CAPÍTULO I

1. ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN Y MARCO TEÓRICO SOBRE DISEÑO, INTRUSOS, INFORMATICA, HONEYNET, VMWARE.

1.1 Generalidades.

Este capítulo presenta en su contenido los conceptos e información de la seguridad de la información así como aspectos teóricos sobre informática, intrusos informáticos, Honeypot, Honeynet, VMware.

El capitulo introduce y extiende la comprensión de los sistemas de información, la seguridad de la misma, análisis de riesgos, para luego conocer los tipos de enemigos cibernéticos y que los motiva hacer actividades de intrusión a los sistemas de la información y los tipos de ataques que ejercen.

Posteriormente se presenta la teoría de la herramienta de seguridad diseñada para ser sondeada, atacada y comprometida por un intruso e introduce como primer paso la definición de Honeypots así como sus ventajas y desventajas, luego define la Honeynet, Honeynet Virtuales y sus categorías y las herramientas de virtualización que existe para desarrollar la honeynet virtual.

Finalmente se presentas aspectos y repercusiones legales que podrían ser de importancia para la detección de los intrusos informáticos.

1.1.1 Objetivos.

General

Introducir y presentar la información teórica acerca seguridad de la información, Honeypots, honeynet, intrusos informáticos, software de virtualización, vmware, así como también facilitar la comprensión total de los conceptos que permitirán el desarrollo de Honeynets Virtuales utilizando vmware.

Específicos.

a. Introducir los conceptos de sistemas de la información, seguridad, intrusos informáticos sus ataques y motivaciones.

b. Definir y conocer los términos de honeypots, honeynet y honeynets virtuales, vmware como herramienta de virtualización.

c. Conocer los aspectos legales que amparan que el desarrollo de Honeynet virtuales sea una herramienta de utilidad para conocer origen del ataque y su finalidad.

1.2 Sistemas de información y seguridad informática.

En la actualidad, en el mundo cambiante de tecnología, la facilidad de recursos por medio de herramientas electrónicas y sistemas de computación ha influido grandemente para beneficio de las vidas de las personas. Cada día la comunicación es casi instantánea con cualquier persona sin importar la ubicación geográfica que éstas tengan, el manejo y reciprocidad de información y transferencias en línea son ejemplos de lo que la tecnología ha hecho en las vidas de las personas, instituciones y corporaciones.

El crecimiento de tecnología para fines benéficos, el robo informático y el daño a infraestructuras virtuales son actividades o prácticas diarias por entidades o personas inescrupulosas que dañan de manera electrónica.

Por tal motivo las herramientas de seguridad informática en el campo de las telecomunicaciones juegan un papel protagónico en la infraestructura con igual o mayor importancia de lo que representa la seguridad física misma, ya que se debe de proteger servicios importantes como lo son; transferencia de dinero, almacenamiento y manejo de información, entre otros.

1.2.1 Definición de sistemas de información (SI).

Un sistema de información contiene información de sus procesos y su entorno. Como actividades básicas producen la información que se necesita: entrada, procesamiento y salida. La retroalimentación consiste en entradas devueltas para ser evaluadas y perfeccionadas. Proporciona la información necesaria a la organización o empresa, donde y cuando se necesita. Tipos: Transaccionales, de apoyo a las decisiones y estratégicos. Se puede decir que este es un conjunto de elementos como lo son el hardware, software, datos, personas, y procedimientos necesarios para usar la información como recurso en una organización cualquiera que sea su rubro de acción.

Con el propósito de que se comprenda el término para el desarrollo de este tema, se hace mención de la siguiente definición.

Sistema de información: conjunto de funciones o componentes interrelacionados que forman un todo, es decir, obtiene, procesa, almacena y distribuye información (datos manipulados) para apoyar la toma de decisiones y el control en una organización. Igualmente apoya la coordinación, análisis de problemas, visualización de aspectos complejos, entre otros aspectos.[1]

1.2.2 Información.

Los datos se perciben mediante los sentidos, éstos los integran y generan la información necesaria para producir el conocimiento que es el que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia social. Algunas definiciones acerca de Información:

a. Conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno los cuales sirven eminentemente para toma de decisiones. [2]

b. Fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información por tanto, procesa y genera el conocimiento humano.[3]

1.2.3 Seguridad informática.

La seguridad informática, consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió. Así entonces la seguridad es una

1 Principles of information security. Michael Withman Pág 15

2 Información-http://www.monografias.com/trabajos14/datos/datos.shtml

3 Información-http://enciclopedia.us.es/wiki.phtml?title=Informaci%C3%B3n

característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. [4]

Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debemos de dotar de tres características que abajo se plasman.

a. Integridad.

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen.

Es un riesgo común que el atacante al no poder descifrar un paquete de información y sabiendo que es importante, simplemente lo intercepte y lo borre. [5]

b. Confidencialidad.

La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada. [6]

4 Principles of information security. Michael Withman

5 Integridad-http://www.bradanovic.cl/pcasual/ayuda3.html

6 Confidencialidad-http://www.bradanovic.cl/pcasual/ayuda3.html

c. Disponibilidad.

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por mala operación accidental o situaciones de fuerza mayor. [7]

1.2.4 Seguridad.

Se puede clasificar por dos tipos:

a. Seguridad física.

Puede asociarse a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.

b. Seguridad lógica.

Protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía.

1.2.5 Términos relacionados con la seguridad informática.[8]

a. Activo.

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

7 Disponibilidad-http://www.bradanovic.cl/pcasual/ayuda3.html

8 Principles of information security. Michael Withman

b. Amenaza.

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

c. Impacto.

Consecuencia de la materialización de una amenaza.

d. Riesgo.

Posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

e. Vulnerabilidad.

Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

f. Ataque.

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

g. Desastre o contingencia.

Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio. Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad está ligada a una amenaza y el riesgo a un impacto.

1.2.6 Análisis de riegos.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta: “lo que no está permitido debe estar prohibido” y esto es lo que debe hacer ésta seguridad lógica. Los objetivos para conseguirlo son:

a. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

b. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

c. Asegurar que se utilicen los datos, archivos y programas de forma adecuada en un procedimiento correcto.

d. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.

e. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

f. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o softwares empleados.

1.3 Marco teórico sobre intrusos, informática y honeynets.

1.3.1 Conociendo al enemigo.

En general cualquier daño malicioso es considerado como delito informático, se puede definir ligeramente como toda acción consciente y voluntaria que provoca un perjuicio a una entidad personal, natural o jurídica el cual produce un beneficio ilícito por medio de actividades informáticas o que involucren a estas.

Según estadísticas relacionadas con la problemática, la mayoría de los delitos informáticos realizados en el mundo mediante una computadora, son cometidos por empleados de la propia empresa afectada, quienes son los que mejor conocen las debilidades del sistema. El mayor inconveniente relacionado con los delitos informáticos es el vacío legal.

Es interesante la evolución de la tecnología, en un inicio el delito informático solo apuntaba al reconocimiento “del haberlo hecho” o “mi lista de los hecho” la cual el delincuente solo trataba de ser reconocido como la persona que violento un sitio sin necesidad de adquirir fraudulentamente información pero en el transcurrir los años la los delitos informáticos están enfocados al comercio electrónico o al robo de información personal o empresarial.

Por lo antes dicho es necesario el definir comercio electrónico que es una metodología moderna para hacer negocios que se apoya en la tecnología informática. Su éxito radica en que está en sintonía con la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los mismos.

El perfil.

Conocer al enemigo cibernético es un componente crítico de la seguridad computacional, identificar y entender a los actores y su motivación para realizar actividades que ponen de manifiesto sus habilidades técnicas para penetrar a las redes de computadoras, de la misma forma conocer técnicas y herramientas que se usan para descubrirlos.

Una vez que el individuo o grupo de individuos han penetrado la seguridad de Red y compromete a la computadora, ¿cuáles son los pasos que siguen?, esos pasos pueden determinar el nivel de amenaza del lado del sistema computacional o de la red en cuales están expuestos. Los individuos pueden ser motivados por curiosidad y no destruir la información y las consecuencias de este tipo de intrusión depende de la naturaleza de la organización.

Existen amenazas externas, sin embargo en las amenazas internas interviene la relación entre la compañía y el empleador. Un perfil idóneo prácticamente no existe, pero si un acercamiento. El Hacker es alguien compulsivo y obsesivo por acumular conocimientos. Es extrovertido e investiga todo lo relacionado con la electrónica y la informática. Es el tipo de personas que suelen abrir todos los aparatos de consumo de casa o lee los ficheros de su ordenador hasta modificarlos para ver qué sucede.

Un Hacker no es el típico personaje con gafas y pelo engominado o graso. Ni es un tipo delgado con la cara cubierta de granos. Tampoco es un despistado ni muestra una calavera en la parte posterior de la camisa, es alguien normal, con sus miedos y sus dudas, pero que posee una fuerte voluntad para pasarse horas delante de una computadora probando cosas.

Le encanta descubrir cómo funcionan los programas o por lo menos para que sirve cada cosa. Cuando ha adquirido bastantes conocimientos, es capaz de desproteger un programa o copiar una tarjeta electrónica.

1.3.2 Identidad de los intrusos.

No existe una traducción exacta de la palabra Hacker. Algunos utilizan “pirata informático”. Una definición cercana de un Hacker es la persona que se divierte explorando con mucho detalle la programación de los sistemas y como expandir sus capacidades y en opuesto a otros usuarios que prefieren aprender lo mínimo requerido. Los medios noticieros asociaban el comportamiento criminal con el termino Hacker cuando reportaban incidentes relacionados con el crimen computacional, sin embargo los individuos dentro de la comunidad quienes se hacen llamar Hackers fatigados de la identificación negativa redefinieron ese acto malvado como Cracker.

El término hacker procede del inglés “hack” (recortar) y es la palabra utilizada en determinados ámbitos de las nuevas tecnologías para denominar las pequeñas modificaciones que se le pueden hacer a un programa. Su derivado, “hacker”, parece provenir del prestigioso Instituto Tecnológico de Massachussets (MIT), donde los investigadores encargados de hacer “hacks” (alteraciones) de programas se convirtieron en los “hackers” de sistemas y equipos. Desde entonces, ha habido dos cosas que han contribuido a alterar el significado inicial de la palabra: la prensa y Kevin Mitnick.

Kevin David Mitnik, alias “El Cóndor”, es el hacker más famoso del planeta. A los 17 años cumplió su primera condena por entrar en las oficinas de Cosmos (Computer System for Mainframe Operations) de la compañía Pacific Bell y obtener la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales del sistema.

1.3.3 Tipos de hackers.

Hoy día existen tres tipos de “hackers” que dependen siempre de la finalidad de su trabajo: White Hat Hackers, por su significado en inglés “hackers” de sombrero blanco. Black Hat Hackers, por su significado en inglés “hackers” de sombrero negro o crackers. Blue Hackers, por su significado en inglés los “hackers” azules.

Hacker de sombrero blanco defiende la libertad de información. Según su ética, todo el software debería ser accesible al usuario. Rechazan los programas de código propietario, puesto que limitan la libertad del usuario y reducen al mínimo su conocimiento sobre sus propias herramientas. Si bien sus actividades favoritas incluyen destripar programas y encontrar agujeros de seguridad, lo hacen siempre como reto y como contribución a la seguridad de la Red.

Su filosofía establece que no pueden utilizar sus “poderes” para el mal, lo que significa que no pueden crear perjuicio a terceros. Pero “el mal” es un concepto complejo que depende casi siempre del cristal con que se mira, y muchas empresas de software propietario mantienen una guerra contra estos “hackers”, que gustan de romper los precintos de sus programas y hacerlos transparentes.

Los hackers de sombrero negro o “cracker”, por el contrario, es un hacker que irrumpe en sistemas informáticos ajenos para aprovecharse de otros, robar o, sencillamente, crear problemas. Cracker es el término creado en 1985 por la comunidad hacker precisamente para defenderse de las acusaciones indiscriminadas de los medios de comunicación.

El hacker azul, originalmente experto en seguridad que trabaja para entidades de investigación y de gobiernos que analizan estos hechos y a estos individuos poniendo sus habilidades al servicio de la Ley.

1.3.4 Motivación de los hackers.

Los motivos dentro de la Comunidad: La clave para entender a los individuos, grupos y sus acciones son los grandes percutores para las actividades maliciosas. La motivación es uno de los elementos principales para comprender que es lo que mueve a estos individuos a realizar sus actos. El buró federal de investigación de los Estados Unidos encaja 4 elementos importantes mediante las siglas en inglés MICE que viene de los acrónimos, dinero (Money), ideología (Ideology), compromiso (Compromise) y ego (Ego). Sin embargo esta definición de motivaciones se extiende a las siguientes seis:

a. Dinero.

El dinero es uno de los aspectos que los atacantes toman como una principal motivación partiendo del punto de vista que deben de explotar sus conocimientos para beneficio propio. Un ejemplo sencillo de lo mencionado es cuando se aprovechan de los recursos de llamadas internacionales telefónicas a través de Internet, ¿pero qué sucede más allá de esto? Aquellos que ofrecen servicios de robo de archivos o números de tarjetas de crédito beneficiándose por una suma de dinero, son lo que se consideran como un atacante.

b. Entretenimiento.

El entretenimiento es probablemente una de las motivaciones que tiene menores repercusiones ya que el objetivo final de estas es más que un juego que de una forma destructiva.

c. Ego.

El ego es una de las motivaciones más grandes que existen conjuntamente a la económica. Pero definitivamente esta palabra debería de estar íntimamente ligada a la reputación que tratan estos individuos de obtener por medio de actividades delincuenciales de forma digital. La satisfacción personal de sobrepasar obstáculos, aplicando técnicas aprendidas y/o utilizando herramientas artesanales en ambos casos propios, tratando de penetrar o alterar sistemas e información que están protegidos siendo unos de los blancos más usuales que estos tipos de individuos tratan de perseguir.

d. Causa.

La Causa (ideología) es una motivación usualmente está formada por diferentes factores como es el de la orientación geopolítica, las influencias culturales, religiosas, sociales, de pensamiento e históricas. La causa o la ideología dio paso a una actividad llamada “hack-tivismo” el cual encierra las anterior mencionadas como motivación para el daño o robo de información de forma electrónica, un ejemplo de esto es aquellos motivados a que toda la información debería de ser gratuita, los piratas cibernéticos irrumpen en grandes corporaciones para extraer información y publicarla a través de todo lado.

e. Aceptación a un grupo social.

La Aceptación del grupo social es una motivación que abarca la necesidad de pertenencia y reconocimiento. Cada persona necesita pertenecer a un grupo en cuyo interior se sienta aprobado y respetado. Esta calificación solo puede ser lograda en estos grupos realizando y sorteando actividades vandálicas como retos, hechos y meritos formando lo que hoy en día se conoce como la “meritocracia”.

f. Estatus.

El estatus resulta ser una de las partes más importantes como individuos, la necesidad de sobresalir o de una simple jerarquización en donde el que posee un peldaño más arriba se traduce en poder.

La comunidad de hacker y crackers están también basadas es este punto siendo esta unas de las motivaciones reales para crear algún daño, demostrando que la persona posee más conocimientos ó que posee una mayor habilidad en quebrantar sistemas. Debido a lo anterior esta motivación es una de las que tienen riesgos medios para corporaciones, pero el resultado siempre es negativo.

1.3.5 Ataques a los sistemas informáticos.

Los ataques se presentan en todas las formas, tamaños y en diferentes métodos, para penetrar y explotar los sistemas de las cuales existen dos tipos: ataques activos y pasivos.

Aunque las herramientas blackhat (Sombrero Negro) o técnicas sean conocidas y los proveedores de software hayan liberado las últimas vacunas para proteger los sistemas esto no significa que estén seguros. Si un atacante no ha tenido éxito es porque no ha podido correr los ataques, pero existen otros ataques que son más antiguos y corren con más frecuencia y que afectan a las organizaciones que no tienen sus sistemas con seguridad.

Algunos ataques son más complejos y algunos son básicos y se detallan continuación:

Ataques Activos.

Un ataque activo implica una acción deliberada de un atacante para obtener acceso a la información y los atacantes están activamente haciendo intentos para penetrar en la organización, estos ataques son bastante fáciles de detectar, sin embargo algunos ataques no son detectados porque las organizaciones desconocen que observar. Entre los ataques activos se tienen:

a. Denegación de Servicios (DoS).
b. Penetrando los sitios informáticos.

Ataques Pasivos.

Un ataque pasivo está orientado en recopilar la información en comparación con el acceso a ella directamente para luego lanzar un ataque activo. Los ataques activos son más fáciles de detectar pero la mayoría de organizaciones no lo logra por lo tanto la oportunidad de detectar los ataques pasivos es casi nulo. Existen muchas alternativas que un atacante puede escoger para acceder y utilizar los sistemas, sin embargo se han identificado algunas tendencias que con frecuencias son seguidas por los atacantes. Entre los ataques pasivos se tienen:

a. Sniffing (Olfateando).
b. Reuniendo Información.

1.3.6 Pasos frecuentes para penetrar y utilizar los sistemas.

Reconocimiento activo.

La idea que está detrás de este paso es identificar las vulnerabilidades de los sistemas. Un atacante puede que no esté interesado en entrar a un sistema

especifico pero si a muchos sistemas como le sea posible, como resultado se enfocan a eliminarlos.

Los atacantes más avanzados o con mayor experiencia pueden tomarse tiempo adicional escaneando el perfil del sistema si están interesados en entrar. Si los atacantes quieren entrar, los siguientes elementos son información clave que podrían intentar descubrir durante el reconocimiento activo.

a. Las estaciones que son accesibles.
b. La localización del enrutador y los Firewall (muralla de fuego).
c. Sistemas operativos que corren componentes claves.
d. Puertos abiertos.
e. Servicios.
f. Versiones de las aplicaciones.

Es crítico que se tenga una forma de detectar y revisar las actividades de reconocimiento activo, si no se cuenta con la herramienta para bloquear este punto, la oportunidad de detectarlos decrementa considerablemente.

Utilización del sistema.

Cuando los atacantes entran a un sistema, la mayoría de ellos piensan en ganar acceso. Sin embargo hay otras dos actividades involucradas para entrar a un sistema: aumento de privilegios y DoS. Las tres actividades son usadas dependiendo del tipo de ataque que el hacker quiere lanzar. Los atacantes pueden entrar comprometiendo la cuenta de otro usuario porque ellos no tienen derechos de super-usuario, no pueden copiar archivos, hasta este punto los atacantes tienen que correr un ataque de elevación de privilegios para incrementar el nivel de tal manera que puedan acceder los archivos apropiados.

1. Ganando acceso: Este es el más popular, existen varias alternativas que lo atacantes pueden usar para ganar el acceso al sistema, pero el nivel más fundamental es obtener ventaja de algunos aspectos de una identidad. La identidad es una computadora con sistema operativo o aplicación.

    i. Ataques a los sistemas operativos: Es usado cuando no se tiene aplicada ninguna seguridad, por ejemplo cuando WINDOWS NT y UNIX no son configurados en forma personalizada, solo tienen dos opciones de funcionalidad como Server o como estaciones de trabajo con un nivel de seguridad alto, no fueron designados a ser Firewall o Servidor Web seguro, pero que con otras opciones pueden configurarse más seguros.

    Los puertos y los servicios son puntos de acceso y en base a esto se puede asegurar que una configuración predeterminada del sistema operativo tiene al menos un numero de servicios y puertos abiertos, si se dejan porque son requeridos entonces se sabe que existe un control de los puntos que comprometen el sistema.

    ii. Ataques a la capa de aplicación: Si el software tiene todos los aspectos y características necesarios contra las vulnerabilidades de seguridad, puede experimentar otros tipos de consecuencias cuando se carga demasiados datos o información dentro del rango aceptado por el sistema y presenta un problema de desbordamiento de memoria.

    iii. Ejemplos de programas de ataques: Cuando la fuente del sistema operativo o la aplicación es instalada, los fabricantes distribuyen ejemplos de archivos para una mejor comprensión del programa y puede ser de mucha utilidad, pero una de las áreas más comunes

de este tipo son los ejemplos de scripts o guiones para el desarrollo web, por ejemplo las versiones de los servidores APACHE y algunos buscadores que vienen con muchos de ellos y que presentan vulnerabilidades.

Otro ejemplo más clara es el Microsoft Internet Information Server (Servidor de información en Internet de Microsoft) de la cual hace sus herramientas de administración remota disponibles en su página principal, los atacantes pueden usar esta herramienta para comprometer el sistema.

iv. Ataques de desconfiguración.

Este tipo de ataque ocurre cuando el sistema que está lejos de ser seguro son atacados porque no están configurados correctamente por administradores que desconocen como configurarlos y detienen servicios que son funcionales. Para fortalecer las computadoras es preciso deshabilitar los servicios que no son necesarios.

2. Aumento de privilegios: La última meta de un atacante es ganar accesos de administrador, por ejemplo muchas organizaciones guardan la cuenta de invitado con privilegios y los que hacen uso de ella pueden tener accesos mínimos al sistema. En este caso un atacante puede comprometer esta cuenta y actualizar el nivel de privilegios de la cuenta y tener accesos adicionales.

3. Denegación de Servicios (DoS): DoS es el acrónimo "Denial of Service" (Denegación de Servicio). Un ataque DoS a un servidor conectado a Internet tiene como objetivo agotar sus recursos, ya sean de ancho de banda o de procesamiento, para que sea prácticamente imposible acceder a él.

En principio, el realizar un ataque DoS está a disposición de cualquiera que disponga de mayor ancho de banda que el servidor atacado y/o haya descubierto alguna vulnerabilidad del sistema operativo que gestiona el servidor (o los routers). Está claro que la primera opción no está al alcance de cualquiera por lo que los ataques DoS suelen ser del segundo tipo.

Accesos seguros: cargando programas.

Se trata de programas que, cuando son ejecutados, causan algún tipo de daño en el sistema sobre el que se ejecutan. Este grupo de programas incluye virus, caballos de troya y gusanos, entre los daños que pueden causar están la pérdida de información, la pérdida de capacidad de procesamiento, la pérdida de espacio en memoria o incluso el permiso de acceso s su interior a un intruso.

Cubriendo pistas.

Primero el atacante busca el archivo de registros para limpiar las entradas relacionadas con el ataque, porque si un administrador del sistema entra y revisa el archivo, no sospecharía ya que no está completamente vacío. Segundo, la mayoría de sistemas colocan una entrada en un archivo de registros indicando que el archivo ha sido limpiado. Estas configuraciones activan una bandera roja que advierte al administrador del sistema. También es importante enviar copia del archivo de registro hacia otras computadoras para resguardar la información en forma replicada.

Los sistemas descritos a continuación presentan un enfoque innovador con respecto a los sistemas de seguridad tradicionales tales como cortafuegos o detectores de intrusos. En vez de repeler las acciones de los atacantes, utilizan técnicas para monitorizarlas y registrarlas, para así aprender de ellos.

1.3.7 Honeypots.

Antecedentes históricos de los honeypots.

Las primeras referencias de honeypot se agrupan en el proyecto de HoneyNet, este proyecto se inició informalmente en la lista de correo “Wargames” en abril de 1999 gracias a los correos cruzados entre varios expertos en seguridad de redes que culminaron con el desarrollo formal del proyecto antes de finalizar el año.

En junio de 2000 y por espacio de tres semanas, el Honeypot del proyecto fue atacado y comprometido por un famoso grupo de hackers, lo que permitió el estudio del comportamiento de este grupo en “real” así como demostrar la viabilidad y utilidad de esta nueva herramienta de seguridad.

Este conocido incidente catapultó el concepto de Honeypot como la última tendencia en seguridad de redes convirtiendo su libro en un best-seller de lectura obligatoria para todos los profesionales de la seguridad.

A inicios de 2001 se convirtió en una organización sin fines de lucro dedicada al estudio de los hackers (blackhats) que actualmente está compuesta por más de 30 miembros permanentes. Algunas definiciones son:

a. Los Honeypots o redes de trampa es una tecnología altamente dinámica que provee información para conocer al enemigo.

La definición formal de un honeypot se presenta a continuación.

a. Recurso de un sistema de información cuyo valor reside en el uso no autorizado o ilícito de dicho recurso. [9]

Cualquier recurso digital puede constituir un honeypot, desde un servidor o un equipo de red, hasta un archivo de una computadora. Sin embargo, la característica común de todos los honeypots es que no forman parte de los servicios en producción de la organización.

Por consiguiente, nadie (equipo, usuario ni aplicación) debería interactuar con ellos y cualquier transacción con un honeypot se considera como no autorizada.

Como su nombre lo implica, el objetivo de esta tecnología es "endulzar" (de ahí el término honey o miel en español) a los enemigos para atraerlos a la trampa.

Pasos para implantar un sistema de honeypot.

Los pasos para implantar un sistema honeypot se pueden resumir en:

a. Colocar un recurso que no contenga información de producción, por lo que nada ni nadie debería interactuar con él.

b. Registrar cualquier transacción que se realice desde o hacia el recurso, pues significará un acceso no autorizado.

Ventajas y desventajas de los honeypots.

9 The Honeynet Project. *Know your enemy: learning about security threats.* Segunda Edición. Addison Wesley. Julio, 2004

La simplicidad en la concepción de los honeypots es la que le brinda sus grandes ventajas y desventajas.

Ventajas.

La principal ventaja de los honeypots reside en la forma de recopilar la información. No contienen tráfico de producción por lo que los datos colectados son extremadamente valiosos, producto de algún tipo de intrusión. El esquema de enfocarse en reunir únicamente datos producto de accesos no autorizados, facilita su administración, análisis y difusión. Además, permite solucionar problemas típicos de la detección de ataques como los falsos positivos y los falsos negativos.

Un falso positivo es cuando un sistema de Seguridad de la Información reporta como ataque algo que en realidad constituye tráfico normal. Similar al problema de las alarmas de los carros que se activan por las vibraciones que genera un camión que pasa muy cerca.

Si la activación se repite constantemente, se decide ignorarla. Los honeypots reducen significativamente los falsos positivos porque prácticamente cualquier actividad es, por definición, no autorizada.

Un falso negativo es cuando se falla en detectar ataques desconocidos. Si el ladrón de carros diseña un nuevo ataque para desactivar la alarma, se lo robará sin que se genere una alerta. Una vez más, cualquier interacción con el honeypot es, por definición, no autorizada, independientemente de la táctica o herramienta utilizada. Por ello, puede detectar y generar alertas ante nuevos ataques.

Por último, los honeypots constituyen una tecnología altamente flexible y adaptable a cualquier ambiente. El recurso que proveen para ser atacado puede ser de diversa índole como computadoras con diferentes sistemas operativos

(Windows, Linux, Unix, etc.), un equipo de red (enrutador, firewall, etc.), un servicio (correo electrónico, página web, base de datos, etc), en fin, cualquier recurso.

Desventajas.

La misma simplicidad en su concepción es la que origina las desventajas de los honeypots. La principal es su limitado campo de visión, pues solo detectan los ataques que interactúan con ellos y no los dirigidos a otros recursos. Adicionalmente, todo honeypot conlleva riesgos. Uno es la identificación, pues si el atacante detecta la existencia de la red de trampa, podría introducir datos que lleven a conclusiones erróneas. Otro riesgo es que el atacante logre comprometer la red de trampa, pues puede utilizarla para lanzar ataques a otros recursos, internos o externos, que si contengan información de producción.

1.3.8 Honeynets.

Honeynet es un Honeypot de alta interacción que consta de una red de sistemas, cuyo propósito es ser comprometida por algún usuario malicioso, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios.[10]

Esta red captura y controla mediante un firewall todo el tráfico destinado a los equipos dentro de ella para su posterior análisis. Los equipos que pertenecen a la

10 Honeynet Project. Know Your Enemy; Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Addison Wesley, 2002.

Honeynet y que se comportarán como Honeypots pueden ser sistemas Unix, Windows, Solaris, dispositivos Cisco, etc. La finalidad es crear una infraestructura en la que no sólo haya sistemas reales, sino servicios reales tales como DNS, HTTP, SMTP, etc, que permitan al intruso estar en un ambiente más realista, pero controlado.

Otra de las ventajas de que en una Honeynet no se emule ningún servicio, es el hecho de que se puede replicar cierta infraestructura de una organización (aquella en la que estemos interesados por conocer sus debilidades) hacia una Honeynet, de esta manera cualquier evento que llegue a comprometer algún equipo dentro de la Honeynet, podría en cierta manera funcionar con los equipos en producción de la organización que fueron replicados. Esto quiere decir que si alguna organización utiliza un servidor Apache con una base de datos MySql y PHP, se podrá implantar una infraestructura similar en la Honeynet, para que de esta manera se pueda aprender sobre los riegos que existen en un ambiente como este.

Honeynets virtuales.

Las Honeynets Virtuales toman el concepto de las tecnologías de las Honeynets, y las implementan en un único sistema. Las Honeynets Virtuales no son un nuevo concepto, de hecho toman el concepto actual de Honeynet y las implementan de una forma diferente. Esta implementación tiene sus ventajas y desventajas comparadas con las Honeynets tradicionales. Las ventajas son coste reducido y más fácil manejo, ya que todo está; combinado en un único sistema. Sin embargo, esta simplicidad también resulta costosa.

Primero, la limitación de qué tipos de sistemas operativos se puede implantar debido al hardware y al programa virtual. Segundo, las Honeynets virtuales traen

un riesgo, específicamente que un atacante puede salirse del programa virtual y tomar el sistema Honeynet, saltándose los mecanismos de Control de Datos y de Captura de Datos. Se ha dividido las Honeynets Virtuales en dos categorías, Auto-Contenidas e Híbridas.

a. Honeynet virtual auto-contenida.

Una Honeynet Virtual Auto-Contenida es una red entera Honeynet condensada en un sólo computador.

La red entera está virtualmente contenida en un único y físico sistema. Una red Honeynet típicamente consiste de un cortafuego para Control de Datos y Captura de Datos, y los honeypots dentro de la Honeynet.

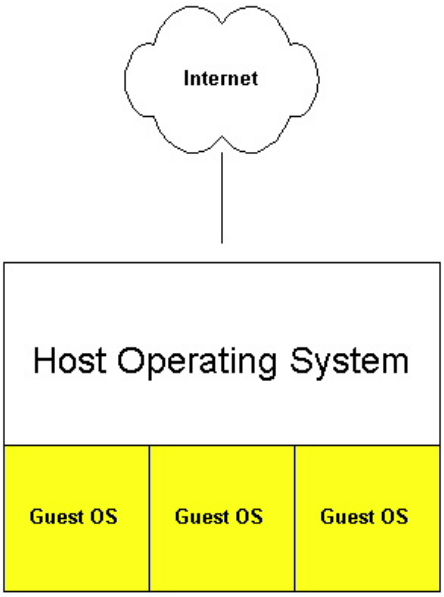

Figura 1: Honeynet Virtual Auto-Contenida[11]

Algunas ventajas de este tipo de Honeynet(s) virtual(es) son:

11 Honeynet Virtual Auto-Contenida - WikiLearning_com.htm

Movible: las Honeynets Virtuales pueden ser situadas en un portátil y llevadas a donde quiera.

Conectar y escoger: se puede escoger una máquina y simplemente conectarla en cualquier red y estará preparada para recolectar información de los blackhats. Esto hace que la implantación sea más fácil, ya que físicamente estás implantando y conectando un sólo sistema.

Económica en costo y en espacio: sólo se necesita un computador, así que reduce los gastos de hardware. Ocupa poco espacio y solo necesita un puerto de la red.

Desventajas: único punto de fallo: si algo va mal con el hardware, la honeynet entera queda sin funcionar.

Computador de alta calidad: aunque las Honeynets Auto-Contenidas sólo requieren un computador, tendrá que ser un sistema potente. Dependiendo de la configuración, se puede necesitar bastante memoria y procesador.

Seguridad: ya que todo puede estar compartiendo el mismo hardware, hay peligro de que un atacante acceda a otras partes del sistema.

Software Limitado, ya que todo tiene que ejecutarse en una máquina.

b. Honeynet virtual híbrida.

Una honeynet híbrida es una combinación de la clásica Honeynet y del software virtual.
Captura de Datos, como por ejemplo cortafuegos, y Control de Datos, como por ejemplo sensores IDS y almacenamiento de logs, están en un sistema separado y aislado. Este aislamiento reduce el riesgo de compromiso.

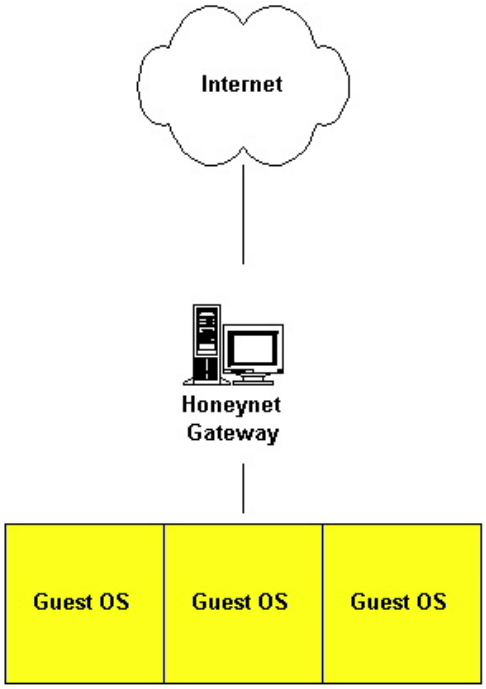

Figura 2: Honeynet Virtual Híbrida[12]

Las ventajas de esta configuración son:

Segura: Como vimos en las Honeynets Auto-Contenidas, existe un peligro de que el atacante acceda a otras partes de la honeynet (como el cortafuegos). Con las Honeynets Híbridas, el único peligro sería que el atacante accediera a otras honeypots.

Flexible: puede usarse una gran cantidad de software y hardware para el Control de Datos y la Captura de Datos de la red Híbrida. Un ejemplo sería que puede usarse el sensor OpenSnort en la red, o un Cisco Pix. Se puede incluso ejecutar cualquier clase de honeypot que se requiera porque simplemente se añade otro computador en la red (además de la computadora con la Honeypot Virtual).

12 Honeynet Virtual Hibrida - WikiLearning_com.htm

Algunas desventajas son:

No movible, ya que la red honeynet consistirá en más de una máquina, es más difícil moverla.

Costosa en tiempo y en espacio, se tendrá que pasar más electricidad, espacio y posiblemente dinero puesto que hay más de un computador en la red.

Honeynets distribuidas.

El siguiente paso que se está realizando con las Honeynets es la aplicación del viejo principio de “la unión hace la fuerza”. El escenario con el que nos encontramos puede ser el de una gran organización internacional con múltiples redes en múltiples países o varios equipos de expertos en seguridad diseminados por todo el planeta que desean compartir la información generada por sus Honeynets.

Obviamente, la posibilidad de centralizar (o al menos comunicar) las distintas Honeynets para la recolección de información es básico puesto que nos permitirá la correlación de resultados así como la comunicación de nuevos descubrimientos de forma más rápida y eficiente.

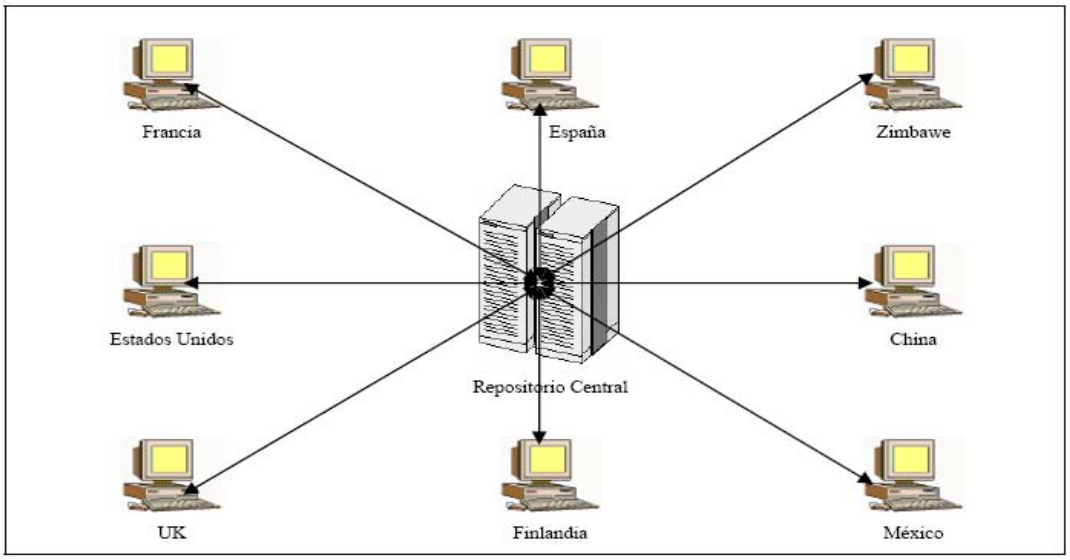

Figura 3: Arquitectura Distribuida de Honeynets[13]

1.3.9 Herramientas de virtualización.

Algunas de las herramientas de virtualización que se pueden utilizar para el desarrollo de Honeynets virtuales son: User Mode Linux, VMware Workstation, GSX Server y Microsoft Virtual PC.

User Mode Linux.

Es un modulo del kernel que permite la ejecución simultanea de varios sistemas Linux como procesos de otra máquina Linux. Su utilización tiene una serie de ventajas:

13 SEGURIDAD EN REDES IP: Honeypots y Honeynets, Gabriel Verdejo Alvarez, http://tau.uab.es/~gaby

a. Se trata de una herramienta de código abierto, por lo que se puede revisar, corregir y adaptar a las necesidades de la Honeynet.
b. Se puede utilizar sin necesidad de licencia.
c. Permite capturar las sesiones del intruso de forma pasiva a través del kernel del sistema anfitrión.

Desventajas:

a. Sólo alberga maquinas virtuales Linux.
b. No ofrece interfaz gráfica y su utilización no resulta sencilla de manejar.
c. Carece de soporte técnico.

Vmware

Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (una computadora) con unas características hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a una computadora física, con CPU, BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro, etc.

Un virtualizador por software permite ejecutar (simular) varios servidores o computadoras (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

VMware es similar a su homólogo Virtual PC de Microsoft, aunque existen diferencias entre ambos que afectan a la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales (CPU, RAM, etc.) asignados al sistema virtual. Lo anterior lo podemos observar en la figura 4 en donde se muestra que los recursos físicos son compartidos mientras que los recursos y sistemas son virtualizados.

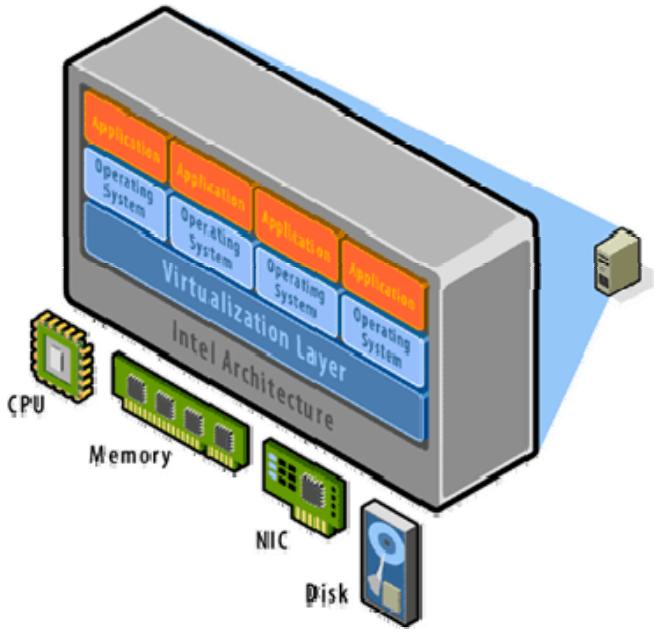

Figura 4. Virtualización y compartimiento de recursos físicos.

VirtualPC emula una plataforma x86, Vmware la virtualiza, de forma que la mayor parte de las instrucciones en VMware se ejecutan directamente sobre el hardware físico, mientras que en el caso de Virtual PC se traducen en llamadas al sistema operativo que se ejecuta en el sistema físico. Dos productos de vmware se pueden utilizar para tal labor siendo estos el Workstation y el GSK server que a continuación se describen.

VMware Workstation.

Es una herramienta de virtualización comercial diseñada para ejecutarse sobre equipos con sistemas Windows o Linux y presenta las siguientes ventajas:

a. Puede hospedar máquinas virtuales con sistemas operativos Windows, Linux, Netware y FreeBSD, aunque potencialmente es capaz de albergar cualquier sistema que se ejecute sobre la plataforma X86 de Intel.

b. Se administra desde una interfaz gráfica de usuario y ofrece una documentación detallada. El proceso de instalación de un sistema operativo en una maquina virtual es el mismo que se utiliza en los equipos físicos.

Como inconveniente al utilizar la herramienta es la exigencia de pago de la licencia y que es un software propietario, por lo que no se debe acceder al código fuente y no existe el derecho de realizar modificaciones en la aplicación.

VMware GSK Server.

Es una herramienta de virtualización para ser utilizada en sistemas Windows o Linux y tiene mayores ventajas que la versión Workstation, por lo que se agregan las siguientes:

Puede albergar máquinas virtuales más potentes y redes más complejas. Permite la administración remota de la herramienta a través de una interfaz Web y una consola remota que permite el acceso a las máquinas virtuales instaladas. Incluye una API que permite el control de las máquinas virtuales. Existe soporte técnico al cual se puede optar por contratar.

Microsoft Virtual PC

Es una herramienta diseñada para funcionar sobre Windows, OS/2 y MAC OS que es comparable, tanto en rendimiento como en funcionalidades, a la versión Workstation de VMware.

1.4 Aspectos legales.

Asegurar un sistema no sólo consiste en tomar las medidas necesarias para protegerlo ante ataques u otros problemas, sino estar al tanto de los aspectos relacionados con el tema. La implementación de un sistema de honeynets muchas ocasiones implica incumplimiento de requisitos impuestos por la ley en los países que las poseen.

Cumplir con estas obligaciones permite perseguir a los culpables mediante procesos legales o judiciales. Los registros e informes proporcionados por un sistema de honeypots o de honeynets podrían ser requeridos como pruebas que ayuden a localizar o condenar responsables de actos vandálicos.

Lastimosamente, los sistemas legales de muchos países no se han adaptado a la misma velocidad que el desarrollo de las tecnologías, dejando vacíos que permiten a los criminales delinquir con total impunidad.

1.4.1 Legalidad de los honeynets.

Algunos de los problemas que se asocian al uso de los honeynets se centran en el aspecto legal, sin dejar a un lado el alto riesgo de que se comprometan mas sistemas partiendo desde la Honeynet. La supuesta tentativa generada por el uso de los honeypots es uno de estos problemas. Se podría pensar que el hecho de colocar un equipo en la red con la finalidad de que sea comprometido, puede ser

tomado como una tentativa de comprometer a otros sistemas y fomentar la actividad maliciosa en la red.

Uno de los principales puntos el cual sorprende a muchos y es la aseveración siguiente: “no solo por ser el administrador propietario de una red de computadoras, significa que se posea la autoridad legal de monitorear a los usuarios en la red”. Muchas compañías multinacionales poseen políticas internas, estatutos o acuerdos que pueden llegar a prohibir el hacer un monitoreo de la información que los usuarios manejan, de tomarse en cuenta en algunos países puede significar caer en ilegalidad civil o criminal.

Es por tal motivo que antes de realizar una implementación de sistemas honeynets en corporaciones multinacionales o instituciones de gobierno es necesario y mandatario el realizar una investigación de la apertura de monitorear tráfico o datos en la red.

1.4.2 Repercusiones legales.

La ley norteamericana (al igual que la europea) protege la inviolabilidad de las comunicaciones personales (interception of communications) de una forma muy estricta. El punto de discusión se basa en que dependiendo del tipo de Honeynet que se utilice, se puede violar esta ley al recoger una serie de información sobre el atacante que la ley protege. Los Estados Unidos suelen ser los primeros en regular todo lo referente a la seguridad informática, y en especial a cualquier cosa que afecte Internet. Muchas leyes estatales y/o europeas se basan en las americanas.

Tal y como se ha explicado anteriormente, los honeynets en producción tienen un objetivo mucho más concreto (proteger la red), que los honeynets de investigación (cuyo interés se centra en conseguir tanta información de los atacantes como sea posible para comprender/estudiar su comportamiento y técnicas).

Lance Spitzner quien es uno de los fundadores del proyecto de investigación de Honeynet y que a su vez trabaja como arquitecto especialista de seguridad para Sun Microsystems, desglosa las posibles responsabilidades legales derivadas del uso de honeypots y las Honeynet en tres cuestiones básicas:

a. Trampa: Es el proceso realizado por los cuerpos policiales (law enforcement) de “inducir” a alguien a cometer un acto punible con el objetivo de iniciar la acción judicial pertinente.

   En este caso del Honeypot, aunque es un elemento pasivo creado por cuenta propia para ser atacado no se desea perseguir judicialmente esta intrusión en el Honeypot así mismo que no se realiza ninguna trampa. El objetivo del Honeypot es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.

b. Privacidad: Que el Honeypot recoge información es innegable. Sin embargo, la información recogida puede dividirse en información transaccional (transactional) e información de contenido (content). La información transaccional (meta-información) no hace referencia a la información en sí, sino a aspectos de esta como la dirección IP, la fecha y hora, valores de las cabeceras de los paquetes IP.

c. La información de contenido es propiamente la comunicación que realiza el atacante con terceros. Precisamente este es el objetivo del debate (y también el de los Honeypots de investigación). La

intercepción de una comunicación privada es la piedra angular que puede permitir a un atacante demandar ante un juzgado y probablemente ganar, en el caso de las leyes aplicables como en países como Brasil, Estados Unidos y España; pero en El Salvador es un punto que no tiene validez ya que no existe una legislación que lo apruebe o lo prohíba – por el momento.

d. En cualquier caso, todos los autores están de acuerdo que se deberían incluir mensajes de advertencia y renuncia (disclaimer). Sin embargo esto no exime del problema, ya que el hecho de que se ponga un aviso no significa que un eventual atacante lo vea o lea.

e. Responsabilidad (Liability): Este aspecto hace referencia a las posibles demandas que se puede recibir en el caso de que un atacante utilice el Honeypot como plataforma de lanzamiento de ataques. Las demandas se basarían en que se ha realizado unos mínimos esfuerzos de seguridad en la red propia, sino que al contrario, se ha facilitado el acceso a los recursos para que sean utilizados en todo tipo de ataques.