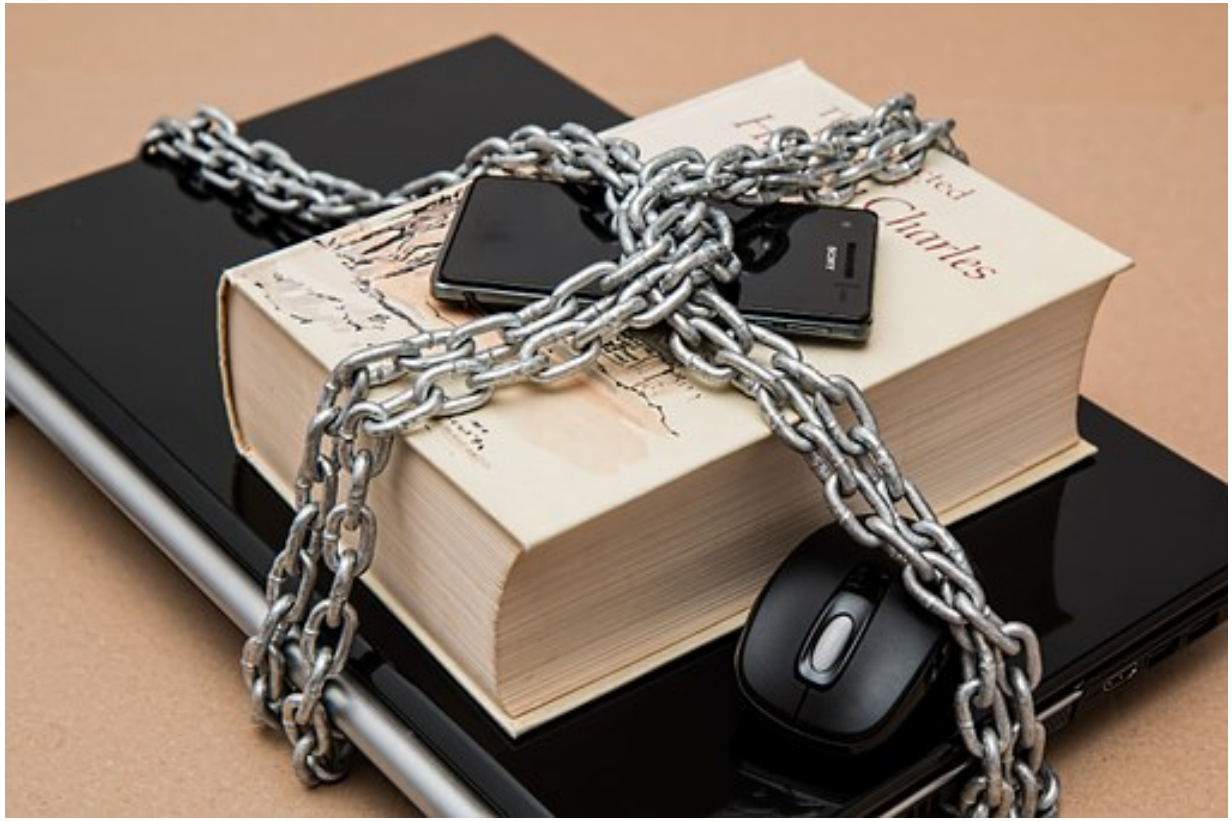
Capítulo 8: Seguridad en redes



Contenido de esta clase

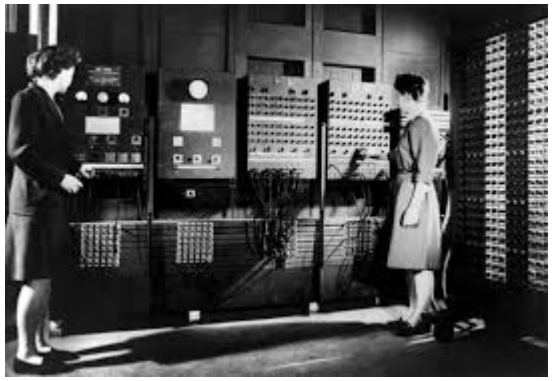
- Fundamentos de la seguridad
- Un poco de historia de la seguridad informática
- Línea de Tiempo
- Definición de la Seguridad
- Conceptos y terminología de seguridad
- Gerencia de la seguridad de la información

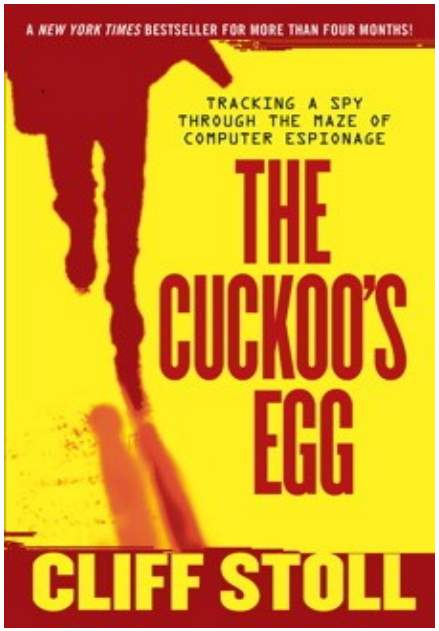
Historia de la seguridad informática

Los primeros intentos en seguridad informática pueden ir tan temprano como la época de Julio Cesar y sus famosos mensajes cifrados. Sin embargo, las primeras técnicas de ocultamiento y resguardo de seguridad informática comenzaron durante la segunda guerra mundial con equipos como el enigma. Pero cuando realmente se hizo necesaria fue cuando las computadores se hicieron de propósito general y multiusuario, en ese momento el panorama de la seguridad de la información se tornó complejo.

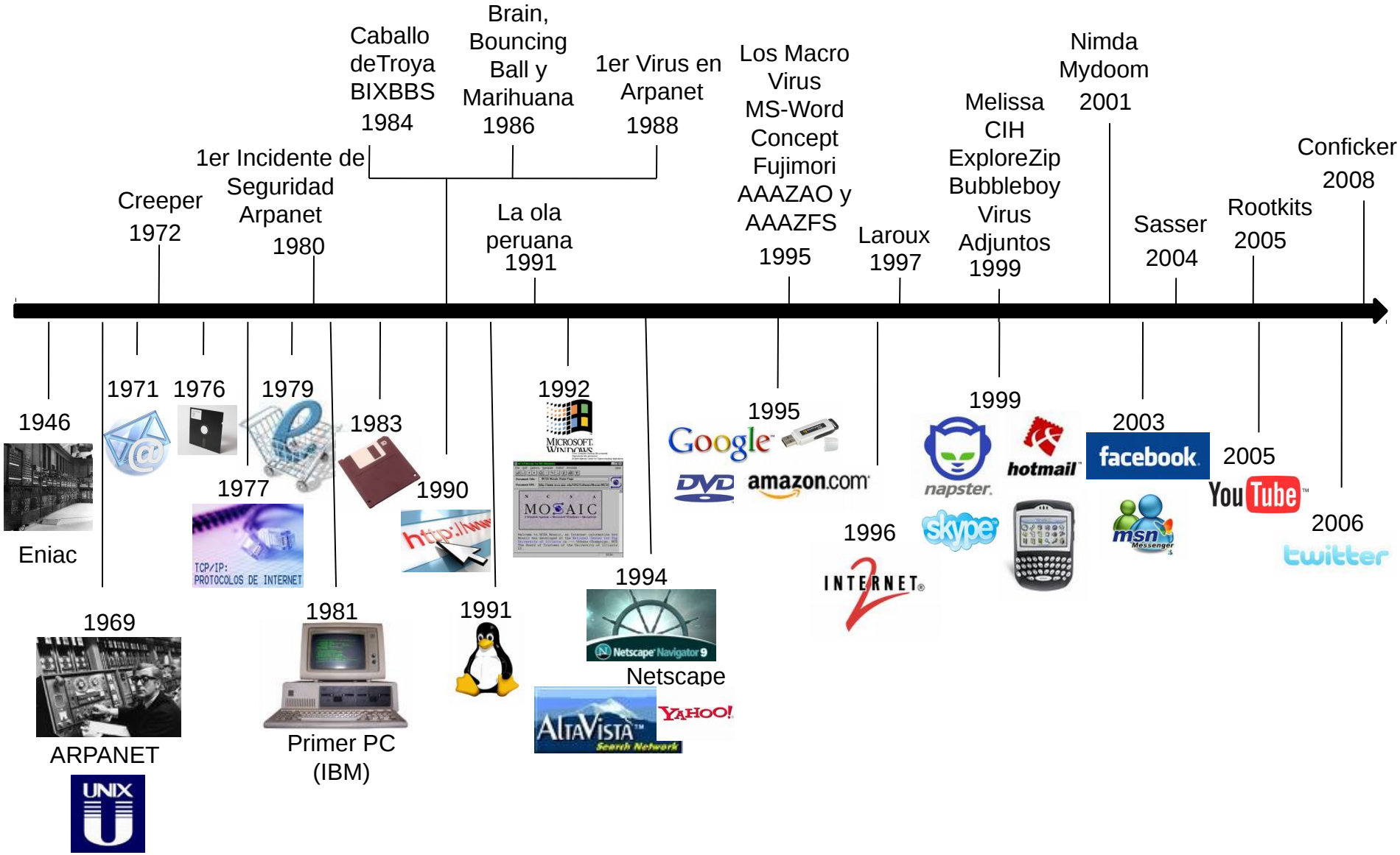
Historia de la seguridad informática

El surgimiento equipos computacionales como el Eniac hizo que se desarrollaran aplicaciones muy diversas pero la más crítica de ellas era un sistema de defensa antimisiles, este sistema continuo desarrollándose y se transformó durante 10 años hasta llegar a un sistema distribuido con más de 50 empleados en 23 centros de operación. Es allí en dónde comienzan toda clase de amenazas de seguridad a la información manejada por diversas personas en un mismo centro de cómputo.

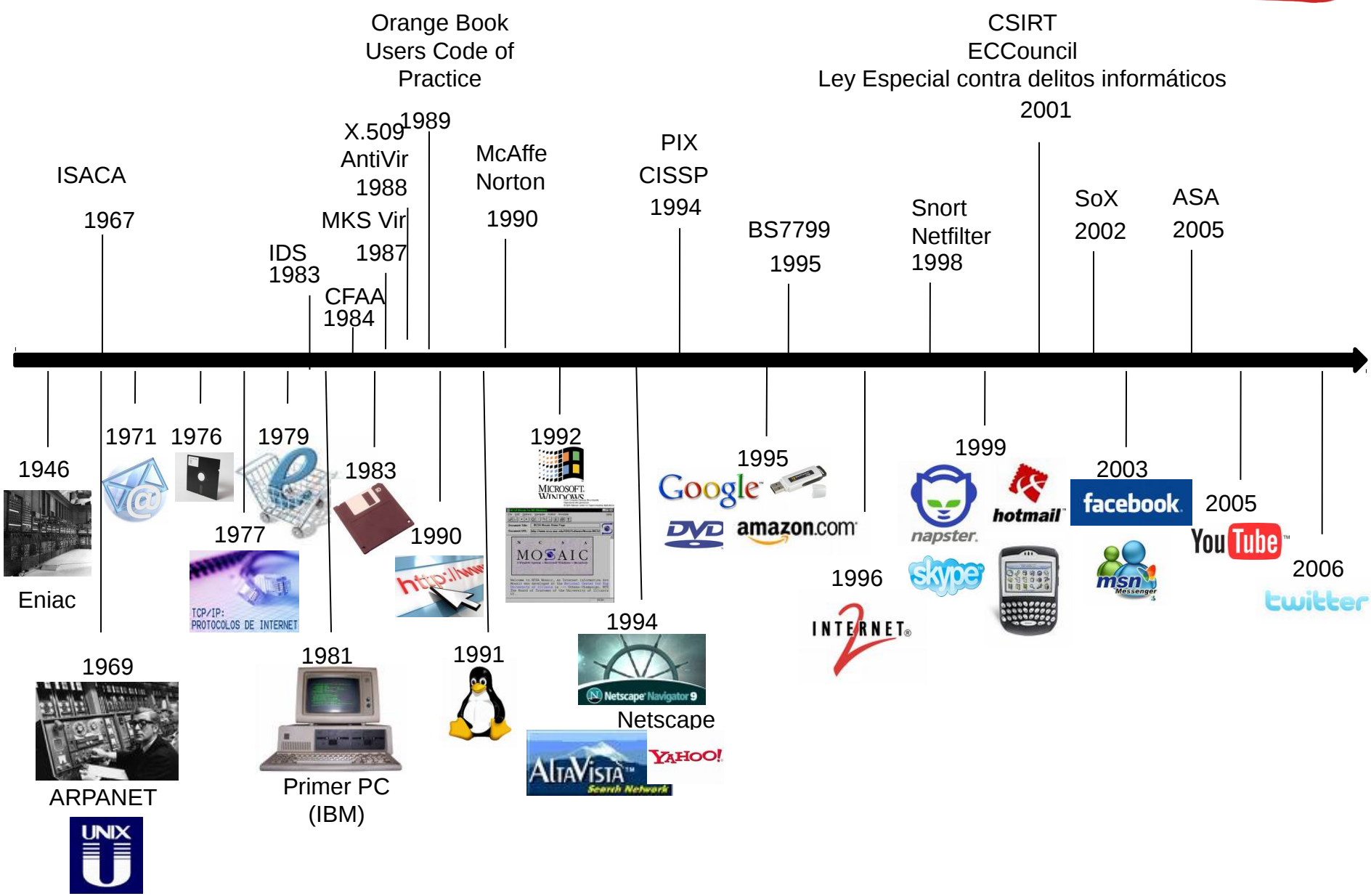




Línea de Tiempo de los virus informáticos



Línea de Tiempo de la Seguridad Informática



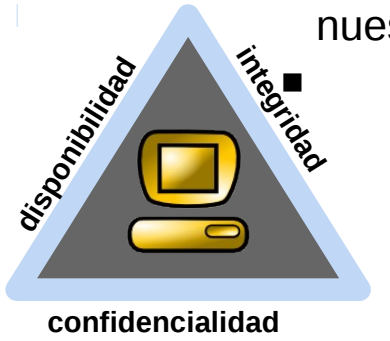
Desarrollo de la Seguridad Informática

- A partir de los años 80 el uso de la computadora personal comienza a ser común. Asoma por tanto la preocupación por la integridad de los datos.
- En la década de los años 90 aparecen los virus y gusanos y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.
- Además, comienzan a proliferar ataques a sistemas informáticos. La palabra hacker aparece incluso en prensa.
- Las amenazas se generalizan a finales de los 90; aparecen nuevos gusanos y malware generalizado.
- En los años los acontecimientos fuerzan a que se tome muy en serio la seguridad informática.

Definición de la seguridad Informática

- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la “cualidad de seguro”. Buscamos ahora seguro y obtenemos “libre y exento de todo peligro, daño o riesgo”.
- A partir de estas definiciones no podríamos aceptar que seguridad informática es “la cualidad de un sistema informático exento de peligro”, por lo que habrá que buscar una definición más apropiada.
- Algo básico: la seguridad no es un producto, sino un proceso.
- Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:

  “Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico.”
- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.
-



Conceptos básicos en seguridad

Cifra o cifrado:

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreta, no será posible descifrarlo o recuperarlo.

No obstante, la RAE define cifrar como “Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar” ... también muy poco técnica ☹.

En algunos países de Latinoamérica, por influencia del inglés, se usa la palabra encriptar.

Si bien se entiende, esta palabra todavía no existe y podría ser el acto de “introducir a alguien dentro de una cripta”, ... ✝☠✝ ... algo bastante distinto a lo que deseamos expresar... ☺.

Jorge Ramió

Libro Electrónico de Seguridad Informática y Criptografía
Versión 4.1 de 1 de marzo de 2006

Objetivos de la seguridad

Confidencialidad: Los datos sólo deben ser conocidos y accedidos por quienes estén debidamente autorizados durante su almacenamiento, procesamiento o transmisión.

Integridad: Los datos sólo pueden ser modificados y/o eliminados por quienes estén autorizados para ello y los sistemas y aplicaciones sólo deben ser operados por personal autorizado

Esto incluye: *Autenticidad*, *No repudiación* y *Contabilidad*

Disponibilidad: Los sistemas que albergan datos e información deben garantizar su acceso, cuando así se requiera, por quienes tengan derecho a ello

El objetivo del proceso de seguridad informática es obtener un nivel aceptable de seguridad, entendiéndose por aceptable un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de nuestra organización fracasen en cualquier intento de ataque contra los mismos. Asimismo, se encarga de establecer los mecanismos para registrar cualquier evento fuera del comportamiento normal y tomar las medidas necesarias para restablecer las operaciones críticas a la normalidad.

Conceptos básicos en seguridad

¿Qué es la información?

Desde el punto de vista de la ingeniería:

- Estudio de las características y estadísticas del lenguaje que nos permitirá su análisis desde un enfoque matemático, científico y técnico.

Desde el punto de vista de la empresa:

- Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización.

En las empresas se entenderá como:

- Todo el conjunto de datos y archivos de la empresa.
- Todos los mensajes intercambiados.
- Todo el historial de clientes y proveedores.
- Todo el historial de productos.
- En definitiva, el *know-how* de la organización.

Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir siendo competitiva. Por este motivo, es vital que se implanten unas políticas de seguridad y que, además, se haga un seguimiento de ellas.

Conceptos básicos en seguridad

No Repudio

- Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático.
- Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación.
- Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.

Conceptos básicos en seguridad

Hackers: El concepto "hacker" surgió a finales de la década de los 60 y principios de la década de los 70 del siglo pasado, cuando algunos programadores del Massachussets Institute of Technology (MIT) se llamaron a sí mismos hackers, para mostrar que podían realizar programas o acciones que nadie había podido hacer antes, específicamente para hacer uso de acceso telefónico a redes.

A pesar de que existen diversas connotaciones para el término “hacker” es comúnmente aceptado que un “hacker” es una persona que trata de conseguir acceso a un sistema, equipo no aplicación de forma remota y sin autorización.

De este término, se establecen diferencias entre los **propósitos que tenga el hacker** al entrar en un sistema determina el tipo de hacker:

Conceptos básicos en seguridad

De sombrero negro (Cracker): entra a los sistemas con el objetivo de obtener información clasificada o confidencial, destruir sistemas, causar una denegación de servicios. Sus intenciones son de carácter delictivo y fraudulento.

De sombrero gris: es un hacker que utiliza sus conocimientos de forma ofensiva y defensiva. Normalmente, sus acciones ofensivas no tienen cómo objetivo el lucro o fraude sino la demostración de una vulnerabilidad o debilidad en un sistema operativo, aplicación, etc.

De sombrero blanco: Son aquellos individuos que se encargan de detectar vulnerabilidades y contrarrestarlas. Asimismo, publica sus hallazgos para que las debilidades encontradas sean solventadas.

Su propósito fundamental es mejorar los niveles de seguridad de sistemas operativos,

Script kiddie: Un inexperto, normalmente un adolescente, que usará programas que se descarga de Internet para atacar sistemas.

Conceptos básicos en seguridad

Amenaza

Cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Ejemplos de amenazas son los ataques humanos, los desastres naturales, los errores humanos inadvertidos, fallas internas del hardware o el software, etc.

Vulnerabilidad

Consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

Conceptos básicos en seguridad

Amenaza

Es cualquier acción que explota una vulnerabilidad.

Exploit

Un exploit es un método específico para hacer uso de una vulnerabilidad. Pueden encontrarse en el mercado en forma de scripts, crackers, etc.

Conceptos básicos en seguridad

Flujo Normal

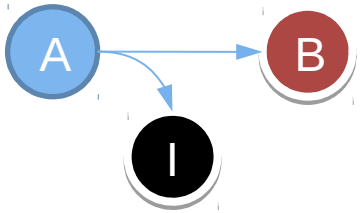
Interrupción

Interrupción

En el caso de una interrupción un activo del sistema se pierde, se hace no disponible o inutilizable. Un ejemplo de ello puede ser la destrucción maliciosa de un dispositivo de hardware o el borrado de un programa o archivo.

Conceptos básicos en seguridad

Flujo Normal



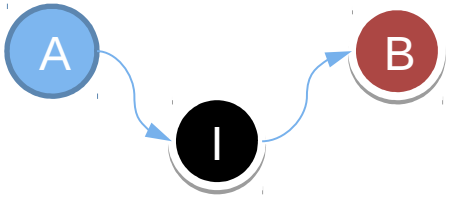
Intercepción

Intercepción

En el caso de una intercepción implica que alguien logre acceso no autorizado a un activo del sistema. Esta parte no autorizada puede ser una persona, programa, dispositivo, etc. Un ejemplo de ella puede ser el copiado de datos, la intervención de un canal de red.

Conceptos básicos en seguridad

Flujo Normal



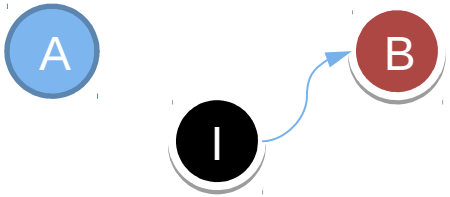
Modificación

Modificación

En el caso de que se realiza una intercepción y la parte no autorizada logra acceso a un activo del sistema y tiene la capacidad de manipularlo se trata de una amenaza por modificación.

Conceptos básicos en seguridad

Flujo Normal



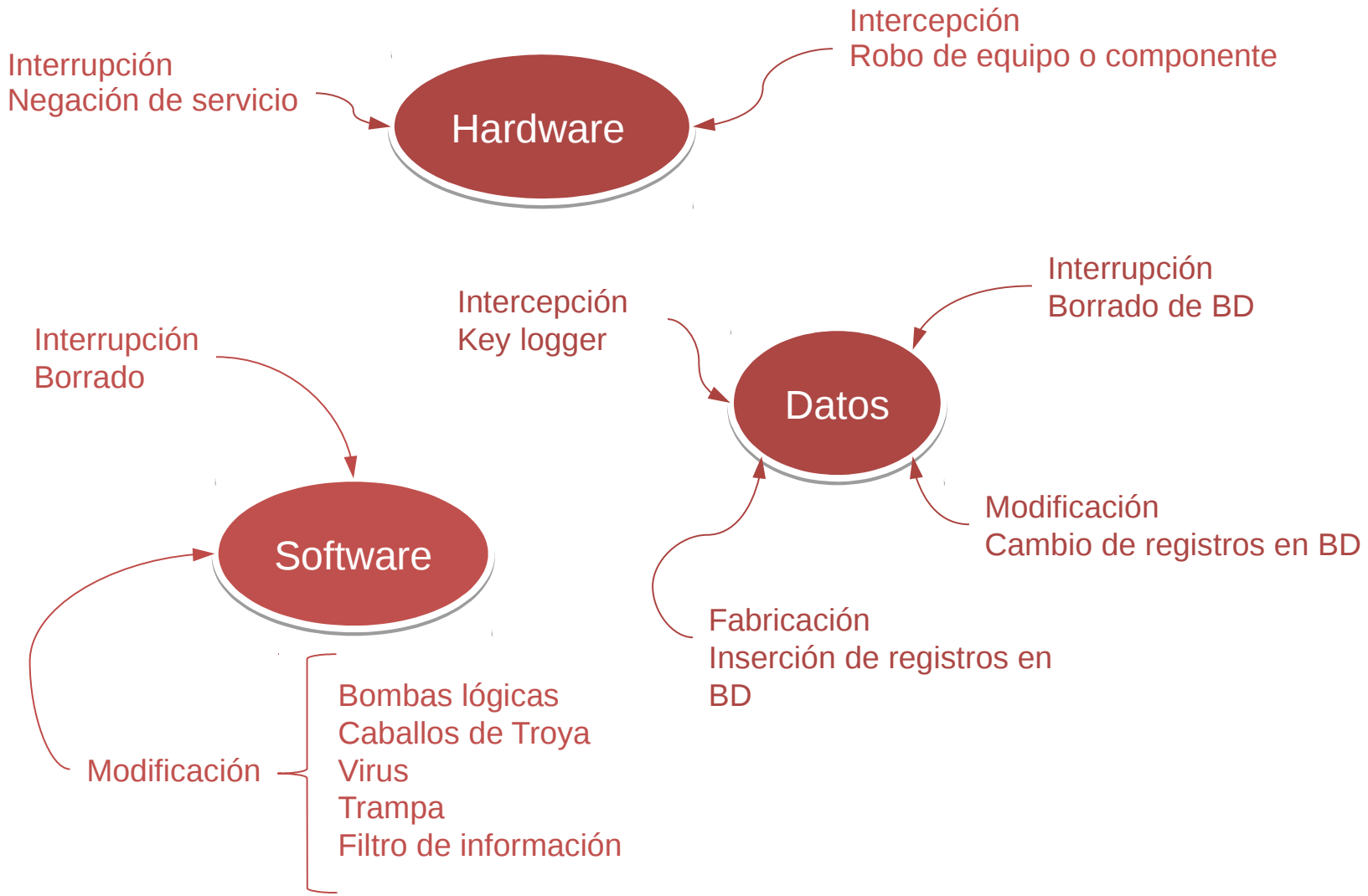
Fabricación

Fabricación

La parte no autorizada que accede al sistema también puede crear objetos falsos en un sistema. Ejemplo de ello son la inserción de transacciones en un sistema o BD, fabricación de paquetes de datos, etc.

Conceptos básicos en seguridad

Algunos ejemplos



Conceptos básicos en seguridad

Caballos de Troya

Virus que entra la compuradora y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

Spam

El spam o correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y muchos dolores de cabeza.

Virus

Código diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, las macros de aplicaciones y archivos ejecutables.

Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

Amenazas más características

- Hardware:
  - Agua, fuego, electricidad, polvo, cigarrillos, comida.
- Software:
  - Además de algunos típicos del hardware, borrados accidentales o intencionados, estática, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.
- Datos:
  - Tiene los mismos puntos débiles que el software. Pero hay dos problemas añadidos: no tienen valor intrínseco pero sí su interpretación y, por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público: hay leyes que lo protegen.

Denegación de servicio

Podríamos definir los ataques DOS (Denegation Of Service) como la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

Existen tres tipos básicos de denegación de servicio:

Consumo de recursos: El atacante intenta consumir los recursos del servidor hasta agotarlos: ancho de banda, tiempo de cpu, memoria, disco duro…

Destrucción o alteración de la configuración: Se intenta modificar la información de la máquina. Este tipo de ataques necesitan de técnicas más sofisticadas.

Destrucción o alteración física de los equipos: Se intenta denegar el servicio destruyendo físicamente el servidor o algunos de sus componentes, cortando el cable de conexión, o el cable de la red eléctrica.

Denegación de servicio

Los sistemas de DOS más utilizados:

Mail Bombing: El primer sistema de denegación de servicio fue el denominado mail bombing, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio.

Smurfing: Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping. Esta trama lleva como dirección de origen la dirección IP de la víctima (usando IP Spoofing) y como dirección de destino la dirección broadcast de la red atacada. De esta forma todos los equipos de la red contestan a la víctima de tal modo que pueden llegar a saturar su ancho de banda.

SYN Flood: El sistema atacante utiliza una IP inexistente y envia multitud de tramas SYN de sincronización a la víctima. Como la víctima no puede contestar al peticionario (porque su IP es inexistente) las peticiones llenan la cola de tal manera que las solicitudes reales no puedan ser atendidas.

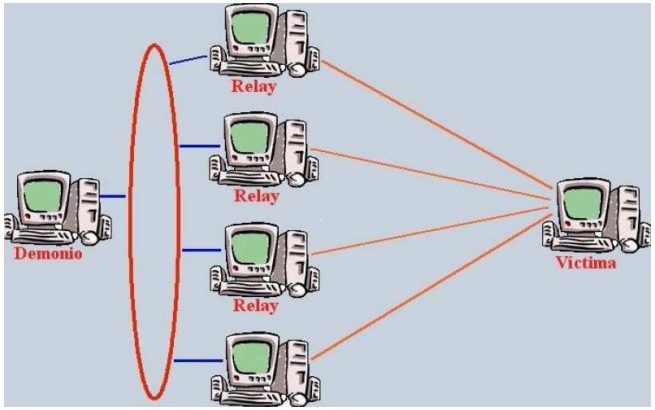


Fig. 1 Smurfing

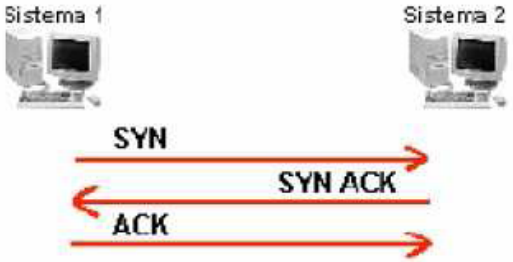
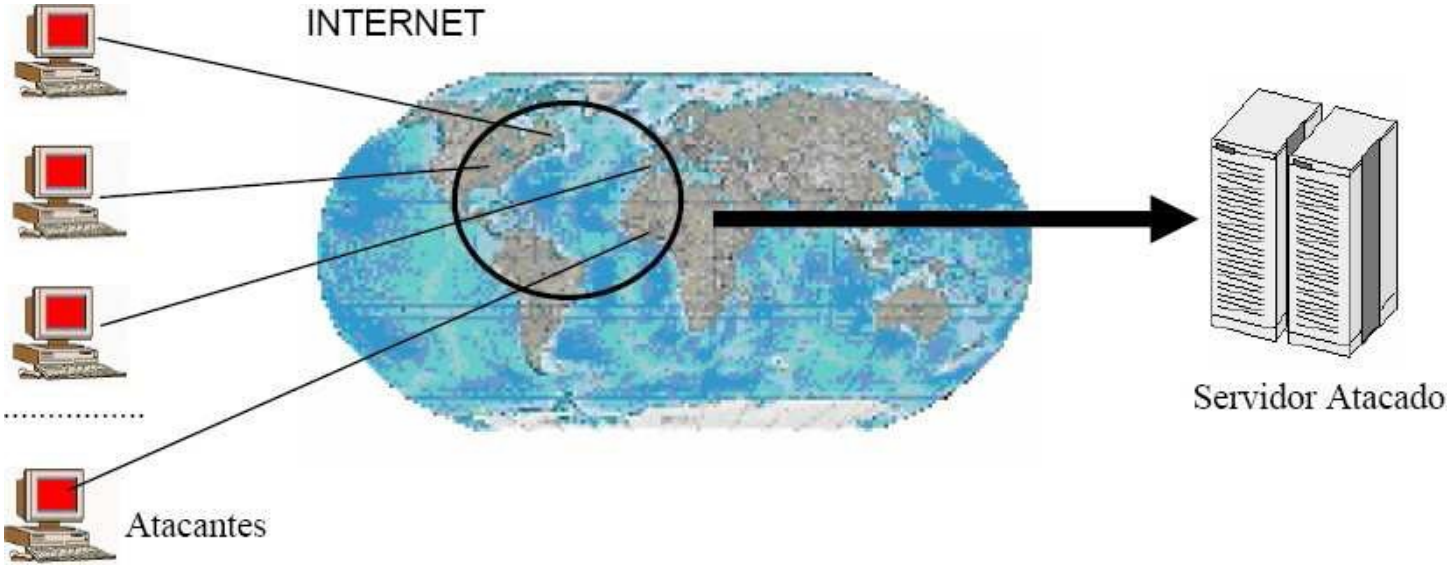


Fig. 2 Syn Flood

Denegación de servicios distribuida

Podemos definir el ataque DDOS como un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino.

Es decir, el ataque DDOS es una ampliación del concepto DOS sumándole la capacidad de acceso simultáneo y desde cualquier punto del mundo que ofrece Internet.



Denegación de servicios distribuida

Existen diferentes tipos de ataques DDOS pero todos tienen en común un gran consumo de ancho de banda. Aquí está el gran peligro de este tipo de ataques que tienen dos vertientes:

Denegación del servicio: Es su objetivo principal, hacer que un sistema no pueda cumplir su cometido.
Saturación de la red: Debido a que los paquetes de estos ataques comparten las mismas rutas que el resto de comunicaciones.
El crecimiento del número de nodos conectados y la mejora del ancho de banda hacen que existan cada vez más atacantes potenciales. Se puede dar el caso de cientos de atacantes coordinados pero este fenómeno no se da en la realidad:

- Es muy arriesgado para un atacante usar su propio equipo.
- Es muy difícil coordinar a muchos atacantes.

Denegación de servicios distribuida

¿Cómo lo hacen?

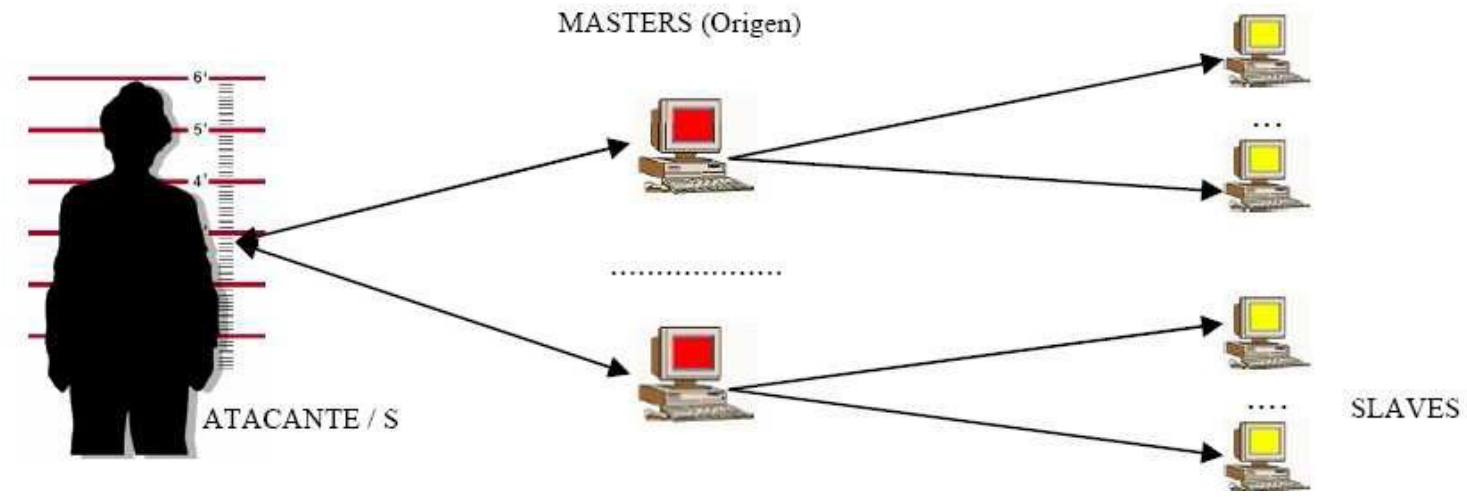
Uno o varios hackers buscan sistemas vulnerables. Esto es fácil ya que:

- Cada vez hay más nodos conectados permanentemente a internet.
- Muchos equipos carecen de las actualizaciones críticas de sus sistemas operativos o éstos son antiguos.
- El desconocimiento de muchos de los usuarios hace que no sean conscientes de que sus equipos están infectados por algún programa malicioso.
- Se realiza un ataque sobre esos nodos y se les instala el programa.
- Estos son los nodos “masters”, es decir, los que tienen una conexión directa con el atacante.
- A su vez el programa instalado en estos nodos busca un segundo nivel de nodos (“esclavos”) que serán los encargados de realizar el ataque final.
- Los atacantes dan la orden de manera sincronizada para que todos los nodos esclavos ataquen al sistema “victima”.

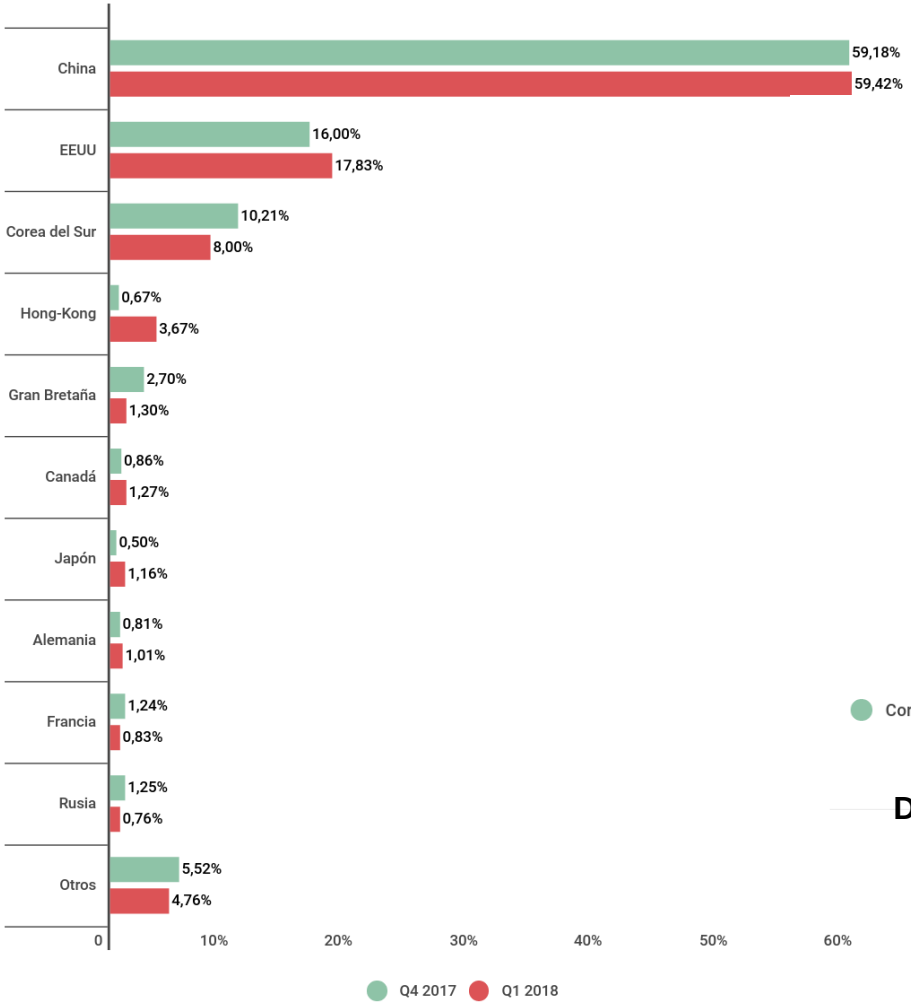
Denegación de servicios distribuida

¿Cómo lo hacen?

La gran ventaja de este sistema es que permite mantener el anonimato de los atacantes ya que analizan el trafico de los nodos slave y cuando detectan que están siendo analizados cierran la conexión, posteriormente limpian cualquier prueba en el master y finalmente cierran su conexión con el master.

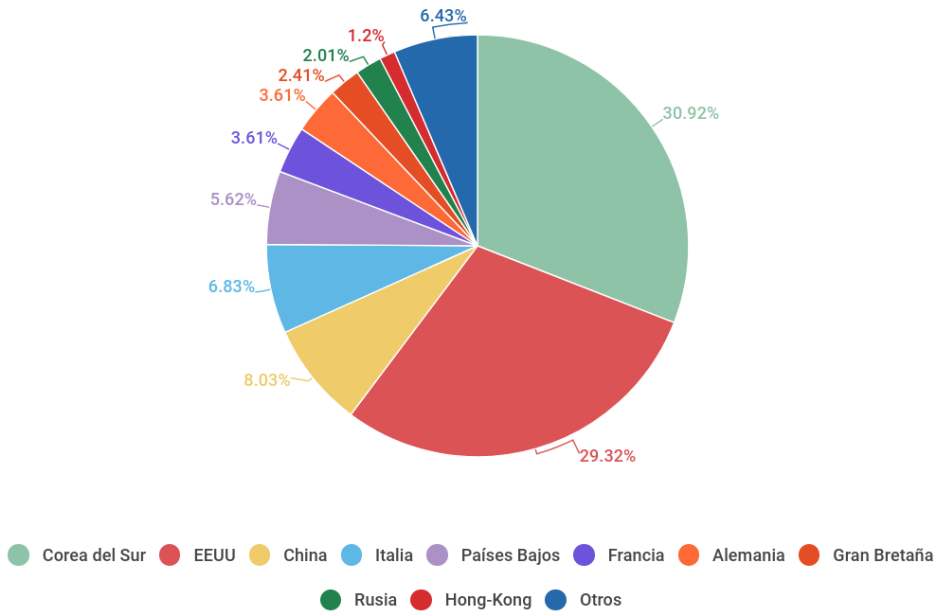


Denegación de servicios distribuida



DDOS por país primer cuatrimestre del 2018

KASPERSKY lab



Distribución de servidores administradores de BotNets

KASPERSKY lab

MyDoom

El virus MyDoom ha sido uno de los más extendidos (1 million de máquinas afectadas según F-Secure).

Su propagación ha sido una de las más rápidas, en 4 segundos ya era una verdadera epidemia.

Inicialmente este virus fue concebido para hacer un ataque DDoS sobre el servidor de SCO (www.sco.com), aunque existen teorías de que su verdadera intención era la recopilación de direcciones de e-mail para Spam.

El ataque tuvo la SCO en jaque durante 1 semana hasta que SCO cambió su dominio (www.thescogroup.com).

Su predecesor MyDoom.B no llegó a tener el mismo impacto ya sea por su menor propagación o por la capacidad de respuesta de su objetivo (www.microsoft.com), que cambió sus servidores solo 2 segundos después del inicio del ataque.

Blaster y Sasser

Blaster ha sido uno de los últimos virus con gran expansión por la red.
Su objetivo era un DDoS sobre los servidores de Microsoft. Especialmente contra el sitio www.windowsupdate.com

Su infección se producía por una vulnerabilidad de Windows.

Aunque el número de ordenadores infectados resulto ser bastante grande 1,2 millones, no provocó grandes problemas.

El virus Sasser que, al igual que Blaster, aprovecha las vulnerabilidades de Windows para su distribución por la red. Sus consecuencias fueron menores que las de Blaster.

Debilidades más características

- Hardware: pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- Software: puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- Datos: puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.
- Memoria: puede producirse la introducción de un virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- Usuarios: puede producirse la suplantación de identidad, el acceso no autorizado, visualización de datos confidenciales, etc.

- Es muy difícil diseñar un plan que contemple minimizar de forma eficiente todas estas amenazas, y que además se entienda y pase desapercibido por los usuarios.
- Debido al principio de acceso más fácil, el responsable de seguridad informática no deberá descuidar ninguno de los cinco elementos susceptibles de ataque al sistema.

Delitos informáticos

Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminal o como mero símbolo. (Carlos Sarzana, Mx)

Se conceptualiza en forma típica y atípica, entendiendo la primera como *las conductas típicas, antijurídicas y culpables en que se tienen las computadoras como instrumento o fin*, y por la segunda *actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.* (Julio Tellez Valdés, Mx)

Toda acción dolosa que cause un perjuicio a personas naturales o jurídicas que puede producir o no un beneficio material para su autor, pudiendo o no perjudicar de manera directa o indirecta a la víctima, caracterizando dicha acción dolosa por la utilización de actividades o medios informáticos. (Orlando Solano B. Col.)

Delitos informáticos

Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. El autor no logra normalmente con ello beneficios económicos pero pone en jaque mate a la organización.

Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

Delitos informáticos

Elementos Comunes a las definiciones

Revisando las definiciones se identifican elementos comunes:

Sujeto actor o actores de la conducta dañosa que produce el hecho

- No es clara en todas las definiciones presentadas
- Algunas veces se deja por fuera de la definición o se asume implícita

Un medio adecuado para comenter el acto ilícito, o sea el dispositivo informático por medio del cual se lleva a cabo la acción.

- Se encuentra referenciado en todas las definiciones
- Se hace particular énfasis a medios informáticos
- En pocas definiciones se hace claridad sobre el lugar de la evidencias, dado el medio utilizado.

Un objeto, o sea, el bien que produce el beneficio ilícito para el o los autores

- Se consideran generalmente los objetos resultado de procesamiento de datos, los datos, la información resultado.

Delitos informáticos

- Suponiendo que todos entendemos más o menos qué es un delito informático, algo no muy banal dado que muchos países no se ponen de acuerdo, parece ser que es un buen negocio:
  - Objeto pequeño: la información que se ataca está almacenada en contenedores pequeños: no es necesario un camión para robar un banco, llevarse las joyas, el dinero, etc.
  - Contacto físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del propio delincuente.
  - Alto valor: el objeto codiciado tiene un alto valor. Los datos (el contenido a robar) puede valer mucho más que el soporte que los almacena: servidor, computador, disco, CD, etc.

Delitos informáticos

Son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información.

Ataques a un sistema informático:

- Fraude
- Malversación
- Robo
- Sabotaje
- Espionaje
- Chantaje
- Revelación
- Mascarada
- Virus
- Gusanos
- C. de Troya
- Spam

Delitos informáticos

Amenazas comunes:

Cartas nigerianas: correo electrónico que comenta la necesidad de sacar una gran cantidad de dinero de un país normalmente africano a través de un “cómplice” de otro país, justificando una persecución política, herencia, etc.

Ingeniería social: La Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Phishing: simulación, algunas veces perfecta, de una página Web de un banco solicitando el ingreso de claves secretas, con la excusa de la aplicación de nuevas políticas de seguridad de la entidad.

Administración de la seguridad

La gerencia de la seguridad de la información involucra el control y verificación de procesos no sólo en el área de las TIC. Por ello se habla de varios niveles de gobierno:

Gobierno de las tecnologías de la información:

Es el sistema: normas, procedimientos, organización, infraestructura que gestiona y controla todas las tecnologías de la información de una organización

Gobierno de la empresa:

Es el sistema: normas, procedimientos, métodos, organización, procesos que dirige y controla una organización

Gobierno de las tecnologías de la información es parte del gobierno de la empresa:

Información y conocimiento generado por uno o más sistemas de información que influyen en la dirección de una empresa e impactan en la actividad del negocio

Arquitectura de seguridad

La arquitectura de seguridad se refiere a los conceptos, principios, estructuras y estándares usados para diseñar, implementar, monitorizar y asegurar los sistemas operativos, los equipos, las redes y las aplicaciones. La arquitectura de seguridad define los controles usados para hacer cumplir los niveles de disponibilidad, integridad y confidencialidad.

Una arquitectura de seguridad completa abarca protección a varios niveles y contra amenazas accidentales e intencionales:

Protección del recurso humano: Ante amenazas físicas y lógicas

Protección de la infraestructura física: Ante amenazas físicas.

Protección de la red: Ante ataques pasivos y activos.

Protección de los servicios: Tanto internos como externos a la organización (evitar ataques desde dentro de la organización hacia servicios externos a la organización).

+ conceptos de seguridad

Evidencia digital

Es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.(Casey 2000)

Computación forense

Es la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación. (Kovacich 2000)

Cibercrimen

De acuerdo con CASEY.2000.

- Cualquier actividad criminal que involucra computadores y redes. En particular esta definición está orientada a revisar situaciones donde el computador de una red no fue usado para el crimen, sino que contiene evidencia digital relacionada con el crimen. - *ORIENTADA A LA EVIDENCIA*

De acuerdo con PARKER.1998. Pág.57:

- Toda actividad que conlleva un abuso (atentado contra *la* información, causando pérdida de utilidad, integridad y autenticidad) y mala utilización (atentado *con* la información, causando pérdida de disponibilidad, posesión y confidencialidad) de la información, asociada con el uso del conocimiento de sistemas de información o tecnologías informáticas. - *ORIENTADA AL DISCURSO LEGAL*

Delitos informáticos

Seguridad Física

El objetivo de la seguridad física es proporcionar un ambiente seguro para todos los activos e intereses de la organización, incluyendo las actividades del sistema de información.

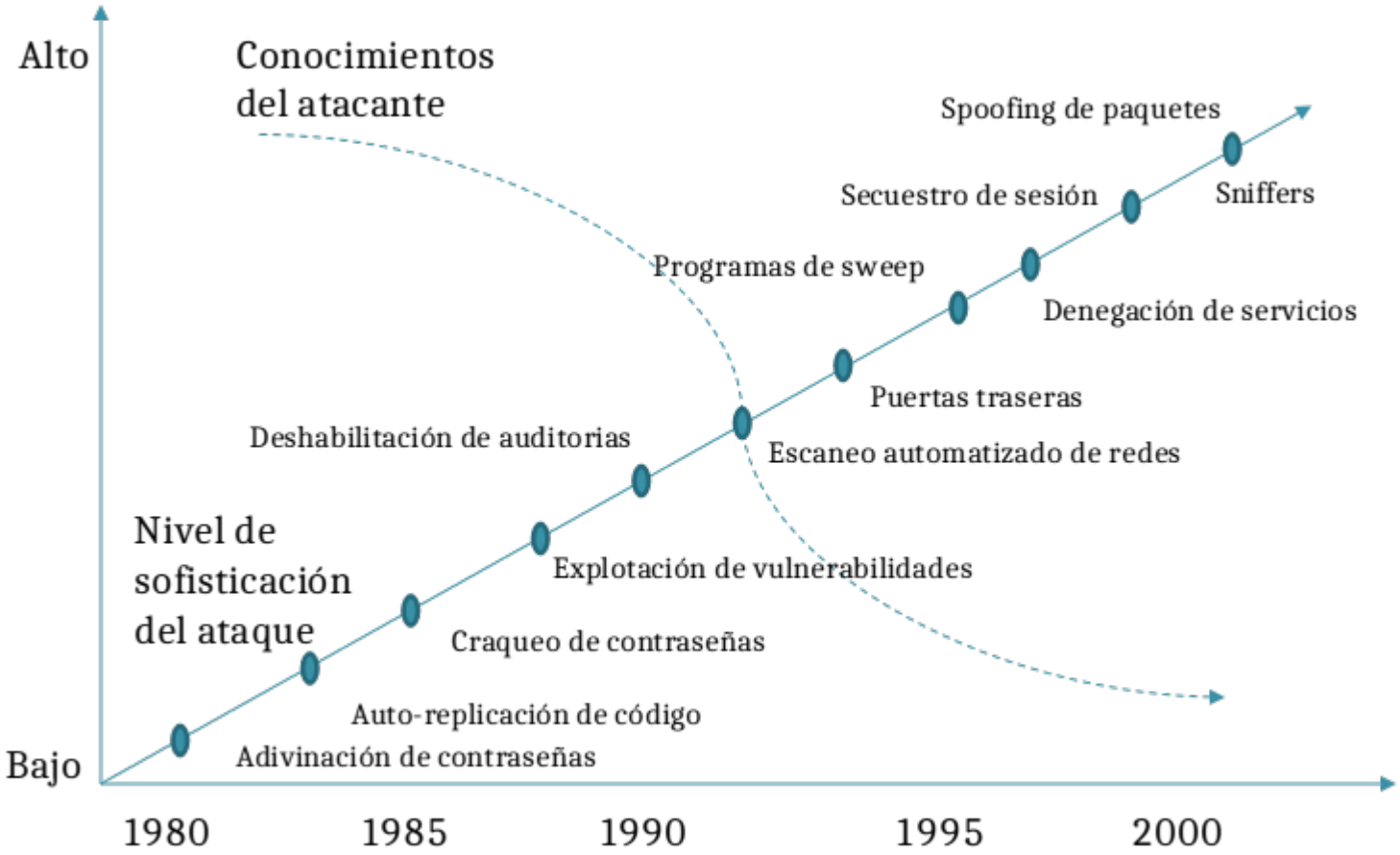
La seguridad física proporciona protección para los edificios o cualquier estructura (vehículos) que hospede el sistema u otros componentes de redes. Los sistemas son caracterizados como estáticos, móviles o portátiles.

Seguridad Lógica

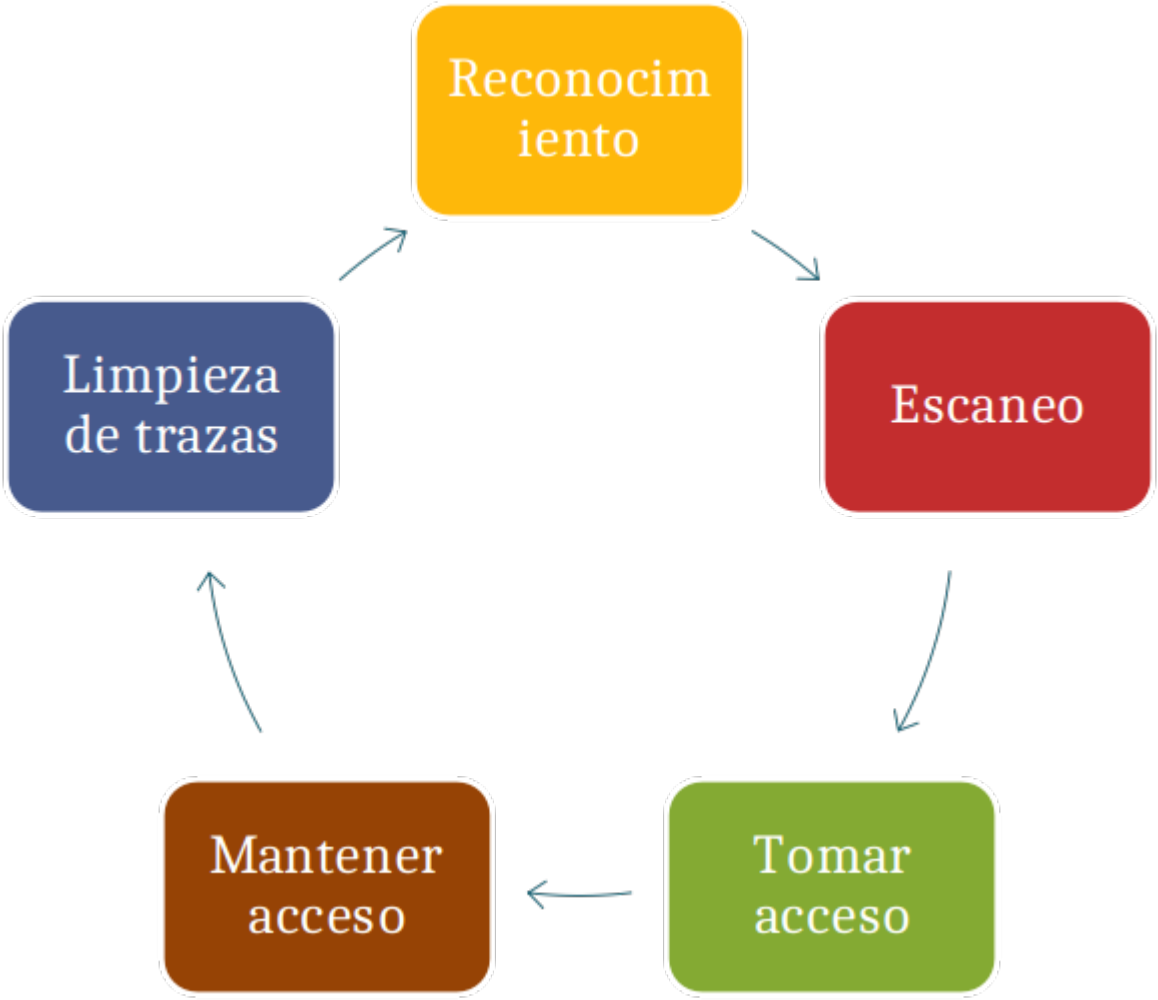
Los objetivos que se plantean para lograr la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Se disponga de pasos alternativos de emergencia para la transmisión de información.

Hackeo ético



Hackeo ético: fases del hackeo



Hackeo ético: reconocimiento

El reconocimiento en términos de hackeo se refiere al levantamiento de información de la víctima de forma metodológica. Normalmente, la fase de reconocimiento se refiere a la fase preparatoria en la que el hacker se documenta sobre su víctima, recolecta toda la información que le pueda ser útil sobre ella:

- Páginas web
- Correos electrónicos
- Dominios
- Hardware
- Software, Actualizaciones
- Compras, Ventas
- Socios
- Búsqueda de empleados

Hackeo ético: reconocimiento

El reconocimiento es una de las tres fases preparatorias al ataque. En estas 3 etapas el atacante puede gastar hasta el 90% de su tiempo.
Existen dos formas de hacer reconocimiento:

Pasivo: en este tipo de reconocimiento se busca información de la víctima sin hacer contacto directo con ella.

Por ejemplo: En los avisos de empleo se busca personal con calificaciones específicas como programadores web de java, python, php

Publicaciones de prensa en los que se anuncian proyectos: "La empresa xxx pionera en el uso de Microsoft Vista..."

Activo: en este tipo de reconocimiento el hacker hace contacto con la víctima, se utilizan principalmente técnicas de ingeniería social para obtener información de utilidad para el hacker, principalmente se usa la vía telefónica o correos electrónicos para obtener información de la misma.

Hackeo ético: reconocimiento

Conoce tu víctima...

Hackeemos con Google…

- Sólo usemos la filosofia de google

  Pones una palabra y encontrarás miles de respuestas

- Es una gigante base de datos que contiene casi todo lo que necesita
  - Consoliida gran cantidad de información
- ¿Quien lo usa?

Prácticamente…todos…

Estudiantes…

Empresarios…

Terroristas…

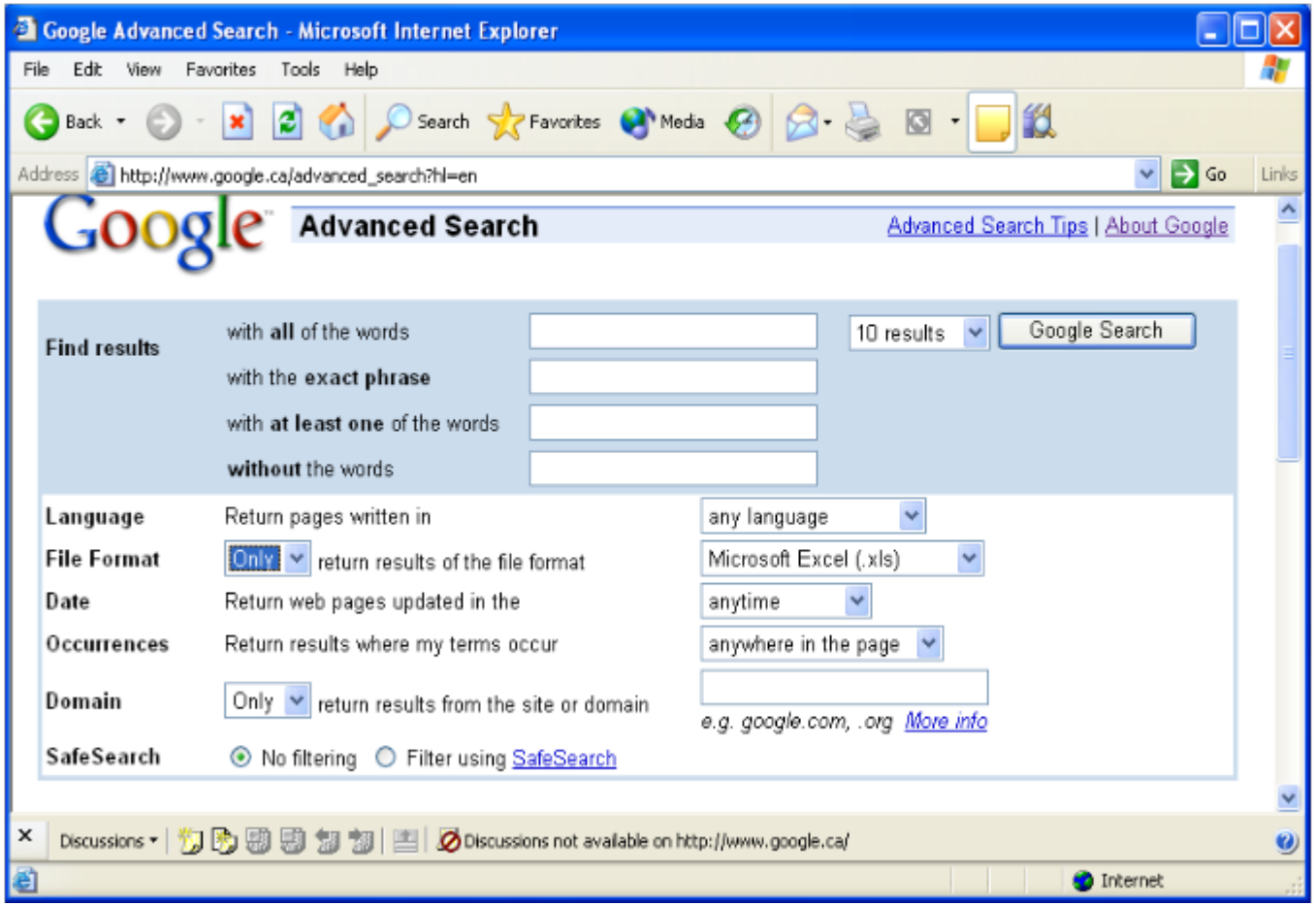
Hackers…

En un solo lugar puedes encontrar fotos, mapas, direcciones e información técnica.

Hackeo ético: reconocimiento

Conoce tu víctima...

Entremos a Google en búsqueda avanzada...



Hackeo ético: reconocimiento

Conoce tu víctima...

Entremos a Google en búsqueda avanzada…

- Los operadores de búsqueda en Google:

  Los operadores son utilizados para refinar las búsquedas. Lo que maximiza el valor de los resultados.

  Estos operadores son herramientas para el usuario común para el hacker son armas!

- Operadores básicos:

  +, -, ~ , ., *, “”, |, OR

- Operadores avanzados:

  allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores básicos

(+) fuerza la inclusión cosas comunes
Google normalmente ignora palabras comunes (dónde, cómo, cuándo, letras solas) por omisión
Por ejemplo: Star Wars Episode +I

(-) excluye el término en la búsqueda
Por ejemplo: manzana –roja

(“) utiliza comillas alrededor una frase exacta que desees buscar.
Por ejemplo: “Robert masse ”

Robert masse sin comillas “” da un resultado de 309.000, sin embargo, “robert masse” Sólo arroja 927 resultados. Reduce las respuesta irrelevantes un 99%

Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores básicos

(+) fuerza la inclusión cosas comunes
Google normalmente ignora palabras comunes (dónde, cómo, cuándo, letras solas) por omisión
Por ejemplo: Star Wars Episode +I

(-) excluye el término en la búsqueda
Por ejemplo: manzana –roja

(“) utiliza comillas alrededor una frase exacta que desees buscar.
Por ejemplo: “Robert masse ”
Robert masse sin comillas “” da un resultado de 309.000, sin embargo, “robert masse” Sólo arroja 927 resultados. Reduce las respuesta irrelevantes un 99%

(~) busca sinónimos:
Por ejemplo: ~comida
Da cómo resultado una búsqueda sobre términos similares: recetas, alimentos, etc.

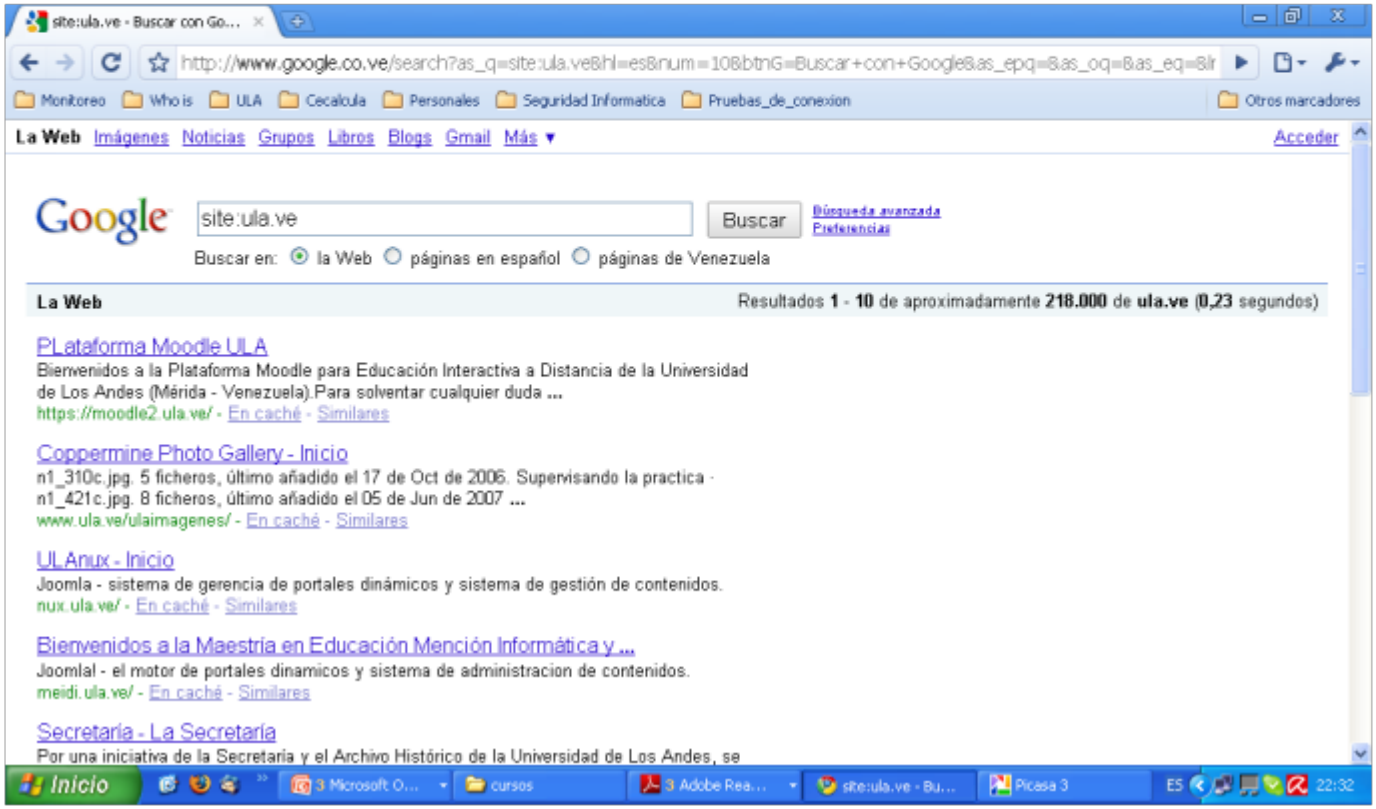
(.) carácter mágico:
Por ejemplo: m.trix
Da cómo resultado: M@trix, matrix, metrix.....
(*) palabra mágica...

Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores avanzados:

Site: nombre de dominio. Busca las páginas en ese dominio.
Por ejemplo:
Site:ve
Site:ula.ve
Site:www.ula.ve



Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores avanzados:

Filetype: tipo de extensión. Busca documentos con la extensión indicada.
Se pueden buscar las siguientes extensiones:

- HyperText Markup Language (html)
- Adobe Portable Document Format (pdf)
- Adobe PostScript (ps)
- Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
- Lotus WordPro (lwp)
- MacWrite (mw)
- Text (ans, txt)
- Microsoft PowerPoint (ppt)
- Microsoft Word (doc)
- Microsoft Works (wks, wps, wdb)
- Microsoft Excel (xls)
- Microsoft Write (wri)
- Rich Text Format (rtf)
- Shockwave Flash (swf)

También se puede buscar asp, php y cgi si son compatibles con el formato de texto.

Por ejemplo:

site:com.ve presupuesto filetype:xls

Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores avanzados:

Intitle: Busca en el título de la página web
Allintitle: buscador1, buscador2, buscador3 busca páginas web cuyo título contenga esos términos
Estas búsquedas son súper útiles para buscar listados de directorios...

Por ejemplo:
Intitle:Index.of"parent directory"

Inurl:buscador1 encuentra el término en la dirección de la página web
Allinurl: buscador1, buscador2, buscador3 busca en la dirección de la página web múltiple términos

Es muy útil para hackear!

Por ejemplo:
Inurl: cgi-bin
Allinurl:cgi-bin password

Hackeo ético: reconocimiento

Conoce tu víctima...

Operadores avanzados:

Intext: buscador1 Busca el término en cuerpo de un documento
Allintext: buscador1, buscador2, buscador3 busca múltiples términos en el cuerpo de un documento

Por ejemplo:
Intext: administrator
Allintext: administrator login

Cache: buscador1 Busca el término en un versión vieja de un website. Algunas veces aunque un sitio haya sido actualizado se puede encontrar información sensible en el Cache.

Por ejemplo:
Cache:www.gosecure.com

Hackeo ético: reconocimiento

Conoce tu víctima...

Algunas búsquedas de hackeo:

allintext:cédula cuenta tarjeta nro. filetype:xls

intext:cedula filetype:xls site:com.ve

intitle:index.of + mp3 + "grandaddy" -html -htm -php -asp -txt –pls

“index of cgi-bin”

Localización geográfica

Existen herramientas que luego de localizar las Ips que nos interesan que nos permiten localizar geográficamente estos equipos.

Las herramientas más comunes para ello son:

LACNIC www.lacnic.net
ARIN www.arin.net
RIPE www.ripe.net
APNIC www.apnic.net

Hackeo ético: reconocimiento

Conoce tu víctima...

Enlaces interesantes

www.archive.org
www.proxy4free.com
www.nuclearwintercrew.com
www.leetupload.com
www.securiteam.com
www.cybercrime.org
www.milw0rm.com
www.bladesoftware.com
www.websitewatcher.com
www.ethicalhacker.net
www.remote-exploit.org
http://www.phrack.org/
http://www.2600.org/
http://www.rootkit.com/
http://www.toorcon.org/2007/intro.php
http://www.openrce.org/
http://www.uninformed.org/
http://www.defcon.org/
http://www.blackhat.com/html/bh-blackpage/
http://www.shmoocon.org/
http://www.chebucto.ns.ca/~rakerman/trojan-
http://www.sans.org/resources/idfaq/oddports.
http://www.petri.co.il/trojan_ports_list.htm

Hackeo ético: reconocimiento

Conoce tu víctima...

Google APIS:

www.google.com/apis

Remove:

http://www.google.com/remove.html

Googledorks:

http://johnny.ihackstuff.com/

O'reilly Google Hack:

http://www.oreilly.com/catalog/googlehks/

Google Hack Presentation, Jonhnny Long:

http://johnny.ihackstuff.com/modules.php?op=modload&name=

ownloads&file=index&req=viewdownload&cid=1

"Autism: Using google to hack:

www.smart-dev.com/texts/google.txt

"Google: Net Hacker Tool du Jour:

http://www.wired.com/news/infostructure/0,1377,57897,00.html

Hackeo ético: reconocimiento

Escaneo

Objetivos:

1. Direcciones IP específicas
2. Sistemas operativos
3. Arquitectura de sistema
4. Servicios activos en cada equipo

Tipos de escaneo

De puertos

- Se envían mensajes para verificar qué servicios está corriendo

De redes

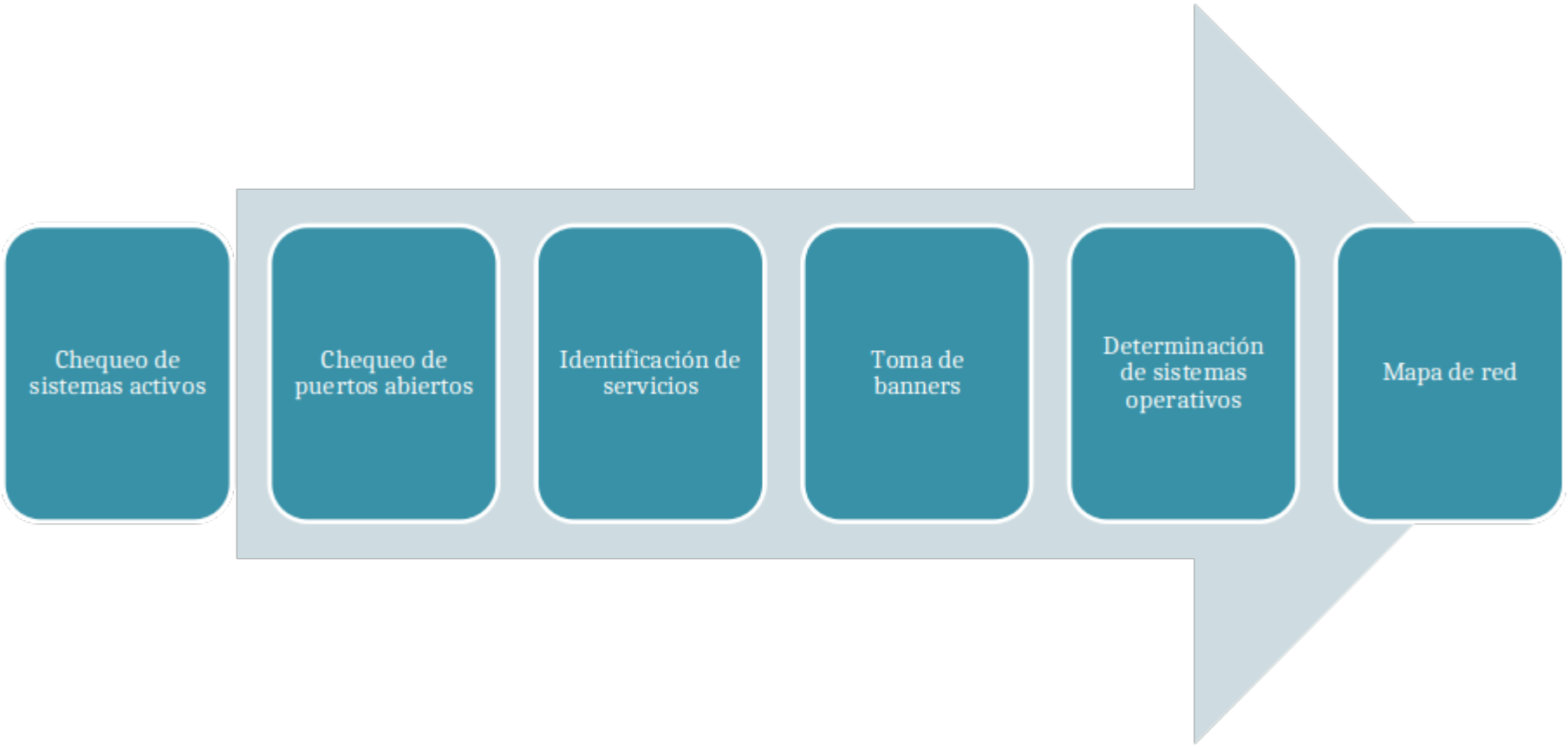
- Se utiliza para identificar los equipos activos en una red
- Se usa para atacarlas o para identificarlas

De vulnerabilidades

- Utiliza procesos automáticos de verificación de vulnerabilidades

Hackeo ético: reconocimiento

Escaneo



Hackeo ético: reconocimiento

Escaneo

Para realizar escaneo de red, determinación de puertos y sistemas operativos existe un conjunto de herramientas que veremos a continuación.

Normalmente la forma más rápida de escanear es realizando pruebas ICMP (ping) para obtener mejores resultados podemos modificar la opción -t

NMAP: es una herramienta de comando que permite realizar escaneo de puertos en un equipo o una red. NMAP se utiliza para: detección de sistemas operativos, detección de versiones, ping sweep y muchas otras técnicas de escaneo. Puede escanear muchos equipos en poco tiempo y en un línea de comando. Existen versiones de NMAP para múltiples sistemas operativos y posee múltiples variables para la realización de todos los tipos de pruebas a puertos, equipos o redes.

Métodos de escaneo en NMAP:

Xmas Tree: el atacante revisa chequea los servicios TCP de un equipo enviando paquetes Xmas.
Syn Stealth: se refiere al escaneo "medio abierto" cuando una conexión TCP no llega a abrirse.
Null Scan: es una forma avanzada de escaneo que permite evadir cortafuego.
ACK Scan: es utilizado para descubrir las reglas de un cortafuego.
Windows Scan: es similar al ACK Scan pero permite ver puertos.

Hackeo ético: reconocimiento

Escaneo

Repaso de banderas TCP:

Syncronize: también llamada "SYN" se utiliza para comenzar una conversación entre equipos.
Acknowledgement: también llamada "ACK" se utiliza para establecer una conversación entre equipos.
Push: también llamada "PSH" le indica al equipo que lo recibe que envíe de inmediato toda la data acumulada en buffer.
Urgent: también llamada "URG" le indica al equipo que lo recibe que la data contenida en el paquete debe ser procesada de inmediato.
Finish: también llamada "FIN" le indica al equipo que lo recibe que no habrá más paquetes que transmitir.
Reset: también llamada "RST" también le indica al equipo que lo recibe que no habrá más paquetes que transmitir.

Hackeo ético: reconocimiento

Escaneo

Tipos de escaneo con NMAP:

Syn Stealth o Half Open:
Primero se envia un paquete SYN a un puerto del equipo, lo que sugiere que se está solicitando una conexión, una respuesta es esperada...
Si el puerto está abierto enviará un paquete SYN/ACK. Por el contrario, si el puerto está cerrado enviará un paquete RST. Apenas se recibe el paquete SYN/ACK se responde con un RST para cortar la comunicación en lugar de un ACK que sería lo esperado en el protocolo de comunicación.

La ventaja de este tipo de escaneo es que muy pocos sitios registran este tipo de escaneo.

Xmas Scan:
Este tipo de escaneo sólo funciona con equipos con TCP/IP desarrollo de acuerdo al RFC 793 por lo tanto no funcionará con sistemas windows, si se realiza con windows la respuesta será que todos los puertos están cerrados.
El escaneo consiste en enviar un FIN/URG/PSH, si el puerto está abierto se recibirá NO RESPONSE...si el puerto está cerrado se recibirá un RST/ACK.

FIN Scan:
Este tipo de escaneo sólo funciona con equipos con TCP/IP desarrollo de acuerdo al RFC 793 por lo tanto no funcionará con sistemas windows, si se realiza con windows la respuesta será que todos los puertos están cerrados.
El escaneo consiste en enviar un FIN, si el puerto está abierto se recibirá NO RESPONSE...si el puerto está cerrado se recibirá un RST/ACK

Hackeo ético: reconocimiento

Escaneo

Tipos de escaneo con NMAP:

FIN Scan:
Este tipo de escaneo sólo funciona con equipos con TCP/IP desarrollo de acuerdo al RFC 793 por lo tanto no funcionará con sistemas windows, si se realiza con windows la respuesta será que todos los puertos están cerrados.
El escaneo consiste en enviar un FIN, si el puerto está abierto se recibirá NO RESPONSE...si el puerto está cerrado se recibirá un RST/ACK

NULL Scan:
Este tipo de escaneo sólo funciona con equipos con TCP/IP desarrollo de acuerdo al RFC 793 por lo tanto no funcionará con sistemas windows, si se realiza con windows la respuesta será que todos los puertos están cerrados.
El escaneo consiste en enviar un paquete sin banderas configuradas, si el puerto está abierto se recibirá NO RESPONSE...si el puerto está cerrado se recibirá un RST/ACK.

IDLE Scan:
Este tipo de escaneo inventado por un investigador de seguridad informática llamado Antirez, no envia paquetes a la equipo que se desea escanear. Por ello, se conoce como el escaneo completamente ciego. Se utiliza un equipo zombie que interactua con el equipo a escanear lo cual permite el anonimato de quien escanea.

Hackeo ético: reconocimiento

Escaneo

Tipos de escaneo con NMAP:

Window Scan:
Este escaneo es similar al ACK, excepto que a veces puede detectar puertos abiertos así como puertos filtrados/o sin filtros debido a una anomalía en el tamaño de la ventana TCP reportada por algunos sistemas operativos.

ICMP Echo Scan:
Esta opción no es realmente un tipo de escáneo dado que ICMP tiene abstracción de puertos, pero es útil para determinar qué equipos de una red están arriba haciendo ping.

List Scan:
Este tipo de escaneo simplemente genera e imprime la lista de Ips/nombres sin hacer ping o escaneo de puerto. En realidad se realiza una resolución de DNS.

Hackeo ético: reconocimiento

Escaneo

Opciones para ejecutar un NMAP:

-sT (TcpConnect)
-sS (SYN scan)
-sF (Fin Scan)
-sX (Xmas Scan)
-sN (Null Scan)
-sP (Ping Scan)
-sU (UDP scans)
-sO (Protocol Scan)
-sI (Idle Scan)
-sA (Ack Scan)
-sW (Window Scan)
-sR (RPC scan)
-sL (List/Dns Scan)
-P0 (don't ping)
-PT (TCP ping)
-PS (SYN ping)
-PI (ICMP ping)
-PB (= PT + PI)
-PP (ICMP timestamp)
-PM (ICMP netmask)

Hackeo ético: reconocimiento

Escaneo

Opciones para el formato de salida en NMAP:
-oN(ormal)
-oX(ml)
-oG(repable)
-oA(ll)

Opciones para el tiempo en NMAP:
-T Paranoid – serial scan & 300 sec wait
-T Sneaky - serialize scans & 15 sec wait
-T Polite - serialize scans & 0.4 sec wait
-T Normal – parallel scan
-T Aggressive- parallel scan & 300 sec timeout & 1.25 sec/probe
-T Insane - parallel scan & 75 sec timeout & 0.3 sec/probe
--host_timeout –max_rtt_timeout (default - 9000)
--min_rtt_timeout –initial_rtt_timeout (default – 6000)
--max_parallelism --scan_delay (between probes)

Opciones generales en NMAP:
--resume (scan) --append_output
-iL <*targets_filename*> -p <*port ranges*>
-F (Fast scan mode) -D <*decoy1 [,decoy2][,ME],*>
-S <*SRC_IP_Address*> -e <*interface*>
-g <*portnumber*> --*data_length* <*number*>
--randomize_hosts -O (OS fingerprinting) -I (dent-scan)
-f (fragmentation) -v (verbose) -h (help)
-n (no reverse lookup) -R (do reverse lookup)
-r (don't randomize port scan) -b <ftp relay host> (FTP bounce)

Hackeo ético: reconocimiento

Escaneo

Otras herramientas:

Angry IP: esta herramienta nos permite realizar escaneos a través de windows. Puede escanear cualquier rango de red. Simplemente realizar pings ICMP a los equipos de una red y determina cuales estás activos.
Provee información del BIOS de los equipos con los cuales podemos conocer el nombre del equipo, el grupo de trabajo del equipo y la dirección MAC.

HPING2: es una herramienta de comando, que trabaja en en cmd de windows. Soporta ICMP, UDP y TCP. Puede realizar traceroutes y tiene la habilidad de utilizar canales encubiertos. Nos ayuda a: probar cortafuegos, escaneo avanzado de puertos, pruebas de redes, fingerprint de sistemas operativos, etc.

Hping2 10.0.0.1 realiza un ping tcp con paquetes nulos al puerto cero del equipo 10.0.0.1
Hping2 10.0.0.1 -p 80 envia el paquete al puerto 80

Hackeo ético: reconocimiento

Escaneo

Mtr

Es una herramienta de diagnóstico combina la funcionalidad de un traceroute y la herramienta ping. Cuando mtr comienza a funcionar verifica las distintas conexiones entre el emisor y el host final. Para hacerlo utiliza paquetes con un ttl lento, notando los tiempos de respuesta en los diferentes IP del camino. Un repentino incremento en las pérdidas de paquetes es un indicio de un equipo con sobrecarga o en mal estado.

Opciones

-r--report
mtr se ejecutará por un número dado de cyclos en la opción –c e imprime las estadísticas de la calidad de la conexión al final .
Es importante destacar que cada ejecución de mtr incrementa el tráfico por lo que usarlo excesivamente puede generar problemas
-**COUNT--report-cycles** COUNT Esta opción se usa para definir el número de pings a realizar entre ambos equipos.
-s BYTES--psize BYTESPACKETSIZE estas opciones determinan el tamaño en bytes del paquete. Si se usa un número negativo utilizará tamaños

Hackeo ético: reconocimiento

Escaneo

Determinando el sistema operativo

La determinación de sistemas operativos puede realizarse de formas, pasiva y activamente.

Determinación activa: Basados en que los desarrolladores de los diferentes sistemas operativos manejan las pilas activas de distintas formas, se pueden construir paquetes especialmente armados y que son enviados al sistema y se verifica la respuesta a los mismos. Las respuestas se verifican con bases de datos para determinar cual sistema operativo tiene el sistema. Un cortafuegos registra los escaneos de toma de banners porque estás probando directamente el sistema.

Determinación pasiva: se refiere a escanear de forma indirecta el sistema para revelar el sistema operativo. Está basado en la implantación de pilas de distintas maneras y verificar cómo responde.
Utiliza técnicas de sniffing en lugar de escaneo. Es menos confiable que la determinación activa.

Hackeo ético: reconocimiento

Escaneo

Detección de vulnerabilidades

Los análisis de vulnerabilidades permiten localizar en el sistema de la víctima los posibles huecos del sistema por dónde el atacante pueda tomar control del equipo. El objetivo es determinar la vulnerabilidad, buscar un exploit específico para dicha vulnerabilidad y utilizarla en el sistema víctima.

Nessus: es un escaner de vulnerabilidades que busca huecos en el sistema software

Las características principales de Nessus son:

- Arquitectura Plug-in y cliente-servidor
- Utiliza un lenguaje de scripts que se llama NASL (Nessus Attack Scripting)
- Puede probar un número de equipos ilimitado simultaneamente.
- Posee una base de datos que puede ser actualizada fácilmente (como la de un antivirus).
- Posee una presentación con licencia gratuita.

LanGuard: es un escaner de vulnerabilidades que analiza desde el sistema operativo, las aplicaciones que se están ejecutando en una red y los huecos de seguridad presentes. Puede escanear redes completas, IP por IP, provee información tan específica cómo los niveles de parches en el equipos, los parches que no han sido actualizados, etc.

Hackeo ético: reconocimiento

Escaneo

Utilización de proxies

Proxy: es un servidor que puede ser utilizado cómo intermediario para conexiones con otros equipos. Son utilizados para diferentes propósitos:

- Cómo un cortafuego, un proxy proteje redes locales de acceso externo.
- Cómo servidor DHCP, un proxy permite dar conexión a Internet a múltiples equipos cuando se tiene una sola dirección IP.
- Los proxies también pueden ser utilizados para navegación anónima.
- Cómo filtro de contenido o material no requerido o autorizado.

Proxies gratuitos:

Los ataques que utilizan miles de proxies gratuitos son dificiles de verificar. Simplemente colocando “free proxies” en Google puedes encontrar lugares para conectarte y hacer más dificil que verifiquen quien realiza el ataque