comunes están los micrófonos de ambiente, cámaras espías, aparatos para intervenir líneas telefónicas, *keylogger* de *hardware*, etc. La utilización o no de estos dispositivos dependerá de lo que se haya establecido en las reglas de enfrentamiento.

8. HACKEANDO EQUIPO INALÁMBRICO

8.1. Introducción

La tecnología inalámbrica hace referencia a la posibilidad de conectar varios dispositivos entre sí o a una red sin necesidad de cables. Las ventajas de las redes inalámbricas son bajo costo, portabilidad *y* velocidad de implementación. Bajo costo porque ya que no hay que gastar en cableado, su portabilidad porque lo usuarios podrán trabajar desde cualquier lugar dentro del alcance de la red *y* la velocidad de implementación, ya que una red puede ser implementada rápidamente, lo único que se necesita es un punto de acceso conectado a la infraestructura física.

La desventaja fundamental de esta tecnología de red existe en el campo de la seguridad. Existen programas capaces de capturar paquetes, trabajando con la tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Este problema se agrava si se considera que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista, por ejemplo, desde fuera de una oficina, o desde una vivienda colindante.

8.2. Equipo necesario

Para atacar una red inalámbrica es necesario contar con el equipo de *hardware* y *software* adecuado. A continuación se enumera lo básico con lo que debiera contar un equipo de penetración.

8.2.1 Computadora portátil

Es ideal porque permite que el equipo se movilice más eficientemente, puede estar configurado con cualquier sistema operativo.

8.2.2 *Backtrack*

Backtrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Cuenta con las siguientes herramientas:

- *Aircrack-ng*, herramientas para auditoría inalámbrica
- *Kismet*, *sniffer* inalámbrico
- *Ettercap*, interceptor/*sniffer*/registrador para LAN
- *Wireshark*, analizador de protocolos
- Medusa, herramienta para ataque de fuerza bruta
- Nmap, rastreador de puertos

Las herramientas se encuentran agrupadas en 11 familias:

- Recopilación de información
- Mapeo de puertos
- Identificación de vulnerabilidades
- Análisis de aplicaciones *web*
- Análisis de redes de radio (Wi-Fi, *Bluetooth*, RFID)

- Penetración (*Exploits* y herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de acceso
- Forenses
- Ingeniería inversa
- Voz sobre IP

8.2.3 Estándares en las redes inalámbricas

- 802.11: define los modos básicos de operación y la especificación de las capas física y de acceso al medio (MAC).
- 802.11a: trabaja con tasas de 6 Mbps a 54 Mbps en condiciones ideales a una frecuencia de 5,8 GHz.
- 802.11b: trabaja con tasas hasta de 11 Mbps a una frecuencia de 2,45GHz (definida como frecuencia pública)
- 802.11g: trabaja con tasas de 6 Mbps a 54Mbps pero sobre la banda de los 2,45Ghz. ofrece mejoras en cuanto a control de interferencia sobre la señal y mecanismos de seguridad.

.

8.3. ¿Qué es criptografía?

Ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras. Los mensajes encubiertos, como los ocultos en textos infantiles o los escritos con tinta invisible, cifran todo su éxito en no levantar ninguna sospecha; una vez descubiertos, a menudo no resultan difíciles de descifrar.

Los códigos, en que las palabras y las frases se representan mediante vocablos, números o símbolos preestablecidos, por lo general resultan imposibles de leer si no se dispone del libro con el código clave. “La palabra criptografía se limita a veces a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como a diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados”.

8.3.1 WEP y WPA

Hay un número de maneras en que los puntos de acceso inalámbrico se puede asegurar (o al menos hacer más seguras). El método más común es el uso de cifrado. La codificación asegura que el tráfico sólo es legible por aquellos que tienen la llave y, en las redes inalámbricas, la clave es lo mismo que la contraseña que el usuario utiliza para acceder a la red. Las dos principales variantes de encriptación inalámbrica son WEP y WPA.

8.3.1.1 WEP

WEP, acrónimo de *Wired Equivalent Privacy* o “Privacidad Equivalente a Cableado”, es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes *Aircrack* para cifrar la información que se transmite. A pesar de que WEP se sabe que tiene defectos graves que dan lugar a que sea roto de forma rápida y sencilla, sigue siendo utilizado en los hogares y las empresas como único mecanismo de seguridad. Y aunque en 2001, se demostró por primera vez la falla, sigue siendo la primera opción que al menos se debe implementar para asegurar un acceso inalámbrico.

8.3.1.2 WPA/WPA2

WPA es la abreviatura de *Wifi Protect Access y* consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (*Transition Security Network*). WPA utiliza TKIP (*Temporal Key Integrity Protocol*) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits.

Una extensión de WPA es WPA2, que utiliza el más fuerte algoritmo de encriptación, el AES en lugar de RC4 WPA. Con WPA2, usted tiene la opción de utilizar fuertes esquemas de autenticación más allá de cifrado de clave compartida, sin embargo, cuando se usa en el modo de clave compartida, los métodos utilizados para romperlo son idénticos a la forma en que WPA.

La fuerza de WPA/WPA2 se encuentra en la fortaleza de la contraseña. Si es demasiado corto, puede ser roto rápidamente y fácilmente, pero si es de más de 20 caracteres, es probable que se necesiten años para romperlos con la tecnología actual.

8.3.2 *Wardriving*

Se le llama así a la búsqueda de redes inalámbricas desde un vehículo en movimiento, se requiere un equipo portátil equipado con Wi-Fi, un *software* para detectar puntos de accesos. Este *software* puede ser desde la herramienta

que proporciona Windows “ver Conexiones Inalámbricas Disponibles”, o con herramientas más sofisticadas como *NetStumbler* o *Kismet*. Una clara ventaja de Kismet sobre otros programas es que es capaz de detectar señales inalámbricas que no propagan su SSID.

8.3.2.1 NetStumbler

Netstumbler es un programa para Windows que permite detectar WLANs usando tarjetas *Aircrack* 802.11, 802.11b y 802.11g. Tiene varios usos, como:

- Verificar la correcta configuración de la red inalámbrica
- Analizar cobertura o señal que se tiene en diferentes puntos, de las instalaciones
- Detectar otras redes que pueden causar interferencias
- Sirve para detectar puntos de acceso no autorizados (Rogue AP’s)
- Por último, también sirve para *Wardriving*, es decir, detectar todos los Aps que están en los alrededores

8.3.2.2 Airodump

Se usa para capturar paquetes *Aircrack* 802.11 y es útil para ir acumulando vectores de inicialización Ivs con el fin de intentar usarlos con *Aircrack* y obtener la clave WEP.

8.3.2.3 AirCrack

Es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. *Aircrack-ng* puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con *Airodump*. Este programa parte del grupo

de programas de *Aircrack*-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario.

8.3.3 Rompiendo la encriptación

La principal fuente de vulnerabilidad asociada con las redes inalámbricas son los métodos de encriptación. Es por ello que las herramientas de ataque se centran en ello y para hacerlo necesitan analizar los paquetes que son transmitidos entre una tarjeta inalámbrica y un punto de acceso. Primero hay que buscar una red inalámbrica para ello es necesario utilizar las herramientas específicas para *Wardriving*. Ya que se ha encontrado una red inalámbrica puede que esta no requiera autenticación ni cifrado *y* este sería el escenario más sencillo donde el acceso a la red inalámbrica seria de inmediato.

Ahora bien si la red requiere autenticación es necesario determinar qué tipo de cifrado tiene para dirigir un ataque especifico *y* lograr mejores resultados.

8.3.3.1 Rompiendo la encriptación WEP

Para romper la encriptación WEP una de las herramientas más utilizadas es *AirSnort*. Opera realizando escaneos pasivos progresivos, la clave WEP puede ser obtenida o descifrada cuando una cierta cantidad de paquetes transmitidos han sido interceptados. *AirSnort* requiere aproximadamente 5-10 millones de paquetes cifrados, una vez que los paquetes han sido recogidos, puede encontrar la contraseña de encriptación en menos de un segundo.

Cuando se craquea WEP, los métodos estadísticos son esenciales para acelerar la recuperación de la clave. Es un ataque criptoanalítico contra fallas inherentes en el protocolo, razón por la cual se puede romper tan rápidamente.

8.3.3.2 Rompiendo la encriptación WPA/WPA2

En el caso de WPA/WPA2 para crackearlo es necesario utilizar *Airodump* que se encarga de capturar paquetes y cuando ya se han obtenido suficientes se utiliza *Aircrack*, para analizarlos y descifrarlos aunque en este tipo de cifrado sólo la fuerza bruta funciona. No importa cuántos paquetes o vectores de inicialización IV se capturen la clave cifrado no es estática. La única manera de recuperar la clave es mediante la interceptación en un proceso de autenticación y negociación conocido como *handshake*, entre un cliente y un punto de acceso.

Con esta negociación es posible lanzar un ataque de fuerza bruta (es decir, intentar todas las claves posibles) hasta encontrarla, esto es muy costoso y solo si la contraseña es muy corta y se pueden encontrar en un diccionario el ataque será exitoso, de lo contrario jamás la encontrará.

8.4 Evitando un filtrado por MAC *Address*

El filtrado MAC es un intento para proporcionar seguridad adicional en una red inalámbrica, permitiendo sólo los clientes con direcciones MAC conocidas al punto de acceso. Las direcciones MAC conocidas se almacenan en una lista blanca que se hace referencia cuando un cliente intenta conectarse. Los clientes cuyas MAC no están registradas son ignorados. Aunque parece que se tiene control este mecanismo se ve vulnerado de la siguiente manera.

- Herramientas, como *Airodump*, muestran las direcciones MAC asociadas a cualquier punto de acceso, que de inmediato le dice que MAC se encuentran en la lista blanca. No hay manera de prevenir esto.

- Un atacante puede cambiar su dirección MAC a la de un dispositivo en la lista blanca lo que de inmediato vulnera este mecanismo.

- Si ha adquirido una clave WEP o WPA/WPA2 y sigue sin poder asociarse con el punto de acceso, es probable que el filtrado MAC está en ese lugar.

8.5 Deshabilitando la propagación del SSID

La mayoría de los puntos de acceso tienen la opción de deshabilitar la difusión del SSID o nombre de la red – en teoría nunca van a aparecer en la lista de redes inalámbricas disponibles *y* solo podrá ser especificado manualmente con el fin de unirse a la red. Una gran cantidad de administradores de red creen que esto significa que los *hackers* no serán capaces de encontrar sus redes. Sin embargo las herramientas como *Kismet* y *Airodump* son capaces de detectar las señales inalámbricas, ver las redes y el tráfico de red, independientemente de si estás tienen o no radiodifusión de su SSID.

8.6 Atacando clientes *wireless*

Atacar el cliente no se trata de romper el cifrado y comprometer la red inalámbrica por medio de alguna debilidad en protocolo de autenticación. Para atacar una *laptop*, solo se necesita crear puntos de acceso virtuales y el uso de varios trucos para obligar a un cliente a asociarse en él. Una vez que esto sucede, usted puede atacar al cliente de varias formas. Bajo ciertas

circunstancias, es incluso posible trazar una ruta a través de una computadora portátil cliente y a la red destino. Cuando se ejecuta correctamente, estos ataques pueden ser devastadores incluso a la red más segura.

Hay tres enfoques que puede utilizar para atacar a un cliente inalámbrico: el pasivo, el activo y el indiscriminado. Cada uno de estos enfoques hace uso de *Backtrack* 4, específicamente las herramientas *Airbase* y Metasploit. *Airbase* es una herramienta que puede utilizarse para crear un punto de acceso inalámbrico virtual. Metasploit es un conjunto de herramientas de *hacking*. La meta es lograr que el objetivo se conecte al punto de acceso falso y cuando lo haya hecho atacarlo utilizando Metasploit.

8.7 Montando un ataque pasivo

Un ataque pasivo implica la creación de un punto de acceso falso y abierto (sin criptografía) y configurarlo para que cualquiera pueda conectarse a él, con *Airbase* fácilmente se puede crear un punto de acceso y aparte ofrece la posibilidad de:

- Implementar un ataque a un cliente “Caffe Latte WEP”
- Implementar el ataque “Hirte WEP *client attack*”
- Captura del *handshake* WPA/WP2
- Puede actuar como un punto de acceso “*ad-hoc*”
- Puede actuar como un punto de acceso normal
- Puede filtrar por SSID o dirección MAC del cliente
- Puede manipular y reenviar paquetes
- Puede encriptar los paquetes enviados y desencriptar los recibidos

Y al utilizarlo junto con Metasploit, es posible ofrecer servicios de POP3, SMTP, DNS, servidor *web*, para que al momento de que un usuario se conecte y navegue toda su información será redireccionada a la máquina que tiene el punto de acceso falso, este ataque es devastador, porque aparte que permite apoderarse de la contraseña de la red inalámbrica también da posibilidad de apoderarse de información sensible del usuario que se haya conectado.

Con *Airbase* se pueden realizar ataques en dos formas:

- Ataque Hirte: muy efectivo pero tanto la tarjeta "inyectora" como el punto de acceso víctima deben soportar fragmentación.

- Ataque Café con Leche: que su nombre debe venir de lo que se tarda en obtener la clave WEP *y* está indicado para los casos en que no se pueda o el punto de acceso no sea vulnerable frente ataques por fragmentación.

Ambas técnicas se basan en lo mismo, encontrar la manera de engañar al cliente habilitado con la WEP para hacerle pensar que está registrado en una red que ya conoce.

8.8 Montando un ataque activo

Un ataque pasivo no siempre es viable por lo que una variante *más* agresiva es necesaria. Este ataque es idéntico al anterior *y* la variación consiste en que al momento de iniciar el *Airbase*, se le haga parecer como un punto de acceso legítimo en la red destino. Por ejemplo, se determino, con *Airodump* que el punto de acceso destino se llama LithexCorp y tiene un BSSID de 00:14:6C:7C:40:80 y que está escuchando en el canal 9.

Lo que hay que hacer es cambiar la MAC *Address* del punto de acceso falso al que tiene el punto de acceso legítimo, luego se procede a cambiar el nombre del punto de acceso falso al que tiene el punto de acceso legítimo. Para hacer más convincente el ataque se pueden utilizar algunas opciones disponibles en *Airbase*, como por ejemplo: establecer las banderas de encriptación, aunque en realidad no existe tal cifrado, esto significa que el usuario podrá ver en su portátil que el punto de acceso utiliza WEP o WPA como cifrado, dando la apariencia que es un punto de acceso seguro.

Aparte de estos cambios, el ataque es idéntico al ejemplo de pasivo, sin embargo, su intención es hacer que el cliente se asocie al punto de acceso falso y no al punto de acceso genuino. Existen sistemas de detección de intrusos capaces de detectar un ataque como este pero por lo general estas soluciones son muy caras, por lo que no se utilizan muy a menudo.

.

8.9 Montando un ataque indiscriminado

Una interesante extensión del ataque anterior es la capacidad de Airbase de enmascararse, no sólo como un punto de acceso corporativo sino como cualquier punto de acceso que es detectado por los clientes inalámbricos, los cuales realizan repetidas pruebas de detección para ver si hay puntos de acceso inalámbricos disponibles. Este ataque es útil en dos escenarios.

- El objetivo está trabajando en su portátil, pero no está conectado físicamente a ninguna red. Sin embargo la portátil sigue buscando redes inalámbricas disponibles, *Airbase* responde a la detección y le dice que hay un punto de acceso disponible *y* la computadora de forma automática se conecta.

- El objetivo está trabajando en su portátil y se encuentra conectado físicamente a un punto de acceso de la red de la empresa *y* tiene habilitado la búsqueda de redes inalámbricas disponibles, como en el caso anterior *AirBase* responde a la detección y le indica que hay un punto de acceso disponible, la computadora se conecta, es claro que si se logra vulnerar con éxito a este objetivo se tendrá un acceso a la red corporativa.

  En este punto es necesario vulnerar al cliente para lograr acceder a la red corporativa, por lo que habrá que usar herramientas como Metasploit para encontrar alguna vulnerabilidad que se pueda aprovechar para tener acceso y control de esta máquina.

8.10 Como atacar dispositivos *Bluetooth*

Los ataques contra dispositivos *Bluetooth* (sobre todo teléfonos móviles) se dividen en tres categorías:

- *Bluejacking:* esto significa utilizar un teléfono para enviar mensajes anónimos a las personas que utilizan el protocolo *Bluetooth*. Esto puede ser muy útil como herramienta de publicidad y tiene su utilidad en un contexto de ingeniería social.

- *Bluesnarfing*: esto significa tomar los detalles de los teléfonos móviles sin necesidad del permiso del propietario. Esto puede incluir las entradas de calendario, la dirección anotaciones en cuenta *y* el servicio de mensajes cortos (SMS). En general, sólo los teléfonos con más capacidades son vulnerables a *Bluesnarfing*.

- Ataques espionaje: mucha gente utiliza los audífonos *Bluetooth*. A veces es posible captar y grabar este tráfico de voz. Hay herramientas como *Car Whisperer* que le permite interceptar el tráfico de voz y escucharlo directamente en el radio de su carro.

8.10.1 Bluejacking

Se refiere a una técnica que consistente en enviar mensajes no solicitados entre dispositivos *Bluetooth*, como por ejemplo teléfonos móviles, PDAs o portátiles. La tecnología *Bluetooth* tiene un alcance limitado de unos 10 metros normalmente en dispositivos pequeños (como teléfonos móviles) aunque otros aparatos más grandes (como portátiles) con transmisores más potentes pueden alcanzar los 100 metros.

Generalmente es inofensivo, pero la gente que ha sufrido un "*bluejacked*" no sabe muy bien qué ha podido ocurrir en su teléfono móvil, por este motivo la gente piensa que su teléfono móvil simplemente funciona mal. Normalmente un *bluejacker* sólo enviará un mensaje de texto, aunque en los modelos de teléfonos más recientes es posible enviar también imágenes y sonido. Con el aumento del uso de la tecnología *Bluetooth* en dispositivos móviles se ha fomentado la aparición de *bluejackers* y con ellos *software* malicioso cuyo objetivo se basa en el funcionamiento de un virus troyano.

8.10.1.1 Herramientas para hacer *Bluejacking*

La mayor parte del desarrollo de este *software* sucedió desde el año 2000 hasta 2004, donde múltiples vulnerabilidades *Bluetooth* se descubrieron. En dispositivos modernos se ha añadido un método de seguridad que trata de solicitar un código de confirmación cuando un dispositivo trata de conectarse a

nuestro aparato, pero existen maneras de saltarse esa solicitud (o directamente introducir códigos sencillos que vienen predeterminados en los aparatos) por lo que no es una manera definitiva de estar seguros.

Actualmente hay varios programas utilizados para esta práctica (como *Bluetooth Messenger*, *Blueshoot*, *Easy* Jack, etc.), aunque el más utilizado es *Mobiluck*. Ahora se está empezando a utilizar BTInfo, que hace muchas más cosas: apaga el teléfono de la víctima, explora su agenda y sus SMS *y* hasta puede llamar y enviar mensajes.

8.10.2 Bluesnarfing

Es el acceso no autorizado de información de un dispositivo inalámbrico a través de una conexión *Bluetooth*, a un teléfono móvil, portátil o PDA. Esto permite acceder al calendario, lista de contactos, correos electrónicos y mensajes de texto *y* en algunos teléfonos, los usuarios pueden copiar fotos y vídeos privados. Actualmente los programas disponibles permiten la conexión y "enlazado" a otro teléfono para copiar el contenido.

Cualquier dispositivo con conexión *Bluetooth* activado y ajustado a "detectable" (capaz de ser detectado por otros dispositivos *Bluetooth* dentro del alcance) pueden ser susceptibles a *bluesnarfing*. Al desactivar esta característica, la víctima puede estar aun más segura, aunque un dispositivo que se ajusta a "oculto" puede ser encontrado al adivinar la dirección MAC del dispositivo a través de fuerza bruta. Al igual que con todos los ataques de fuerza bruta, el principal obstáculo de este enfoque es el gran número de direcciones.

8.10.2.1 Herramientas para hacer *Bluesnarfing*

***BlueSweep*:** es un *software* gratuito proporcionado por AirMagnet Inc. *y* que ha sido diseñado para identificar y rastrear la actividad de dispositivos *Bluetooth* cercanos a la computadora en que se instale esta herramienta. El programa identifica también todos los servicios en esos dispositivos, además de marca y fabricante *y* todo ello en tiempo real.

***Bluescanner*:** es un scanner de dispositivos *Bluetooth* con la capacidad de extraer información contenida en los dispositivos como calendarios, listas de contactos, imágenes, mensajes de texto e incluso realizar llamadas.

9. RECOPILANDO EL EQUIPAMIENTO CORRECTO

9.1. Introducción

La recopilación del equipamiento adecuado dependerá de la naturaleza de la prueba de penetración que se realizará. Y puede ser desde equipo manual hasta equipo electrónico. Sin embargo algo con lo que se debe contar siempre y aunque no sea equipo es la carta de autorización de la prueba de penetración.

9.2. Carta de autorización

Esta carta deberá estar firmada y sellada por los directivos de la empresa que requirió los servicios, deberá indicar claramente que le autoriza realizar la prueba. Deberán estar los datos de contacto, la información sobre el equipo de pruebas, tales como nombres, el nombre de la compañía que está realizando la prueba *y* los objetivos declarados. Es importante que cada miembro cuente como mínimo con dos copias originales, en caso de perder alguna. Cuando una prueba de penetración no resulta como se esperaba y algún integrante se ve obligado a utilizarla, porque de lo contrario será puesto a disposición de la ley, es cuando esta carta toma un gran valor tanto como cualquier equipamiento que se tenga disponible.

9.3. Equipo de vigilancia y fotografía

9.3.1 Cámaras fotográficas

Una cámara es útil en todas las etapas de la prueba. No es necesario que sea una cámara con un gran desempeño y cara, basta con que tome buenas fotos y que tenga buena capacidad de almacenamiento. Si se cuenta con presupuesto una muy buena opción la línea PowerShot, de Canon, en la que sobresale la PowerShot G10, que es lo más reciente de la serie G, que busca ofrecer una cámara delgada y fácil de transportar.

Figura 38. **Cámara fotográfica Canon PowerShot G10**

Fuente: http://www.fayerwayer.com/2008/09/canon-powershot-g10-delgada-y-profesional/. 17/01/2011

9.3.2 Binoculares

Resultan muy útiles al momento de realizar vigilancia a distancia de objetivo, la ventaja es que son relativamente baratos y hay en diferentes tamaños que facilitan su transporte. Si se cuenta con presupuesto una muy

buena opción son los Binoculares Nikon *Action*. 10x50 CF muy resistentes, recubiertos en goma para soportar humedad, suciedad y golpes. Se trata de un producto con un gran acabado y calidad de imagen gracias a la lente asférica que elimina la distorsión.

Figura 39. **Binoculares Nikon *Action***

Fuente: http://technologyspeaks.blog.com/2010/11/25/nikon-binoculars-action-1650/. 17/01/2011

9.4. Equipo de cómputo

Sin lugar a dudas una computadora portátil será de gran apoyo durante todo el ciclo de vida de la prueba física, sin embargo es aconsejable que cumpla con las siguientes características.

Tabla II. **Características máquina portátil recomendada**

Componente	Recomendable	Observaciones
Procesador	*Core* 2Duo	Más velocidad de procesamiento
Memoria	>= 2GB	Mejor rendimiento

Continuación Tabla II.

Disco duro	>= 320G	Para almacenar • imágenes, videos • grabaciones • etc.
Batería	Vida promedio entre 4 y 5 horas	Considerar comprar baterías de repuesto.
Red	• Conexión ethernet • *Wireless*	
Software	• Windows XP Professional	O superior
Otros:	• *Firewire* • *Bluetooth*	Para conectar cámaras fotográficas video y dispositivos móviles.

Fuente: elaboración propia.

9.5. *Software*

9.5.1 *Backtrack*

Actualmente la versión 4, puede ser descargada de http://www.*Backtrack*-linux.org/. Entre las distribuciones recomendables que pueden ser descargadas, esta la versión ISO y una imagen para utilizar con VMWARE (ver Tabla III).

Tabla III. **Distribuciones *Backtrack* 4 R2 *Release***

Distribución	Nombre	Tamaño
ISO	bt4-r2.iso	2 000MB
Vmware *Image*	bt4-r2-vm.tar.bz2	2 400MB

Fuente: elaboración propia.

9.5.2 *Software* para virtualizar

Será de mucha ayuda contar con *software* que permita ejecutar aplicaciones en Linux o Windows en una misma portátil sin tener que estar reiniciándola o corriendo distribuciones de liveCD. Con el *software* de virtualización esto se simplifica y se podrá tener en una misma máquina diferentes máquinas virtuales con diferentes sistemas operativos. Entre los mejores están VMWARE *y Virtual Box*.

9.6. Equipo inalámbrico

Es recomendable contar con *Access Point*, tarjetas inalámbricas PCI *y* tarjetas adaptadoras para portátiles, adaptadores *Bluetooth*, antenas amplificadoras para *wireless* y *Bluetooth, etc*.

Figura 40. **Equipo inalámbrico necesario**

- *Access point*
- Tarjetas inalámbricas PCI
- Adaptadores para portátiles

- Antenas receptoras de *wireless*.

Continuación Figura 40

- Adaptadores *Bluetooth*
- Antenas amplificadoras de *Bluetooth*

Fuente: http://www.google.com/images. 17/01/2011

9.7. Herramientas para abrir cerraduras

Para abrir cerraduras es necesario contar con toda la variedad de ganzúas disponibles, así como contar con cilindros de entrenamiento para practicar y ganar experiencia y habilidad.

Figura 41. **Herramientas para abrir cerraduras**

Fuente: http://www.google.com/images. 17/01/2011

9.8. Sistema de posicionamiento global (GPS)

Para Guatemala hay disponibles solamente mapas generales (como el mapsource de Garmin) o los mapas detallados de Google *Earth* y Microsoft *Live*, aunque en Guatemala aún no hay mapas gratuitos disponibles. Existe MapasRed.com, un sitio *web* con medios de consulta para ubicaciones y coordenadas precisas de ubicaciones, sus mapas incluyen calles y avenidas bien detalladas. La interface no es tan sencilla o poderosa pero es útil.

9.9. Equipo forense

Hay dos etapas en el proceso forense, adquisición de datos y análisis de datos. Para la adquisición de datos, se recomienda RoadMASSter-3, este es un sistema informático forense que fue construido para contar con todas las herramientas necesarias para adquirir y analizar los datos de las tecnologías actuales de interfaz comunes, incluyendo *FireWire* 1394A / B, USB, IDE, SATA, SAS y SCSI. Con características como el soporte de múltiples medios, el apoyo a múltiples modo de captura, potente procesador para el análisis, RoadMASSter-3 es una herramienta forense versátil y potente (ver figura 42).

Para el análisis de los datos es recomendable contar con la herramienta Helix, que tiene una serie de herramientas que le permiten realizar un análisis profundo de los datos capturados, incluso si el archivos en cuestión se han suprimido y/o los discos duros han sido formateados, Helix es capaz de recuperarlos.

Figura 42. **RoadMASSter-3**

Fuente: http://www.atp-p51.com/shop/product.php?productid=16162&cat=254&bestseller=Y. 17/01/2011

9.10. Equipo de comunicación

Lo indicado son los teléfonos celulares, con la clara ventaja que no levantara sospecha su uso, a menos que claramente este prohibido su uso dentro de las instalaciones, tal y como ocurre en las instalaciones de un banco.

9.11. Equipo contra mordedura de perros

Algunas organizaciones hacen uso de perros de seguridad, para la detección de explosivos, refuerzo de la vigilancia, de guardia. Si es probable que el equipo de penetración se los tope es necesario contar con prendas protectoras para evitar ser mordidos. Por lo versátil y cómodo es recomendable contar con protección para brazos y piernas.

Aunque claramente su uso reflejaría que su intensión es pasar por este medio de control. Pero si dentro de las reglas del enfrentamiento se aprobó el pasar por este tipo de control es bueno contar con la indumentaria necesaria para evitar salir mordido. Básicamente la protección es en los brazos, en el costado y en las piernas.

Figura 43. **Vestimenta contra mordedura de perros**

Fuente http://www.bite-sleeve-schutzhund-arm.com/. 17/01/2011

9.12. Chaleco antibalas

Hay que tener presente que muchas organizaciones hacen uso de la seguridad armada, por lo que siempre existe el riesgo inherente de lesión o muerte, de cualquier integrante del equipo de penetración. Si existe el riesgo de toparse con seguridad armada lo mejor es contar con alguna prenda de protección *y* lo recomendable es un chaleco antibalas. Un chaleco antibalas es una prenda protectora que absorbe el impacto de balas disparadas al torso y esquirlas provenientes de explosiones.

Los chalecos están hechos de varias capas de fibras laminadas o de tejido sintético y protegen a la persona que lo usa de proyectiles disparados por

armas de fuego y de la metralla de algunos artefactos explosivos como granadas de mano.

Figura 44. **Chaleco antibalas**

Fuente: http://www.chalecoantibalas.net/. 17/01/2011

9.13. Otros *Gadgets*

En la actualidad y tras la llegada de la nanotecnología (rama de la ciencia dedicada a hacer dispositivos cada vez más pequeños), es posible encontrar un sin fin de aparatos como cámaras de video y micrófonos tan diminutos que se pueden esconder en cualquier sitio o vestimenta.

10. POLÍTICAS DE SEGURIDAD

10.1. Introducción

Uno de los activos más valiosos para cualquier organización es su información, por lo que la seguridad debe estar siempre enfocada a protegerla. La seguridad debe ser tratada desde un punto de vista general, contemplando, además de la propia información, aspectos tales como el *hardware*, el *software*, las redes, los datos y el personal que manipula o da soporte a esta infraestructura. La información puede encontrarse en tres estados fundamentales transmisión, almacenamiento y proceso. Y debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios que se utilicen en dichos estados.

Asimismo, la información posee las siguientes características relacionadas con la seguridad (estas son las garantías que se deben salvaguardar para cualquier información o documentación en que se empleen medios electrónicos, informáticos y telemáticos -en adelante, Medios EIT-):

- Confidencialidad: característica que previene contra la puesta a disposición, comunicación y divulgación de información a individuos, entidades o procesos no autorizados.

- Integridad: característica que asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.

- Disponibilidad: característica que asegura que los usuarios autorizados tienen acceso a la información cuando se requiera y previene contra intentos de denegar el uso autorizado a la misma.

- Autenticidad: característica por la que se garantiza la identidad del usuario que origina una información. Permite conocer con certeza quién envía o genera una información específica.

- Conservación de la información: en un sentido amplio, es el conjunto de procesos y operaciones que se conjugan para estabilizar y proteger los documentos del deterioro. A la hora de hablar de la gestión de recursos digitales, sea cual sea su forma o función, se debe tener en cuenta todas las etapas que componen el ciclo de vida de los documentos para aplicar las medidas de preservación lo antes posible. Por lo tanto, más que a una característica intrínseca de la información se hace referencia a la gestión del ciclo de vida de la información.

- Trazabilidad: característica de la información que asegura el conocimiento de aspectos clave de las operaciones de creación, modificación y consulta, tales como: ¿quién realizó la operación?, ¿cuándo se realizó la operación?, ¿qué resultados tuvo la operación?

Una política de seguridad es la documentación que establece las directrices básicas y duraderas para la protección eficaz y eficiente mediante un enfoque preventivo, detective, reactivo y dinámico que deben cumplirse antes de que una organización puede ser considerada segura. Las políticas de seguridad deben ser desarrolladas siguiendo y aplicando el principio de proporcionalidad, en cuya virtud solo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza de la organización.

10.2. Ámbito de aplicación

El documento de las políticas de seguridad debe definir claramente el ámbito de aplicación por ejemplo en una empresa, el ámbito seria doble ya que la empresa debe proteger la información de los empleados, así como deberá cumplir con las leyes que condicionan el uso de tecnologías de la información.

10.3. Estándar de definición

Se recomienda para definir las directrices de la política de seguridad la utilización del estándar ISO/IEC 27002:20051, que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco tecnológico, organizativo y procedimental de seguridad se soportará en un conjunto de normas o medidas, estándares, procedimientos y herramientas de seguridad para la protección de activos de información.

10.4. ISO/IEC 27002:2005

A continuación se exponen los diferentes dominios de seguridad que son cubiertos por la presente política y normativa de seguridad. Así como una explicación del dominio.

P.5. Política de seguridad

Este dominio proporciona las directrices generales de gestión y apoyo a la seguridad de la información en concordancia con los requerimientos del servicio al ciudadano y el marco regulatorio vigente.

P.5.1 Política de seguridad de la información

P.5.1.1 Documentar la política de seguridad de la información

P.5.1.2 Revisión de la política de seguridad de la información

P.6. Aspectos organizativos de los SI

Este dominio se refiere a la organización interna de la seguridad de la información y a la identificación de los riesgos del acceso de terceros, de clientes y de personal subcontratado.

P.6.1 Organización interna

P.6.1.1 Compromiso de la dirección con la SI

P.6.1.2 Coordinación de la seguridad de la información

P.6.1.3 Asignación de responsabilidades relativas a la SI

P.6.1.4 Proceso de autorización de recursos para el tratamiento de la información

P.6.1.5 Acuerdos de confidencialidad

P.6.1.6 Contacto con las autoridades

P.6.1.7 Contacto con grupos de especial interés

P.6.1.8 Revisión independiente de la seguridad de la información

P.6.2 Terceros

P.6.2.1 Identificación de los riesgos derivados del acceso de terceros

P.6.2.2 Tratamiento de la seguridad en la relación con los clientes

P.6.2.3 Tratamiento de la seguridad en contratos con terceros

P.7. Gestión de activos

Este dominio proporciona una protección adecuada de los activos (incluyendo mantenimiento, inventario y clasificación), identificando a los propietarios de estos activos, cuya responsabilidad es el mantenimiento de los controles adecuados sobre los mismos.

P.7.1 Responsabilidad sobre los activos

P.7.1.1 Inventario de activos

P.7.1.2 Propiedad de los activos

P.7.1.3 Uso aceptable de los activos

P.7.2 Clasificación de la información

P.7.2.1 Directrices de clasificación

P.7.2.2 Etiquetado y manipulado de la información

P.8. Seguridad ligada a los recursos humanos

Este dominio trata de asegurar que cualquier persona que tenga acceso a los activos inventariados dentro del ámbito de aplicación descrito (todos los empleados, tanto de la organización, de empresas subcontratadas, encargados del tratamiento y subcontratados de estos últimos) sepan y acepten sus responsabilidades en materia de seguridad de los sistemas de información y recursos con los cuales trabajan durante todo el ciclo de vida del empleado (antes de la contratación, durante la contratación y una vez finalizado la relación laboral).

P.8.1 Antes del empleo

P.8.1.1 Funciones y responsabilidades

P.8.1.2 Investigación de antecedentes

P.8.1.3 Términos y condiciones de contratación

P.8.2 Durante el empleo

P.8.2.1 Responsabilidades de la dirección

P.8.2.2 Concienciación, formación y capacitación en SI

P.8.2.3 Proceso disciplinario

P.8.3 Cese del empleo o cambio de puesto de trabajo

P.8.3.1 Responsabilidad del cese o cambio

P.8.3.2 Devolución de activos

P.8.3.3 Retirada de los derechos de acceso

P.9. Seguridad física y del entorno

Este dominio trata de asegurar los activos físicos descritos (tangibles) a través del control de acceso y la protección contra contingencias externas (medioambientales). Las garantías que cubre este dominio son la disponibilidad, la integridad, la disponibilidad y la confidencialidad de la información.

P.9.1 Áreas seguras

P.9.1.1 Perímetro de seguridad física

P.9.1.2 Controles físicos de entrada

P.9.1.3 Seguridad de oficinas, despachos e instalaciones

P.9.1.4 Protección contra las amenazas externas y de origen ambiental

P.9.1.5 Trabajo en áreas seguras

P.9.1.6 Áreas de acceso público y de carga y descarga

P.9.2 Seguridad de los equipos

P.9.2.1 Emplazamiento y protección de equipos

P.9.2.2 Instalaciones de suministro

P.9.2.3 Seguridad del cableado

P.9.2.4 Mantenimiento de los equipos

P.9.2.5 Seguridad de los equipos fuera de las instalaciones

P.9.2.6 Reutilización o retirada segura de equipos

P.9.2.7 Retirada de materiales propiedad de la empresa

P.10. Gestión de comunicaciones y operaciones

Este dominio trata de asegurar que la explotación de la infraestructura se realiza de forma segura y controlada, se supervisa su estado y se reportan incidencias. Para ello, define varios objetivos de control como: procedimientos y responsabilidades operacionales, gestión de servicios de terceros, planificación y aceptación de sistemas, protección contra código malicioso, copias de seguridad, gestión de la seguridad de red, gestión de dispositivos de almacenamiento, control sobre el intercambio de información entre sociedades, control de los servicios de comercio electrónico y monitorización de sistemas.

P.10.1 Responsabilidades y procedimientos de operación

P.10.1.1 Documentación de los procedimientos de operación

P.10.1.2 Gestión de cambios

P.10.1.3 Segregación de tareas

P.10.1.4 Separación de los recursos de desarrollo, prueba y operación

P.10.2 Gestión de la provisión de servicios por terceros

P.10.2.1 Provisión de servicios

P.10.2.2 Supervisión y revisión de los servicios prestados por terceros

P.10.2.3 Gestión del cambio en los servicios prestados por terceros

P.10.3 Planificación y aceptación del sistema

P.10.3.1 Gestión de capacidades

P.10.3.2 Aceptación del sistema

P.10.4 Protección contra el código malicioso y descargable

P.10.4.1 Controles contra el código malicioso

P.10.4.2 Controles contra el código descargado en el cliente

P.10.5 Copias de seguridad

P.10.5.1 Copias de seguridad de la información

P.10.6 Gestión de la seguridad de las redes

P.10.6.1 Controles de red

P.10.6.2 Seguridad de los servicios de red

P.10.7 Manipulación de los soportes

P.10.7.1 Gestión de soportes extraíbles

P.10.7.2 Retirada de soportes

P.10.7.3 Procedimientos de manipulación de la información

P.10.7.4 Seguridad de la documentación del sistema

P.10.8 Intercambio de información

P.10.8.1 Políticas y procedimientos de intercambio de información

P.10.8.2 Acuerdos de intercambio

P.10.8.3 Soportes físicos en tránsito

P.10.8.4 Mensajería electrónica

P.10.8.5 Sistemas de información empresariales

P.10.9 Servicios de comercio electrónico

P.10.9.1 Comercio electrónico

P.10.9.2 Transacciones en línea

P.10.9.3 Información públicamente disponible

P.10.10 Supervisión

P.10.10.1 Registros de auditoría

P.10.10.2 Supervisión del uso del sistema

P.10.10.3 Protección de la información de los registros

P.10.10.4 Registros de administración y operación

P.10.10.5 Registro de fallos

P.10.10.6 Sincronización del reloj

P.11. Control de acceso

Este dominio cubre uno de los aspectos más importantes y evidentes respecto a la seguridad: la problemática del control de acceso a los sistemas de información. Para ello plantea los siguientes objetivos de control: requisitos del negocio para el control de acceso, gestión de los accesos de los usuarios, responsabilidades del usuario, control de acceso de red, control de acceso del sistema operativo, control de acceso a las aplicaciones y a la información. Las garantías que cubre este dominio son autenticidad y confidencialidad. También es el control base que asegure una buena trazabilidad.

P.11.1 Requisitos de negocio para el control de acceso

P.11.1.1 Política de control de acceso

P.11.2 Gestión de acceso de usuario

P.11.2.1 Registro de usuario

P.11.2.2 Gestión de privilegios

P.11.2.3 Gestión de contraseñas de usuario

P.11.2.4 Revisión de los derechos de acceso de usuario

P.11.3 Responsabilidades de usuario

P.11.3.1 Uso de contraseñas

P.11.3.2 Equipo de usuario desatendido

P.11.3.3 Política de puesto de trabajo despejado y pantalla limpia

P.11.4 Control de acceso a la red

P.11.4.1 Política de uso de los servicios en red

P.11.4.2 Autenticación de usuario para conexiones externas

P.11.4.3 Identificación de los equipos en las redes

P.11.4.4 Protección de los puertos de diagnóstico y configuración remotos

P.11.4.5 Segregación de las redes

P.11.4.6 Control de la conexión a la red

P.11.4.7 Control de encaminamiento (*routing*) de red

P.11.5 Control de acceso al sistema operativo

P.11.5.1 Procedimientos seguros de inicio de sesión

P.11.5.2 Identificación y autenticación de usuario

P.11.5.3 Sistema de gestión de contraseñas

P.11.5.4 Uso de los recursos del sistema

P.11.5.5 Desconexión automática de sesión

P.11.5.6 Limitación del tiempo de conexión

P.11.6 Control de acceso a las aplicaciones y a la información

P.11.6.1 Restricción del acceso a la información

P.11.6.2 Aislamiento de sistemas sensibles

P.11.7 Ordenadores portátiles y teletrabajo

P.11.7.1 Ordenadores portátiles y comunicaciones móviles

P.11.7.2 Teletrabajo

P.12. Adquisición, desarrollo y mantenimiento de SI

Este dominio trata de asegurar que la seguridad es una parte que está integrada en los sistemas de información. Para ello establece varios objetivos de control: requisitos de seguridad que afectan a los sistemas de información (sean adquiridos o desarrollados), correcto procesamiento de las aplicaciones, controles criptográficos, seguridad en los sistemas de ficheros, seguridad en los procesos de desarrollo y soporte y gestión de vulnerabilidades técnicas. Este dominio trata de cubrir las garantías de disponibilidad, confidencialidad e integridad.

P.12.1 Requisitos de seguridad de los sistemas de información

P.12.1.1 Análisis y especificación de los requisitos de seguridad

P.12.2 Tratamiento correcto de las aplicaciones

P.12.2.1 Validación de los datos de entrada

P.12.2.2 Control del procesamiento interno

P.12.2.3 Integridad de los mensajes

P.12.2.4 Validación de los datos de salida

P.12.3 Controles criptográficos

P.12.3.1 Política de uso de los controles criptográficos

P.12.3.2 Gestión de claves

P.12.4 Seguridad de los archivos de sistema

P.12.4.1 Control del *software* en explotación

P.12.4.2 Protección de los datos de prueba del sistema

P.12.4.3 Control de acceso al código fuente de los programas

P.12.5 Seguridad en los procesos de desarrollo y soporte

P.12.5.1 Procedimientos de control de cambios

P.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

P.12.5.3 Restricciones a los cambios en los paquetes de *software*

P.12.5.4 Fugas de información

P.12.5.5 Externalización del desarrollo de *software*

P.12.6 Gestión de la vulnerabilidad técnica

P.12.6.1 Control de las vulnerabilidades técnicas

P.13. Gestión de incidentes en la SI

Este dominio trata de garantizar que los eventos y debilidades en la seguridad asociados a la IT y las aplicaciones soporte de la e-administración sean comunicados para, de este modo, poder realizar las acciones correctivas

oportunas y adecuadas. Este es un dominio que está enfocado principalmente a cubrir las garantías de disponibilidad, confidencialidad e integridad.

P.13.1 Notificación de eventos y puntos débiles de la SI

P.13.1.1 Notificación de los eventos de seguridad de la información

P.13.1.2 Notificación de puntos débiles de seguridad

P.13.2 Gestión de incidentes y mejoras de la SI

P.13.2.1 Responsabilidades y procedimientos

P.13.2.2 Aprendizaje de los incidentes de seguridad de la información

P.13.2.3 Recopilación de evidencias

P.14. Gestión de la continuidad del negocio

Este dominio trata de asegurar la disponibilidad de la IT que soporta las aplicaciones de la e-administración en caso de catástrofe. El objetivo es establecer un plan de acción para minimizar los efectos de una catástrofe. Las garantías que este dominio cubre son la integridad, la disponibilidad y la conservación de la información.

P.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

P.14.1.1 Inclusión de la SI en el proceso de gestión de la continuidad del negocio

P.14.1.2 Continuidad del negocio y evaluación de riesgos

P.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la SI

P.14.1.4 Marco de referencia para la planificación de la continuidad del negocio

P.14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad

P.15. Cumplimiento

Este dominio trata de evitar el incumplimiento del marco normativo y cualquier requerimiento de seguridad que éste obligue mediante el cumplimiento en los sistemas de información de las políticas y estándares de seguridad desarrollados a través del presente Manual de Seguridad. Este dominio es horizontal y cubriría las garantías definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

P.15.1 Cumplimiento de los requisitos legales

P.15.1.1 Identificación de la legislación aplicable

P.15.1.2 Derechos de propiedad intelectual (DPI)

P.15.1.3 Protección de los documentos de la organización

P.15.1.4 Protección de datos y privacidad de la información de carácter personal

P.15.1.5 Prevención del uso indebido de recursos de tratamiento de la información

P.15.1.6 Regulación de los controles criptográficos

P.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

P.15.2.1 Cumplimiento de las políticas y normas de seguridad

P.15.2.2 Comprobación del cumplimiento técnico

P.15.3 Consideraciones sobre las auditorías de los SI

P.15.3.1 Controles de auditoría de los sistemas de información

P.15.3.2 Protección de las herramientas de auditoría de los sistemas de información

10.5. Sistema de seguridad basado en ISO/IEC 27001:2005

Sistema de Gestión (SG) de la Seguridad de la Información (SI), basado en el estándar (ISO/IEC 27001:2005) con el objetivo de establecer un proceso de mejora continua de la seguridad.

10.5.1 Política de seguridad

La dirección establecerá claramente las directrices de la política en línea con los objetivos del servicio y demostrará su apoyo y su compromiso con la seguridad de la información a través de la publicación y mantenimiento de una política de seguridad de la información. Al ser un dominio de posicionamiento general respecto a la seguridad de la información, debe de cubrir todas las garantías definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad, conservación y trazabilidad.

Documento de política de la seguridad de la información

El departamento de IT, con la participación del departamento de seguridad, tiene la responsabilidad de elaborar el manual de seguridad, definiendo normativas, estándares y procedimientos, con la finalidad de definir un marco de aplicación de la seguridad en el ámbito de las aplicaciones informáticas y sobre el entorno físico.

Revisión de la política de la SI

El departamento de IT, como responsable de la elaboración del manual de seguridad, asume responsabilidad de la creación, la revisión periódica, la adecuación y el alineamiento de su contenido con los planes estratégicos de la empresa. Y debe actualizarse considerando los cambios producidos en el marco legal vigente, inclusión de resultados relevantes de auditorías o análisis de riesgos, sugerencias de mejora al Manual de Seguridad, etc.

10.5.2 Aspectos organizativos de la información

Para la consecución del primer objetivo es importante que la organización apruebe la política de seguridad de la información, asigne los roles de seguridad, coordine y revise la implementación de la seguridad en toda la administración. Para la consecución del segundo objetivo es importante controlar cualquier acceso a las tecnologías de información y el procesamiento y comunicación de la información realizado por externos.

Al ser un dominio que versa sobre el cuidado y el control respecto al mantenimiento y seguimiento de implantación de la política de seguridad incidirá en las garantías de seguridad definidas en la introducción:

confidencialidad, integridad, disponibilidad, autenticidad, conservación y trazabilidad. El titular del departamento de seguridad asume las funciones de aprobación de presente documento, que asegura la disponibilidad de los recursos dedicados a la seguridad de la información e informa del nivel de seguridad en las aplicaciones informáticas que sirven de soporte a la tramitación telemática.

10.5.3 Gestión de activos

La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado para su manejo. Este dominio tiene especial incidencia sobre la garantía de confidencialidad, aún así, es importante reseñar que la asignación de responsables por activo y el deber de éstos últimos de cumplir con las política de seguridad sobre estos activos hace que sea un dominio horizontal a las garantías de seguridad definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

Se debe mantener un inventario de los activos de información de las aplicaciones informáticas que sirven de soporte a la tramitación telemática, velando porque exista un responsable y custodio para cada uno de los mismos. Este inventario debe ser actualizado de forma regular. Con la finalidad de establecer un nivel de seguridad y tratamiento de la información adecuados, los activos de información deben ser clasificados de acuerdo a su sensibilidad y criticidad. Se deben elaborar las guías de clasificación de la información y las medidas de protección asociadas.

10.5.4 Seguridad ligada a los recursos humanos

La principal garantía que se quiere cubrir es la confidencialidad mediante el uso de cláusulas referentes a obligaciones y responsabilidades del empleado. Otro de los objetivos es reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios. La organización proporcionará la formación apropiada a los usuarios en lo que respecta al presente manual de seguridad, incluyendo requerimientos de seguridad y responsabilidades legales.

Los usuarios deben de ser conscientes de la importancia de la seguridad en los sistemas de información de la organización. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades, comprometiéndose con las mismas. Éstos deben conocer los motivos de las medidas de seguridad física y lógica establecidas y también las consecuencias de violar la seguridad.

La organización debe establecer un plan de comunicación que incluya sesiones de formación de seguridad para los empleados, que pueden realizarse como sesiones específicas o incluidas en reuniones que cubran otros aspectos relacionados. Estas sesiones podrán ser sustituidas por herramientas de formación distribuidas en soporte magnético o a través de la *intranet*.

10.5.5 Seguridad física y del entorno

Con esta finalidad, dicha infraestructura debe estar ubicada en áreas de acceso restringido, con diferentes niveles de seguridad, a las cuales únicamente pueda acceder personal debidamente autorizado. Los accesos a cada uno de los niveles deben ser registrados por mecanismos de control de acceso, quedando disponibles para posteriores auditorías. Los sistemas y la

información que soportan deben estar adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

10.5.6 Gestión de comunicaciones y operaciones

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso de la infraestructura deliberado o por negligencia. Se requieren ciertas precauciones para prevenir y detectar la introducción de *software* dañino. El *software* y los recursos de tratamiento de información son vulnerables a la introducción de *software* dañino como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas.

Los usuarios deben conocer los peligros que tiene el *software* dañino o no autorizado. Se deberán implantar controles y medidas especiales para detectar o evitar su introducción en puestos de trabajo, servidores y pasarelas de conexión a redes públicas o privadas, necesarias para evitar la infección de los sistemas de información de la organización por virus o cualquier otro tipo de *software* dañino. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en las computadoras personales.

Es de obligado cumplimiento la actualización periódica y regular de los mecanismos antivirus para todo la organización. Se establecerán procedimientos rutinarios para conseguir la estrategia aceptada de respaldo haciendo copias de respaldo, ensayando su oportuna restauración, registrando eventos o fallos y monitorizando el entorno de los equipos cuando proceda. La gestión de la seguridad de las redes que cruzan las fronteras de la administración requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

Se deben establecer los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con aquellos sistemas externos, independientemente de la plataforma, protocolos o aplicaciones que las soporten. Se establecerán los procedimientos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema frente a daño, robo y acceso no autorizado.

El almacenamiento, manipulación, transporte, la destrucción o desecho de cualquier activo de información de la organización, que contenga información sensible deberá garantizar la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado. Se controlarán los intercambios de información y *software* entre organizaciones, que deben cumplir con toda la legislación vigente. Se realizarán los intercambios sobre la base de acuerdos formales.

Se establecerán procedimientos y normas para proteger los soportes en tránsito. Se considerarán las implicaciones de la seguridad asociadas al comercio, correo e intercambio de datos electrónicos (EDI, servicios de interoperabilidad), así como los requerimientos para las medidas y controles de seguridad. Con la finalidad de asegurar la exactitud, relevancia y veracidad de los contenidos públicos de la organización, así como el cumplimiento de la legislación vigente relativa a la publicación de información en medios de difusión masiva, los procesos de publicación de contenidos deben utilizar una solución que provea una infraestructura de aprobación de los contenidos publicados.

Se debe crear la estructura organizativa multidisciplinaria necesaria para acometer la resolución de incidentes de seguridad.

10.5.7 Control de acceso

Los permisos de acceso a las redes, sistemas y a la información que esos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones. Se establecerán procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos cubrirán todas las etapas del ciclo de vida del acceso a usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se prestará especial atención si cabe al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

Todos los accesos realizados a las aplicaciones informáticas que sirven de soporte a la tramitación telemática por los usuarios registrados llevarán asociado un proceso de identificación, autenticación y autorización. Se establecerán mecanismos de registro, monitoreo de acceso y uso de los sistemas. Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso.

Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Debido a que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la efectividad de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

El acceso a los servicios desde redes externas e internas debe ser controlado de forma tal que se asegure que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios. El acceso remoto a las aplicaciones informáticas que sirven de soporte a la tramitación telemática desde redes públicas debe garantizar la confidencialidad de la información que se transmite, así como la identidad de los usuarios autorizados a hacer uso del servicio de acceso remoto mediante mecanismos de autenticación fuerte.

Se necesita restringir el acceso a las computadoras para permitir sólo usuarios autorizados. Las computadoras que atienden a múltiples usuarios deberían ser capaces de: identificar y verificar la identidad de cada usuario autorizado (y si procede, el terminal o la ubicación física del mismo). Suministrar mecanismos de gestión de contraseñas que garanticen la calidad de las mismas. Cuando proceda, restringir la conexión de usuarios o ventanas horarias.

Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se debe establecer o activar sistemas de registro de actividades que almacenen los datos generados por las actividades de sistemas, aplicaciones y usuarios en los activos.

10.5.8 Adquisición desarrollo y mantenimiento de SI

Los proyectos de desarrollo que se inicien en la administración y afecten directamente a las aplicaciones informáticas que sirven de soporte a la tramitación telemática deben llevarse a cabo considerando requisitos específicos de seguridad durante todo su ciclo de vida. El desarrollo y mantenimiento de las aplicaciones dentro del ámbito especificado debe incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas de seguridad en la programación.

Especialmente, se usarán sistemas y técnicas criptográficas cifrado, firma digital, no repudio para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada. La información residente en las aplicaciones informáticas que sirven de soporte a la tramitación telemática debe estar protegida contra modificaciones no autorizadas empleando mecanismos que aseguren la integridad de la misma.

Se debe proveer de las guías, estándares, recomendaciones y procedimientos necesarios para facilitar la inclusión de la seguridad durante las etapas del ciclo de vida de desarrollo, tales como uso de controles criptográficos, gestión de claves, programación segura, etc. Los entornos que forman parte del ciclo de vida de desarrollo informático deben estar convenientemente separados o segmentados en todos y cada uno de los sistemas.

Asimismo *y* con la finalidad de evitar el acceso o divulgación de datos que residan en los entornos, se debe controlar el intercambio de datos reales entre el entorno de producción y el resto de entornos. En los entornos de

pruebas o desarrollo, para las aplicaciones o infraestructura deben estar disponibles juegos de datos de prueba, preparados específicamente, donde las relaciones entre datos y personas hayan sido disociadas o enmascaradas.

10.5.9 Gestión de incidentes en la SI

Se establecerán procedimientos formales para informar y priorizar eventos de seguridad. Todo el personal afectado deberá conocer los procedimientos para informar de los diferentes tipos de eventos y debilidades que pudieran impactar en la seguridad de las aplicaciones informáticas que sirven de soporte a la tramitación telemática. Se establecerán responsabilidades y procedimientos formales para manejar los eventos de seguridad y debilidades con eficacia una vez que éstas hayan sido comunicadas.

Además, se establecerá un proceso formal de mejora continua sobre toda la gestión de incidentes de seguridad. Se recopilarán las evidencias necesarias por cada incidente con el fin de cumplir con la legalidad vigente.

10.5.10 Gestión de la continuidad del negocio

Este proceso se desarrollará mediante un plan de continuidad del servicio que debe ser probado de forma periódica y regular y que se debe mantener actualizado en todo momento. Para ello, se debe evaluar el riesgo y el impacto asociado ocasionado por la ausencia de continuidad de los sistemas de información que den soporte o estén implicados en la actividad de la organización.

10.5.11 Cumplimiento

Es responsabilidad de todas las áreas implicadas conocer y cumplir la legislación vigente de aplicación en sus ámbitos de actuación. El personal de la organización adquiere el deber de secreto, es decir, la responsabilidad de no divulgar ningún tipo de información que haya adquirido en la realización de su trabajo. Las aplicaciones informáticas que sirven de soporte a la tramitación telemática se deben someter periódicamente a una auditoría, encargada de verificar el cumplimiento de la normativa de seguridad y de los procedimientos e instrucciones vigentes en materia de seguridad de la información.

El proceso de auditoría debe verificar el cumplimiento de las iniciativas de seguridad planificadas a corto plazo, realizar periódicamente revisiones del grado de instauración de los controles y de su efectividad desde el punto de vista de la seguridad y ser independiente de las comprobaciones realizadas internamente por la organización. Se establecerán las medidas necesarias para evitar la desactivación, accidental o malintencionada, de los mecanismos de seguimiento y auditoría.

Se realizarán revisiones regulares en cuanto a la seguridad de la IT y de las aplicaciones de la e-administración.

10.6. Gestión de la seguridad

Para ello se realizarán revisiones periódicas, al menos una vez al año, en la que se llevará a cabo la revisión del alcance del sistema de seguridad entre otras acciones. Estas revisiones también se realizarán en respuesta a cualquier evento que pudiese afectar el alcance del sistema de seguridad, como:

- Cambios de legislación
- Cambios en la organización
- Cambios del entorno técnico
- Incidencias que puedan afectar a la gestión del sistema de seguridad

El objetivo de estas revisiones será:

  - Conocer en qué nivel afecta el evento al alcance del sistema de seguridad
  - Modificar el alcance, si procede
  - Definir e implementar un nuevo sistema de seguridad, si procede

Las reuniones podrán tener carácter físico o virtual, disponiéndose de un repositorio centralizado donde se recogerán las actas, propuestas y decisiones que afecten al sistema de seguridad.

10.7. Desarrollo normativo

10.7.1 Fichas

El desarrollo de las medidas de seguridad se realiza mediante fichas. Las medidas de seguridad se aplicarán para alcanzar la seguridad debida y proporcionada a la categoría del sistema de información a proteger, el tipo de activos que constituyen el sistema a proteger y las dimensiones de seguridad relevantes en el sistema a proteger. Por todo ello, cada ficha dispone de los siguientes campos:

- Medida: nombre de la medida

- Código: referencia unívoca

- Objetivo: relaciona la medida con un apartado de la política de seguridad

- Alcance: indica la obligatoriedad de adopción de la medida

- Clasificación baja: las fichas clasificadas como “bajo”, color verde, indican que la medida de seguridad debe ser aplicable a todos los sistemas de información

- Clasificación medio: las fichas clasificadas como “medio”, color amarillo, indican que la medida de seguridad debe de ser aplicable a sistemas de información que dispongan de una clasificación media

- Clasificación alto: las fichas clasificadas como “alto”, color rojo, indican que la medida de seguridad debe de ser aplicable a sistemas de información que dispongan de una clasificación alta

- Garantías: indica las garantías de seguridad que cubre la medida de seguridad

- Destinatarios: roles funcionales que debería tener en cuenta la medida de seguridad

- Desarrollo:
    - El texto de la medida se subdivide a su vez en:
        - Un “propósito”: que define el objetivo de la medida de seguridad
        - Una “exposición”: que desarrolla la medida de seguridad en sí

- Una “actividad”: de seguridad en el caso que la medida lo requiera. El conjunto de actividades formarán parte de los procedimientos de seguridad.

10.8. Ejemplo de Fichas Medida de Seguridad Física y del Entorno

10.8.1 Medida áreas seguras -control de acceso

Medida	Código	Objetivo	Alcance
Áreas seguras - control de acceso	M-5-1	Seguridad física y ambiental	Bajo
Garantías		**Destinatarios**	
Integridad, confidencialidad y disponibilidad		Todos los usuarios	
Desarrollo			
Propósito Prevenir los accesos físicos no autorizados y las intromisiones en las instalaciones y, por tanto, en la información de la organización. Por áreas seguras se entiende que son las áreas dedicadas para el resguardo de la IT. También abarca las zonas físicas y públicas de la administración. Debido a la diversa naturaleza de los activos implicados, el resguardo de la IT se encuentra muy disgregado (varias localizaciones, varias casuísticas) y en ocasiones algunos activos de la IT compartirán ubicación con activos de otros orígenes. Con lo cual no se pueden definir medidas específicas en el ámbito de la IT sino que se deberán adoptar muchas de carácter general.			

continuación

Exposición

Medidas generales.

Sobre áreas de resguardo de servidores:

- Se tratará, preferentemente. En el caso de tratarse de áreas compartidas con otros usos, éstas no requerirán un acceso frecuente por parte del personal.

- Las áreas permanecerán cerradas siempre que no se encuentre personal en su interior.

- Sólo tendrán autorización de acceso los responsables de aquellos activos (equipamientos) que se alojen en su interior, el responsable de su administración o mantenimiento, los servicios de vigilancia y aquellos otros a quienes éstos hubieran autorizado explícitamente.

Sobre los edificios (instalaciones) y el acceso a los mismos:

Toda instalación (incluidas las instalaciones externas a la administración), debe estar dotada con aquellos mecanismos de seguridad física que permitan:

- Impedir el acceso a personas no autorizadas a las zonas seguras donde se procese o almacene información.

- Asegurar la protección de los recursos informáticos. ver M-5-2.

continuación

Por tanto, será preciso definir un perímetro de seguridad física dentro del cual se debe ubicar a IT. El perímetro de seguridad debe comprender tanto barreras físicas de seguridad como mecanismos de control de acceso apropiados.

Sobre las barreras físicas:

- El perímetro de los edificios que contengan recursos de tratamiento de información deberá tener la solidez física suficiente que evite entradas no autorizadas, mediante muros externos y las protecciones de las puertas y ventanas.

- Estas medidas se podrán complementar con el uso de mecanismos de control, alarmas, verjas y cierres en los diversos puntos de acceso al edificio, incluidas ventanas. Estos mecanismos incrementarán la robustez del perímetro de seguridad de dichos edificios, de acuerdo a los requisitos de seguridad de la información.

Sobre los mecanismos de control de acceso:

- Se deberán controlar adecuadamente las zonas de carga y descarga de los edificios.

- Se definirán los requisitos específicos para garantizar la seguridad dentro de las oficinas administrativas, abiertas al público o no, las áreas de servidores y centros de explotación, zonas de archivo,

continuación

áreas de equipamiento eléctrico o comunicaciones *y* cualquier otra zona que en virtud del activo albergado deba ser considerada como segura. Por tanto, el control de acceso deberá ser acorde con la clasificación de los activos y la función de tratamiento que en ellas se desarrolle.

- En las zonas dotadas de control de acceso, los permisos de acceso y permanencia que se otorguen, se establecerán en función de las necesidades derivadas de la actividad profesional.

- Se deberá mantener actualizada en todo momento, una lista de las personas con permiso de acceso por zonas. Los accesos temporales a las distintas zonas, incluyendo los accesos fuera de horario habitual, deberán ser expresamente autorizados.

- Los accesos (entradas y salidas) serán registrados por el mecanismo de control de acceso que corresponda.

- Toda persona deberá portar, permanentemente y en lugar visible, mientras permanezca en las instalaciones, un identificador.

- El personal de mantenimiento y limpieza será tratado a efectos de acceso al igual que el resto de personal autorizado.

Además de los sistemas de información, los soportes de almacenamiento que residan en edificios propios o en los de los externos deberán estar protegidos contra daño físico o hurto,

continuación

utilizando mecanismos de control de acceso físico que aseguren que únicamente personal autorizado tiene acceso a los mismos.

- Queda expresamente prohibido manipular los mecanismos de control de acceso, provocando su incorrecto funcionamiento, como por ejemplo obstaculizando el correcto cierre de las puertas.

- Dependiendo del tipo de activos que contenga el área segura, se aplicarán controles de acceso específicos y acordes al riesgo que se pretenda evitar.

- El equipamiento que forma parte de los sistemas de información y comunicaciones de la administración no deberá ser sacado fuera de sus instalaciones sin la previa autorización por parte del responsable del activo.

- Cuando haya necesidad de sacar temporalmente algún elemento que forme parte de los sistemas de información y comunicaciones fuera de las instalaciones a las que dicho elemento esté adscrito, se deberá registrar su salida. Cuando el elemento retorne a su ubicación, se cerrará el registro que fue abierto a su salida.

- Así mismo, toda entrada de equipamiento que se produzca en las instalaciones de la administración deberá ser registrada con el fin de controlar dicho equipamiento.

continuación

Sobre archivos y otros contenedores de oficina: • Los archivos deberán estar cerrados con llave *y* para su ubicación se evitarán zonas de paso abiertas al público. **Actividades:** Autorización de acceso físico.

10.8.2 Medida áreas seguras – seguridad ambiental

Medida	**Código**	**Objetivo**	**Alcance**
Áreas seguras – seguridad ambiental	M-5-2	Seguridad física y ambiental	Bajo
Garantías		**Destinatarios**	
Disponibilidad e integridad		Todos los usuarios	
Desarrollo			
Propósito Prevenir los daños físicos a IT. **Exposición** Medidas generales. Sobre áreas de resguardo de servidores: • Las áreas deberán incorporar diferentes sistemas que permitan mantener la infraestructura de IT bajo condiciones de operación óptimas. Además, estas medidas deberán permitir la detección			

continuación

de eventos físicos que pudieran poner en peligro físicamente el departamento de IT:

- Sistemas de detección de humos
- Sistemas automáticos de extinción de incendios
- Sistemas automáticos que permitan controlar la temperatura y humedad de la sala
- Falso techo y falso suelo técnico
- Sistemas de alimentación ininterrumpida

Sobre armarios y otros contenedores de oficina:

- En el caso que se trate de armarios ubicados en zonas de oficina, éstos serán adecuados a la naturaleza del equipamiento albergado y atendiendo a características que permitan la protección frente amenazas externas como por ejemplo polvo, fuego y humedad.

10.8.3 Medida seguridad en equipos

Medida	Código	Objetivo	Alcance
Seguridad en equipos	M-5-3	Seguridad física y ambiental	Bajo
Garantías		**Destinatarios**	
Integridad, disponibilidad y confidencialidad		Administradores de sistemas	
Desarrollo			
Propósito Evitar la pérdida, daño, robo o compromiso de los equipos personales y			

continuación

la interrupción de las actividades de la empresa y sucursales. Esta medida se orienta a los equipos personales que pueden estar fuera de áreas seguras tal como se expresa en M-5-1.

Exposición

- Se debe ubicar o proteger los activos de IT para evitar amenazas y peligros ambientales y accesos no autorizados. Se deben ubicar en lugares en los que se minimice el acceso innecesario.
- Se deben mantener correctamente los equipos para asegurar su disponibilidad e integridad.
- Se debe aplicar seguridad a los equipos que se encuentren fuera de los locales o áreas seguras de la empresa teniendo en cuenta los diferentes riesgos que implica trabajar fuera de dichos locales. Sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera de la empresa debe ser autorizado.
- El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadoras personales, agendas, teléfonos móviles, tarjetas inteligentes u otras formas que se utilicen para trabajar desde locales ajenos a los propios de la organización.
- Los riesgos de seguridad como daño, robo o pérdida pueden variar sensiblemente entre sucursales y se debe tomar esto en cuenta para determinar los controles más apropiados.

11. CONTRAMEDIDAS

11.1. Introducción

Las organizaciones están expuestas a muchos ataques y no todas están preparadas para hacerles frente. Es por ello que las organizaciones deben evaluar su nivel de riesgo, porque solo entonces podrán tomar medidas para reducirlo. La protección de una organización y sus intereses, de todas las amenazas que van en contra de ella, se puede ver como la preparación para una batalla. Por lo que es importante conocer al enemigo y predecir sus ataques y comprender sus propias debilidades y tratar de minimizarlas.

A continuación ejemplos de contramedidas que pueden ser aplicadas a los principales riesgos que son:

- Exposición de la información
- Ataques de ingeniería social contra el personal
- Ataque telefónico
- Monitoreo electrónico
- Buceo en la basura
- *Tailgating* u observación directa

11.2. Exposición de la información

11.2.1 Información pública expuesta

Área de riesgo	
Información pública expuesta	
Tácticas del atacante	
• Identifica al objetivo • Investiga en áreas públicas • Investiga en *internet* • Investiga en medios sociales • Investiga en sitios *web* corporativos y personales • Complementa información con ingeniería social.	
Estrategia de combate	
• Reducir la exposición de la información • Concientizar a los usuarios del riesgo que tienen de publicar información sensible personal • Educar a los empleados sobre conceptos de seguridad • Mostrar a los usuarios el impacto que pudiera tener la exposición de cierta información • Entrenar a los usuarios • Realizar monitoreo buscando información sensible de los usuarios *y* de encontrar llamarles la atención	

11.3. Ataques de ingeniería social

11.3.1 Área de riesgo - *internet*

Área de riesgo	
Internet	
Tácticas del atacante	
• "*Password guessing*" • Encuestas, concursos, falsas actualizaciones de datos • Anexos con troyanos, *exploits*, *spyware*, *software* de navegación remota y *screen rendering*	
Estrategia de combate	
• Refuerzo continuo del conocimiento de los cambios a los sistemas y redes • Entrenamiento en el uso de contraseñas • Inducción en la creación de contraseñas "fuertes" • Mantenga una actitud cautelosa y revise constantemente sus tendencias de ayudar a personas que no conoce • Verifique con quien hablando especialmente si le están preguntando por contraseñas, datos de empleado u otra información sensitiva • Al teléfono, obtenga nombres e identidades (Nro. de empleado, por ejemplo). Corrobórelos y llámelos a su pretendida extensión • No se deje intimidar o adular para terminar ofreciendo información • No se intimide con alguien con aparente conocimiento	

11.3.2 Área de riesgo - teléfono

Área de riesgo	
Teléfono (PBX)	
Tácticas del atacante	
• Personificación falsa y persuasión • Personificación falsa en llamadas a *helpdesks* y CRM's • Robo de contraseñas o claves de acceso telefónico	
Estrategia de combate	
• Entrenar a los empleados en nunca dar *passwords* • Todos los empleados deben tener un PIN específico al *Helpdesk* • Controlar llamadas larga distancia • Monitorear llamadas • Rehusarse a transferencias sospechosas • Nunca dar información sensible por teléfono • Nunca revelar información confidencial • Nunca contestar encuestas telefónicas • No de números móviles de directivos • Si es posible confirme, la existencia del lugar de donde indican están llamando • Confirme un dato que no le han dado para ver la reacción	

11.4. Protección contra monitoreo electrónico

11.4.1 Área de riesgo – sitio de trabajo

Área de riesgo	
Sitio de trabajo	
Tácticas del atacante	
• Monitoreo electrónico	
Estrategia de combate	
• Inspeccionar todos los cables que llevan información rutinariamente • Utilice cables blindados, cuando quedaran expuestos • Evite dejar cables expuestos • Sospeche de regalos extraños que reciba • Sospeche de nuevos objetos que aparezcan en su escritorio • Utilice bloqueadores de celulares • Utilice barrido electrónico y telefónico • Si tiene sospecha contrate los servicios de *pentest* físico, lo más pronto posible	

11.5. Asegurando los desechos

11.5.1 Área de riesgo – contenedores de basura

Área de riesgo	
Contenedores de basura	
Tácticas del atacante	
• "*Dumpster diving*" ó "Buceo en la basura"	
Estrategia de combate	
• Educar a los empleados para que pongan atención de que están tirando y colocar la información sensible y confidencial en contenedores especiales para su trituración y destrucción • Mantenga toda la basura en áreas aseguradas y monitoreadas • Borre y destruya medios magnéticos (diskettes y cintas) • Raye los medios ópticos (CD-ROMS, DVD's) • Utilice contenedores de seguridad • Agregue cámaras de vigilancia • Evite tirar dispositivos electrónicos y si lo hace asegúrese que están borrados	

continuación

• Subcontratar empresas especializadas en el manejo de desechos sensibles *y* que suministren sus propios contenedores • Ubique los contenedores dentro de las instalaciones de la empresa • Ilumine bien el área • Patrullas nocturnas	

11.6. Protección contra *tailgating* y observación directa

11.6.1 Área de riesgo – sitio de trabajo

Área de riesgo	
Sitio de trabajo	
Tácticas del atacante	
• Acceso físico no autorizado • *Tailgating* • Observación directa • Robar, fotografiar o copiar documentos sensibles • Pasearse por los pasillos • Intentos de ganar acceso al cuarto de PBX y/o servidores	
Estrategia de combate	
• Entrenamiento en uso del carnet de acceso • Presencia de vigilantes	

continuacion

• No escriba contraseñas con alguien viendo • Restrinja uso de fotocopiadoras, escáneres, cámaras digitales • Requiera que las visitas sean escoltadas • Cierre y monitoree la oficina de correspondencia, cuartos de servidores y PBX • Marque la información confidencial y manéjela apropiadamente	

11.7. Realizar pruebas de penetración

Realizar *pentest* físicas regulares es un elemento crítico en la estrategia global de seguridad. Las pruebas dan una buena idea de en qué posición se encuentra la fortaleza de su seguridad y la cantidad de trabajo que tiene que hacer, para llegar a una posición aceptable. El propósito de las pruebas físicas consiste en determinar:

- La eficacia de los controles de seguridad perimetral
- La eficacia de los controles internos de seguridad en las instalaciones
- La vulnerabilidad del personal a la manipulación
- La susceptibilidad de una organización a la fuga de información
- La eficacia de una política de seguridad que se ha implementado
- La amenaza global de una organización se enfrenta a los ataques físicos

Cuando se ejecuta correctamente, una prueba de penetración física puede decirle mucho acerca de su vulnerabilidad. Por lo general, le dirá que áreas son vulnerables, una de las ventajas de las pruebas de penetración física es que se pueden especificar los objetivos o lo que se desea evaluar, por ejemplo:

- Identificar los puntos débiles en áreas específicas
- Poner a prueba la aplicación de los sistemas desplegados recientemente o procedimientos
- Como parte de una auditoría periódica para comprobar el cumplimiento de una política de seguridad
- Verificar de forma independiente la existencia de riesgos a los que sabe o sospecha están presentes (esto suele ser necesario a fin de justificar el presupuesto aumenta)
- Para simular un ataque de un grupo específico o categoría de amenaza

La pruebas de penetración física son relativamente recientes, (en el sector comercial por lo menos), por lo que puede ser difícil decidir a quién contratar. Esta dificultad se hace más compleja por el hecho que la naturaleza del trabajo puede ofrecer informes muy subjetivos y efímeros. Es mucho más difícil de medir la competencia y la experiencia de los equipos de penetración física. Por lo que antes de contratar asegúrese de:

- Experiencia probada: las empresas deben ser capaces de demostrar el éxito de su trayectoria en la ejecución de las tareas de esta naturaleza. Pida referencias. Si usted nota respuestas evasivas como "por razones de seguridad no le puedo decir", debe terminar la conversación inmediatamente.

- Documentos de metodología: cualquier prueba debe ser repetible. Exija que le digan cual es la metodología que emplean. En caso de no utilizar, debe terminar la conversación inmediatamente.

- El respeto en la industria: cualquiera puede hacer un sitio *web* y llamarse a sí mismos lo que quieran, pero los verdaderos profesionales destacan.

11.8. Seguridad física

La seguridad física, son los mecanismos de prevención como barreras, cercas y muros, así como sistemas de detección de intrusos, cámaras de circuito cerrado, guardias de seguridad, destinados a proteger al recurso humano, las oficinas, áreas de reuniones, parqueos, etc. así como cualquier objeto o recurso necesario para que la organización funcione y alcance sus objetivos. Para implementar la seguridad física se recomienda primero hacer una lista de control, para no pasar por alto algún elemento que necesite seguridad.

Lista de control de seguridad física

- Alrededores de la compañía
- Instalaciones
- Recepción
- Servidor
- Área de las estaciones de trabajo
- Puntos de acceso inalámbricos
- Control de acceso
- Mantenimiento de equipo de trabajo
- Escuchas telefónicas
- Accesos remotos
- Otros equipos como faxes *y* dispositivos removibles

11.8.1 Control en los alrededores de la compañía

Control:	
Alrededores de la compañía	
Implementar	
• Barreras • Paredes • Guardias • CCTV • Alambre espigado en las paredes	
Estrategias	
• Paredes de 2,40mt. de alto • Realizar rondas de seguridad • Agregar alambre de púas a las paredes • Agregar alambre electrificado • Vigilancia con cámaras • Buena iluminación	

11.8.2 Control dentro de las instalaciones

Control:	
Dentro de las instalaciones	
Implementar	
• Seguridad en terrazas • Seguridad ductos de ventilación • CCTV	

continuación

• Sistemas de detección de intrusos • Instalar botones de pánico • Instalar alarmas contra robos • Instalar balcones en las ventanas Utilizar candados
Estrategias
• Chequear acceso por medio de los ductos de ventilación • Chequear acceso desde las ventanas • Monitoreo constante del circuito cerrado • Ubicar en puntos estratégicos las cámaras

11.8.3 Control en la recepción

Control:
En recepción
Implementar
• No dejar documentos, ni medios removibles en el escritorio • Confirmar cualquier intento de localización de algún empleado • Los monitores deben estar colocados de tal forma que no se pueda ver la pantalla por las personas que visitan • Teclados, monitores y *mouse*, deben estar asegurados, para evitar que se los lleven
Estrategias
• Diseñe los escritorios de recepción de tal forma que desalienten el

continuación

intento de sobrepasarlos • Si la recepcionista se levanta que bloquee su computadora • Apagar el equipo en horarios fuera de oficina

11.8.4 Control en el servidor

Control:	
En el servidor	
Implementar	
• El servidor no debe ser usado para realizar actividades diarias • Debe estar asegurado para prevenir algún movimiento físico • Acceso únicamente por personal autorizado o de mantenimiento • El cuarto donde este alojado deberá de tener aire acondicionado	
Estrategias	
• Deshabilitar dispositivos externos • DOS debe ser removido de los servidores basados en Windows para evitar que puedan usar la consola • El arranque desde el disco debe estar deshabilitada y unidades de CD-ROM	

11.8.5 Control en puntos de acceso inalámbrico

Control:	
En puntos de acceso inalámbrico	
Implementar	
• Utilice encriptación WPA/WPA2 • No revele el SSID • Los puntos de acceso deben ser protegidos con contraseña para entrar • Las contraseñas deben ser lo suficientemente fuertes para que no pueda ser fácilmente rotas.	
Estrategias	
• Utilice contraseñas largas • Utilice *backtrack* 4, para probar la vulnerabilidad de la red inalámbrica	

11.8.6 Control de acceso

Control:	
Control de acceso	
Implementar	
• Controles de acceso biométricos • Tarjetas magnéticas • Utilización de gafetes para empleados y visitantes	
Estrategias	
• Lector de huellas	

continuación

• Reconocimiento facial • Iris *scan* • Reconocimiento de voz • Utilizar tarjetas inteligentes • Utilizar *tokens* • Utilizar RFID	

CONCLUSIONES

1. El ser humano es el elemento más débil en todo sistema por lo que es importante darle entrenamiento y capacitación.

2. Las pruebas de penetración física por sí solas no pueden proporcionar una protección adecuada en una organización, sin embargo, son un componente muy importante en un programa integral de seguridad.

3. Una prueba de penetración proporciona una orientación clara y concisa sobre cómo asegurar una infraestructura de tecnologías de información de los ataques del mundo real y el impacto que pudiera tener una vulnerabilidad.

4. Cada organización debe probar periódicamente su programa de seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de datos.

5. Cada día surgen nuevas amenazas, nuevas formas de ataque por lo que las pruebas deben ser repetidas frecuentemente y deben ser parte de un programa integral de seguridad, que incluye evaluaciones completas de seguridad en la red interna y externa, exámenes de las políticas de seguridad y el conocimiento del usuario final sobre aspectos de seguridad

6. El usuario es el objetivo primario de un ataque de ingeniería social, por lo que es sumamente importante entrenarlo en las tácticas más comunes

que los atacantes utilizan, para que al momento de ser atacado, sea capaz de reconocer el ataque y sepa contraatacar.

7. Es importante que los usuarios se informen y eduquen. No todo aquello que es recibido por *internet*, desde cualquier medio, es fidedigno y, si no fue solicitado, hay grandes posibilidades de que se trate de un *malware* o de un intento de engaño.

8. Es importante que las empresas realicen una evaluación de riesgos para que conozcan que tan preparados están para un ataque *y* puedan así tomar medidas, para llegar a un nivel aceptable.

9. Todas las empresas deben contar con un plan de seguridad *y* cumplirlo.

10. Con un adecuado seguimiento a un plan de seguridad es posible reducir el riesgo a un ataque.

RECOMENDACIONES

1. Se recomienda para definir las directrices de la política de seguridad la utilización del estándar ISO/IEC 27002:2005, que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente.

2. La dirección debe establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

3. La dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la organización.

4. La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debe ser reducida por la introducción de un servicio o producto externo.

5. Todos los activos deben ser justificados, identificados y tener un propietario asignado *y* asignarles la responsabilidad del mantenimiento de los controles adecuados.

6. Se debe clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

7. Las responsabilidades de la seguridad se deben definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.

8. Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deben seleccionar adecuadamente, especialmente para los trabajos sensibles.

9. Los servicios de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deben estar protegidas físicamente contra accesos no autorizados, daños e interferencias.

10. Deben protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

11. Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencia.

12. Se deben controlar los accesos a la información, quien la procesa y la forma en que esta se distribuye dentro de la organización.

13. Todos los requisitos de seguridad deben identificarse en la fase toma de requerimientos de un proyecto y ser justificados, aceptados y

documentados como parte del proceso completo para un sistema de información.

14. Todos los empleados, contratistas y terceros deben estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.

15. Se debe implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.

BIBLIOGRAFÍA

1. ALLSOPP, Will. *Unauthorised access – Physical penetration testing for IT Security Teams*. United States of America: John Wiley & Sons, 2009. 287 p.

2. BISCIONE Carlos A. *Ingeniería social para no creyentes*. [en línea] Disponible en Web: http://www.acis.org.co /fileadmin/ Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_ CarlosBiscione.pdf [Consulta: 24 de febrero de 2011].

3. FABI, Mark. *WYRM*. España: Ceac, 1998. 414 p.

4. JAMES, Michael Stewart. ED TITTEL, Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*. 4a ed. United States of America: John Wiley and Sons, 2008. 888 p.

5. LONG, Johnny. *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. United States of America: Syngress, 2008. 285 p.

6. MITNICK, Kevin; SIMON William. *El arte de la intrusión : como ser un hacker o evitarlos*. México: Alfaomega, 2007. 380 p.

7. MITNICK, Kevin; SIMON William. *The Art of deception: controlling the human element of security*. México: Alfaomega, 2008. 380 p.

8. ZEMÁNEK, Jakub. *Cracking sin secretos*. México: Alfaomega, 2008. 384 p

9. *Mitigating IT security risks with penetration tests the first step in total network protection* [en línea]. Disponible en Web: <http://www.intmp.com/CDs/CUNALNZDUE/files/TracGOVE/MitigateRisk_w_PenTests_TS.pdf> [Consulta: 1 de enero 2011].

10. *Ted the tool, Guide to Lock Picking* [en línea]. Disponible en Web: <http://www.capricorn.org/~akira/home/lockpick/> [Consulta: 5 de mayo 2011].