GUÍA DE INICIACIÓN AL HACKING

Orientada a sistemas Windows 95 /98 / ME /NT /2k /XP

REALIZADA POR: HeChiCeRa
Con la colaboración de: NoRegret.
http://www.hackingparanovatos.com

Índice.

1. Introducción

Esta guía está pensada para todo aquel que quiere iniciarse en el Hacking, pero que no sabe por donde empezar. Los conocimientos que se requieren para comprender todo de lo que se va a hablar aquí son: conocimientos de informática en general, conocimientos amplios de Internet (no os vamos a enseñar como buscar en el google...) y soltura en el manejo de un sistema Windows.
Que quede claro que esta guía, está pensada para un entorno Windows, pero recordad que sí de verdad queréis ser alguien en este mundillo, debéis usar un sistema Unix, puesto que Windows está verdaderamente limitado, en cuanto a que no dispone de herramientas de las que dispone un Unix, bueno, que no me enrollo más, ¡empecemos de una vez!

** Notas: Las palabras escritas en rojo, significan que son palabras que vamos a definir.
Las palabras escritas en azul significan que son comandos que vamos a utilizar.

1.1 ¿Qué equipo informático necesitas?

Un ordenador normalito (Pentium 100 te llega).
32 Megas de ram
Conexión a Internet en casa, claro.
Sistema Operativo: Windows 95 / 98 / NT / XP / 2000

En fin, ahora viene la pregunta crítica ¿Por donde empezamos?, bueno, yo creo que deberíamos empezar porque conozcas como funciona tu equipo a nivel de red local y red Internet.

###############...
Red local: tu ordenador en casa conectado con el de tu hermanito, para compartir la conexión y echar batallitas al Quake.
Red Internet: cuando te conectas y tu modem hace pittt, piit, ... xD. En serio, es cuando te conectas con tu proveedor de Internet, para ver páginas webs, chatear...
###############...

1.2 Repaso de red local y red Internet.

Tu red local, tiene asignados unos números llamados IPs (vendría a ser como una matrícula para identificar a tu ordenador a las demás personas o máquinas) que tienen el siguiente formato:

xxx.xxx.xxx.xxx
Ejemplos de ips: 213.42.34.56; 80.54.67.34;
Nunca ningún número puede superar el 255, es decir, números de IPs INVÁLIDOS:
276.543.56.34; 123.45.267.645

Si no tienes más que un ordenador, entonces hablaremos de localhost (ordenador local traducido a spanish), entonces tu ordenador tendrá la siguiente IP: 127.0.0.1 <---- ESTA ES TU IP LOCAL cuando tu máquina no está conectada a ninguna otra.
** Nota: la IP que tiene asignado tu PC (127.0.0.1) tiene asignado un nombre, que es "Localhost", así que si introduces un comando haciendo referencia a tu PC, da igual que pongas: comando 127.0.0.1 o esto: comando localhost. Esta dirección siempre existe, tengas o no red local.

Hagamos una prueba:
Abre una ventana de MS-Dos escribe: ***ipconfig*** te saldrá algo como esto:

```
=======================================
Configuración IP de Windows

Adaptador Ethernet Internet          : # Estos son los datos que utilizas para conectarte Internet
      Sufijo de conexión específica DNS:
      Dirección IP. . . . . . . . . . . : 82.21.102.180 <---------------- IP que utilizas cuando te conectas
      Máscara de subred . . . . . . . . : 255.255.255.191
      Puerta de enlace predeterminada   : 82.21.102.1

Adaptador Ethernet Conexión de área local          : #Datos que utiliza tu red local.

      Sufijo de conexión específica DNS:
      Dirección IP. . . . . . . . . . . : 192.168.0.1 <------------------- IP en tu red local
      Máscara de subred . . . . . . . . : 255.255.255.0
      Puerta de enlace predeterminada   :
=======================================
```

Y ahora te estarás preguntando: ¿Qué es eso de Adaptador Ethernet Internet y ....???¿?

Tranquilo, vayamos por partes:
1º. La información que he puesto ahí arriba será similar a la que te aparezca a ti, es decir, SIMILAR así que luego no me escribáis diciendo es que a mi no me sale todo eso. :P

Bien, ahora imaginemos que en vez de tener un sólo ordenador tienes dos, eso quiere decir que tú has configurado la conexión entre esos dos ordenadores, así que no te tendría que explicar nada, pero bueno, le daremos un repaso.

Cuando hiciste lo de ***ipconfig***, pudiste ver esta info:

==========
Adaptador Ethernet Conexión de área local : #Datos que utiliza tu red local.

Sufijo de conexión específica DNS :
Dirección IP. . . . . : 192.168.0.1 <---------- IP en tu red local
Máscara de subred . . . . . : 255.255.255.0 <---------- Mascara en tu red local
Puerta de enlace predeterminada :
==========

Cuando configuras una red local, a tu ordenador le asignas una IP que suele ser esta: 192.168.0.1
Y porqué esta IP y no otra? pues por convenio, se ha decidido que el rango del 192.168... loquesea será para ordenadores en una red local. El último número (el 1) es para indicar que es el ordenador uno en esa red. Aunque ya te digo, esta IP puede variar, por ejemplo: 192.128.0.2, 192.168.1.35....

Con lo que sabemos de la red local ya es suficiente, si quieres saber más profundamente te aconsejo de que busques por la red algún manual. Porque esta es una guía de hacking !! :P

En cuanto a la IP de Internet decirte que es la que aparece a continuación:
==========
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 82.21.102.180 <---------- IP que utilizas cuando te conectas
Máscara de subred . . . . . : 255.255.255.191
Puerta de enlace predeterminada : 82.21.102.1
==========
Esta IP es estática (fija, que no cambia) si tienes una conexión permanente a Internet (adsl, cable,...) o es dinámica (cambia cada vez que te conectas) si tienes tarifa ((semi)plana, conexión de modem...)

2. Manejándonos con comandos de red del MS-Dos

Ahora nos vamos a familiarizar con comandos del MS-Dos, relacionados con Internet claro ! (no os vamos a explicar el dir, ni el cd...)

2.1. ***Ping***: sirve para saber si un determinado ordenador está conectado.

Ejemplo: ping www.yahoo.es y te devuelve:

==========
Haciendo ping a www2.vip.lng.yahoo.com [217.12.3.11] con 32 bytes de datos:

Respuesta desde 217.12.3.11: bytes=32 tiempo=324ms TTL=243

Respuesta desde 217.12.3.11: bytes=32 tiempo=189ms TTL=243
Respuesta desde 217.12.3.11: bytes=32 tiempo=672ms TTL=243
Respuesta desde 217.12.3.11: bytes=32 tiempo=214ms TTL=243

Estadísticas de ping para 217.12.3.11:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 189ms, Máximo = 672ms, Media = 349ms
==========
Esto significa que yahoo te responde y que sus ordenadores están online (conectados).

Pero si te aparece esto:
==========
Haciendo ping a xxx.xxx.xxx.xxx con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para xxx.xxx.xxx.xxx:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
==========
Significa que esa máquina está offline (no conectada) o que no devuelve los pings, es decir, podemos configurar nuestro sistema para que cuando alguien nos haga un ping a nuestra IP le aparezca la info de offline, pero eso lo veremos más adelante. ;)

Ahora hacemos una pausa, porque para el siguiente comando necesitas saber que es un puerto. Así que, haya vamos:

Los ***puertos*** son como buzones de correo, nada más que en vez de tener un buzón de correo como en tu casa, pues tienes unos 65000, así que ya tenemos claro una cosa: un puerto es como un buzón lógico, por el cual entra y sale información. En tu ordenador probablemente tengas algunos puertos abiertos, y la mayoría de ellos cerrados. ¿Porqué tienes puertos abiertos? Pues porque esos determinados puertos que tienes abiertos necesitan estar abiertos para mandar en algún momento información. Pero como veremos más adelante podemos configurar nuestro ordenador para que los puertos se abran sólo cuando haya que enviar información y no que siempre estén abiertos.

2.2 *netstat*

Este comando muestra los puertos que tenemos abiertos en ese momento, la dirección remota que está utilizando ese puerto y el estado.

En la misma ventana de MS-Dos escribe: netstat, te aparecerá algo como esto:

```
==========================================================
  Proto  Dirección local       Dirección remota                    Estado
  TCP    mipc:3499             dclient217-162-98-205.hispeed.ch:4661  ESTABLISHED
  TCP    mipc:3935             cliente-217216001234.cm128.alnpa.supercable.es:4662  TIME_WAIT
  TCP    mipc:3953             elx1-interjet256-146-186.medtelecom.net:4662  ESTABLISHED
  TCP    mipc:4950             cm10537.telecable.es:4662           ESTABLISHED
  TCP    mipc:2869             mipc.mshome.net:3942                TIME_WAIT
  TCP    mipc:2869             mipc.mshome.net:3950                TIME_WAIT
  TCP    mipc:3943             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3944             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3947             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3948             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3949             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3951             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:3952             mipc.mshome.net:2869                TIME_WAIT
  TCP    mipc:9078             mipc:0                          LISTENING
  TCP    mipc:1027             mipc:0                          LISTENING
  TCP    mipc:3001             mipc:0                          LISTENING
```

TCP --> es el protocolo correspondiente a ese puerto.
Hagamos un paréntesis para explicar lo que es un protocolo.

Protocolo: es un conjunto de reglas (leyes, formalidades, ...) que tu ordenador utiliza para comunicarse con otros ordenadores y que se entiendan, es decir, es como su lenguaje para entenderse entre ellos. :)
Dirección local --> ahí aparece el nombre de nuestra red y el nº del puerto.
Dirección remota --> la dirección que está conectada a nuestro PC, en ese ejemplo tenemos a cuatro usuarios o servidores conectados a nuestro PC:

dclient217-162-98-205.hispeed.ch:4661
cliente-217216001234.cm128.alnpa.supercable.es:4662
elx1-interjet256-146-186.medtelecom.net:4662
cm10537.telecable.es:4662

Estado --> Established: significa que hay una conexión establecida entre un ordenador ajeno y el nuestro.

Time_Wait: tiempo en espera, es decir, una vez cerrada la conexión, el puerto está en espera de recibir más datos.

Listening: el puerto se encuentra disponible, por si necesitamos acceder a él.

** Nota: este comando tiene unos parámetros que si quieres puedes utilizarlos o no, si los utilizas recuerda que deben ser introducidos a continuación del nombre, ejemplo: netstat -a, no los voy a explicar todos porque sino sería muuuuuy largo y pesado. Sólo decirte que si quieres más información escribe:

netstat /? o netstat -help

2.3. *nbtstat*

Este comando no puede ser utilizado como el anterior, es decir, no funciona con poner simplemente nbtstat, tienes que ponerle a continuación algún parámetro o parámetros.
El nbtstat nos mostrará las conexiones actuales del protocolo TCP/IP usando NetBios.

NetBios: protocolo utilizado para compartir archivos y/o impresoras en una red. En este caso utiliza el puerto
139, si fuera mediante el protocolo UDP en vez del TCP/IP utilizaría el 137 y el 138.

Si escribimos: nbtstat -a IP (donde IP, es una dirección de alguien o la nuestra) nos aparecerá algo como esto:

```
=====================================================
        NetBIOS Remote Machine Name Table

    Nombre                  Tipo          Estado
   ---------------------------------------------------------------------
   MiPC                        <00>    Único      Registrado
   Zoy tonto              <20>    Único      Registrado
   MiPC                   <00>    Grupo      Registrado
   MiGrupo                     <1E>   Grupo      Registrado
   MiPC                        <03>    Único      Registrado
   ..__MSBROWSE__.         <01>    Grupo      Registrado

   Dirección MAC = 00-C0-49-48-6E-67          <-------- Esto, en principio, no nos interesa, es el nº interno que tiene su                                                                modem.
=====================================================
```

Nombre --> aquí aparece el nombre del PC y del grupo de trabajo, esto no nos interesa mucho.
Tipo --> esto sí que es importante, sobre todo los números que hay entre los símbolos "<>":
<00> /<03> -->Estos números son valores en hexadecimal que indican algo al sistema, el <20> que es el que nos interesa indica que ese ordenador tiene recursos compartidos hacia el exterior, que quiero decir con esto de recursos, pues que tiene carpetas, archivos (fotos, música, ...), impresoras, etc,. Muchas veces estos recursos compartidos estarán protegidos con contraseña para que no pueda acceder ningún intruso, pero otras veces estarán sin contraseña por lo que cualquier persona puede hacer lo que quiera con los recursos compartidos de ese ordenador.

Si al ejecutar el comando nbtstat -A IP, os aparece "Host no encontrado", significa que esa IP no existe, no está conectado o tiene cerrado el puerto 139.

** Nota: este comando dispone de más parámetros, si deseas más información escribe: nbtstat.
** Nota2: más adelante veremos como proteger nuestro PC, para que podamos compartir archivos

y que ningún intruso se nos cuele en el PC

2.4. net

Este comando nos muestra información de nuestra red. Tiene muchos parámetros que no los vamos a explicar aquí porque nos podría llevar 100 hojas y os dormiríais antes de llegar a la hoja 3. Sólo deciros que si queréis más
info tenéis que escribir net help.
Pero sí os voy a nombrar uno de los parámetros más importantes: view. Poned esto:
net view \\IP (donde IP, es la IP del ordenador anterior que hemos comprobado con el comando nbtstat) --> os mostrará los discos duros y /o carpetas que tiene compartido ese ordenador

```
==============================================================================
Nombre de recurso compartido            Tipo      Usado como      Comentario
-------------------------------------------------------------------------------
Documentos                              Disco
Juegos                          Disco
Mp3                             Disco
Programas                               Disco

Se ha completado el comando correctamente.
```

Como podemos ver este PC tiene compartido las carpetas: "Documentos", "Juegos", "Mp3", "Programas". Si quisiéramos ver todo lo que hay dentro de esas carpetas, lo que tendríamos que hacer es: abrir una ventana de nuestro navegador y escribir \\IP\nombre de la carpeta. Por ejemplo: \\IP\Juegos

3. Obteniendo IPs

Una de las preguntas que más me a han preguntado es la "¿Cómo resolver IPs?", a continuación voy a explicar como resolver IPs a través de determinados programas.

3.1 A través del IRC

Para obtener la IP de una persona conectada al IRC lo único que tienes que hacer es escribir:
/dns nick y te aparecerá la IP de ese nick.
Esto sólo es válido en servidores que no asignen IPs virtuales, es decir, si te aparece algo como esto:
v34lvdf.345fd.sfl3@sinectis.com.ar no te vale. La única forma de averiguar la IP de servidores donde la encriptan es enviarle un fichero a esa persona o iniciar una conversación por dcc y te aparecerá la IP en la pantalla de Status (estado, en spanish) de tu cliente de IRC, si no te aparece lo que tienes que hacer es enviarle el fichero o la conversación y mientras este se esté enviando abres una ventan de MS-Dos y escribes el comando ***netstat -a***, y ahí te saldrá la IP de esa persona.

Una pregunta que me han hecho varias veces es: "Al hacer ***netstat -a*** me aparecen muchas IPs, ¿Cómo sé cual es la IP de ese nick? Bueno, lo mejor, sino controlas mucho aún, es que antes de enviarle el fichero, ejecutes el netstat -a y veas las IPs que te aparecen, luego cuando estés enviando el fichero y vuelvas a ejecutar el comando, fíjate bien cual es la IP nueva que te acaba de aparecer. Ahm, y te aconsejo que mantengas todos lo programas que puedas cerrados, menos el que vas a utilizar para enviar el fichero. Es decir, no abras páginas web mientras tanto, cierra el programa de descargas, si tienes alguno (eDonkey, Kazza,....).
De esa forma te saldrán menos IPs.

3.2 A través de correo electrónico

Si te ha llegado un email y deseas saber la IP de quien te lo envío, lo único que tienes que hacer es: botón derecho encima del mensaje y a continuación escoges la opción: Propiedades, te aparecerá una ventanita que tiene dos solapas: General y Detalles, a nosotros la que nos interesa es la de Detalles.
Te aparecerá información similar a esta:

**Nota: las letras en cursiva son los comentarios que he puesto para explicaros las líneas del mensaje.
** Nota 2: he suprimido líneas, sólo he dejado las de mayor importancia

==========

Received: from 201.11.113.127 [201.11.113.127] by th09.opsion.fr id 200204081905.106d;
** Aquí vemos la IP de quien nos mandó el mensaje, en este ejemplo es: 201.11.113.127 **

Mon, 8 Apr 2002 19:05:17 GMT ** Fecha y hora en la que nos mandó el email **

From: "zoyyo" <zoy_yo@hotmail.com> ** Email de la persona que nos mandó el mensaje **

To: mi_email@viva_el_hacking.es ** Nuestra dirección de email **

Bcc: ** Si este campo está en blanco singnifica que no le mandó copia del mensaje a otra persona **

Subject: ¡¡Hola!! ¿Hasta donde quieres hackear hoy? ** Asunto del mensaje **

Content-Type: text/plain; charset=iso-8859-1; format=flowed ** Tipo de formato en el que se envío el mensaje **
==========

Como podrás ver, es en la primera línea donde aparece la IP del remitente.

3.4 A través de la mensajería instantánea

Es similar a los pasos seguidos para obtener una IP a través del Chat. Tienes que enviarle un archivo a la persona de la que quieres averiguar su IP, abres una ventana de MS-Dos, le envías el archivo y mientras se está transfiriendo escribes en la ventana de MS-Dos: ***netstat -a***, ahí te aparecerá su IP. Nuevamente te recuerdo que intentes mantener todos los programas que puedas cerrados de esa forma te saldrán menos IPs.

3.4 A través del nombre de dominio

Antes de explicarte cuales son los pasos a seguir, definiremos dominio.

Dominio: nombre asignado a una determinada IP. Ejemplo de nombres de dominio: www.google.com, www.terra.com, www.yahoo.com …

Para averiguar la IP debemos utilizar el comando anteriormente mencionado en la sección 2.1 --> ***Ping***
Abrimos una ventana de MS-Dos y escribimos: ***ping*** -a www.google.com, nos aparecerá algo como esto:

==========
Haciendo ping a www.google.com [216.239.39.101] con 32 bytes de datos:
** Esta IP que aparece es la que corresponde a Google **

Respuesta desde 216.239.39.101: bytes=32 tiempo=233ms TTL=47
Respuesta desde 216.239.39.101: bytes=32 tiempo=184ms TTL=47
Respuesta desde 216.239.39.101: bytes=32 tiempo=197ms TTL=47
Respuesta desde 216.239.39.101: bytes=32 tiempo=242ms TTL=47

Estadísticas de ping para 216.239.39.101:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 184ms, Máximo = 242ms, Media = 214ms
==========

4. Telnet

Programa incluido en el propio sistema operativo, para conectar a otra máquina de forma remota. Para ejecutar esta utilidad lo único que tienes que hacer es abrir una ventana de MS-Dos y escribes: ***Telnet***

** Nota: te recomiendo que utilices el "Putty", es un telnet muuuucho mejor que el de Windows, lo puedes encontrar en http://www.hackingparanovatos.com

Una vez abierto el Telnet, para conectar a una máquina escribes:
open "IPdelaMakina" "puerto"
(por cierto.... SIN las comillas ¡¡ eh !!)

NO es necesario que primero pongas telnet y luego open "IP" "puerto"; puedes ponerlo directamente así:
telnet "IP" "puerto"

** Nota: el puerto que utiliza el programa telnet es el 23

Ejemplo:
Abre una consola de MS-Dos escribe: telnet bbs.zruspas.org 23
Te aparecerá una pantallita de bienvenida, pues para saber lo que tienes que hacer, sólo tienes que leer lo que te va indicando, está todo en español así que es muy difícil que te pierdas. :)
Dependiendo a que bbs o servidor te conectes tendrás que seguir unos pasos determinados, que por lo general te los van indicando, si estás perdido no tienes más que escribir help.

En ocasiones cuando intentes entrar te pedirá un login y un password, a veces podremos conectar escribiendo como login guest (invitado) y el pass lo dejamos en blanco.
Si estás intentando introducirte en el ordenador de alguien por medio de telnet y no puedes conectar puede ser por:
- Tiene el puerto de telnet cerrado (el puerto 23)
- Tiene el puerto de telnet abierto, pero no permite conexiones al exterior
- Tiene el puerto de telnet abierto, pero no permite conexiones anónimas, es decir, como invitado. Por lo que necesitarás saber el login y password para conectar.
Si tu programa de Telnet te pregunta que emulación de terminal quieres usar (como queremos que nos muestre la información), escoge la VT100 es la estándar para las comunicaciones basadas en terminales

Los comandos fundamentales de telnet son:
Close: termina la conexión.
Quit: sale del programa Telnet
Set echo: si no ves lo que estás escribiendo.
Open: abre una conexión a la máquina especificada

5. FTP

Programa que se utiliza para transferir información almacenada en ficheros desde nuestra máquina local a una remota y viceversa.
Para ejecutar nuestro programa abrimos una ventana de MS-Dos y escribimos: ***ftp*** "IP" "puerto" o ***ftp*** "dominio" "puerto"

Ejemplo:
FTP www.yahoo.es o también
FTP 217.12.3.11

Una vez conectados nos preguntará el nombre de usuario y la clave, para la mayoría de los casos nos servirá con introducir como nombre de usuario: guest o sino anonymous y para pass no ponemos nada.

Comandos esenciales para manejarnos con el FTP:

open: abrimos conexión con una IP(123.53.45.33) o host(www.yahoo.com) especificado:.
close: cerramos la sesión a la que estamos conectados, pero NO sale del programa FTP.
quit: cerramos la sesión a la que estamos conectados y sale del programa FTP.
help: nos muestra todos los comandos del programa FTP.

Comandos que debemos utilizar una vez conectados a la máquina:

cd: para moverse de un directorio a otro.
lcd: para movernos a otra unidad de Nuestro PC. Es decir, nos movemos de C.\ a A:\ etc.
dir: para listar el contenido de un directorio.
!: para ejecutar un comando.
delete: para borrar ficheros.
mkdir: para crear un directorio.
pwd: para saber en el directorio en el que estamos
get: para bajarnos a nuestro ordenador un fichero de esa máquina.
put: para subir un fichero que está en nuestro ordenador a la máquina remota.

Ahora os voy a poner un ejemplo de como transferir un fichero llamado Foto que se encuentra en un servidor a nuestro ordenador.

C:\> ftp sol.sis.ucm.es <---- Aquí conectamos a la máquina remota
Welcome to National Center for Supercomputing Applications <-- Mensaje de bienvenida

FTP version 2.6.05 2/4/02 <---- Versión del FTP usado en ese servidor

220 sol FTP server (SunOS 4.1) ready.
***Username:* anonymous** <--- Introducimos anonymous como nombre de usuario.
331 Guest login ok, send ident as password.
Password: <-- Probamos a no introducir nada o introducimos nuestro email.

230 Guest login ok, access restrictions apply.
ftp> **lcd a:** <-- Nos situamos en nuestra unidad a:\
Local directory now B:
ftp> **cd /pub** <-- Vamos a la carpeta Pub de la máquina remota
250 CWD command successful
ftp>;**get foto** <-- Y nos bajamos el archivo foto a nuestra unidad a:\
200 PORT command successful.
150 ASCII data connection for INDICE (147.96.2.166,47293) (4850 bytes).
Transferred 4994 bytes in 2 seconds (2.438 Kbytes/sec)
226 ASCII Transfer complete. <-- Nos avisa de que la transferencia se ha completado
*ftp>***quit** <-- cerramos la sesión y salimos del programa
221 Goodbye.

6. Contraseñas

6.1 Archivos de contraseñas

Todas las contraseñas del Windows 95/98 se guardan en la carpeta Windows, bajo el nombre de usuario.pwl, donde usuario es el nombre que hayas introducido tú al instalar el Windows y pwl es la extensión de ese archivo.
Pwl son las siglas de PassWord List, es decir, lista de passwords.
Jamás bajo ningún motivo debes enviar tu archivo usuario.pwl por email, Chat, ... no se lo debes pasar a nadie.

¿Porqué? Pues porque como he dicho antes, en ese archivo se guardan tus contraseñas de Inicio de sesión de Windows,
login y password para conectarte a Internet, ... Más adelante explicaré como crackear estos archivos pero de otros usuarios, para averiguar sus contraseñas.
En Windows NT y Windows XP la cosa cambia, es decir, ahora los archivos de contraseña se guardan en:
windows/system32/config, con el nombre de sam.log, repito nuevamente que en la sección Crackeadores explicaré la forma de crackear este archivo para obtener el password de otro usuario.

6.2 Obtener contraseñas de e-mail

En principio y sin usar métodos más complicados (fallos en el servidor de correo), la única forma de obtener una contraseña de Email es mediante ingeniería social, es decir, manipulando a la víctima para que revele su contraseña, aquí entra en juego tu imaginación no te lo vamos a dar todo hecho.
Y la otra forma es mediante Brute Forcing (Fuerza Bruta), para ello necesitarás un programa crackeador como el Brutus, y unos diccionarios de palabras. ¿Por qué? Pues porque la fuerza bruta consiste en ir probando palabras como posibles
passwords hasta encontrar la correcta y el programa encargado de hacerte todo el trabajo es el

Brutus.
Nunca caigas en la trampa de "Envíame tu email, tu password y el email de la persona a la que quieres entrar en su cuenta", porque esto es una ¡¡¡trampa!!! y sí, ahora dirás: "Que tontería como voy a hacer caso a eso, si me está pidiendo mi login y mi pass, para robarme y/o curiosear mi cuenta", pues a pesar de que no lo creas muuuuucha gente ha caído por la desesperación de querer ver el mail de su novio/a y no se da cuenta de que le están timando.
Estos dos métodos (ingeniería social y brute forcing) son los únicos métodos que tienen probabilidades de funcionar, he dicho probabilidades!, no creas que al hacer brute forcing vas a conseguir el password, imagínate si fuera tan fácil de conseguir el pass de un email, sin tener a penas conocimiento de hacking, pues ¡¡ nadie tendría email!!.
También existen otros programas, de funcionamiento similar a cualquier troyano que han sido realizados específicamente para obtener contraseñas de email, son: MSN-Hack y XMAS2000, ambos puedes encontrarlos en http://www.hackingparanovatos.com

7. Enviar emails anónimos mediante telnet.

La forma más fácil para enviar emails anónimos es crearte una cuenta de correo en Hotmail o yahoo, insertando todos datos falsos.

La segunda forma (menos sencilla) es:
Encontrar un servidor que permita conectarse a él mediante telnet y permita el envío de email a través del telnet.
Una vez que hayamos encontrado un servidor, abrimos una ventana de MS-Dos y escribimos: telnet "servidor" "puerto".

** Una vez conectados saludamos al servidor*: *
helo

250 servidor.subdominio.dominio Hello IDENT:usuario@equipo.subdominio.dominio * Mensaje del servidor: *

** Luego escribimos la dirección de quien envía el email: **
mail from: zerocurrl@soyhacker.com

250 2.1.0 zerocurrl@soyhacker.com... Sender ok * Mensaje del servidor: *

** A continuación escribimos la dirección a quien va dirigido el email: **
rcpt to: spiderman@superheroe.com

250 2.1.5 spiderman@superheroe.com... Recipient ok * Mensaje del servidor: *

Ahora escribimos el mensaje y cuando queramos terminar pulsamos enter para ir a la línea de abajo y escribimos un "." (punto)

Escribimos Quit para salir del servidor.

8. Cómo proteger nuestra máquina

Lo primero que tienes que pensar es que nunca podrás tener una máquina 100% segura teniendo un Windows como sistema operativo (siento decirlo, pero es la verdad... Tarde o temprano si de verdad te interesa esto tendrás que aprender Unix), en fin, pero aún así podemos intentar tener un sistema bastante seguro, para que ningún lamer, se nos cuele o nos fastidie.

8.1 Firewalls

Si tienes un Windows 9x / NT / 2k
A grandes rasgos podríamos decir que un firewall es un programa de seguridad, que crea una especie de barrera entre nuestro ordenador y la red tanto interna (red local) como externa (Internet) El tráfico que se produce entre la Red y tu PC es autorizado o denegado por el firewall, siguiendo las instrucciones que le hayamos dado, es decir, que si alguien intenta entrar en tu máquina por un puerto determinado el firewall te avisará y te mostrará la IP del lamer que intenta acceder.

Algunos Firewalls gratuitos son:

Zone Alarm ..... http://www.zonelabs.com
Tiny Personal Firewall ..... http://www.tinysoftware.com/
Agnitum Outpost Firewall ..... http://www.agnitum.com/products/outpost
Sygate Personal Firewall ..... http://www.sygate.com/

Pregunta que debe de estar rondando por tu cabeza: ¿Y cuál me recomiendas?, la verdad es que como yo utilizo Linux, pues no utilizo Firewall. He probado el Zone Alarm en un Windows y la verdad es que no me gusto mucho porque te pide autorización cada vez que se intenta hacer una conexión y no te permite hacer una configuración sin más.
Te recomiendo que antes de instalar un firewall vayas a su sitio web y mires las características que posee y luego lo pruebas, sino te convence desinstalas y listo ;)
Creo que no hace falta decir, que te bajes el Firewall correspondiente a tu sistema Windows 9x / NT / 2k / XP.
Aquí puntualicemos una cosa:

Si tienes un Windows XP
Si dispones del XP, has de saber de que este sistema ya trae por si mismo su propio Firewall y por lo que he visto
y probando con el, es bastante bueno.
¿Donde está el famoso firewall? Haces click con el botón derecho del ratón en "Mis sitios de red" --> Propiedades.
Se te abrirá una ventanita que te mostrará tus conexiones de red, por lo general se suelen tener dos: Una la de red local (si es que tienes) y la otra es la de Internet. Haces click con el botón derecho

encima de la de
Internet y escoges Propiedades.
Ahora escoges la solapa (o pestaña, en fin, como le llames) "Avanzadas" y activas la primera opción que pone:
"Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet"
Clickea en el botón Configuración.
Solapa "Servicios":
Verás una lista de servicios algunos seleccionados y otro no (Escritorio remoto, servidor de Telnet, servidor de FTP...)
Debes seleccionar aquellos que quieres utilizar. Pero también deberás añadir aquellos servicios que quieres utilizar y no aparecen en esa lista, por ejemplo habilitaremos el del IRC:
Botón Agregar -->

Descripción del Servicio: IRC
Nombre o dirección IP... : 192.168.0.1 (Es nuestra IP local)
Número de puerto externo... : 1080
Número de puerto interno... : 1080
TCP

Por lo general el puerto externo suele coincidir con el externo.

Solapa "Registro de seguridad": Activa la segunda opción: "Registrar conexiones correctas", ahora todas la conexiones que se intenten hacer a tu máquina, ya sea de programas como el MS Messenger o algún "listo" que intente introducirse, no podrá gracias a la buena configuración de tu Firewall XP, y además quedará su IP guardada en el archivo de log, ubicado en C:\WINDOWS\pfirewall.log
Solapa "ICMP": selecciona todas MENOS la primera: "Permitir solicitud de eco entrante", de esa forma si alguien te hace un ping a tu IP para saber si estás conectado le devolverá que no estás conectado y además no podrán nukearte, ya que los programas nukes se basan en enviar muchos pings al ordenador para que este se cuelgue. :)

Este firewall tiene más posibilidades como es el redireccionamiento de puertos pero eso no se explicará aquí.

Si deseas saber más acerca del firewall, ve a la ventana anterior y en la solapa "Avanzadas" clickea en "Más acerca de Servidor de seguridad de conexión a Internet"

8.2 Antivirus

Al igual que los firewall no es obligatorio tener uno instalado pero si recomendable, si te empiezas a mover por el mundillo under, comenzarás a recibir emails con archivos adjuntos, virus, troyanos y similares metidos en cualquier tipo de formato: jpeg, txt, html.... A mi me llegan de todo tipo, lo peor de todo es pensar en el tiempo que pierden esos pobres ignorantes pensando en que yo voy ejecutar el archivo adjunto xDDD
También es recomendable tenerlo porque si bajas cosas de Internet es mejor no fiarse y no sea que algún graciosillo meta un virus en un archivo JS (JavaScript) o cualquier cosa que se le ocurra.

Lo que sí te puede pasar y el lo mas seguro que si te bajas troyanos, snifferes, keyloggers, ftps invisibles, mailbombers, joiners, etc. tu antivirus te los detectará como virus, ya que al ser herramientas hack pues los cataloga como peligrosos para el sistema.

Así que si en cualquier momento quieres trabajar con troyanos tendrás que desactivar el antivirus sino no te dejará ni descomprimir el archivo.

8.3 Anti-Spywares

Spyware es el nombre que se le da al software espía oculto en nuestro sistema. La finalidad de cualquier Spyware es obtener información personal del usuario, para posteriormente vender nuestra información a terceras empresas, con la consecuencia de ser bombardeados con publicidad.

¿Cómo sabemos si tenemos software espía instalado en nuestro ordenador? Pues para ello existe un programa muy conocido y muy fiable llamado "Ad-aware", este programa se encarga de avisarnos de todo el software espía que se encuentra en nuestro sistema y posteriormente nos ofrece la posibilidad de eliminarlo.

Este programa no dispone de una web oficial, puedes encontrar la última versión en español en nuestra página: http://www.hackingparanovatos.com

9. Programas

En este apartado hablaremos de algunos programas que todo el que se inicie en el hacking debe conocer a la perfección. Está claro que no voy a comentar todo los programas que existen porque me podría llevar años y muchas páginas. :)
Debes saber que esto sólo es una guía de iniciación en la que se explican a grandes rasgos la utilización de ciertos programas, si de verdad te interesa el mundillo hack, tienes que aprender tú por tu cuenta a utilizar muchos programas y sobre todo ¡¡¡ Inténtalo!!! Hay muchos que se bajan un programa, ven que está en inglés y que trae muchas opciones y nos escriben diciendo ¿Cómo se utiliza el... Notepad (por ejemplo)?, sin antes haberse molestado en haber probado todas la opciones y leyendo la ayuda que trae el propio programa. Ok, ok no me enrollo más, vamos allá!!!

9.1 Troyanos

Cuando se crearon los troyanos su utilización estaba pensada como herramienta de administración remota, pero a medida que paso el tiempo la gente lo empezó a utilizar para controlar ordenadores ajenos. Es decir, hoy en día cualquier antivirus detecta a los troyanos como "virus". Un troyano posee dos partes:
El archivo "Server" (o servidor en español) y el "Client" (o cliente en español).
El archivo que JAMAS se debe ejecutar es el Server, porque sino estarás infectado y correrás el

riesgo de que cualquier persona entre en tu ordenador.
La utilización de un troyano es muy fácil, simplemente se le envía el Server a la víctima y cuando esta lo ejecute, tú con el archivo Client y teniendo la IP de la víctima tendrás el control total de su máquina.
Hay muchos tipos de troyanos y cada uno de ellos tienen características muy variadas, pero a grandes rasgos todos funcionan de la misma forma.
Ejemplos de troyanos: Littlewitch, BackOrifice, SubSeven, Donal Dick....

9.2 Keyloggers

Un keylogger es un programa que se ejecuta de forma invisible para el usuario, capturando todo lo que este teclea.
La utilización de un keylogger es muy sencilla, ejecutamos el programa en el ordenador de la víctima sin que este se entere (por ejemplo: ejecutamos un keylogger en un ordenador de nuestra universidad y cuando el chico o chica de turno aproveche para ver su email nuestro keylogger habrá capturado su contraseña, jejeje), tiempo después miramos el log que ha generado nuestro keylogger (este log estará guardado en un determinado lugar dependiendo del keylogger que usemos o dependiendo de la configuración que le hayamos asignado).
Hay keyloggers que permiten el envío de log a nuestro email, de esta forma nos ahorramos tener que volver al ordenador de la víctima.
Encontrarás muchos keyloggers en http://www.hackingparanovatos.com, la utilización de uno es muy similar a la de otro, algunos son comerciales y otros freeware, como siempre digo: prueba varios y quédate con el que más te guste :)

9.3 Crackeadores

Mediante un programa Crackeador conseguiremos desvelar las contraseñas de un Windows. Lo primero que tenemos que tener es el archivo .pwl en caso de Windows 9x / ME o el archivo sam.log en caso de un 2k / NT / XP. La forma de conseguirlo corre por tu cuenta, utiliza ingeniería social para que alguien te lo envíe, o bien cuélale un troyano y luego le robas el archivo de contraseñas o etc, etc. :)

- Para Windows 9x / ME

Por si algún despistado se perdió vuelvo a repetir que estos dos sistemas guardan sus contraseñas en la carpeta Windows\ bajo el nombre siguiente: nombredeusuario.pwl
Los programas para crackear este tipo de archivos son muy diversos, uno muy famosos es el PwlTool funciona en sistemas 9x / ME / NT / 2k / XP su web oficial es esta de: http://www.soft4you.com/vitas/pwltool.asp y también puedes bajártelo de nuestra web.

Su utilización es muy sencilla:
- Instalas el programa y lo ejecutas
- Escoges la opción "File" --> "Open pwl file"

Automáticamente el programa te pondrá el nombre de usuario. Que es el mismo nombre que tiene

el archivo.
- Por último escogemos la opción Brute Force --> "Search Password Fast"

Este programa tiene muchas opciones, utilízalas para conseguir el password, puedes seleccionar la cantidad de dígitos que se compone el password, buscar contraseña, buscar contraseña de forma rápida, introducirle un diccionario de palabras e intentar encontrar el password entre esa lista de palabras....

- Para Windows 2000 / NT / XP

En el caso de estos tipos de sistemas las contraseñas se alojan en Windows\system32\config bajo el nombre de sam.log
El programa más extendido y más famoso es el "LOphtCrack", su utilización también es muy sencilla:
- Te bajas el programa de: http://www.evadenet.com/downloads/lophtcrack.shtml
- Lo instalas y ejecutas
- Selecciona la opción Tools y dentro de esta --> Dump Passwords from registry

Nos aparecerá una ventana en donde debemos seleccionar el equipo del que escogeremos los ficheros sam, por defecto nos aparece el nombre de nuestra máquina local. Le damos al botón Ok y listo
Si queremos coger el fichero de una máquina remota lo tenemos más difícil, porque al insertar la IP en esa misma ventana nos aparecerá un error: "Failed to open key....." eso es debido a que no tenemos privilegios de administrador en esa máquina. Así que antes debemos conseguir el fichero sam de otra forma (ingeniería social, mediante keyloggers, troyanos, ...)
Una vez que tengamos el archivo Sam no tenemos más que ir a Tools ---> "Import sam file"
Para utilizar un diccionario de palabras seleccionamos la opción "Open wordlist file"

10. Como mantener nuestro anonimato

Una de las mayores preocupaciones de cualquier hacker es mantener su anonimato durante su instancia en la red. Ello lo podemos conseguir mediante la utilización de proxys y utilizando un ordenador de intermediario cuando queramos hacer "actividades" poco comunes (jejeje...)

10.1. Proxy

Un proxy es una pasarela entre tu ordenador e Internet, de esa forma cuando visualizas una página ese servidor creerá te conectas desde esa máquina, en vez de tu propio ordenador.
En Internet encontrarás montones de listas proxys, ve a un buscador por ejemplo www.google.com y buscas: "listas de proxys", ahora tienes que abrir tu navegador. En el caso del Internet Explorer vas a Herramientas --> Opciones de Internet -->
Solapa Conexiones --> Configuración de LAN, Activas la opción "Utilizar un servidor proxy para su lan...." en dirección escribes la IP o el host y en la siguiente casilla el puerto. Aceptas todas la

ventanas y listo.
En el caso del Netscape Navigator te vas a las opciones y escoges Proxy, y ahí introduces los datos correspondientes.

Una vez que hayas introducido los datos de ese proxy puedes comprobar que el proxy funciona abriendo nuevamente la página de www.google.com si la página se carga correctamente es que el proxy funciona, y si te devuelve que no se encuentra la página solicitada es que el proxy no funciona.

Si en algún momento quieres dejar de utilizar el proxy, tienes que volver a Herramientas --> Opciones de Internet --> Conexiónes --> Configuración Lan y DESactivas la casilla "Utilizar proxy..."
En el caso del Netscape lo mismo, vas a opciones y en la parte de proxy deshabilitas la opción de utilizarlo.

10.2. Obtención y utilización de una cuenta shell

Una cuenta shell es una cuenta en una máquina con algún tipo de Unix a la que se pueden conectar usuarios remotamente mediante telnet. Algunas páginas donde se dan cuentas gratuitas son http://www.cyberspace.org o http://sdf.lonestar.org.

Si conectas directamente por telnet, las direcciones que deberás usar son cyberspace.org y sdf.lonestar.org por el puerto 23 como de costumbre. Una vez que conectes, te irán apareciendo las instrucciones sobre lo que tienes que hacer para crear una cuenta nueva, eso sí, en inglés. Lee detenidamente todo antes de continuar. Si no sabes inglés puedes buscar algún sitio que ofrezca shells gratuitas en español. Sino, si te interesa mucho siempre puedes optar por una de pago...

Si sigues las instrucciones paso a paso tendrás una cuenta nueva y podrás utilizarla de forma similar a estar delante de esa máquina, lo cual quiere decir que todo lo que hagas desde esa shell aparecerá con la IP de esa máquina con lo que consigues ocultar tu IP. Teniendo en cuenta que se trata de un servidor permanentemente conectado se puede usar para muchas más cosas pero eso ya se deja para la imaginación de cada uno :)

11. Despedida

Bueno, hasta aquí hemos llegado, espero que te está guía te haya servido de ayuda para iniciarte en el hacking.
Para cualquier comentario, sugerencia o sino has entendido algo de lo que está explicado aquí no tienes mas que dejarnos un mensaje en los foros de http://hackingparanovatos.dhs.org o también puedes ponerte en contacto con nosotros a través de IRC, en el servidor: irc.redhispana.org en el canal #hackingparanovatos.

Y por supuesto para futuras actualizaciones de la guía visita: http://www.hackingparanovatos.com

Saludos a los operadores del canal: S4D^|^3ND, ^_Brassoy_^, KuRLD y ||R[0]oT|| y a todos los que entrán, que son muchos así que mejor no los nombramos, que sino no acabamos hasta mañana xDD

Nota final: Puedes distribuir esta guía libremente siempre y cuando no modifiques absolutamente nada ;)

Realizada por HeChiCeRa con la colaboración de NoRegret. ;)