

¿Sabes que es un Hacker?



T. en C.F.C. Gabino Adrian Vergara Morales
admin@sanvicentechicoloapan.com.mx

¿Para ti que es un Hacker?



Un Hacker es . . .

✓ *“Un hacker es un experto en computadoras, pero también es un revolucionario, un inconforme, un pistón de la sociedad.”*

✓ *“afición a lo técnico y en el placer de resolver problemas sobrepasando los límites.”*



Existe una comunidad, una cultura compartida, de programadores expertos, cuya historia se remonta décadas atrás a los tiempos de los primeros miniordenadores de tiempo compartido y los tempranos experimentos con ARPAnet.

Los miembros de esta cultura crearon el término "hacker".

Los hackers construyeron Internet.

Los hackers hicieron de Unix el sistema operativo que es hoy día.

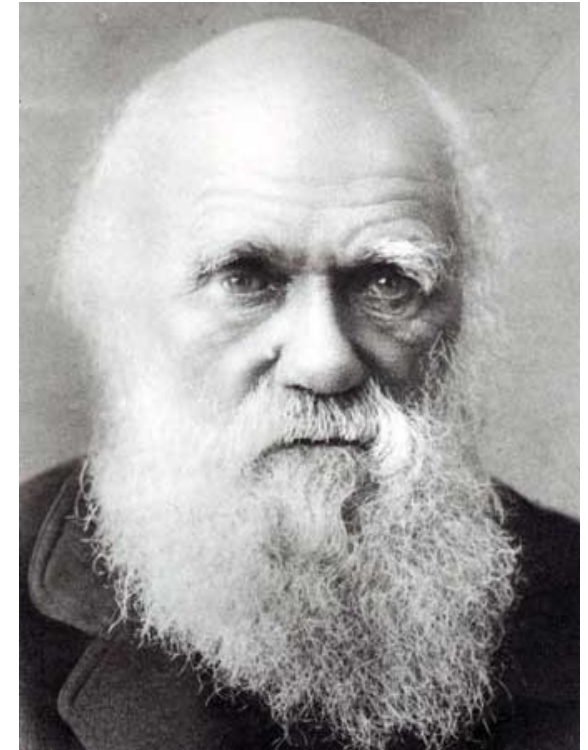
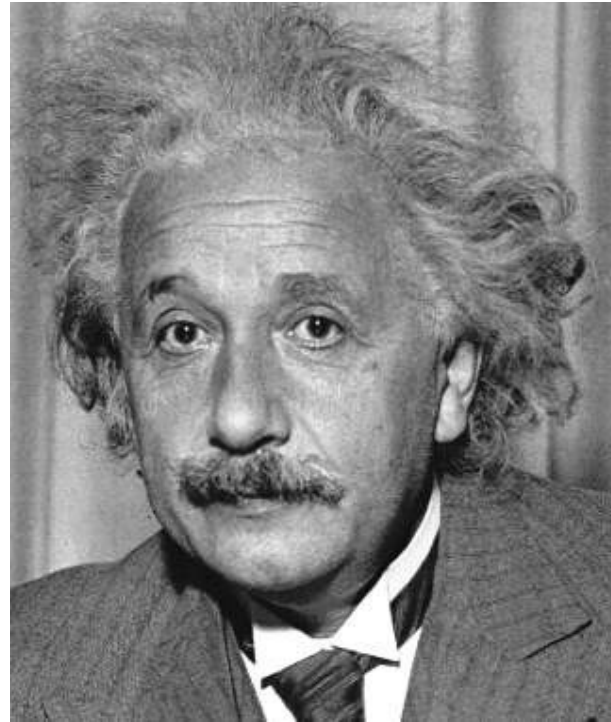
Los hackers hacen funcionar la WWW.

Si eres parte de esta cultura, si has contribuido a ella y otras personas saben quién eres y te llaman hacker, entonces eres un hacker.

Los mentalidad hacker no está confinada a esta cultura del software.

Hay gente que aplica la actitud de hacker a otras cosas, como la electrónica o la música.

Los hackers de software reconocen estos espíritus emparentados en otras partes y pueden llamarlos "hackers" también— y algunos sostienen que la naturaleza hacker es en realidad independiente del medio particular en el cual el hacker trabaja.



Nos centraremos en las habilidades y actitudes de los hackers de software, y en las tradiciones de la cultura compartida que originó el término "hacker".

Existe otro grupo de personas que se llaman a sí mismos hackers, pero que no lo son.

Son personas (generalmente varones adolescentes) que se divierten irrumpiendo ilegalmente en ordenadores.

Los auténticos hackers tienen un nombre para esas personas: "crackers", y no quieren saber nada de ellos.

Los auténticos hackers opinan que la mayoría de los crackers son perezosos, irresponsables y no muy brillantes, y fundamentan su crítica en que ser capaz de romper la seguridad no le hace a uno un hacker.

Desafortunadamente, muchos periodistas y escritores utilizan erróneamente la palabra "hacker" para describir a los crackers; esto causa enorme irritación a los auténticos hackers.



La diferencia básica es esta:
Los hackers construyen cosas;
los crackers las destruyen.



La actitud del hacker

Los hackers resuelven problemas y construyen cosas, y creen en la libertad y la ayuda voluntaria mutua.

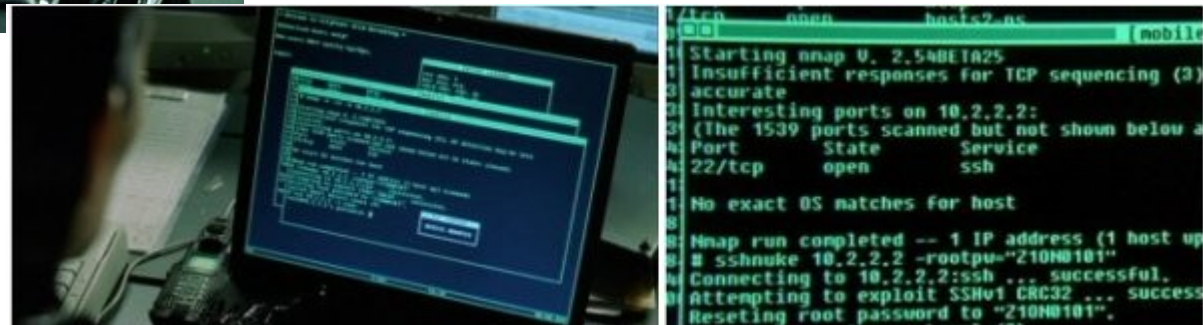
1. El mundo está lleno de problemas fascinantes que esperan ser resueltos
2. Ningún problema tendría que resolverse dos veces
3. El aburrimiento y el trabajo rutinario son perniciosos.
4. La libertad es buena.
5. La actitud no es sustituto para la competencia.



"Le Chant du Cygne"

Habilidades básicas para el hacking

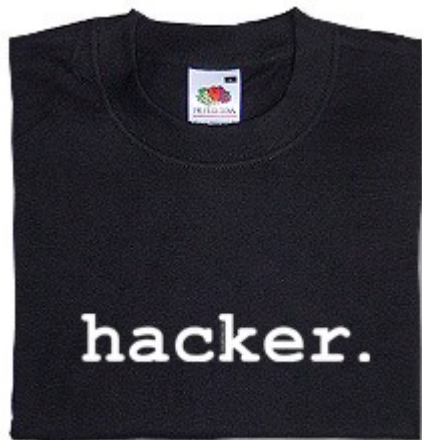
1. **Aprende a programar.** Python, C, Java, Php, Perl
2. **Consigue uno de los Unices libres;** aprende a usarlo y a ponerlo en funcionamiento. Unix es el sistema operativo de Internet. Linux, BSD.
3. **Aprende a usar la Web y a programar en HTML.** tu página debe tener contenido —debe ser interesante y/o útil para los otros hackers.
4. **Si no tienes un inglés funcional, apréndelo.**



Estatus en la cultura hacker

El hackerismo es lo que los antropólogos denominan **una cultura del don**. Adquieres estatus y reputación no mediante la dominación de las otras personas, ni por ser hermoso/a, ni por tener cosas que las otras personas desean, sino por donar cosas. Específicamente, al donar tu tiempo, tu creatividad, y el resultado de tu destreza.

1. Escribir software de fuente abierta.
2. Ayudar a probar y depurar software de fuente abierta.
3. Publicar información útil.
4. Ayudar a mantener en funcionamiento la infraestructura.
5. Hacer algo por la cultura hacker en sí misma.



Cuestiones de estilo

Para ser un hacker, debes desarrollar la mentalidad del hacker. Existen algunas cosas que puedes hacer cuando estás sin ordenador, que pueden ayudarte.

- ✓ Aprende a escribir correctamente en tu lengua.
- ✓ Lee ciencia-ficción. Ve a las reuniones sobre ciencia-ficción.
- ✓ Estudia zen, y/o practica artes marciales.
- ✓ Desarrolla un oído analítico para la música.
- ✓ Aprenda a tocar correctamente algún instrumento musical, o a cantar.
- ✓ Desarrolla inclinación por los dobles sentidos y los juegos de palabras.

Cuanto más cosas de estas hayas hecho, es más probable que poseas material natural para hacker.

Trabaja tan intensamente como juegas y juega tan intensamente como trabajas. Para los verdaderos hackers, la diferencia entre "juego", "trabajo", "ciencia" y "arte" tienden a desaparecer, o mezclarse en un alto nivel de creatividad. Además, no te des por satisfecho con tener un estrecho rango de habilidades.

B asado en el artículo de Eric S. Raymond



¿Como convertirse en un hacker?

Sólo se puede ser hacker de las cosas que uno le gustan y entusiasman. No se puede ser hacker por obligación.

El código de ética del hacker —que no tiene porque coincidir con el código legal ;-)- — puede resumirse en los siguientes puntos:

1. El acceso a los ordenadores, y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo debería ser ilimitado y total.
2. Básate siempre en el imperativo de la práctica.
3. Toda información debería ser libre.
4. Desconfía de la autoridad y la tradición: piensa por tí mismo.
5. Los hackers deberían ser juzgados únicamente por su habilidad en el hackeo, no por criterios sin sentido como los títulos, edad, raza o posición social.
6. Todo es copiable.
7. Los derechos de propiedad intelectual, son inmorales.
8. Se puede ser artista frente a una computadora.
9. Cracker = perdedor

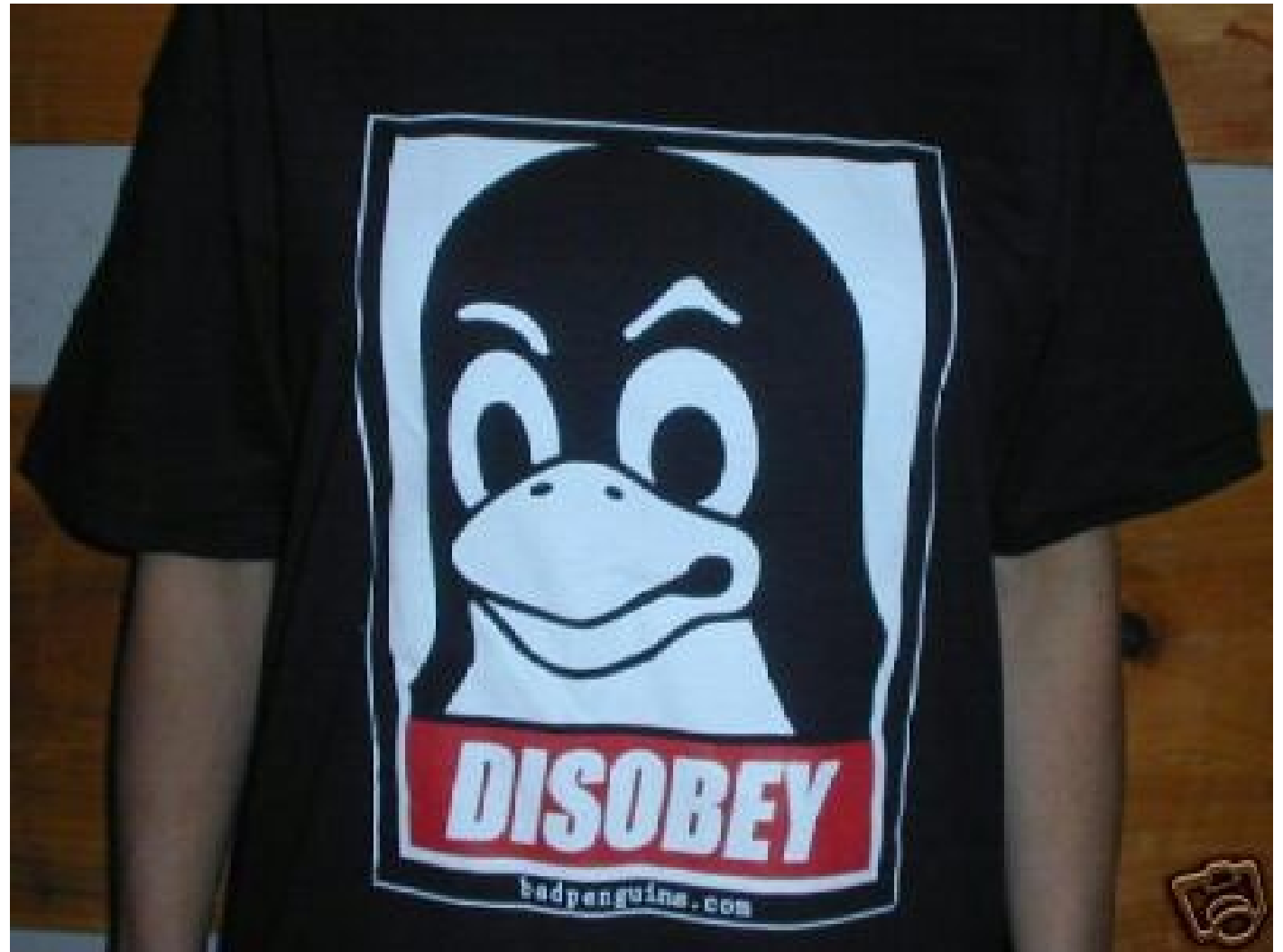
Pasos que se deben seguir para convertirse en un hacker. Entre ellos están:

- * **Crea tu página en internet.** Dado que la mayoría del hackeo se hace sobre el Web, debes tener claro como se hacen los sitios de Internet.
- * **Instala Linux en tu computadora.** Esto sin duda es lo más importante, Linux te obliga a revisar código y opciones de configuración que te hacen entender cómo funciona una computadora "hacia adentro" y "hacia afuera".
- * **Regala tanto CDs de software libre como puedas.** Hay que hacer algo por la causa.
- * **Aprende un lenguaje de programación y SQL.** Esto es fundamental, te sorprenderás como en unos pocos meses aprendes a dominar Python y comienzas a desarrollar tus propios programas de hackeo.
- * **Practica, practica, y practica.** Todas las horas que puedas.
- * **Publica las cosas que vas aprendiendo.** Mantén tu sitio actualizado de las cosas que vas descubriendo.
- * **Ayuda a los demás.** Sé generoso, cuando ya seas un hacker recuerda que hay otra generación de hackers detrás de ti y hay que pasarles la antorcha.

De esta manera llegarás a ser un hacker respetado dentro de la comunidad.

Niveles y técnicas de hackeo:

- ✓Change Coding
- ✓SQL Injection
- ✓Phising
- ✓Dictionary's attack
- ✓buffer overflow
- ✓Denegation of Service o
DOS
- ✓Root hacking



✓Change Coding.

Este tipo de hackeo es muy divertido y, la mayoría de las veces, inocuo. Se trata simplemente de modificar el código que despliega una página de Internet agregando órdenes en javascript o VB Script desde la barra URL del navegador. Incluso la elemental página de Google ha sufrido este tipo de hacking.



<http://bunnyherolabs.com/dhtml/monster-info.php>

Ejemplo:

```
javascript: document.body.contentEditable = 'true';  
document.designMode = 'on'; void 10
```

Fuente: <http://www.youtube.com/watch?v=lzdRgHabqI4>

SQL Injection

Como habrás notado, muchos sitios en la red muestran una caja de "Buscar" o "Search". En SQL el punto y coma (;) funcionan como el fin de comando y el doble guión (--) como comentario. Si sabes el nombre de la tabla (o intentas adivinarlo) donde se guardan los passwords de los usuarios puedes jugar un poco enviando cosas como: UPDATE users SET password="hack"; este tipo de hackeo es muy entretenido (horas y horas de sana diversión ;-)) y te sorprenderás del hecho de que incluso sitios de grandes empresas internacionales no poseen ningún sistema de filtrado. SQL Ruleezzz!!!



Ejemplo:

modules.php?name=Statistics

SQL: modules.php?

name=Search&type=comments&

%20%20%20query=&

%20%20%20query=loques

ea&instory=/**/UNION/**/SELECT/**/0,0,p
wd,0,aid/**/FROM/**/nuke_authors

Fuente.

<http://maxicap14.mforos.com/1321251/7977886-deface-a-las-webs-en-php-nuke-sql-tutorial/>

Phising.

Es una técnica que consiste en duplicar (hasta en el más mínimo detalle) un sitio web verdadero en nuestro propio servidor. Debemos ir a Hotmail, Gmail, Yahoo!, etcétera, ver el código HTML y guardarlo en nuestro propio server. Luego enviamos un email a la persona de la cual deseamos su clave con algo como "Alguien muy especial te ha enviado una Ciber-tarjeta, haz click aquí" y lo enviamos a nuestro propio Webserver en Linux. El usuario cree que está entrando en la página de inicio de Hotmail e introduce su login y password, ¡pero ahora es nuestro!



BBVA Bancomer

- Inicio
- Personas
- Patrimonial
- Privada
- Negocios PyMEs
- Empresas
- Gobierno
- Corporativos
- Preferred Customers

- Productos y Servicios**
- Productos y Servicios
- Conócenos**
- Grupo BBVA Bancomer
 - Estudios Económicos
- Unidades de Negocio**
- Afore
 - Asset Management / Fondos
 - Casa de Bolsa
 - Inmuebles
 - Mercados Globales
 - Pensiones
 - Seguros
 - Hipotecaria Nacional

Regístrate y usa **Bancomer móvil** y ¡participa en el sorteo!



Más información aquí

Consejos de Seguridad




Regístrate y Gana Winner Card **Bancomer móvil**

Becalos

Con Winner Card... gana al instante una membresía con 12 boletos para ir al cine y pasa unas vacaciones de película. [mas >>](#)

Lunes 23 de Agosto del 2010	
IPC	24,150.94
DOWJONES	8,497.18
DOLAR INTB. CPA,	13.41
DOLAR INTB. VTA,	13.42
EURO CPA,	18.71
EURO VTA,	18.72
CETES 28	5.01
TIIE 28	5.2250
BBVA*	155.01 más >>

Tarifas y Comisiones
Empleo | Seguridad | Legal

Ayuda Bancomer

Acceso Banca en Línea

Numero de Tarjeta

Registro/activación Banca en Línea

- Servicios en Línea**
- Impuestos
 - Alertas al celular
 - B-mail
 - Sucursales y cajeros
 - Contactanos
 - Noticias
 - ¿Sabias que?

y **Débito Bancomer**



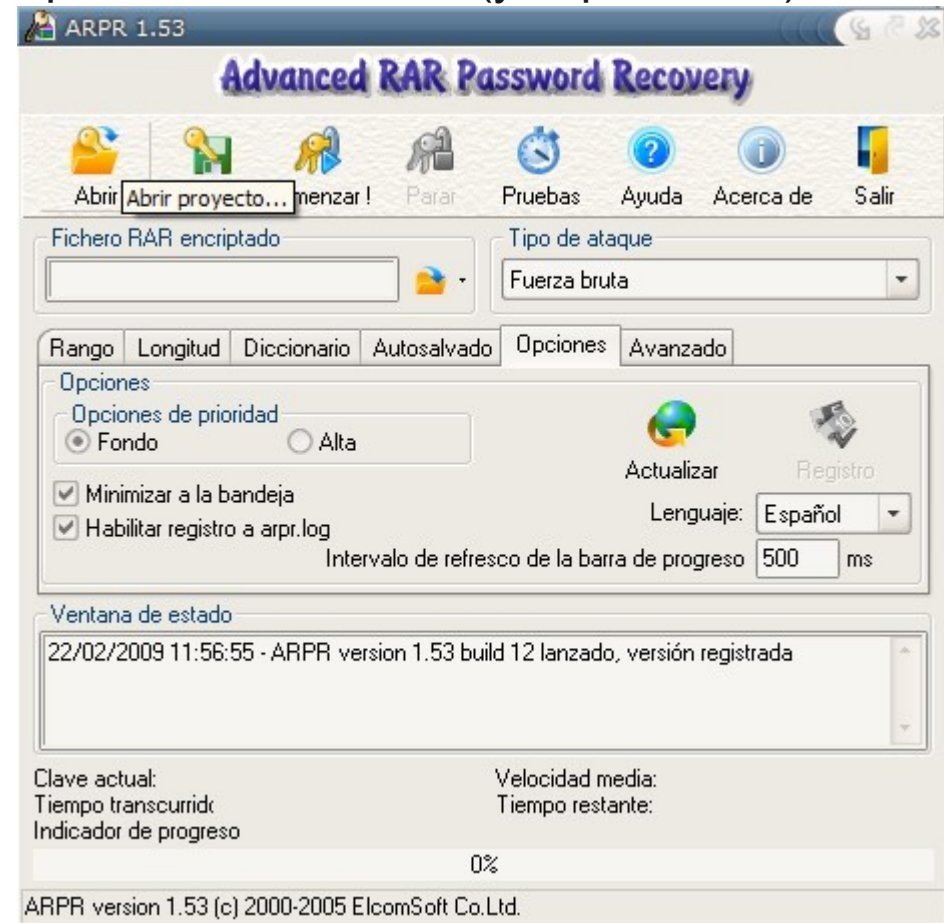
Dictionary's attack

Existen personas (y administradores de sistemas) que piensan que por usar palabras como "fanerogama" o "porfirogeneta" como password, nadie los podrá adivinar. Pero en realidad esas palabras existen en cualquier diccionario, y los diccionarios que sirven para revisar la ortografía en los procesadores de texto como AbiWord, también pueden ser usados para intentar logearse dentro de un sistema ajeno. Existen scripts que usan cada palabra de los diccionarios en español, inglés, francés, finlandés, turco, etc. para hacer un login. Estos scripts pueden tardarse mucho tiempo hasta encontrar un password que corresponda a la palabra y cuando lo hacen, envían un email al hacker para avisarle cual palabra es un password. Los hackers que se consideran a sí mismos elegantes y creativos sienten aversión por este tipo de hackeo pues en el simplemente se aplica la fuerza bruta (y la paciencia).

HOW SECURE IS MY PASSWORD?



It would take
About 42 trillion years
for a desktop PC to crack your password



buffer overflow (o simplemente overflow). Los programas se almacenan en buffers (secciones contiguas de memoria), bajo ciertas circunstancias los datos que se envían al buffer sobrepasan su capacidad y la memoria se "desparrama", generalmente esto provoca que el programa colapse pero muchas veces, durante una pequeña fracción de segundo, la información enviada al buffer puede ejecutarse con los permisos del usuario dueño del proceso. El hacker (que debe conocer bien C y ensamblador) aprovecha esto, envía muchos datos al buffer, para desbordarlo y ejecutar código malicioso. Existen pocos hackers con el suficiente talento como para aprovechar un overflow recién descubierto, el problema es que luego de un par de semanas de conocido el exploit, comienzan a aparecer en la red scripts que automatizan el hackeo y todos los script kiddies comienzan a ejecutarlos. Solución: coloque un "apt-get -f -y dist-upgrade" en el cron y manténgase informado.

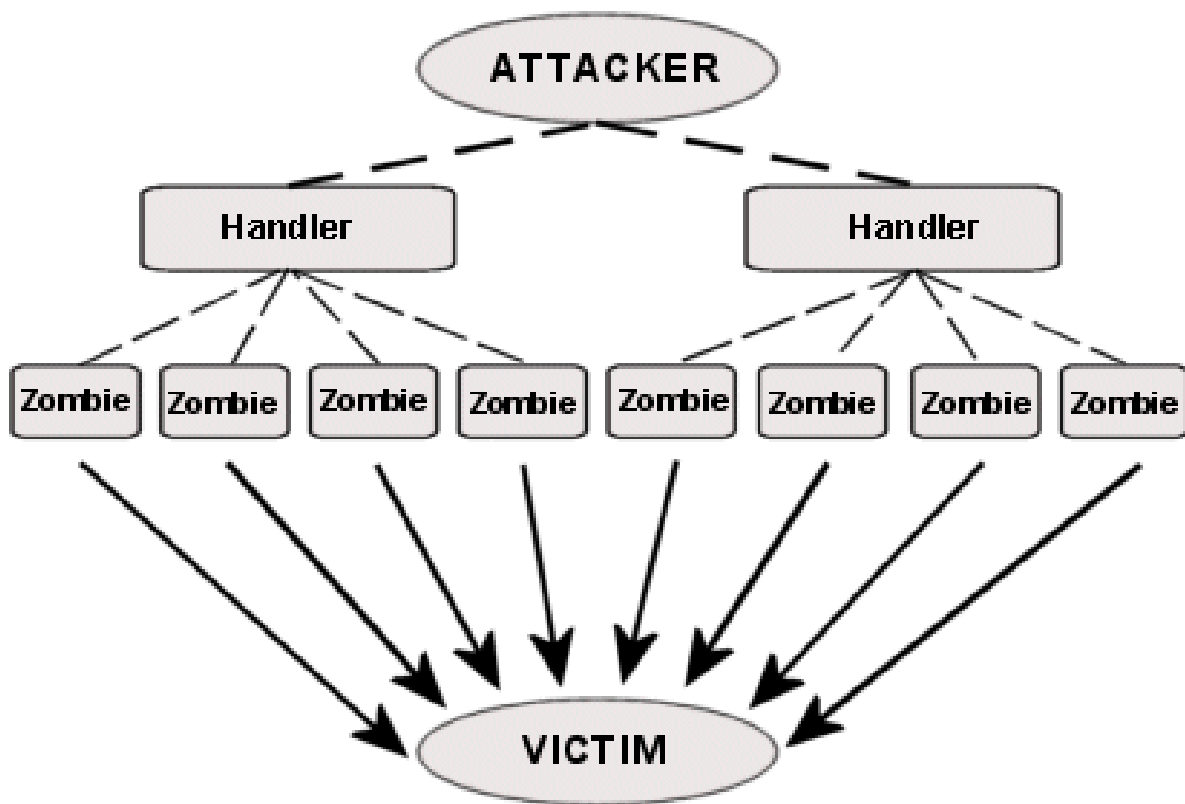
Ejemplos:

<http://www.securitytube.net/Exploiting-a-buffer-overflow-under-Linux-kernel-2.6-with-ASLR-through-ret2reg-video.aspx>

Denegation of Service o DOS

La denegación de un servicio implica que el hacker ha aprovechado un bug en un programa para "tirar" un servicio del servidor. Generalmente se trata del Webserver. El IIS de Microsoft es particularmente vulnerable a este tipo de ataques. Tanto el Change Coding como el DOS son hacks relativamente benévolos pues no implican (necesariamente) a un intruso en el sistema.

Architecture of a DDoS Attack



OPERATION PAYBACK

After GMlegal taking down their own site before the countdown ended, effectively surrendering, we changed target to MinistryOfSound.com and brought them down within minutes, along with their sales page, for about 24h.

Now it's time for a new target: www.sgae.es [217.116.5.84]

Their slogan is "believe in culture".
They don't understand that our culture is: "Sharing is caring"

Join us on IRC [irc.skidsr.us](irc://irc.skidsr.us) #savethepiratebay
or open TIEVE.TK in your browser.

TOOLS:

(no hivemind mode available for macflags)
Windows & Linux: [Mac users can use JavaLOIC: sourceforge.net/projects/javaloc/](http://sourceforge.net/projects/javaloc/)
IRC-LOIC with HIVEMIND feature: <http://github.com/NewEraCracker/LOIC/downloads>
Set server to gibson.skidsr.us and click "hivemind" and you're done!
Hivemind mode lets us set target and start the attack without you having to do anything, so you can leave your PC on and go to work/school and still be part of this.
Make a shortcut and add `/hivemind gibson.skidsr.us /hidden` to the "goal" to start it in hivemind mode invisibly (hidden to background) [use "*" instead of "/" on linux]

TIME OF ATTACK

Countdown: www.3.ly/4nRe

23:00 UTC // 6PM EST

Application level

Esto ya es más serio, alguien se ha apropiado de una aplicación del sistema. La mayoría de las veces se trata de una aplicación Web como PHP-Nuke o MyAdmin. Sin embargo en ocasiones el dominio de una aplicación conduce a tener más accesos y facilidades en el hackeo.

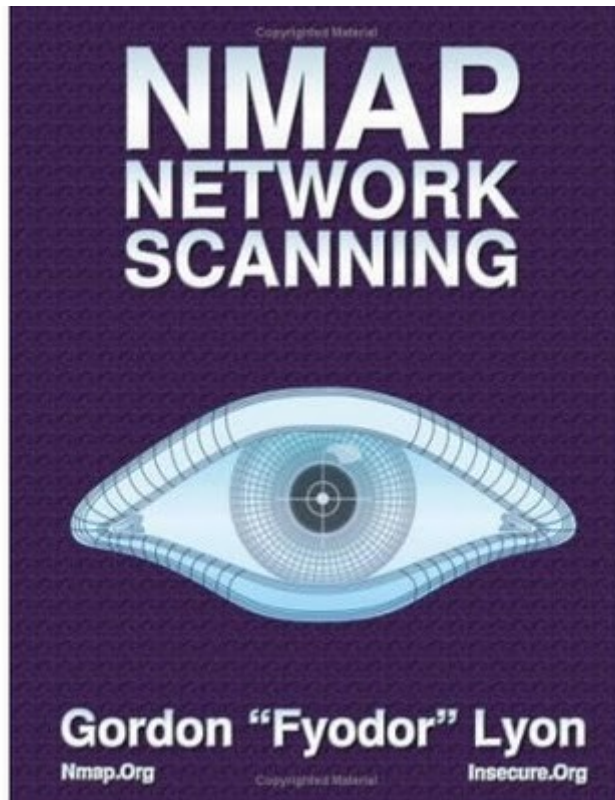
Root hacking

Este es el hack más grave, el hacker ha tomado el control del sistema y puede hacer lo que quiera con él. Generalmente el hacker tratará de pasar desapercibido y creará un usuario con todos los derechos para entrar cuando quiera al sistema y regodearse de lo poco hábil que es el administrador.

Escaneo de puertos.

Permite conocer que puertos y servicios ofrece un Equipo.

```
nmap -sS -sV -P0 www.pagina.com
```



```
airdump@:~$ nmap -sT -F -PT 192.168.1.1

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-02 19:23 CET
Interesting ports on 192.168.1.1:
Not shown: 1253 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

Nmap finished: 1 IP address (1 host up) scanned in 23.401 seconds
airdump@:~$
```

<http://airdump.net>

*Básado en el texto de aarkerio. manuel_ARRROBA_mononeurona.org
<http://mononeurona.org/pages/display/148>*

Hackeando con Google

- ✓ <http://enlinea.guadalajara.gob.mx:8800/Licenciasayb/sql%27s/licenciasc.sql>
- ✓ <http://www.lapaz.gob.mx/sistemaimages/>
- ✓ <http://edn.issste.gob.mx/nod/>
- ✓ http://secundaria1.sep.gob.mx/Desktop/alumnos_sadok.sql

Sitios Recomendados.

Grupo de Usuarios Linux de Chicoloapan

<http://linux.sanvicentechicoloapan.com.mx>

Mononeurona.org

barrapunto.com

Login | Créate una cuenta | Bitácoras

Secciones

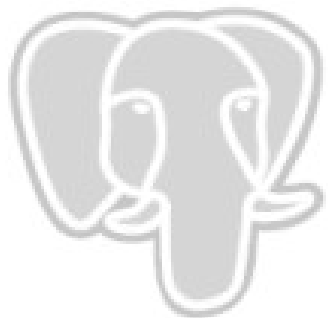
Slashdot NEWS FOR

▶ Stories  [Recent](#) [Popular](#) [Search](#)



Comunidad de Alumnos y Egresados del CECyTEM Chicoloapan
<http://cecytemchicoloapan.net>

PostgreSQL



Google™
app engine



ORACLE®

