Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECCIÓN 1
SER UN HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior Highschool students, and Highschool students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

AVISO

El proyecto Hacker Highschool es una herramienta de aprendizaje, y como tal existen riesgos. El mal uso de algunas lecciones puede terminar en daño físico. Existen riesgos adicionales ya que no existen estudios suficientes sobre los posibles efectos de las emisiones en algunas tecnologías. Los estudiantes que sigan estas lecciones deberían ser supervisados y motivados a aprenderlas, probarlas y utilizarlas. No obstante, ISECOM no acepta responsabilidad alguna por el mal uso de la información presentada.

Las siguientes lecciones y cuadernos de trabajo son abiertos y accesibles al público bajo los siguientes términos y condiciones de ISECOM:

Todas las obras del proyecto Hacker Highschool se proporcionan para su uso no comercial con estudiantes de escuelas primarias, secundaria y bachillerato ya sea en centros públicos, instituciones privada, o educación en casa. Este material no puede ser reproducido para su venta bajo ningún concepto. Impartir cualquier clase, formación o actividad con estos materiales cobrando por ello está expresamente prohibido sin la adquisición de una licencia, incluyendo cursos en escuelas, clases universitarias, cursos comerciales, cursos de verano, campamentos de informática, y similares. Para adquirir una licencia, visite la sección LICENCIA en la página web de Hacker Highschool en www.hackerhighschool.org/licensing.html.

El proyecto HHS es resultado del esfuerzo de una comunidad abierta. Si encuentra útil este proyecto, le pedimos que nos apoye mediante la compra de una licencia, una donación o patrocinio.

Table of Contents

For the Love of Hacking....5

¿Por qué ser un hacker?....7
Cómo hackear....9
Dos formas de obtener lo que quieres....9
Alimenta tu mente: Espionaje....10
Hackear para tomar control de tu mundo....11
El proceso de cuatro puntos....12
El proceso Eco (Echo)....13
Qué hackear....14
Enriquece tu mente: Clases y Canales....14
Enriquece tu mente: Porosidad....17
Recursos....18
Libros....18
Revistas y Periódicos....19
Enriquece tu mente: Especulación....21
Motores de búsqueda....22
Páginas web y Aplicaciones web....23
Zines....24
Blogs....25
Foros y Listas de correo....25
Grupos de noticias....26
Wikis....27
Redes sociales....27
Chat....28
P2P....29
Certificaciones....29
Seminarios y jornadas....30
Lecturas adicionales....31

Contributors

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Shaun Copplestone, ISECOM
Greg Playle, ISECOM
Jeff Cleveland, ISECOM
Simone Onofri, ISECOM
Tom Thomas, ISECOM
Alfonso Arjona, @alfonsoarjona.net
Adrian Crespo, madrid.crespo@gmail.com

ISECOM

For the Love of Hacking

Introducción de Pete Herzog

A pesar de lo que hayas podido escuchar sobre los hackers, lo cierto es que hacen algo muy, muy bien: investigar. Los hackers están motivados, son ingeniosos y creativos. Analizan a fondo el funcionamiento de las cosas, hasta el extremo de saber cómo tomar el control de ellas y transformarlas en algo diferente. Esto les permite rediseñar las grandes ideas porque llegan a conocer en profundidad su funcionamiento. Además no tienen miedo de cometer el mismo error dos veces, por una especie de curiosidad científica, para ver si este error siempre devuelve los mismos resultados. Por esta razón, los hackers no ven el fracaso como un error o una pérdida de tiempo, ya que cada error significa algo, y es algo nuevo que aprender. Estas son las características que necesita cualquier sociedad para progresar.

> *Muchas personas que han sido llamados hackers, especialmente por los medios de comunicación, o que se han metido en problemas por "hackear" no son, de hecho, hackers.*

Un hacker es una especie de científico experimental práctico, aunque a veces el término "científico loco" encaja mejor dado que, a diferencia de los científicos profesionales, se concentran en algo siguiendo una intuición en lugar de una hipótesis formal. Eso no es necesariamente algo malo. Muchas cosas interesantes se han descubierto o inventado por personas que no siguieron las convenciones aceptadas sobre lo que se conocía o se creía cierto en ese momento.

El matemático *Georg Cantor*, propuso nuevas ideas acerca del infinito y la teoría de conjuntos que indignaron a mucho de sus colegas matemáticos, hasta el extremo que uno de ellos definió sus ideas como "una grave infección" para las matemáticas.

Nikola Tesla es otra persona considerada como un "científico loco" en su época, pero sabía más acerca del comportamiento de la electricidad que cualquier otro. Diseñó el que fuera, posiblemente, el primer motor sin escobillas que funcionaba con corriente alterna, aunque es más conocido por el Efecto Tesla y las Bobinas Tesla.

También está *Ignaz Philipp Semmelweis,* quien descubrió que los médicos necesitaban lavarse las manos antes de tratar a su siguiente paciente para evitar la propagación de enfermedades. Se preguntó si las enfermedades que perseguían a sus pacientes tras sus visitas eran por su culpa, así que decidió probar a lavarse las manos entre consultas, y por supuesto la transmisión desapareció. Sus ideas iban en contra tanto de las convenciones científicas sobre lo que era conocido en su tiempo acerca de los gérmenes (nada), como de la comodidad de los doctores que sentían que era demasiado problema estar lavándose las manos continuamente.

Puedes pensar que lo que sabes acerca de los hackers es que entran en los ordenadores de otros y toman el control de las cuentas de otras personas. Pueden leer tu correo sin que lo sepas. Pueden observarte a través de tu webcam sin tu permiso y verte y oírte en la supuesta intimidad de tu hogar. No es mentira.

Algunos hackers ven la seguridad de las redes simplemente como otro reto, así que trabajan con formas de engañar al sistema, pero lo que intentan hacer en realidad es pensar como si fueran los instaladores de la red o su diseñador. Averiguan tanto de la red como pueden: de dónde toma sus instrucciones, las reglas que usa, cómo interaccionan con el sistema operativo y con otros sistemas a su alrededor, qué usuarios tienen acceso a ella y sobre los administradores que la gestionan. Entonces usan esa información para probar diversas maneras de obtener lo que quieren. Este tipo de hacking puede ser muy beneficioso para el mundo, ya que permite aprender cómo estar más seguro e incluso desarrollar una tecnología mejor.

Desafortunadamente, algunas veces el hacking se lleva a cabo por criminales, y lo que hacen es ilegal, invasivo y destructivo. Y son estos sobre los que habitualmente lees en las noticias.

Un hacker no es alguien que publica en la cuenta de otro que se ha dejado su página de una red social abierta, o **espía por encima del hombro** las contraseñas para conectarse a la cuenta más tarde. Eso no es hacking. Un hacker tampoco es alguien de descarga una herramienta para **script kiddies** con objeto de entrar en el correo de otras personas. Esos no son hackers: son ladrones y delincuentes.

El Hacking es investigar. ¿Has intentado alguna vez hacer algo una y otra vez de diferentes maneras hasta obtener lo que querías? ¿Has abierto alguna vez un aparato o dispositivo para ver cómo funciona, investigar cuáles son sus componentes, y ajustarlos de forma que lo haga de forma distinta? Eso es hacking. Estás hackeando cuando examinas detenidamente cómo funciona algo con el fin de manipularlo de forma creativa y conseguir que haga lo que tú quieres.

Lo que ocurre es que en la forma en que está diseñado Internet, y la gran cantidad de aplicaciones, sistemas, dispositivos y procesos que existen en ella, es el lugar más habitual para encontrar hackers. Se podría decir que fue construido por hackers, así que es su mejor patio de recreo. Pero no es el único sitio. Puedes encontrar grandes hackers en prácticamente cualquier campo o industria, y todos tienen una cosa en común: dedican tiempo a aprender cómo funcionan las cosas, por lo que pueden hacer que funcionen de una forma nueva. No miran a algo como lo hacen sus diseñadores originales, sino como algo con mayor o mejor potencial para ello, y lo hackean para convertirlo en algo nuevo.

No pienses que puedes ser un gran hacker. Sólo si haces grandes hacks con mucha humildad puedes ser grande.

El hacking "per se" no es ilegal. O por lo menos no más ilegal que tirar una piedra. Todo depende de las intenciones. Si tiras una piedra y tu intención es herir a alguien, es un delito. Si no intentas herir a nadie, pero alguien se hace daño, puede que no sea un delito, pero eres responsable de tus acciones y tendrás que pagar una indemnización. Un proyecto de ISECOM llamado **Hacker Profiling Project** encontró que la mayoría de los daños provocados por el hacking se deben a hackers jóvenes e inexpertos que dañan la propiedad ajena accidentalmente. Sería algo parecido a tirar piedras en la calle por

diversión, pero abollando coches y rompiendo ventanas en el proceso. Puede que el daño no sea intencionado, pero puedes estar seguro de que serás declarado culpable y tendrás que pagar por ello. Así que ten cuidado cuando hackees cerca de la propiedad de otros. Es mejor que hackees tus propias pertenencias.

Puede ser ilegal hackear algo que compraste y te pertenece. Hay hackers que han sido condenados por hackear sus propios dispositivos y ordenadores. Otros hackearon programas, música y películas que compraron, y fueron perseguidos por ello. Para ser más exactos, puede que no estés autorizado a hackear software que has adquirido, incluso si sólo lo haces para comprobar que es suficientemente seguro para ejecutarse en tu ordenador. Esto es debido a que muchas de las cosas que compras pueden venir con un contrato o **End User License Agreement (EULA)** que dice que no puedes. Y te comprometes a ello cuando abres o instalas el producto, incluso si no puedes leerlo hasta que hayas abierto o instalado el producto. Ten esto en cuenta cuando practiques tus habilidades de hacking en la privacidad de tu hogar sobre las cosas que hayas comprado.

¿Por qué ser un hacker?

Piensa en los científicos que hicieron el mapa del genoma humano: usaron un método desarrollado para decodificar contraseñas. Las contraseñas se almacenan habitualmente encriptadas, para que sean difíciles de robar. La técnica "Hierarchical shotgun **brute-forcing"** es una forma de desencriptar contraseñas **crackeando** su encriptación: se rompe el **hash** encriptado de la contraseña, se descifran unos pocos caracteres en cada paso, y luego se une todo de nuevo. Los investigadores del genoma adaptaron la misma técnica para cartografiar los 3.300 millones de pares del genoma humano.

El hacking apareció en la cocina cuando los chefs empezaron a usar nitrógeno líquido como agente congelante para hacer el helado perfecto, o cuando hackean la comida para hacer chips de tomate con salsa de patata en lugar de ketchup, o simplemente cuando necesitaban hacer algo para lo que no tenían las herramientas adecuadas...

Los químicos han estado hackeando elementos y compuestos durante siglos. Por naturaleza, las moléculas son tan selectivas en su comportamiento en diferentes ambientes (calor, frio, en las montañas o en las profundidades del océano) que los químicos necesitan comprender en profundidad las propiedades de las sustancias que emplean, para poder hackearlas y convertirlas en las que necesitan. En ningún otro lugar esto resulta más evidente que en la creación de nuevos productos farmacéuticos, donde cientos de plantas de una región se estudian por sus propiedades químicas, de la raíz a los frutos, se extraen los compuestos y se combinan con otros para obtener nuevos medicamentos. Luego lo intentan una y otra vez, a veces durante años, hasta obtener la combinación correcta y conseguir que hagan lo que ellos quieren.

El hacking se utiliza en los negocios para entender un mercado o los hábitos de compra de ciertos tipos de consumidores. Investigan a fondo las fuerzas que impulsan el área de negocios de su interés, y luego intentan cambiarlas o influir en ellas para que hagan lo que ellos quieren. A veces hackean el producto, y otras te hackean a ti (con la publicidad y el **priming**, algo con lo que trabajarás en la lección de Ingeniería Social).

El hacking también se ha convertido en una parte cada vez más importante en las guerras. Hay soldados altamente preparados que son ingeniosos y creativos cumpliendo con sus objetivos, que es justo lo que hacen los hackers. Los criptógrafos, analistas de inteligencia y agentes de campo emplean lo que son básicamente habilidades de hacking para averiguar qué tiene el enemigo, lo que está haciendo y cómo tomar ventaja de cualquier debilidad en su equipamiento. A medida que más países dependen de los ordenadores y las redes, el uso del hacking para ataques cibernéticos y oara la defensa se ha convertido en una parte muy importante para las Fuerzas Armadas y las operaciones de inteligencia de una nación. ¡Los organismos nacionales e internacionales de seguridad acuden incluso a convenciones de hackers para reclutarlos!

La verdadera razón para ser un hacker es porque es algo realmente importante. Cuando tengas habilidades sólidas de hacking, podrás hacer cosas muy interesantes. Cualquier conocimiento avanzado te proporciona un gran poder. Si sabes cómo funciona algo hasta el extremo de poder tomar su control, entonces tienes un serio poder a tu disposición. Sobre todo, tienes el poder de protegerte y proteger a tus seres queridos.

La vida de la gente está cada vez más presente en Internet, como hacer amistades, encontrar trabajo o ganar dinero. La información puede ser muy valiosa (o peligrosa) y los hackers pueden protegerse a sí mismos mejor que nadie. Pueden investigar lo que ocurre con su información. Pueden asegurarse de revelar sólo lo que ellos desean y, por lo general, mantenerse más seguros y con mayor privacidad. Esto es una gran ventaja competitiva en la escuela, el trabajo y la vida, porque incluso la menor imagen negativa será utilizada en tu contra. Puedes estar seguro de eso.

Hackea todo, pero no dañes a nadie.

Cómo hackear

Contarte cómo hackear es como explicarte la forma de hacer un salto mortal de espaldas en una barra fija: no importa lo detallada que sea la explicación, que no serás capaz de conseguirlo a la primera. Necesitas desarrollar las habilidades, los sentidos y la intuición mediante la práctica o te darás un buen golpe. Pero hay algunas cosas que podemos contarte para ayudarte, y que te animarán a seguir practicando.

En primer lugar, deberías conocer algunos secretillos sobre cómo funciona el hacking. Vamos a tomar estos de **OSSTMM** (www.osstmm.org). Los hackers lo pronuncian "ous-tem". OSSTMM son las siglas de **Open Source Security Testing Methodology Manual** (Manual de Metodología Abierta de Pruebas de Seguridad), y aunque pueda parecerte el manual de un reproductor de DVD, es el principal documento que utilizan muchos hackers profesionales para planificar y ejecutar ataques y defensas. Dentro de ese manual encontrarás algunas joyas que te abrirán los ojos.

Dos formas de obtener lo que quieres

Por ejemplo, debes saber que hay dos formas de robar algo: hacerlo por ti mismo, o que alguien lo haga por ti y te lo entregue. Esto significa que esta acción requiere de la **interacción** entre la persona y el objeto. Obvio ¿cierto? Pero piénsalo un poco más: eso significa que todos los mecanismos de protección intentarán evitar que alguien interactúe con el objeto que están protegiendo. A menos que guardes todo bajo llave en una caja fuerte, no podrás evitar todas las interacciones. Las tiendas necesitan poner sus artículos en estanterías para que los compradores puedan tocarlas. Las empresas necesitan enviar información usando clientes de correo, que se conectarán a servidores de correo y la enviarán a otros servidores.

Todo esto son interacciones. Algunas de estas interacciones se dan entre personas y cosas que son conocidas entre si, por lo que llamamos a estas interacciones **Confianzas**. Cuando las interacciones se dan entre personas o sistemas desconocidos, las llamamos **Accesos**. Puedes usar un acceso para robar lo que quieres por ti mismo, o puedes engañar a alguien que sea conocido por el objetivo para que tome lo que quieres y te lo entregue. Si lo piensas un momento, esto significa que la seguridad significa proteger algo tanto de alguien desconocido, como de alguien que conoces y en quien confías.

Ejercicios

1.1 ¿Qué tipo de interacción se da al utilizar un motor de búsquedas? Piénsalo cuidadosamente: ¿Alguien da acceso? ¿Alguien da confianza?

1.2 Pon un ejemplo sencillo sobre usar Acceso y Confianza para robar una bicicleta encadenada a un soporte.

1.3 Da un ejemplo sencillo de cómo se puede utilizar Acceso y Confianza para iniciar sesión en el webmail de otra persona.

Alimenta tu mente: Espionaje

Cuando el hacking se utiliza en contra de un gobierno extranjero para cometer actos criminales de incursión, allanamiento, robo o destrucción y conseguir ventajas en información política o militar, se llama **espionaje**. Pero cuando el hacking se hace desde una empresa extranjera contra otra en un país distinto para obtener ventajas en los negocios, se llama **espionaje económico**.

Cuando el hacking se emplea para obtener información personal y privada sobre alguien con el objetivo acosarlo y humillarlo públicamente, se denomina **DoXing**. Si se busca información pública sobre una persona o una empresa para un ataque, pero no se cometen delitos para obtenerla, se denomina **document grinding** u **OSInt (Open Source Intelligence)**.

Cuando el hacking se emplea para entender el funcionamiento de la red de una empresa, sus sistemas, aplicaciones y dispositivos para atacarla, pero sin allanar o entrar en sus sistemas, se le llama **network surveying (topografiar la red).**

Cuando el hacking se emplea para entender mejor a un competidor sin quebrantar las leyes (a pesar de que lo que se haga pueda considerarse malo u ofensivo) se le llama **inteligencia competitiva.**

Posiblemente te mueras de ganas por saber qué clase de cosas malas u ofensivas siguen siendo legales. Piensa por ejemplo en infligir estrés o preocupación a alguien para obtener información. Mientras no le mates, mentirle sigue siendo legal (aunque hay leyes sobre provocar el pánico en lugares públicos, como gritar "¡Fuego!" en un cine lleno de espectadores cuando no lo hay).

Imagina que el hacker quiere saber dónde planea instalar una nueva fábrica una empresa. Utilizará document grinding para encontrar qué personas están en los puestos clave para tomar la decisión. Entonces el hacker llamará a sus oficinas para averiguar qué ciudades han visitado, y posiblemente también qué fábricas. Pero, por supuesto, eso es información confidencial de la compañía, y nadie puede contarlo sin dar señales de aviso. Así que el hacker necesita sonsacarles la información. No es difícil imaginarse el proceso:

> Hacker: Hola, soy el Doctor Jones; le llamo desde la escuela de su hija Nancy.
>
> Víctima: ¿En serio? ¿Qué ha hecho ahora?
>
> Hacker: Bueno, tiene una hemorragia nasal persistente que no podemos detener. Me gustaría preguntarle si ha estado expuesta a algún producto químico, como los que se emplean en las fábricas. Los síntomas que presenta son raros, excepto en personas que han estado expuestas a este tipo de productos. ¿Me puede decir algo?
>
> Víctima: (lo cuenta todo)

En muchos sitios, hacer esto no es ilegal, pero causa un estrés innecesario. Por no mencionar que lo que acaba de hacer ha preocupado a un padre.

Hackear para tomar control de tu mundo

Hacking no consiste sólo en interacciones. Lo sabes. Algunas personas dicen que la política es interacción, Puede ser. Pero posiblemente pensaste que el hacking es romper la seguridad. A veces lo es. En realidad se trata de tomar el control de algo o cambiarlo. Comprender las interacciones y su significado en el mundo real, empleando los términos básicos que hemos analizado, es útil cuando estás intentado infiltrarte, descubrir o incluso inventar. ¿Por qué querrías hacer esto? Para tener la libertad de conseguir que algo que posees haga lo que quieres. Y para evitar que otros cambien algo tuyo en nombre de lo que algunos llamarían seguridad (pero no somos ese tipo de personas).

A veces compras algo y la empresa a la que lo compraste intentará, a la fuerza o sigilosamente, que no puedas personalizarlo o modificarlo más allá de sus reglas. Y podemos estar de acuerdo con eso, siempre y cuando aceptes el hecho de que si lo rompes, entonces no se puedes esperar que te lo reparen o reemplacen. Así que hackear algo de tu propiedad lo hace, sin lugar a dudas, aún más tuyo de manera irreversible. Algo tan aterrador como le puede sonar a algunos tiene, sin duda, sus ventajas. Especialmente si necesitas mantener a otros lejos de tus pertenencias.

Para muchas, muchas personas (podríamos poner más veces el adverbio "muchas" para indicar que en realidad queremos decir "infinitamente muchísimas muchas más"), la seguridad es colocar un producto en un lugar, en el cual hay una cerradura, alarma, firewall o cualquier otra cosa que la mantenga segura. Pero en ocasiones estos productos no funcionan tan bien como deberían, o vienen con sus propios problemas que incrementan tu **Superficie de ataque** (Attack Surface), cuando un producto de seguridad debería reducirla. (La "Superficie de ataque" son todas las formas y todas la interacciones que permiten que algo o alguien sea atacado). Y buena suerte cuando adquieras ese producto mejorado para su comercialización masiva, y tengas que pagar periódicamente por su uso y hacer crowd-sourcing; lo compraste tal cual es, y tendrás que vivir con eso. Por eso hackeas tu seguridad. Necesitas analizarla y averiguar dónde falla y saber cómo cambiarla para que funcione mejor. Después, ¡deberías hackearlo un poco más para evitar que la compañía a la cual se lo compraste vuelva a ponerlo en su configuración por defecto!

Así que cuando pienses en el hacking como una forma de romper la seguridad, recuerda que eso sólo es un área de aplicación, porque sin la posibilidad de hacerlo, deberás rendirte y entregar parte de tu libertad y privacidad; y eso no es algo que quieras hacer. (Y puede ser que ahora no te importen ciertas cosas que dices o que envías, pero Internet tiene una gran memoria que mejora con el tiempo y ayuda a otros a recuperar esos recuerdos sobre ti. Lo que ocurre en la Red, se queda en la Red. Así que piensa en el futuro, incluso si hoy no te importa).

Ahora que comprendes el concepto de interacción, vamos a entrar en más detalles. Conoces los tipos básicos de interacciones como Acceso y Confianza, pero ¿Has oído hablar de la **Visibilidad**? Es el tercer tipo de interacción. Es tan potente como los otros dos. En lenguaje policial, se resume como *oportunidad* pero en hacking se trata más de saber si hay algo sobre lo que interactuar o no. Esta interacción trae consigo un montón de nuevas técnicas de seguridad como el engaño, la ilusión, el camuflaje, ¡y todas las nuevas técnicas de hacking para evitar y evadir las medidas de seguridad!

Cuando al famoso ladrón de bancos Jesse James se le preguntó por qué robaba bancos, dijo que porque es ahí donde está el dinero. Lo que quería decir es que a través de la visibilidad sabía qué bancos tenían dinero, además de otras cosas que podía robar o no. Los bancos tienen visibilidad: la gente sabe cuáles son los bienes que poseen. Pero no todo tiene Visibilidad. Es un hecho que la Privacidad es lo opuesto a la Visibilidad, y es una forma eficaz de evitar ser un blanco. Ya sea en calles peligrosas, en la jungla, o en Internet, mantener una baja **Exposición** y evitar la visibilidad es una forma de evitar ser atacado en primer lugar.

Ejercicios

1.4 Internet es conocido por crear mitos y perpetuar historias falsas durante tanto tiempo que es difícil saber qué información es real y cual es un hoax. Así que si quieres ser un buen hacker, adquiere la costumbre de revisar los hechos y aprender la verdad acerca de las cosas. Por este motivo, vas a buscar si Jesse James dijo eso realmente. Y no te quedes con la respuesta corta que aparece en el primer resultado que encuentres. Investiga un poco.

Ahora que te estas acostumbrando a investigar las cosas, encuentra la verdad sobre estos hechos aceptados:

1.5 La palabra "Iglú" viene del idioma Inuit. ¿Qué significa en realidad? ¿Qué tipo de interacciones usas para encontrar su significado?

1.6 Muchos padres afirman que el azúcar vuelve hiperactivos a los niños pequeños. ¿Qué hay de verdad en eso? ¿Qué interacciones se producen realmente en sus tripitas cuando los niños comen muchos dulces o alimentos azucarados que les incitan a hacer tonterías y ser hiperactivos?

1.7 También habrás escuchado que el azúcar agujerea los dientes (caries), pero ¿Cuál es la interacción real que tiene lugar? ¿Qué causa en realidad la caries?Si no es el azúcar, entonces ¿Qué es? Puntos extra si puedes explicar que cepillarse los dientes es una interacción para luchar con la causa real del problema, y encuentras el nombre de al menos un producto químico que ataca la raíz del problema (una pista: no es el Flúor)

El proceso de cuatro puntos

Cuando unes los tres tipos de interacciones, tienes **Porosidad**, la base de un Ataque de superficie. Tal y como indica la palabra, se trata de los poros o "agujeros" en las defensas que necesitas tener para que puedan darse las interacciones necesarias (así como cualquier otra posible interacción desconocida o innecesaria que se produce). Por ejemplo, una tienda sigue teniendo que poner los productos en estantes para que la gente los pueda tocar, ponerlos en una cesta y comprarlos. Son las interacciones que se necesitan para vender las cosas. Pero podrían no ser conscientes de los empleados que están escondiendo material en el área de carga y descarga, y eso es una interacción que no quieren.

La porosidad es algo que necesitas conocer para protegerte o atacar algún objetivo. Pero no es suficiente para analizar algo para poder hackearlo. Para hacer esto, necesitas conocer más profundamente los tres tipos de interacciones que acabas de aprender. Ese es otro pequeño secreto de OSSTMM y se llama **Proceso de Cuatro Puntos(FPP o Four Points Process)**. Este describe cuatro formas en las que estas interacciones se utilizan para analizar algo tan profundamente como sea posible, y por analizar se entiende pasar tiempo con ello para que podamos observarlo y ver qué hace.

El proceso Eco (Echo)

Hemos crecido descubriendo y aprendiendo cosas interactuando directamente con ellas. Los niños pequeños pinchan con un palito una ardilla seca para ver si está muerta. Esto se conoce como el **Proceso de Eco**. Es la forma más simple e inmadura de análisis. Al igual que gritar en una cueva y escuchar la respuesta, el proceso de eco requiere lanzar diferentes tipos de interacciones de acceso sobre un blanco y luego vigilar sus reacciones para averiguar las formas en las que puedes interaccionar con él. El proceso de eco es un proceso de verificación de tipo causa y efecto.

Esto es una forma un tanto extraña de probar algo, porque a pesar de ser un test muy rápido, no es muy preciso. Por ejemplo, cuando se utiliza el proceso de eco en pruebas de seguridad, un objetivo que no responde se considera seguro. Sería lo mismo que no tener Visibilidad. Pero también sabemos que sólo porque algo no responda a un tipo particular de interacción, no tiene que considerarse "seguro". Si esto fuera cierto, los depredadores no matarían a las zarigüeyas cuando estas se hacen las muertas y todo el mundo estaría a salvo de ataques de osos con sólo pasar miedo. Pero eso no es cierto. Evitar la visibilidad puede ayudar a sobrevivir a algunos tipos de interacciones, pero desde luego no a todos.

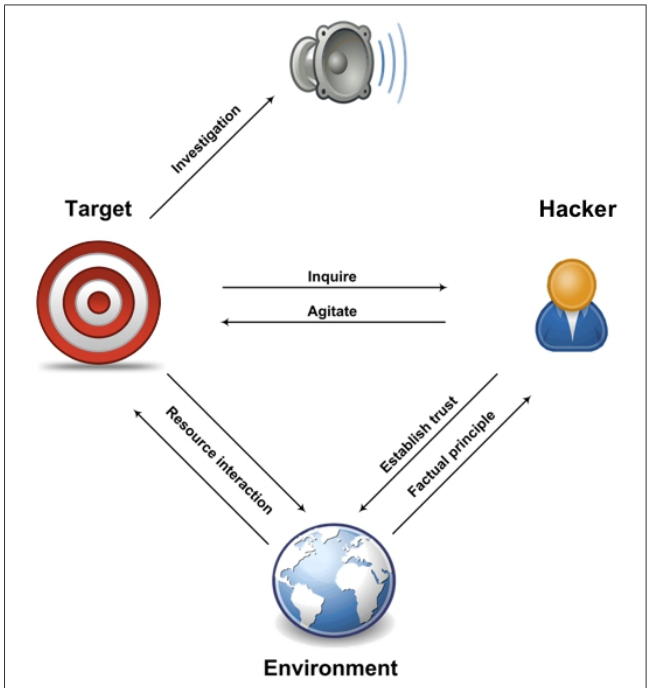

Figure 1.1: The Four Point Process

Por desgracia, la realidad es que la mayoría de las formas que utilizan las personas para investigar las cosas en su vida diaria se basan únicamente en el proceso de eco. Pero se pierde tanta información con este tipo de análisis unidimensionales que deberíamos agradecer que la industria de la salud haya evolucionado más allá del método de diagnóstico "¿Te duele si hago esto?". Si los hospitales usaran el proceso de eco para determinar la salud de una persona, en raras ocasiones podrían ayudar a la gente. Pero mirándolo por el lado bueno, las estancias en las salas de espera serían muy, muy cortas. Por eso algunos médicos, muchos científicos y especialmente los hackers utilizan el Proceso de Cuatro Puntos para asegurarse de no perder nada.

El Proceso de Cuatro Puntos te hace mirar las interacciones de la siguiente manera:

1. **Inducción (Induction)**: ¿Qué podemos decir del objetivo a partir de su entorno? ¿Cómo se comporta en ese entorno? Si el objetivo no se ve influido por el entorno, también es interesante.
2. **Investigación (Inquest)**: ¿Qué señales (emanaciones) emite el objetivo? Investiga cualquier rastro o indicador de esas emanaciones. Un sistema o proceso deja por lo general una firma de sus interacciones con el entorno.

3. **Interacción (Interaction)**: ¿Qué pasa cuando lo investigas? Este punto requiere hacer test de eco, incluyendo las interacciones esperadas e inesperadas con el blanco, para provocar respuestas.
4. **Intervención (Intervention)**: ¿Cuánto puedes forzarlo antes de romperlo? Interponte entre el blanco y los recursos que necesita, como la electricidad, o entrométete en sus interacciones con otros sistemas para saber cual es el rango en el que puede seguir funcionando.

Volviendo a nuestro ejemplo del hospital... las cuatro fases del FPP serían parecidas a estas:

1. La función de **interacción** es el proceso de hecho en el cual el doctor examina a los pacientes, habla con ellos, comprueba sus reflejos en codos y rodillas, y usa otras herramientas del tipo "¿Te duele si hago esto?"
2. La **investigación**, la cual consiste en leer **emanaciones** del paciente como el pulso, la presión sanguínea o las ondas cerebrales..
3. La **intervención** sería alterar o excitar la homeostasis del paciente, su comportamiento, rutinas o nivel de confort para ver que si desencadena algo malo.
4. Y finalmente la **inducción**, la cual examina el entorno, los lugares en que estuvo el paciente antes de enfermar y cómo han podido afectarle. Cosas como qué ha tocado, comido, bebido o respirado.

Ejercicio

1.8 Como has visto, el Proceso de Cuatro Puntos (FPP) te permite investigar en profundidad las interacciones. Ahora prueba tú: Explica cómo puedes utilizar el Proceso de Cuatro Puntos para saber si un reloj funciona (y si lo hace correctamente, dando la hora exacta)

Qué hackear

Cuando estás hackeando, debes establecer unas reglas mínimas. Necesitas el lenguaje y los conceptos para saber que estas hackeando. El **Alcance** (Scope) o **Ámbito de aplicación** es un término que utilizamos para describir el posible total del entorno operativo, y consiste en todas las interacciones que posee lo que vas a hackear.

Enriquece tu mente: Clases y Canales

En terminología profesional (algo muy útil para los hacker), el Alcance se compone de tres **Clases** y se divide en cinco **Canales**:

Clases	Canales
Seguridad Física	Humano

(PHYSSEC)	Físico
Seguridad del espectro (SPECSEC)	Wireless
Seguridad de las comunicaciones (COMSEC)	Telecomunicaciones
	Redes de datos

No deberías preocuparte por las **Clases**, pero debes saber que son las etiquetas oficiales usadas en la actualidad por las industrias de seguridad, gobierno y militar. Las clases definen un área de estudio, investigación u operación. Así que si estás buscando más información sobre cualquier asunto, es bueno que sepas cómo lo llaman los profesionales.

Los **Canales** son la terminología común para referirse a las formas en las que interaccionas con los Activos. No es raro hackear un dispositivo usando el Proceso de Cuatro Puntos sobre cada Canal. Si, puede parecer mucho trabajo, pero piensa en lo emocionante que es descubrir una forma de hacerlo funcionar que no aparece en el manual, o mejor incluso: ¡que ni siquiera sabe el fabricante!

Un **Activo** puede ser cualquier cosa que tenga valor para su propietario. Puede tratarse de una propiedad física como el oro, las personas, unos planos, un portátil, la típica señal telefónica en una frecuencia de 900MHz, el dinero, o bienes intelectuales como información personal, una relación, una marca, un proceso de negocios, contraseñas o algo que se dijo sobre la señal telefónica en los 900MHz.

Las **Dependencias** son aquellas cosas que están fuera de la capacidad del propietario de proporcionarlas de forma independiente. Por ejemplo, no muchos propietarios de computadores generan su propia electricidad. Aunque no sea probable que alguien vaya a cortarte el suministro eléctrico, eso es algo que todavía se encuentra dentro de tu ámbito de aplicación.

El objetivo de la seguridad es la **Separación** entre un activo y sus dependencias, y cualquier amenaza para ellos.

Decimos que **la seguridad es una función de separación**. Hay cuatro formas para crear esa separación:

- Mover el activo y crear una barrera entre él y las amenazas.
- Cambiar la amenaza a un estado inofensivo.
- Destruir la amenaza.
- Destruir el activo. (¡No se recomienda!).

Así que cuando estamos hackeando, buscamos lugares donde las interacciones con el objetivo sean posibles, y donde no lo son. Piensa en las puertas en un edificio. Algunas son necesarias para los trabajadores, mientras que otras son necesarias para los clientes. Algunas pueden ser necesarias para huir de un incendio. Y algunas pueden no ser necesarias en absoluto.

Cada puerta, sin embargo, es un punto de interacción, que ayuda tanto a las operaciones necesarias como a las no deseadas (como el robo). Cuando llegamos a escena como hackers, no lo hacemos sabiendo el motivo de todos estos puntos de interacción, por lo cual los analizamos empleando el Proceso de Cuatro Puntos.

Veamos el ejemplo de una persona que quiere estar completamente a salvo de los rayos. La única manera de hacer esto (mientras siga en La Tierra) es ir al interior de una montaña, donde es completamente imposible que entre un rayo a través de la tierra y las rocas. Suponiendo que no tenga que salir de nuevo podemos decir que su seguridad es absolutamente un 100%. Pero si comenzamos a taladrar agujeros en la montaña, el rayo tendrá un punto más de acceso con cada agujero, y la porosidad aumenta. Por eso, OSSTMM diferencia entre estar **Seguro** (Safe) de los rayos y estar **Protegido** (Secure)de ellos. El hecho es que cuanta más porosidad haya, es más posible que un hacker pueda realizar cambios y controlar lo que quiera.

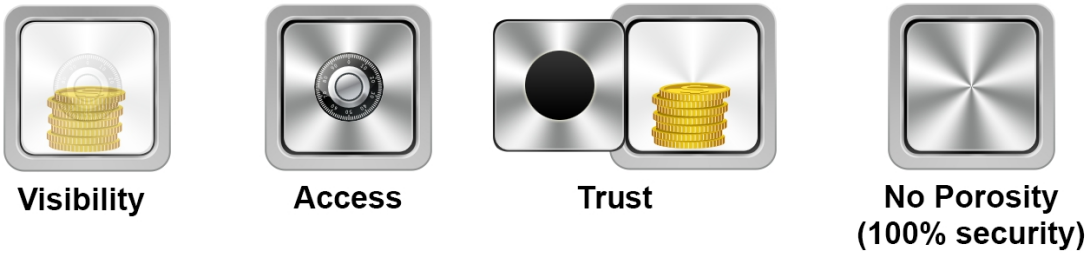

Figure 1.2: Porosidad

Enriquece tu mente: Porosidad

A continuación, presentamos algunos ejemplos para describir cómo encontrar los poros, clasificarlos y determinarlos durante el proceso de hacking.

Término	Definición
Visibilidad (Visibility)	Cuando la policía investiga un crimen, busca los medios, el motivo y la oportunidad. Si un activo es visible, puede ser atacado, pero si no es visible, no puede ser el objetivo (aunque podría ser descubierto). A algunos profesionales de la seguridad les gusta decir que la **ofuscación** es una seguridad deficiente ya que no protege nada, sólo lo oculta. Pero eso no es algo malo sobre todo porque no siempre se necesita un mecanismo de seguridad permanente. A tal efecto OSSTMM ofrece esta pequeña joya: "La Seguridad no tiene por qué durar para siempre, sólo durar más que cualquier otra cosa antes que pueda darse cuenta de que ha desaparecido"
Acceso (Access)	El acceso es el número de lugares diferentes donde pueden producirse interacciones en el exterior del ámbito. Para un edificio podrían ser las puertas de la calle o las ventanas, y para un servidor en Internet podría ser el número de puertos de red abiertos o servicios disponibles en ese equipo.
Confianza (Trust)	La confianza es cuando una entidad acepta la libre interacción con otra entidad dentro de su ámbito. Por eso que no pides a tu madre que se identifique cuando viene a abrazarte. También es la razón por la cual no sospechas que haya envenenado tu comida. Aprendes a confiar en las cosas dentro de tu ámbito. Pero si un día es abducida por una raza alienígena, la sustituyen (como en "**La invasión de los ladrones de cuerpos**") y envenena tu comida, la comerás sin sospechar nada. Así que la confianza es a la vez un agujero de seguridad y un reemplazo común para la autenticación, es decir, la forma de comprobar si una persona es quien creemos que es. La confianza es un tema extraño, porque es algo muy humano y muy valorado por la sociedad. Sin confianza, nunca seríamos capaces de interaccionar libremente. Pero debido a la confianza, es fácil engañarnos, confundirnos, robarnos y mentirnos. Investigaciones recientes sobre la confianza muestran que hay 10 razones para confiar en alguien y si esas diez razones se ven satisfechas, entonces podemos confiar en esa persona con seguridad y sin ningún tipo de preocupación. Pero esa misma investigación muestra que la mayoría de las personas sólo necesitan que se cumpla una razón para confiar, y que los realmente paranoicos o cínicos se ven satisfechos con tan sólo tres razones.

Recursos

Buscar eficazmente y tener capacidad de aprendizaje son las habilidades fundamentales de un hacker. El hacking, en realidad, es un proceso creativo que se basa

más en un estilo de vida que en estudiar lecciones. No podemos enseñarte todo lo que necesitas saber, pero podemos ayudarte a reconocer lo que necesitas aprender. Debido a que la ciencia avanza tan rápidamente, lo que nos enseñan hoy puede no ser relevante mañana. Es mejor para ti adquirir las costumbres de estudio de un hacker, que son probablemente la parte más vital del hacking, y que te diferenciarán de los **script kiddies** (un término hacker que deberías conocer, y que define a las personas que usan herramientas sin saber realmente cómo o por qué funcionan).

Si te encuentras con una palabra o un concepto que no entiendes en esta lección, es esencial que la busques. Ignorar nuevos términos sólo hará que te resulte más difícil entender conceptos en las próximas lecciones. Se te pedirá que investigues un tema y se espera que utilices la información que encontraste para completar los ejercicios de esa lección (pero en esas lecciones no se te explicará cómo hacer las investigaciones). Así que asegúrate de dedicar tanto tiempo como necesites para investigar, de forma que aprendas a usar los recursos que tienes disponibles.

Libros

Puede que te extrañe que no te dirijamos directamente a Internet, pero los libros son la mejor manera de aprender las bases y conocimientos científicos de todo lo que quieres explorar. ¿Quieres saber algo sobre informática, como los detalles del hardware de tu PC? Nada te ayudará más que leer un libro actual sobre el tema. El principal problema de los libros sobre informática es que se vuelven obsoletos rápidamente. El secreto es aprender a ver la base estructural que se encuentra bajo la fina piel de los detalles. MS-DOS y Windows son claramente diferentes, pero ambos se basan en los principios de la lógica Booleana que utilizan los computadores desde que Ada, Condesa de Lovelace, escribió el primer programa de ordenador en el siglo XIX. Los problemas de seguridad y privacidad pueden haber cambiado en los últimos 2.500 años, pero el **Arte de la Guerra** de Sun Tzu cubre principios fundamentales que todavía se aplican hoy. (Por cierto, la forma más rápida de parecer un **n00b** es citar a Sun Tzu. Hay cosas que debes saber, pero no decir. Y citar el Arte de la Guerra demuestra que no lo has leído, ya que Sun Tzu decía que hay que mantener tus conocimientos reales en secreto).

A pesar que la información que encuentres en los libros puede no estar tan actualizada como la que viene de otras fuentes, te darás cuenta de que la información que veas en ellos está mejor escrita que en muchas de las otras fuentes. A veces, también son más precisas. Es más probable que un escritor que dedica un año a escribir un libro compruebe los hechos, que lo haga alguien que actualiza un blog seis veces al día. (Mira la sección sobre Zines y Blogs para más información).

Pero recuerda: precisión no es equivalente a imparcialidad. Las fuentes de información del autor pueden no ser objetivas. "Los libros de historia los escriben los vencedores" (busca esta cita); esto también se aplica a la política, y reglas sociales de una época impiden que cierta información se publique. Esto ocurre habitualmente con los libros de texto seleccionados mediante un proceso político y contienen sólo la información que se considera socialmente aceptable para aprender. No pienses que has encontrado una regla de oro sólo porque lo leíste en un libro. Lo cierto es que cualquiera puede escribir un libro, y cualquier libro puede contener cualquier versión de la verdad.

No mires un libro para luego abandonarlo, incluso antes de empezar a leerlo, porque es muy grande. Nadie de los que veas sentados a tu alrededor lee esos enormes libros de principio a fin. **Piensa en ellos como en páginas web prehistóricas**. Abre uno por una página al azar y empieza a leer. Si no entiendes algo, retrocede y busca la explicación (o sáltatelo y avanza hasta algo que tenga sentido). Salta a través del libro, hacia atrás y hacia delante, tal y como lo harías saltando de un enlace a otro en una página web. Esta forma de lectura no lineal es con frecuencia mucho más interesante y satisfactoria para los hackers, ya que se trata más de satisfacer tu curiosidad que de leer.

Finalmente, algo que adquieren los lectores de libros es la valiosa capacidad de escribir bien. Esta es una gran ventaja cuando intentas participar y entender un nuevo campo. También hacen más creíbles las cosas que quieres contar a otros lectores, especialmente a aquellos que ocupan puestos de autoridad.

Revistas y Periódicos

Las revistas y periódicos son muy útiles para obtener información de forma concisa y puntual. Ambos tipos de publicación pueden ser, sin embargo, muy escuetos en los detalles. Además ten en cuenta que cada periódico o revista tiene su propia audiencia y una linea editorial o temática, a pesar de cualquier anuncio sobre "neutralidad e imparcialidad". Conoce la temática de la publicación: una revista sobre Linux no es precisamente una buena fuente de información sobre Microsoft Windows, dado que Windows es un tema espinoso (un sistema operativo competidor), y sinceramente, el lector de una revista sobre Linux quiere leer sobre la superioridad de Linux. Muchas de las revistas especializadas utilizan **cherry picking,** una técnica que destaca sólo los aspectos positivos de algo que encaja en la linea editorial de la revista, y destaca los aspectos negativos de aquello que no lo hace.

Ten en cuenta los posibles sesgos de la publicación. Ahí es donde te dan opiniones en lugar de hechos, o dejan a un lado los hechos de una historia para satisfacer sus propias opiniones, de forma que no puedes formar tu propia opinión. ¡Ten en cuenta la fuente! Incluso los periódicos "neutrales" pueden estar llenos de prejuicios y especulaciones, una bonita forma de decir "conjeturas", pero a menudo son "elucubraciones" por parte del periodista.

Hay un importante movimiento en el campo médico para que se publiquen todas las pruebas médicas y farmacéuticas (o al menos todos los ensayos financiados con fondos públicos), incluso de aquellas que han resultado fallidas, de forma que los médicos puedan contar con más información a la hora de aplicar tratamientos y tomar decisiones. Mientras que en las revistas médicas actuales publican los "hechos" de los ensayos de investigación, los detalles y las circunstancias detrás de esos hechos siguen siendo turbia. Eso es muy importante cuando se tratan temas que dependen de causas profundas. La causalidad requiere que la causa le preceda y es la razón del efecto.

Otro truco utilizado por las revistas (tanto de forma accidental como a propósito) son las **pruebas anecdóticas**, que son opiniones de personas publicadas como pruebas

independientemente de si son expertos o no; **pruebas expertas**, en las que se presentan a empleados de la industria en cuestión como expertos para dar sus opiniones, o personas que son expertos en un área y dan su opinión en otra en la cual no tienen experiencia; y finalmente, la **especulación**, clasificando algo como cierto porque "todo el mundo" cree que lo es, sin atribuirlo a nadie en particular.

La mejor manera de combatir los problemas de exactitud y temática es leer mucho y bien. Si lees algo interesante en una revista, busca más sobre el tema. Toma partido por una de las opiniones, y busca información que la confirme; luego, ponte del otro lado y busca refutarla. Algunas culturas hacen esto por defecto. Es parte de sus costumbres sociales buscar otra versión de la historia. Esto es un rasgo cultural muy importante, especialmente si intentas garantizar el éxito de una democracia.

Ejercicios

1.9 Busca en Internet tres revistas online que traten sobre Seguridad. ¿Cómo encontraste estas revistas?

1.10 ¿Las tres revistas tratan específicamente sobre seguridad informática? ¿Que otras cosas ofrecen que puedan resultar de ayuda en otros campos o negocios?

Enriquece tu mente: Especulación

El siguiente párrafo es de un artículo sobre un robo publicado en un periódico. ¿Puedes encontrar la especulación? Señala las frases de las que sospeches:

El banco "Lake Meadow Bank and Mortgage Lender" fue atracado el Martes a última hora cuando unos pistoleros enmascarados entraron unos momentos antes de la hora del cierre, y retuvieron a los empleados como rehenes durante una hora en lo que parecía ser un intento de fuga en un SUV último modelo. Ninguno de los rehenes fue herido.

Nadie pudo identificar a los atracadores, lo que hace pensar a la policía que podía tratarse de profesionales, ya que momentos después del robo, el coche fue visto tras el banco alejándose hacia el sur hacia los densos bosques de Bluegreen Mountains. La policía busca a atracadores con experiencia, que puedan tener antecedentes policiales y mantengan relaciones con personas que vivan en la zona.

Con una media de 57 atracos diarios a bancos entre esta zona y el condado de Bluegreen, y una población aproximándose a las 50.000 personas para el año que viene, esto podría ser el comienzo de una oleada de atracos a bancos en esta región. "Parece el comienzo de una moda" declaró el comisario de policía Smith.

A medida que nos volvemos más insensibles a la especulación y permanecemos como ignorantes funcionales sobre la parcialidad de los datos y resultados estadísticos, el futuro de la información pueden ser un único periodista especulando sobre las noticias conforme vayan ocurriendo. En el breve ejemplo anterior sólo hay un dato real: atracaron un banco el martes a última hora. Ahora, para hacerlo aún más obvio, así estaría redactada la noticia si modificamos todas las especulaciones para hacerlas aún más ridículas:

El banco "Righteous Bank and Mortgage Lender" fue atracado el martes a última hora cuando lo que parecían ser unos pollos enmascarados entraron momentos antes del cierre, lo que significa que podrían haber retenido a los empleados como rehenes durante una década antes de lo que parecía ser un intento de fuga en un globo aerostático. No se ha informado sobre si alguno de los rehenes fue emplumado.

Nadie pudo identificar a los pollos, lo que lleva a la policía a creer que debían contar con un profesional del disfraz entre ellos, además de un piloto de aerostatos, dado que instantes después del robo se vio un globo flotando sobre el banco, volando en dirección sur hacia las tundras de la Antártida. La policía se encuentra, posiblemente, buscando a expertos maquilladores que tengan vínculos con los aficionados a los globos.

Con una media de 57 atracos en bancos cada día en el país, y la industria de globos aerostáticos informando de que sus ventas podrían alcanzar los 47 muchimillones de dólares en un futuro próximo, esto podría ser el comienzo de una oleada de robos usando globos. "Parece el comienzo de una moda" dijo el comisario de policía Gordon.

Con el abrumador uso de la especulación y estadísticas en todas los sectores, no es de extrañar que haya entrado en la industria de la seguridad con tanta fuerza. El término usado comúnmente para esto es **FUD**, siglas de **Fear, Uncertainty, and Doubt** *(Miedo, Incertidumbre y Duda)*. Es la forma de utilizar la especulación y los análisis subjetivos de riesgo para llamar la atención sobre los intereses propios y vender soluciones de seguridad. Desafortunadamente, funciona muy bien con los sentimientos primitivos de paranoia de la psique humana y genera un aumento de la insensibilidad a la especulación. Esto ha dado lugar a soluciones de seguridad inadecuadas, aplicadas de forma inapropiada, controles reactivos de seguridad y una falsa sensación de confianza en las autoridades. Es evidente que existe una falta de habilidades en pensamiento crítico en la población, y esto es algo explotado tanto por el sector comercial como por los delincuentes.

Motores de búsqueda

Google es un motor de búsqueda muy conocido, pero no es el único que existe. Bing es muy bueno con preguntas sencillas, y Yahoo lo es para hacer investigaciones exhaustivas. Pero ten en cuenta que todos estos servicios web quieren saberlo todo acerca de ti, y probablemente saben más de lo que deberían. Guardan tus resultados y los sitios visitas después de tus búsquedas.

> Hay motores como AltaVista y DuckDuckGo.com que pueden proporcionarte algo (o mucho) de anonimato, lo cual puede ser bueno cuando buscas en los rincones oscuros.

Los sitios web se pueden consultar mientras están en linea y normalmente mucho tiempo después de eso. Normalmente, se conservan en forma de **páginas cacheadas**. Una caché de Internet es un registro online de las versiones anteriores de un sitio web, o incluso de sitios web que ya no existen. Los motores de búsqueda y los sitios de archivo almacenan esa información indefinidamente, lo que en terminología de Internet significa "para siempre". Es muy importante recordarlo incluso antes de que pongas algo en Internet: no va a desaparecer. Nunca. Puede que tengas que buscarlo en un link a la copia en caché de una página. Google, por ejemplo, solía poner un enlace llamado "Caché" junto al link del resultado. Esto ha cambiado a un menú flotante a la derecha, y puede haber cambiado otra vez cuando leas esto.

Además de los motores de búsqueda, también existen cachés públicas muy útiles en sitios como **Internet Archive (http://www.archive.org).** Puedes encontrar versiones cacheadas de sitios web completos a través de los años, lo cual puede ser muy útil para encontrar información que ha desaparecido.

Una último detalle sobre los sitios web: no asumas que puedes confiar en un sitio web sólo porque aparezca en un motor de búsqueda. Muchos de los ataques de hackers y virus se propagan con sólo visitar un sitio web, descargar programas de aspecto inocente, protectores de pantalla o archivos compartidos. Puedes protegerte no descargando programas desde sitios web no confiables, y asegurándote de que tu navegador se ejecuta en un entorno limitado (**sandbox**). Pero esto puede no ser suficiente. Un navegador es una ventana a Internet y como una ventana, pueden entrar flotando cosas malas tan sólo porque está abierta. A veces ni siquiera lo sabremos hasta que sea demasiado tarde.

Ejercicios

1.11 Hay muchos motores de búsqueda ahí fuera. Algunos son buenos para consultar la **Web Invisible**, áreas de Internet que son difíciles de rastrear para muchos motores de búsqueda, como ciertas bases de datos privadas. Un buen investigador saber cómo usarlos todos. Algunos sitios web se especializan en el seguimiento de motores de búsqueda. Así que encuentra cinco motores de búsqueda que no hayas utilizado o de los que no hayas oído hablar antes.

1.12 También hay motores de búsqueda que buscan otros motores de búsqueda. Se llaman **meta search engines**. Encuentra uno de esos meta search engines.

1.13 Busca "seguridad y hacking" (incluyendo las comillas) y anota los tres primeros resultados. ¿Cuánto difieren los resultados si NO usas comillas?

1.14 Es muy distinto buscar sobre un tema a buscar una palabra o frase. En el ejercicio anterior buscaste una frase. Ahora buscaremos una idea.

Para hacer esto, **piensa en frases que puedan estar en la página que estás buscando.** Si quieres que el motor de búsqueda te devuelva una lista de revistas online sobre hacking, no irás muy lejos si buscas "una lista de revistas online sobre hacking". ¡No hay muchas páginas web que contengan esa frase! Podrás obtener algunos resultados, pero no demasiados.

En lugar de eso, necesitas pensar: "si yo estuviera creando una revista sobre hacking, ¿cual sería una frase típica que pondría en la revista?" Pon las siguientes palabras y frases en un motor de búsquedas y encuentra cual te proporciona los mejores resultados para tu búsqueda:

1. mi lista de revistas favoritas sobre hacking

2. lista de revistas profesionales sobre hacking

3. recursos para hackers

4. revista de hacking

5. revistas hacking seguridad lista recursos

1.15 Busca el sitio web más antiguo de Mozilla en "Internet Archive". Para hacerlo, necesitas buscar "www.mozilla.org" en http://www.archive.org

1.16 Ahora vamos a unir las cosas. Digamos que quieres descargar la versión 1 de navegador Netscape. Utilizando motores de búsqueda y "Internet Archive", mira si puedes localizar y descargar la versión 1.

Páginas web y Aplicaciones web

El estándar *de facto* actual para compartir información es a través de un navegador web. A pesar de clasificar todo lo que vemos como "la web", más y más cosas de las que utilizamos son en realidad "aplicaciones web", dado que no todo en la web es un sitio web. Si compruebas tu correo usando un navegador web, o compras música a través de un servicio web, estás utilizando una aplicación web.

Algunas veces las aplicaciones web requieren privilegios. Esto significa que necesitas un login y un password para acceder. Tener acceso cuando tienes derecho legal a entrar se llama tener **privilegios**. Hackear un sitio web puede significar que tengas acceso, pero como no tienes derecho a estar ahí, no tienes un acceso privilegiado. Conforme vayas utilizando la web, encontrarás muchos sitios que te otorgan acceso a áreas privilegiadas por accidente.

Cuando encuentras algo así, es una buena costumbre avisar al administrador del sitio web. Sin embargo, ten cuidado con las posibles consecuencias legales. Desgraciadamente, muchos administradores fruncen el ceño cuando reciben un informe de vulnerabilidades que no han solicitado.

Para contribuir a hacer de Internet un lugar más seguro mientras te proteges a ti mismo, deberías pensar en utilizar un servicio **anonimizador** (por ejemplo: Tor, remailers anónimos, etc...) para enviar informes de vulnerabilidades a estos administradores. Pero ten cuidado: ¡todas esas tecnologías anonimizadoras tienen su punto débil y puede que no seas tan anónimo como crees! (Más de un hacker lo ha aprendido por la vía dura)

Ejercicios

1.17 Utiliza un motor de búsqueda para encontrar sitios que han cometido el error de dar acceso privilegiado a todo el mundo. Para hacer esto, buscaremos carpetas que nos dejen listar el contenido (un "directory listing"), algo que en condiciones normales no debería estar permitido. Para esto, usaremos algunos trucos con los comandos de Google en http://www.google.com. Escribe esto en la caja de búsqueda:

```
allintitle:"index of" .js
```

Examina los resultados y deberías encontrar alguno que parezca un volcado de directorio (directory listing). A este tipo de búsquedas se le denomina "Google Hacking"

1.18 ¿Puedes encontrar otra clase de documentos usando esta técnica? Encuentra tres directory listing más que contengan archivos .doc files, y .avi.

1.19 ¿Existen otras opciones de búsqueda similares a "allintitle:"? ¿Cómo puedes encontrarlas?

Zines

Los **Zines**, también llamados **e-zines**, son los descendientes de los **fanzines**: revistas pequeñas, generalmente gratuitas con una tirada muy reducida (menos de 10.000 lectores) y frecuentemente producidas por periodistas aficionados y amateurs. Los fanzines se imprimían en papel. Los zines en Internet, como el famoso **2600** o **Phrack web zine**, están escritos por voluntarios; esto implica que, con frecuencia, los editores no editan los artículos buscando errores no técnicos. Algunas veces, el duro lenguaje que emplean puede sorprender a aquellos que no están familiarizados con este género.

Los zines tienen una temática o linea editorial bastante contundente, y tienden a ser bastante parciales. Sin embargo, también son más propensos a mostrar y discutir ambos lados del problema, ya que no tienen que preocuparse por complacer a sus anunciantes y suscriptores.

Ejercicios

1.20 Busca en Internet tres zines sobre hacking. ¿Cómo los encontraste?

1.21 ¿Por qué clasificas esos resultados como zines? Recuerda, sólo porque se etiquetan como zine o ponen "zine" en el título no significa que lo sean.

Blogs

Podemos considerar a los **blog** cómo una evolución de los zines, y cuentan con una plantilla de escritores de una persona. Los blogs se actualizan con más frecuencia que la mayoría de publicaciones escritas o los zines, y crean comunidades alrededor de temas de interés. Es importante leer tanto los comentarios cómo los artículos. Incluso más que en el caso de los zines, en los blogs las respuestas son inmediatas y bastante posicionadas, con comentarios de ambos bandos. Esto es uno de sus valores especiales.

Aunque hay millones de blogs en Internet, sólo un pequeño porcentaje de ellos siguen activos. La información contenida en la mayoría de ellos, sin embargo, sigue disponible.

Ejercicios

1.22 Busca en Internet tres blogs que traten sobre hacking.

1.23 ¿Con qué grupos o comunidades están asociados?

1.24 ¿Hay temas de seguridad, legalidad o académicos en el blog?

Foros y Listas de correo

Los f**oros** y **listas de correo** son medios de comunicación desarrollados por comunidades, muy parecidos a grabar las conversaciones en una fiesta. Se escéptico acerca de todo lo que leas ahí. Las conversaciones cambian de tema con frecuencia, muchas de las cosas que se dicen son rumores, hay **trolling**, surgen **flame wars**, y, cuando la fiesta se termina, nadie está seguro de quién dijo qué. Los foros y listas de correo son similares, porque hay muchas formas de contribuir con información incorrecta (a veces de forma intencionada) y se puede participar anónimamente o suplantando a alguien. Como los asuntos y temas cambian rápidamente, para conseguir toda la información es importante leer el hilo completo de comentarios, y no sólo unos pocos de los primeros.

Puedes encontrar foros sobre casi cualquier tema, y muchas revistas y periódicos online ofrecen foros para que sus lectores escriban réplicas a los artículos que publican. Debido a esto, los foros tienen un valor incalculable para conseguir más de una opinión sobre un artículo: no importa lo mucho que le gustase a una persona, con total seguridad habrá alguien a quien no.

Hay muchas listas de correo sobre temas específicos, pero pueden ser difíciles de encontrar. A veces, la mejor técnica es buscar información sobre un tema en particular para localizar una comunidad de listas de correo que traten sobre él.

Cómo hacker, lo más importante que debes conocer es que no se puede buscar en muchos foros y listas de correo usando los motores de búsqueda más importantes. Mientras que es posible encontrar un foro o lista utilizando un buscador, puede que no encuentres información sobre mensajes individuales. Esta información es parte de la web

invisible porque contienen datos que sólo pueden buscarse directamente en el sitio web o foro.

Ejercicios

1.25 Encuentra dos foros de hackers. ¿Cómo encontraste esos foros?

¿Puedes determinar los temas o asuntos en que se especializan estos sitios web? ¿Los asuntos del foro reflejan la temática del sitio web que los aloja?

1.26 Encuentra dos listas de correo sobre hacking o seguridad.

¿Quién es el propietario (owner) de esas listas? ¿Puedes ver la lista de miembros? (Es posible que tengas que averiguar qué aplicación web se ha empleado en la lista, y buscar en la web los comandos ocultos que te permiten ver la lista de miembros de esa clase de lista de correos)

¿En qué listas esperarías que la información fuera más objetiva y menos sesgada? ¿Por qué?

Grupos de noticias

Los **Newsgroups** o **Grupos de noticias** llevan mucho tiempo entre nosotros. Había grupos de noticias incluso antes de que existiera la web. Google compró el archivo completo de grupos de noticias y lo puso online en http://groups.google.com. Los grupos de noticias son como listas de correo... pero sin el correo. La gente escribía allí directamente, tal y como lo harían comentando en un sitio web. Encontrarás mensajes desde principios de los 90 en adelante.

> Igual que en los archivos web (the web archives), los grupos de noticias pueden ser importantes para encontrar quien tuvo originalmente una idea o quien creó un producto. También son útiles para encontrar esa información oculta que nunca apareció en una página web.

Los grupos de noticias no son menos utilizados hoy en día de lo que se usaban años atrás, antes de que la web se convirtiera en la fuente principal para intercambiar información. Sin embargo, tampoco han crecido ya que su popularidad se ha reemplazado por nuevos servicios web como blogs y foros.

Ejercicios

1.27 Usando Google's groups, encuentra el grupo de noticias sobre hacking más antiguo que puedas.

1.28 Encuentra otras formas de usar los grupos de noticias. ¿Hay aplicaciones que puedas utilizan para leer los Newsgroups?

1.29 ¿Cuantos grupos de noticias puedes encontrar que traten sobre hacking?

1.30 ¿Puedes encontrar una lista actualizada sobre todos los diferentes grupos de noticias que existen en la actualidad?

Wikis

Los **Wikis** son el fenómeno más reciente en Internet. Wikipedia (www.wikipedia.org) es probablemente el más famoso, pero hay muchos otros. Como muchos otros sitios, los wikis los construyen las comunidades. Los informes afirman con frecuencia que los wikis no son precisos porque han contribuido amateurs y fanáticos. Pero esto también es cierto en los libros, listas de correo, revistas y todo lo demás. Lo que es importante es saber que los expertos no son la única fuente de ideas geniales e información objetiva. Como señala OSSTMM, los hechos vienen de los pequeños pasos que damos al comprobar las ideas, y no de grandes avances en los descubrimientos. Por eso los wikis son grandes fuentes de ideas amateurs y profesionales que poco a poco, progresivamente, se verifican entre ellas.

Los wikis también suelen hablar sobre las múltiples facetas de un tema y te permiten seguir como se refuta, refina y cambia la información a través de una lista de ediciones. Por tanto son grandes lugares en los que buscar información, pero con frecuencia tendrás que ir al sitio web del wiki para ejecutar las búsquedas.

Ejercicios

1.31 Busca "Ada Lovelace." ¿Encuentras resultados de wikis?

1.32 Ve a la Wikipedia y repite esta búsqueda. Dale un vistazo al artículo que encontrarás sobre ella. ¿Estaba incluido en la lista de resultados de tu búsqueda?

1.33 Comprueba las ediciones de esa página de la Wikipedia, y busca que clase de cosas se han cambiado y corregido. ¿Qué clase de cosas han cambiado? ¿Hay algo que se haya cambiado y luego devuelto a su estado anterior? Ahora elige una estrella de cine o cantante famoso, ve a esa página en Wikipedia y comprueba las ediciones ¿Puedes ver la diferencia?

1.34 Encuentra otra wiki y haz la misma búsqueda. ¿Alguno de los resultados que aparecen estaban en la primera búsqueda con el motor web?

Redes sociales

¿Usas alguna red social? ¿O más de una? Como hacker estás bien informado de los sitios más populares del momento. ¿Y que hay de esos que no son populares como eran antes? Todavía existen, y todos los datos siguen disponibles en la mayoría de los casos.

Esto significa que existen un gran repositorio de información sobre nosotros, mucha de la cual se ha proporcionado libremente, Y permanecerá allí para siempre.

Las redes sociales, con frecuencia, tienen subgrupos o comunidades con intereses comunes. Los sitios con una temática profesional cuentan frecuentemente con grupos de ciberseguridad, y en los sitios de temática "underground" existen habitualmente grupos de hackers. En los sitios profesionales se espera (todos los demás también) que uses tu nombre real. En los sitios de hackers, no tanto.

Y lo más importante de todo: ¿usas tu nombre real en los medios sociales, o usas un alias? ¿Hay alguna forma de que tu alias sea trazado hasta tu nombre real? Mucha gente no se da cuenta de eso cuando utilizan alias, pero no es raro que publiquen accidentalmente o a propósito su nombre real, dirección, ciudad, escuela, empleo y cosas parecidas cuando usan su alias. Si otro hacker te hace un DoX desde tu alias, entonces puede darse cuenta rápidamente de quien eres precisamente por esos pequeños y estúpidos errores. Si usas un alias para permanecer anónimo ante quien no conoces, asegúrate que continúas así. Y NUNCA te equivoques de alias si tienes más de uno.

Ejercicios

1.35 Búscate a ti mismo. ¿Obtienes algunos resultados tuyos (que sean realmente tuyos)? ¿Alguno de esos vienen de redes sociales?

1.36 Ve a una red social que utilices. No hagas login, pero repite la búsqueda como si no estuvieras registrado. ¿Cuánto puedes encontrar acerca de ti?

1.37 Ve a una red social que utilice un amigo. De nuevo, no te registres si tienes una cuenta. Busca a tu amigo. ¿Cuánto puedes averiguar acerca de él?

Chat

El **Chat**, se presenta como **Internet Relay Chat (IRC)** e **Mensajería instantánea (IM)**, es una forma muy popular de comunicarse.

> Como medio de búsqueda, el chat es extremadamente inconsistente porque estás tratando con individuos en tiempo real. Algunos pueden ser amistosos y otros bastante groseros. Algunos serán bromistas inofensivos, pero otros serán mentirosos malintencionados. Algunos serán inteligentes y querrán compartir información, y otros estarán completamente desinformados, pero no menos deseosos de compartir. Puede ser difícil saber quién es quien.

Sin embargo, una vez que te sientas cómodo con ciertos grupos y canales, puedes ser aceptado en la comunidad. Se te permitirá hacer más y más preguntas, y aprenderás en quien puedes confiar. Llegado el momento, tendrás acceso a los exploits más recientes (los llamados **zero day**, que significa que se acaban de descubrir) y profundizar en tus propios conocimientos.

Ejercicios

1.38 Encuentra tres programas de mensajería instantánea. ¿Qué los hace diferentes ? ¿Pueden utilizarse para hablar uno con otros?

1.39 Busca lo que es un IRC, y cómo puedes conectarte a él. ¿Puedes encontrar que red tiene el canal de ISECOM? Una vez que te unas a la red, ¿Cómo puedes conectarte al canal isecom-discuss?

1.40 ¿Cómo sabes que canales existen en una red de IRC? Encuentra tres canales de seguridad, y tres canales de hacking. ¿Puedes entrar en esos canales? ¿Hay gente hablando en ellos, o son bots?

P2P

Peer to Peer, también llamado **P2P**, es una red dentro de Internet. A diferencia de las redes habituales cliente-servidor, donde cada computador se comunica a través de un servidor central, los computadores en redes P2P se comunican directamente unos con otros. Muchas personas asocian el P2P a descargar MP3 y películas pirateadas, como con el infame Napster, pero hay muchas otras redes P2P (todas con el propósito de intercambiar información y como medio de realizar investigaciones sobre el intercambio de información distribuida)

El problema de las redes P2P es que, mientras que puedes encontrar casi cualquier cosa en ellas, algunas están en las redes ilegalmente. Otras cosas están allí legalmente pero las compañías que las crearon piensan que no deberían estar, y son felices demandando por dinero al propietario de cualquier **portal de Internet** de donde es descargado

> *Por el momento, no hay mucho consenso sobre si el propietario del acceso a Internet que se ha usado para descargar contenidos es responsable, o si la policía debería buscar a la persona que lo hizo. Esto es como decir que si tu coche se ha utilizado para cometer un crimen, es el propietario de coche y no el conductor quien debe ir a la cárcel. Las leyes de Internet actuales no son justas y equitativas, así que se extremadamente cuidadoso.*

Seas o no el tipo de persona que se arriesga descargando propiedad intelectual, no hay duda que las redes P2P pueden ser un recurso vital para encontrar información. Recuerda: no hay nada ilegal en una red P2P (hay muchos ficheros disponibles para ser distribuidos libremente bajo una gran variedad de licencias) pero también hay archivos en esas redes que no deberían estar allí. No tengas miedo a usar redes P2P, pero se consciente de los peligros, y de lo que te estás descargando.

Ejercicios

1.41 ¿Cuáles son las tres redes más populares y utilizadas en P2P? ¿cómo funciona cada una de ellas? ¿Qué programa necesitas usar?

1.42 Investiga el protocolo de una de esas redes P2P. ¿Qué hace, y cómo consigue descargar más rápido?

1.43 Busca "Descargar Linux".¿Puedes descargarte una distribución (o distro) de Linux usando P2P?

Certificaciones

Hay certificaciones OSSTMM para Security Tester y Security Analyst, distintas variantes de certificaciones "hacker", certificaciones basadas en alguna versión de"buenas prácticas" y otros certificados con toda clase de iniciales o símbolos extraños.

> ¿Por qué preocupate por las certificaciones? Pues debido a que puedes obtener algunas de ellas a cualquier edad, ya que no es necesario tener un título universitario para conseguirlas, y porque puede ponerte en la posición de persona codiciada, en lugar de ser una persona que solicita un puesto.

El problema de las certificaciones basadas en "buenas prácticas" es que estas cambian a menudo, debido a que "*buenas prácticas*" no es más que otra forma de decir "lo que está haciendo todo el mundo ahora". Y con frecuencia lo que hacen los demás durante esta semana es incorrecto, y lo seguirá siendo cuando se actualice la semana siguiente.

Luego tenemos las certificaciones basadas en la investigación, que se centran en investigaciones válidas y reproducibles del comportamiento de humanos y sistemas. No hace falta decir que nuestra organización matriz, ISECOM, entra de lleno en el campo de las autoridades de certificación basadas en la investigación. Ya sea de ISECOM o cualquier otra, busca certificaciones basadas habilidades, análisis o **conocimientos aplicados** que te permitan demostrar que puedes aplicar lo que dices haber aprendido. Te resultará muy útil cuando tengas que hacerlo.

Seminarios y jornadas

Acudir a seminarios es una buena forma de escuchar en detalle las explicaciones sobre la teoría, y ver las técnicas puestas en práctica. Incluso es interesante asistir a seminarios que presentan un producto y muestran cómo debe utilizarse, siempre y cuando tengas en cuenta que el evento es marketing y su finalidad es venderlo.

Por nuestra parte, seríamos negligentes si no mencionáramos que podemos ofrecer seminarios de Hacker Highschool en muchos lugares, y que podemos tratar cualquiera de las lecciones disponibles. Los seminarios consisten en hackers profesionales hablando a los estudiantes sobre hacking y cómo ser un hacker, tanto bueno como malo. Estos seminarios dan una visión profunda sobre lo que son los hackers reales desde la perspectiva del **Hacker Profiling Project**, un proyecto de colaboración con Naciones Unidas que investiga quienes son los hackers y porqué hackean. Entonces podrás descubrir el lado positivo del hacking y cómo no siempre está en el Lado oscuro.

Una de las cosas más importantes en las que podemos ayudarte es a encontrar los medios para ser intelectualmente curioso e ingenioso como un hacker. Los hackers triunfan en lo que hacen porque saben cómo aprender, ir más allá del contenido de las lecciones disponibles y aprender las habilidades que necesitan para avanzar.

Así que eres bienvenido si dices a tus padres y profesores que quieres ayudar y crear una delegación de Hacker Highschool en tu colegio. Contacta con ISECOM para obtener más información.

Lecturas adicionales

Ahora deberías practicar hasta que seas un maestro de las búsquedas. Cuanto mejor lo hagas, más rápidamente encontrarás la información y aprenderás más rápido. Pero desarrolla también un ojo crítico. No toda la información es cierta.

> Recuerda que siempre debes preguntarte: ¿Por qué mienten? ¿Hay dinero de por medio al ser deshonesto o perpetuar un rumor o una historia? ¿De dónde vienen los hechos? Y lo más importante, ¿Cuál es el alcance?

Al igual que en el hacking, la investigación incluye un ámbito de aplicación. Eso es muy importante cuando ves las estadísticas (las matemáticas que usan porcentajes, fracciones y probabilidades). Así que mira siempre donde se llevó a cabo el ámbito de aplicación y reconoce que ámbito tienes que aplicar. (*Un ejemplo común para ver esto es la delincuencia nacional o las estadísticas de salud, tomadas de una pequeña muestra en una sola parte del país. Sólo porque algo afecta al 10% de las personas de los 200 estudiados en una sola ciudad, no significa que el 10% de la nación entera tenga ese mismo problema*) Así que séeinteligente acerca de cómo leer la información y de la forma de encontrarla. ¡Entender el alcance de la información siempre es una gran diferencia!

Para ayudarte a convertirte en un mejor investigador para el programa Hacker High School, aquí hay algunos temas adicionales y unos términos para que puedas investigar:

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine
- The Jargon File
- OSSTMM
- ISECOM Certifications:
  - OPST (OSSTMM Professional Security Tester)
  - OPSA (OSSTMM Professional Security Analyst)
  - OPSE (OSSTMM Professional Security Expert)
  - OWSE (OSSTMM Wireless Security Expert)
  - CTA (Certified Trust Analyst)
  - SAI (Security Awareness Instructor)

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM