¿PUEDO LLEGAR A SER UN HACKER EN 24 HORAS?

UNA RESPUESTA EN SERIO A UNA PREGUNTA EXTRAVAGANTE

por Jesús Manuel Márquez Rivera <JmMr> v.1

PREÁMBULO

No. La respuesta es un no rotundo. Ni en 24 ni en 48 horas :) Pero en este tiempo sí puedes tener una idea aproximada y muy básica de lo que es y de lo que *"no es"* un hacker y decidir si quieres convertirte en uno de ellos.

Te recomiendo que visites la web de **Eric S. Raymond** sobre estas cuestiones: es el gurú *(Cómo ser hacker, El archivo de la Jerga, Loginakata, La Catedral y el Bazar, etc)*. La mayoría están traducidos al español.

Recientemente, **rfp** *(Rain Forest Puppy)* ha publicado un artículo muy interesante sobre cómo ser experto en seguridad.

CAPÍTULOS

1. LO QUE SÍ PUEDES HACER EN 24 HORAS.

Tras este título sensacionalista se esconde un tipo de pregunta que bajo mil variaciones inunda los foros, las cuentas de ***correo electrónico*** y los ***grupos de noticias***. Todas son del estilo: *¿puedes enseñarme a ser hacker? ¿puedes ayudarme a hackear los ordenadores de mi instituto para cambiar mis notas?* Generalmente estas preguntas ***esconden un grave error de juicio*** al enfocar la cuestión y suelen desembocar en dos caminos:

- uno, **pasajero**, que lleva a ser un ***novato***,
- y otro, **definitivo**, en el que termina saliendo a la luz el ***"lamer"*** que algunos llevan dentro.

Si este artículo tiene algún valor añadido al número de bytes que termine *"pesando"*, es que voy a contestar a la pregunta sin ironía, de una de las muchas formas en que puede hacerse. Es una vía *(no la única ni la mejor)*, expresada con ***lenguaje sencillo y directo***, de *"aprendiz de brujo"* a *"aprendiz de brujo"*, novato o como quieras considerarte.

No voy a huir de responder a aquello que *"promete"* el subtítulo, enmascarando la cuestión con otras secundarias. *Quieres ser hacker y yo te voy a decir cómo puedes serlo. No administrador de sistemas, no programador, sino hacker. No temamos llamar a las cosas por su nombre.*

Sólo cuando lleves días, semanas, meses, o años... irás descubriendo por tí mismo nuevos conocimientos y conexiones de unos datos con otros, subiendo peldaños de una escalera que no ves, niveles que no están ni pueden ser definidos, en definitiva, abriendo la mente o como dicen en ***"HackIndex"***, *"asimilando la Red"*. *Si tienes "madera" de hacker no te cansarás, porque el viaje es apasionante. Si te diviertes, vas bien, si no...*

Porque pudieras descubrir que no te interesa el esfuerzo y te conformases con ser un usuario avanzado con buenos conocimientos de seguridad.

Hacking en Internet, pero también **phreaking, cracking, virus y gusanos, troyanos y rats, electrónica, telecomunicaciones, criptografía, satélites** ... y quién sabe qué más: el límite está en tu imaginación ;) y en las leyes de la Física.

2. ¿QUÉ ES Y QUÉ NO ES UN HACKER?

Para saber si quieres ser algo debes tener claro qué significa. El ***término hacker está tan gastado y ha sido tan manipulado*** que requiere muchas veces un adjetivo como *"verdadero"* para dejar claro al interlocutor de qué estamos hablando.

Olvídate de los medios de desinformación *(salvo contadas excepciones, como **Mercè Molist**)*, del cine de Hollywood *(unas pocas escenas de unas escasas películas se salvarían de la quema*) y de muchas visiones distorsionadas e ignorantes que ni siquiera se esfuerzan en documentar mínimamente artículos, noticias, entrevistas, documentales y películas. Las aberraciones son tantas que no os voy a ahorrar algunos ejemplos: como noticias disparatadas sobre ciberguerra o *"guerra de la información"* en cadenas de **TV** en horario de máxima audiencia donde consideran ***"tempest"*** como un peligroso virus, o recomiendan el uso de un buen virus para proteger los ordenadores de los ***"hackers"*** *(y no se trata de un error, sino de una ignorancia de cavernícola)*, etc, etc...

Ésta es la parte más importante del texto. Si buscas sólo *"recetas"* para entrar en ordenadores ajenos, como hacen el **FBI** y la **NSA** *(**los crackers por excelencia**)*, para curiosear, destruir o controlarlos remotamente, creo que no es ni buen camino ni buen comienzo, aunque comprendo la satisfacción que a ciertas edades pueda producir. *Allá cada cual con su vida y su libertad ... o la ausencia de ésta.*

Nunca podrán ser las cosas como cuando sólo un grupo reducido de personas tenían acceso a los ordenadores y casi todos eran programadores, o en los comienzos de los BBS o de Internet. La era de las masas ha llegado también al hacking, para bien y para mal.

Según mi experiencia, existen **dos vías fundamentales en la actualidad**, que están muy relacionadas con el tipo de persona que se es:

I. La del que busca **resultados inmediatos** directamente con **técnicas de "hacking" enlatadas** *(colarle el último troyano a tanta gente como sea posible o escanear Internet buscando máquinas infectadas)*. Esos atajos terminan cansando a la mayoría. Esto no es necesariamente malo para empezar, aunque sí **es ilegal**. ***Este grupo es el que da más pasto al sensacionalismo de gobiernos y medios de comunicación. Y luego vienen las leyes condenando al hacker de verdad como a un terrorista***. Es la cantera de *"lamers"*, *"script-kiddies"*, etc.

II. La del que busca al principio **trucos, *"exploits"*** o lo que sea, pero rápidamente da el paso hacia la verdadera curiosidad por saber cómo son las cosas tras la interfaz de ventanas. Busca otros sistemas operativos *(**Linux**)*, información sobre el porqué de las cosas, etc. *Los troyanos están bien, pero mejor está saber cómo se desactivan los antivirus o se saltan los cortafuegos. Pero sin dárselas de nada*. ***Usará Windows para unas cosas, Macintosh para otras, Linux para conectarse a Internet, etc.*** *El que sigue este camino no suele despreciar a los que todavía no saben, ni recibir conocimientos sin dar nada a cambio...*

La idea que defiende este artículo es la del uso legal, ético ... de la información sobre tecnología, informática, (in)seguridad ... que debe ser libre, gratuita.

Hay poca gente capaz de crear, de innovar, de investigar nuevas formas de hacer las cosas. Pero hay mil cosas que se pueden hacer: *escribir, difundir buena información, poner webs sobre asuntos más o menos*

interesantes, "mirrors" (espejos) de ezines, herramientas, código fuente o lo que sea ... ***sobre todo colaborar en el movimiento "open-source" (GNU, Linux, etc)****.*

Aunque el artículo va orientado a los que empiezan, a los que quieren aprender, a la mayoría de los usuarios que tienen un PC con el *"Windoze"* de turno instalado y un acceso a Internet con modem de 56 k, cable o adsl, no por eso me olvido de lo mejor a cambio de lo mayoritario. *Los usuarios de Mac, Linux, Amiga, Spectrum, también existen :)*

Nadie nace sabiendo programar en ensamblador o compilar el kernel de Linux *"a mano"*. ***Lo que no se perdona en este apasionante universo del underground informático es la falta de esfuerzo y aptitud (es decir, la pereza y la estupidez)***.

Hay quienes consideran mal al que usa **Windows 95/98/Me**; otros a los que usan **Windows NT/2000**; otros a los que usando ya **Linux**, eligen **RedHat** o **Mandrake** en lugar de tener **Debian** ... y las combinaciones son infinitas: *un PC en lugar de un Mac, Windows en lugar de Linux, etc.* Pero ***el hacking está más allá de cualquier etiqueta***. Conozco hackers que trabajan con **Spectrum** o con **Amiga**, incluso con **MSDOS**, etc.

El hacker es un eterno aprendiz. El de élite es un genio que no termina nunca de aprender.

Linus Torvalds es el *hacker por excelencia*, en el sentido clásico. Pero una figura como **Boris Floricic**, ***"Tron"***, es lo que la mayoría de los que lean este artículo entienden por un hacker. *Sombrero blanco, sombrero gris... :)*

3. ¿CÓMO PUEDO SER UN HACKER *"DE VERDAD"*? GUÍA REAL.

Responder a esto es aún más difícil que explicar cómo ser un buen médico, o un buen maestro. **No basta con sacar un título**. En nuestro caso se complica porque no hay ninguna carrera de hacker *(todavía :)*. *Existe un nivel del que nadie pasa si no tiene una inteligencia bien desarrollada, aunque se lean diez mil artículos. Pero se pueden hacer bastantes cosas, aunque no tengamos el coeficiente intelectual de* ***Neumann****,* ***Baran*** *o* ***Ritchie****.*

La mayoría de los textos que puedes encontrar en Internet son demasiado difíciles para los que empiezan y no suelen graduar bien los diferentes niveles del lector. Últimamente están apareciendo tutoriales excelentes con muchas capturas de ventanas para facilitar la tarea a los novatos *(****Nautopía****,* ***Troyanos Indetectables*** *y un larguísimo etcétera)*.

Tan poco ético es el ***cracker*** que trabaja a cambio de dinero para un cliente o el ***"script-kiddy"*** que borra el disco duro de un servidor, como el ***"hacker"*** que trabaja para una empresa o gobierno a cambio de una tarjeta de crédito sustanciosa.

Conseguir dinero con los conocimientos es lícito, pero no a costa de una mínima ética.

Cuando uno visita páginas en que está a la venta *"hasta el logotipo"* le queda un *sabor de boca amargo*. El caso de la polémica reciente en torno a alguna web que ha convertido el hacking en artículo comercial sin más, deja clara la actitud de la comunidad hacker.

Por **maty: incluso amenazó a otra, con la ley mordaza española LSSICE en la mano. Todavía no se ha disculpado públicamente.*

*Entrando ya en materia, no es necesario saber **inglés** ni **programar** para dar los primeros pasos. Pero si quieres llegar a algo necesitarás empezar cuanto antes su estudio, porque llegará un momento en que te estancarás sin esos conocimientos (al menos leer con cierta fluidez textos en inglés y código fuente de "scripts" y de sencillas herramientas).*

Vamos a definir **tres fases de un posible camino de aprendizaje** *(los límites entre éstas son artificiales y buscan poder hacerlas comprensibles)*:

1ª FASE: MENTALIDAD DE USUARIO.

Una vez que hayas alcanzado un nivel básico como usuario del ordenador y de la navegación por la Web, estarás en condiciones de iniciar este viaje apasionante.

La persona que va más allá de los usos convencionales de la Informática e Internet, que siente curiosidad, ha dado el primer paso para ser un hacker. *Busca conocer a fondo su máquina, el sistema operativo (aunque sea Windows ;) y adquirir cierta experiencia en la Red, buscando muchas veces información y herramientas de forma compulsiva.*

La clave de esta fase debe ser buscar, leer y leer más aún. Ya llegará el momento de preguntar.

Si te conviertes en un buen novato habrás dado con la clave Todavía hay mucho que aprender *(y*

siempre lo habrá). Saberlo todo de todo es imposible, pero algo de todo sí que es posible.

Utilizar MSDOS es la mejor forma de quitarte el *"síndrome de las ventanas"* que *afecta a todos los usuarios de las generaciones más recientes*. La ***"línea de comandos"***, los directorios, etc. No es como una *"shell"* de **Linux**, pero servirá por ahora.

Los "comandos" de MSDOS para Internet e incluso programas de trazado de ruta visuales pueden ayudarte a lograr un esquema mental de la Red.

La **programación** es esencial, pero casi imposible de entender en esta fase. *Mi consejo es aprender a* ***programar "scripts" de Windows*** *o* ***archivos por lotes batch*** *(con extensión* ***.bat****). Te aseguro que aprenderás muchas cosas útiles y de forma más fácil (puedes hacer hasta virus muy interesantes, naturalmente con fines educacionales).*

Y también es el momento de ***aprender*** el lenguaje para crear páginas web sencillas, el **HTML**. *Consigue una cuenta gratuita y practica lo que vayas aprendiendo.*

Buscar y encontrar en Internet *(el uso de un buen buscador es esencial y probar sus opciones avanzadas)* y leer mucho *(que por lo menos "vayan sonando" las cosas)*.

Hay muchos textos y páginas web **para comenzar:** la **Guía de Carolyn Meinel**, **HackIndex**, **Ezines *(Set, Disidents, Raregazz, etc.)***, revista **Hackxcrack**, **libros sobre hacking *(1 y 2)* de Arroba** ...

2ª FASE: MENTALIDAD DE USUARIO AVANZADO Y ADMINISTRADOR.

La mente se va abriendo. Lo que se ha leído empieza a cobrar sentido y ya puedes relacionar lo que leíste sobre **netbios** con el acceso a los recursos compartidos de Windows o la última herramienta de explotación de bugs de esta vulnerabilidad que acabas de instalar *(y luego samba, y después rpc ...)*

Una vez que has adquirido conocimientos básicos de *"casi todo"* y leído mucho más, puedes empezar a discriminar entre textos, libros, sobre cuales te interesan más y a continuación construir una pequeña base de datos con carpetas temáticas *(netbios, samba, IIS, Linux, troyanos, virus, gusanos, macros, javascript ...)* de la forma más útil para cada uno.

Comienza la preocupación por:

- La **seguridad** *(que va más allá de instalar un cortafuegos gratuito o un antivirus actualizado)*
- El **anonimato** *(pasando del que te ofrecen otros al que uno mismo se fabrica)*
- La **criptografía** (*a nivel divulgativo al menos: leer a tiempo un artículo de calidad puede ser la diferencia entre tener la información realmente protegida o sólo con una protección ficticia)*
- Si en la primera fase te habías iniciado programando ficheros por lotes y HTML, ahora ***necesitas introducirte en Basic (Qbasic) y Visual Basic por el sendero de Windows, y "shell scripts" de bash, perl... para el camino de Linux.***
- Aparece la inquietud por otros sistemas operativos. Además de usar Windows, el **PC con arranque dual Windows / Linux** *(Mandrake o RedHat)* es una **opción muy interesante**.
- **Interés por las redes** *(objetivo: crear una red local en casa para experimentar)*. Si nuestro bolsillo lo permite, *conseguir PCs baratos de segunda mano, tarjetas de red, cableado ... Instalar y probar ... una y mil veces.* Dejas tu partición con un ***Windows servidor*** y entras desde la ***casa de un amigo***, desde un ***cibercafé*** que te deja instalar algunas herramientas, etc. Luego viene tu propio laboratorio en casa, como hemos apuntado antes.

Generalmente, **un tema estudiado en profundidad es una buena entrada en la *"scene"***. *Permite preguntar con inteligencia, escribir algo, responder para ayudar a los que preguntan, incluso llegado el día programar alguna herramienta. Cada día es más difícil encontrar un mentor que te guíe, aunque por probar ...*

Es el momento de volver a **leer lo mismo de la primera fase**: *ahora notarás una mejor comprensión.*

Libros más específicos: *Linux, Unix, Windows NT o 2000, Perl, Visual Basic ...* **Antes de comprar un libro impreso asegúrate de que es de lo mejor en su tema**. Foros, news, listas de correo, buscadores ... *Con **Google**, **Emule**, etc., puedes encontrar bastantes cosas interesantes.*

3ª FASE: MENTALIDAD DE HACKER. PROGRAMACION.

Este nivel es más difícil aún de explicar que los anteriores. *Todavía no serás ni un **gurú** ni un **hacker de élite**, pero ya puedes usar el nombre de hacker sin que se escandalice tu ordenador :)*

Sentirás un interés creciente por la programación en general y muy específico para solucionar determinados problemas *(participar en foros de programación, profundizar en la lectura y estudio del código, hacer modificaciones, etc)*.

Ahora se comprende que ser hacker es investigar a fondo en un campo. Hay hackers en la electrónica, en la música ... aunque este trabajo trata sólo lo que todos entendemos más o menos como hacker: *el apasionado, el "loco" (no el colgado) de los ordenadores y las redes, de la programación ... y cómo no, el lado alternativo de la informática convencional. ;)*

A partir de aquí ya puedes progresar hasta donde tu capacidad y tu esfuerzo te permitan.

Al final de este camino de aprendizaje estarán C y C++, ensamblador, etc. Y luego, a seguir aprendiendo.

Otros sistemas operativos: OpenBSD, FreeBSD, Inferno, etc. Y ante todo, Debian.

Cuando prefieras, por ejemplo, estudiar y modificar el código de un troyano y probarlo en tu red casera a usarlo porque sí, habrás entrado en el apasionante universo del hacking con pleno derecho. Los demás conocimientos vendrán después por añadidura.

Hemos dejado para el final de este apartado lo menos importante de todo, la ***elección de un "nick" (apodo)***. No seas exagerado, aunque el ingenio no está mal. Si envía un mensaje *"El super señor de la oscuridad cibernética"* a un foro o grupo sobre redes con linux, no tendrá la misma acogida que si lo hace *"ciberlópez"* o *"qamikace"*.

4. RECURSOS IMPRESOS Y DIGITALES.

Aunque es cierto que en Internet *(**no sólo es la web**, eh)* hay información para estar estudiando muchos años, también lo es que un libro impreso es muy manejable y cómodo.

- En **inglés**: *tienes los libros de O´Reilly, los de Carolyn Meinel, los de HackingExposed, etc.*
- En **español** las traducciones no suelen ser obras maestras que digamos, entre fallos por desconocimiento y erratas *("Dos" o "navegación" de servicio, puerta de atrás, trojano, etc., sin revisar las ediciones a fondo y sin utilizar los términos ya consagrados en nuestra lengua)*. Aunque para muchos es una opción preferible a comprarlos en inglés.

No te sientas culpable por preferir una explicación bien expresada, sencilla y con ejemplos y capturas de pantalla sobre lo que te interesa. Ya llegará el momento de leer páginas sin ninguna ilustración. (man, rfcs, etc).

Artículos

1. **Eric S. Raymond.** Cómo ser un hacker *(trad. César Ballardini)*.
2. **Eric S. Raymond.** Loginataka. Diálogo entre un gurú y un novato *(trad. Ulandron)*.
3. **Eric S. Raymond.** Cultivando la Noosfera *(Javier Gemignani)*.
4. **Eric S. Raymond.** La Catedral y el Bazar *(trad. José Soto Pérez)*.
5. **Eric S. Raymond.** The New Hacker´s Dictionary.
6. **rfp.** Quiero ser un experto en seguridad informática: ¿dónde empiezo? *(trad. raac)*.
7. Faqs *(y PUFs)* de es.comp.hackers.
8. **Carolyn Meinel.** Guía del hacking inofensivo *(versión de Kriptópolis)*.
9. Proyecto HackIndex.

Ezines en español

SET, Raregazz, Disidents, Raza Mexicana, ProyectoR, NetSearch, Fye ... *junto a artículos flojos hay muchas joyas, entre otras:*

1. Introducción al hacking v. 2.0 por **Daemon** (1998). JJF 3.
2. La superguía del hacker por **Nobody** (1998). JJF 8.
3. Curso de hack por **Conde Vampiro** (1997-1999). JJF 1-8.
4. Infovia?. Oui c'est moi por **Paseante** SET 11 y Firewalls y proxies por **Paseante** SET 9-11.
5. Los artículos del **Profesor Falken** en SET *(El teléfono, Red Telefónica Conmutada, Telefonía Móvil Celular, GSM, etc).*
6. Hacking NT v 1.0 por **Chessy** (1998). SET 15.
7. La Biblia del Hacker de NT por **Tahum** (2001). SET 24.
8. Analisis remoto de Sistemas por **Honoriak**. SET 24.
9. Perl a dolor 1ª EDICION. por **DDiego**. Disidents 3.
10. Sistemas Operativos por **TaSeH/Raciel**. NetSearch 7.

Y MUCHOS MAS:

Libros en español

- Libros de **Arroba**
- Revistas de **Hackxcrack**.
- **RFCs** en español.
- **Lucena, Manuel**. Criptografía y seguridad en computadores (2003).
- **Villalón, Antonio**. Seguridad en Unix y Redes.
- Manuales y Tutoriales del **Proyecto LUCAS**.
- **Wintermute**, Curso de programación de virus.
- **García de Celis, Ciriaco**. El universo digital del IBM PC, AT y PS/2

Libros en inglés

- **Schneier, Bruce**. Applied Cryptography
- **Menezes, Van Oorschot y Vanstone**. Handbook of Applied Cryptography.
- **Tannenbaum, Andrew**. Sistemas Operativos Modernos.
- **McClure, Scambray y Kurtz**. Hackers 3.
- **Ludwig, Mark**. The Little Black Book of Computer Viruses.
- **Ludwig, Mark**. The Giant Black Book of Computer Viruses.

Libros sobre: Linux, Perl, PHP, Python, Windows, MSDOS, TCP/IP, etc.

Libros obre cibercultura:

1. **Sterling, Bruce**. Hacker Crackdown *(La caza de hackers)*.
2. **Mungo y Clough**. Approaching Zero *(Los piratas del chip)*.
3. **Levy, Steven**. Hackers.
4. **Gibson, William**. Neuromante.

<JmMr> Artículos sobre: **Tron, Levin, Morris y Mitnick** *(publicados en la etapa anterior de **Kriptópolis**)*.

Webs *(los sitios y los enlaces son inestables)***:**

Kriptopolis	Rojodos *(?)*	Neworder
Criptonomicon	**Elhacker**	**Packetstorm**
VSAntivirus	Taller de Criptografía	Security Focus
SET ezine	Los primeros pasos de un hacker	Infossysec
NAUTOPIA	**Mercè Molist**	Happyhacker
Troyanos indetectables	Zine Store	*etc.*
Lucas	Alakarga *(?)*	
Cyruxnet	Hackemate	

Ah, y la página de un tipo llamado **Jesús Márquez** *(al menos la sección de enlaces) ;)*

5. LA ERA DE LOS HACKERS.

Cada día que pasa se conectan a la Red miles de ordenadores, dispositivos, aparatos de todo tipo que llevan en sus entrañas un microchip o un microprocesador con algún sistema operativo embebido y posibilidad de conexión a Internet.

> **La interconexión avanza a pasos agigantados:** *billones de dólares viajan por las redes las 24 horas del día en forma de bits, información crítica para gobiernos y corporaciones, millones de correos electrónicos, de operaciones bancarias, de compras con tarjetas en el llamado comercio electrónico, nuevas operaciones a través de teléfonos móviles ...*
>
> **por **maty:** a pasos agigantados, pero ¿y en ESPAÑA y demás países hispanos?*

Mientras tanto, esto es lo que nos ocultan los medios:

- Las **desigualdades reales y las injusticias** crecen día a día en el mundo real entre personas y países
- el **control gubernamental e imperial** crece sobre los internautas
- la amenaza de un **Internet censurado** en lo importante
- convertido en un ***bazar de mercaderes***, en un ***antro de pederastas*** y en una ***enorme base de datos del Gran Hermano que nos vigila*** está a la vuelta de la esquina
- el ***fin de la biodiversidad en arquitecturas de ordenadores, sistemas operativos y aplicaciones ...***

Todos estos problemas **requieren posiciones éticas**, **compromisos claros**, *más allá de las utopías irrealizables y del egoísmo creciente en las sociedades "desarrolladas" del que todos hablamos y del que* ***casi nadie extrae consecuencias personales****.*

La **mente** y el **corazón** del hombre son las dos **armas** más **poderosas y temidas** por aquellos que quieren acabar con *la libertad y la justicia, con la cultura y la dignidad ...* , en los que la ***"información"*** es parte esencial.

"La utopía de las TAZ" esperaba una reacción de los *"hackers"* contra los abusos de los gobiernos y las corporaciones. ¿Quién sabe si ocurrirá alguna vez en la forma que imaginó su autor o ya está ocurriendo de otras maneras?

Los gurús de la tecnología tendrán en sus manos tal poder que no podemos imaginarlo todavía. Ten valor y da el primer paso para comprender lo que está pasando y lo que está por venir. ***Todo lo que merece la pena, ha de ser conseguido con esfuerzo y defendido con tenacidad.***

Este siglo que comienza será *"el siglo de los hackers"*.

No permanezcas al margen.

jesusmarquez @ galeon.com jesusmarquez @ telepolis.com

www.jesusmarquez.net http://club.telepolis.com/jesusmarquez