# DNS SPOOFING
# Y
# PHISHING EN REDES LAN


WRITTEN BY K43L

2011

# DNS SPOOFING Y PHISHING
# EN REDES LAN

## 1. - INTRODUCCION:

En este tutorial se mostrará como podemos llevar a cabo la técnica conocida como Dns Spoofing mas Falseando una página Web que en este caso será la pagina principal del Hotmail, con esta Web falseada podremos obtener fácilmente cuentas de usuario y contraseñas, si no cuentan con el scam del Hotmail con los que se explicará en este tutorial se los dejo en descarga directa, el siguiente link contiene el scam de Hotmail mas el scam del facebook, que posteriormente les puede servir para realizar este mismo ataque u otros.

**http://www.4shared.com/file/jywmt-RA/SCAMS_FACEBOOK_HOTMAIL.html**

## 2.- INSTALANDO UN SERVIDOR WEB LOCAL:

Bueno para poder realizar lo anteriormente mencionado, necesitamos un servidor Web local que este corriendo de manera que podamos acceder a el desde cualquier lugar de nuestra red LAN, para esto os creamos una maquina virtual donde este servirá de servidor Web en nuestra red LAN y con la cual podremos obtener cuentas de usuarios y contraseñas.
Queda de mas explicar como instalar paso a paso un servidor Web en una maquina, para este tutorial se instalará el software **Xampp** en una maquina corriendo Windows Xp, si ustedes gustan pueden instalar su servidor Web local en cualquier otro sistema operativo, solo que en este caso se hará sobre dicho sistema operativo.

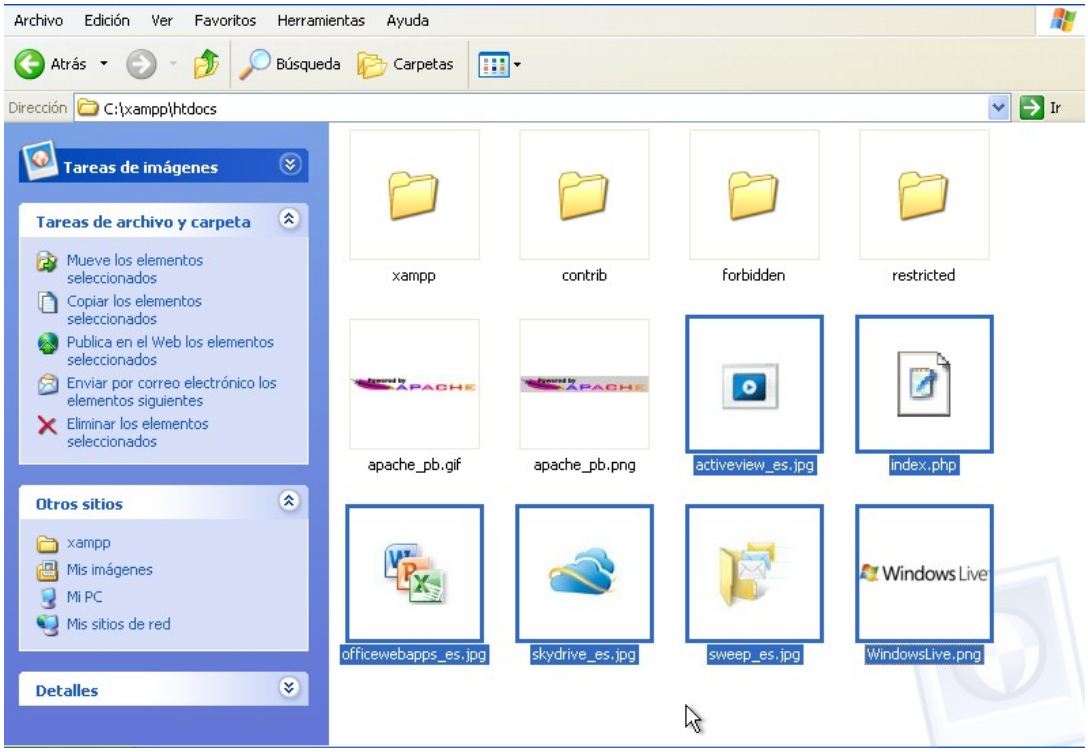
### 2.1.- Copiando el scam dentro del directorio del Xampp:

Primeramente comenzaremos con el scam del Hotmail, para eso debemos copiar los archivos necesarios al directorio “htdocs” que es donde se deben almacenar nuestras

paginas Webs creadas para posteriormente que puedan ser visualizadas desde cualquier explorador de Internet.

El directorio “htdocs” se encuentra en **c:\xampp\htdocs.**

Y se deberán copiar los archivos necesarios a ese directorio, tal y como muestra la imagen siguiente.

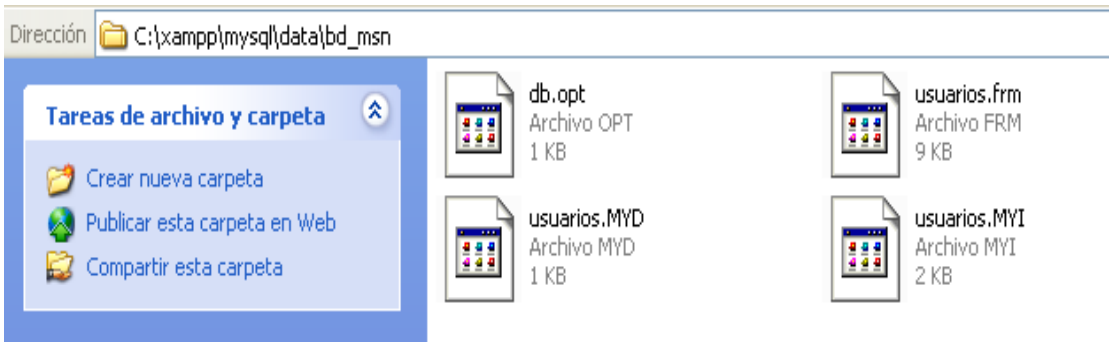



En caso de que exista un archivo con el nombre index.html o index.php, lo reemplazan por el del scam y listo, asi no tendremos problemas de que cuando hagamos correr el scam, se confunda el xampp y nos muestre otra que no sea la nuestra, los archivos que están marcados son todos los que deberás copiar dentro de esta carpeta, la carpeta se llama Hotmail en el cual se encuentran los archivos que se muestran en la imagen anterior, también tiene una carpeta que dice “bd_msn” que después hablaremos de esa carpeta y donde debemos colocarlo.

Una vez que hayamos llegado hasta aquí, lo siguiente que debemos de hacer es copiar el directorio antes mencionado “bd_msn” que es donde se almacenaran las cuentas de usuraios y contraseñas que vallamos a capturar, para esto nos dirigimos al directorio:

**C:\xampp\mysql\data.**

La imagen siguiente muestra de cómo debe quedar una vez copiado esa carpeta a la dirección mencionada:



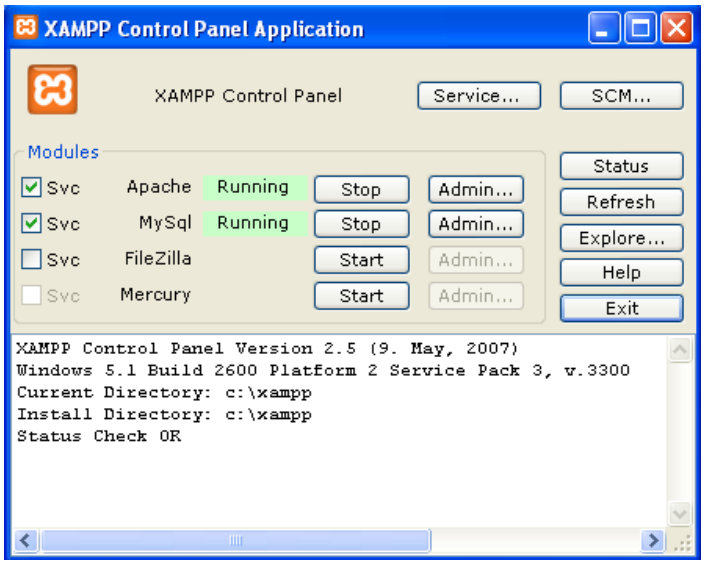

La imagen anterior muestra el contenido de la carpeta "bd_msn" son archivos de bases de datos, es decir tenemos una base de datos creada con una tabla denominada "usuarios" que veremos después con el Phpmyadmin y en donde se almacenarán los correos electrónicos de las victimas con su respectivo password.

Cabe mencionar que este scam fue realizado 100 % por mi, por eso es algo diferente a los scams que normalmente hay en Internet.

Si desean pueden utilizar otros scams, ya que el objetivo principal de este tutorial es mostrar de cómo podemos obtener cuentas de Hotmail y Facebook dentro de una red Lan, y sin la necesidad de subirla a ningún hosting.

**2.2.- Explorando nuestro Scam:**

En esta parte se explicará de cómo podemos asegurarnos de que nuestro servidor Web esta corriendo, para esto nos dirigimos al panel principal del "Xampp" y vemos que los servicios de **APACHE Y MYSQL** estén corriendo y se encuentren activos, abrimos el XAMPP desde el acceso directo hacia el escritorio o también desde el menú inicio, una vez que hayamos abierto debemos de tener una imagen como la siguiente:




Bueno como se puede apreciar en la imagen anterior, tenemos los servicios de **APACHE Y MYSQL** corriendo correctamente, esto nos servirá para poder acceder a nuestro scam y que funcione perfectamente, lo siguiente que tenemos que hacer será dirigirnos a nuestro navegador Web y testear que el scam este corriendo correctamente, para eso nos dirigimos a la dirección http://localhost/

Deberá cargar la pagina principal del Hotmail, si todo ha salido bien deberemos de tener una imagen como la siguiente en nuestro navegador.

En caso de que no les salga esta imagen, puede que tengan varios archivos con el nombre index.php, index.html, o sea que deberán cambiarle de nombre a esos archivos o eliminarlos, ya que solamente debería quedarles un archivo llamada index.php que es el del scam de Hotmail.

## 3.- REALIZANDO EL ATAQUE:

En esta parte se explicará de cómo realizar el ataque en la red LAN, bueno para empezar el ataque se realizará sobre una maquina corriendo Gnu/Linux, mas concretamente en la distribución Ubuntu en su versión 11.04.
El ataque se basa en la conocida técnica **"ARP SPOOFING"** que consiste en envenenar las tablas ARP de las maquinas victimas en nuestra LAN, por medio de esta técnica y de otra conocida como **"DNS SPOOFING"** podremos redireccionar la pagina Web principal del Hotmail hacia nuestro servidor Web local que se encuentra instalado en una maquina virtual.
Si quieren profundizar mas del tema pueden buscar más en la red sobre este tipo de ataques, existe un tutorial que realice sobre **"ARP SPOOFING"** que se encuentra en mi blog, que al final de este tutorial les pondré la dirección de la misma.

### 3.1.- Envenenamiento ARP y falseando DNS:

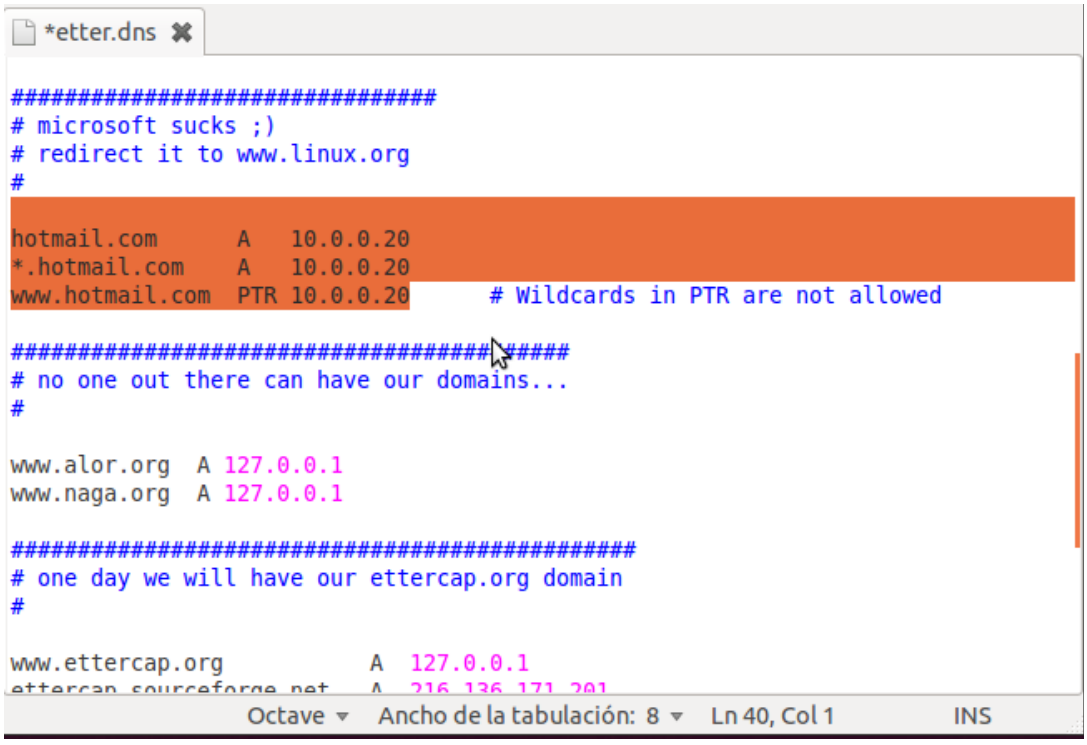
Para realizar este ataque como dije anteriormente se hará sobre la distribución Ubuntu 11.04, la herramienta que se utilizará para este ataque es la conocida herramienta **"ETTERCAP"** que nos permitirá hacer un envenenamiento ARP en toda la red y posteriormente falseando o redireccionando las peticiones que hagan los navegadores Web de las maquinas victimas hacia la pagina principal del Hotmail, solo que en esta parte haremos que redireccione esas peticiones hacia nuestro servidor Web local.

Para realizar esto, el primer paso será abrir una consola en Ubuntu con permisos de Root y poner el siguiente comando en la misma.

**Sudo gedit /usr/share/ettercap/etter.dns.**

Hay que aclarar que antes de que escribamos el comando anterior deberemos de tener instalado la herramienta “ettercap” que se puede instalar desde el gestor de paquetes de ubuntu.

Bueno una vez escrito el comando anterior deberá salirles una imagen como la siguiente:

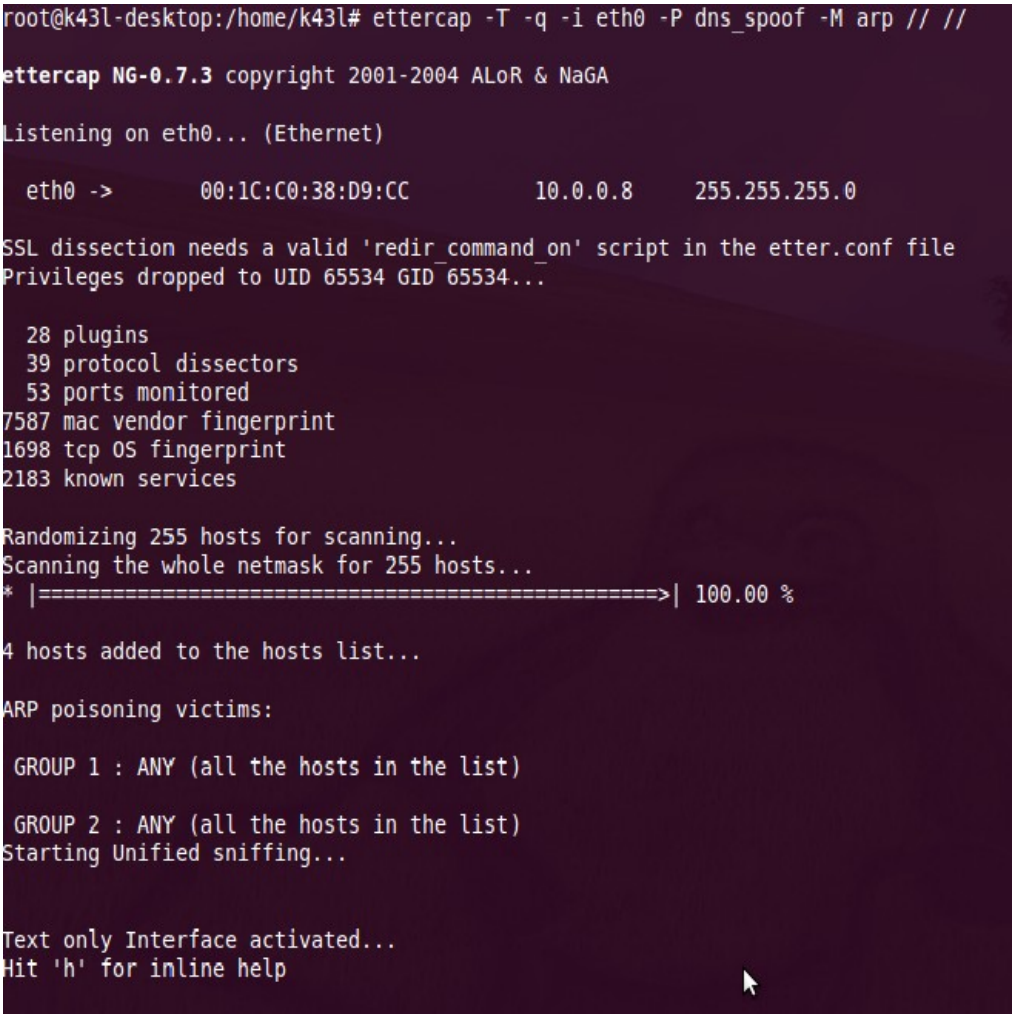



Como muestra la imagen anterior deberemos de cambiar esas líneas que se encuentra coloreadas, en la misma podemos apreciar el nombre de domino de Hotmail y la dirección ip a redireccionar, que en este caso es la IP de nuestra maquina virtual instalada, con esta configuración le estamos diciendo que cuando nosotros hagamos correr esta herramienta, en especifico este tipo de filtro, cada vez que las maquinas victimas coloquen en sus navegadores la dirección de Hotmail lo que hará ese filtro es de redireccionar esas peticiones y llevarlas hacia nuestro servidor Web local con el cual podremos capturar los correos electrónicos y las contraseñas de cualquier maquina que se encuentre en la red LAN.

Bien, una vez llevado a cabo los cambios mencionados anteriormente, cerramos el archivo **“etter.dns”** sin antes haber guardado los cambios en la misma.
El siguiente paso será ejecutar la herramienta **ETTERCAP** para llevar a cabo el ataque, en la misma consola con derechos de Root ponemos el siguiente comando:

**Sudo ettercap –T –q –i eth0 –P dns_spoof –M arp // //.**

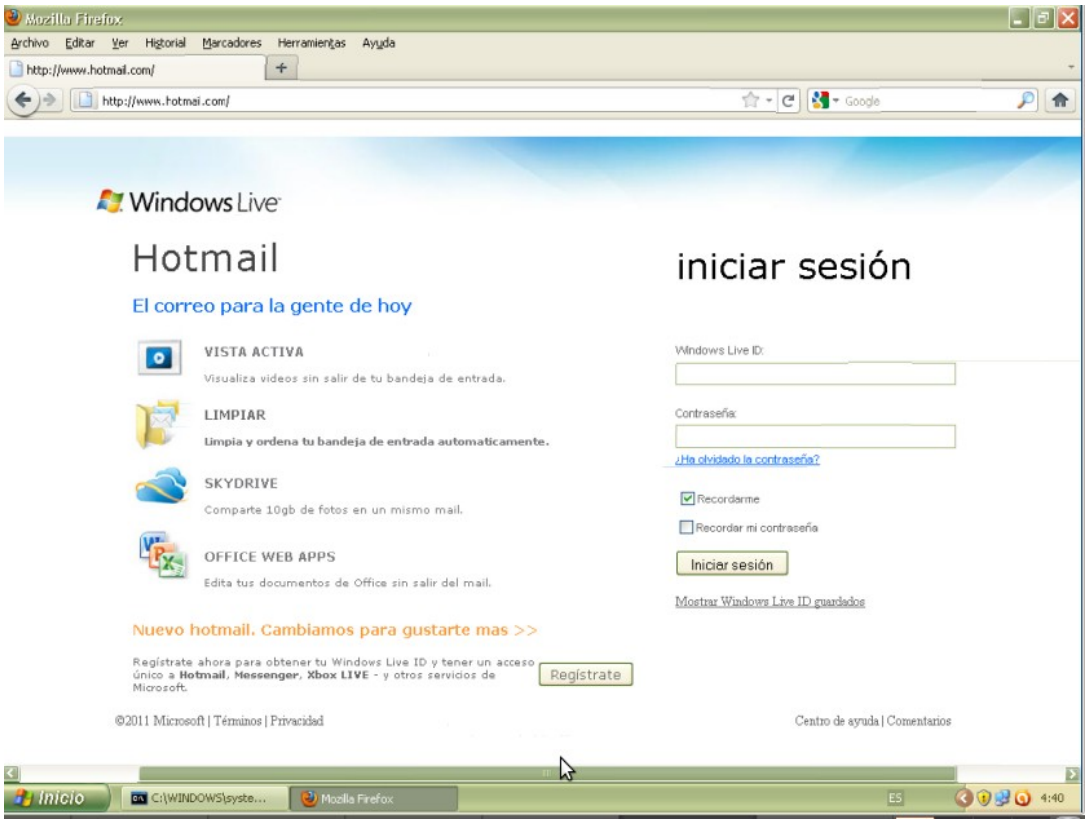
Debo aclarar que en la parte de **-i** debemos de colocar la interfaz de nuestra placa de red, que en este caso es eth0.
La siguiente imagen muestra el proceso de ejecución una vez escrito el comando anterior.



La imagen anterior muestra de cómo se inicia el envenenamiento en la red, se puede apreciar que nos muestra que todas las maquinas en la red que hagan la petición hacia Hotmail serán afectados por el plugin de **"dns_sppof".**

### 3.2.- Capturando Correos Electrónicos y Contraseñas:

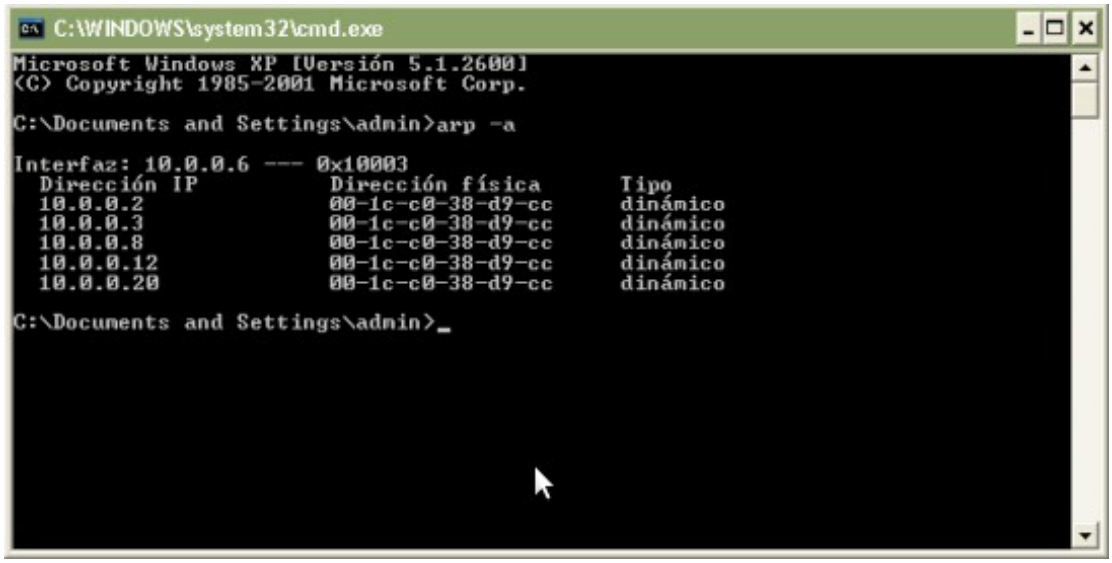
Supongamos que una maquina victima hace la petición hacia la página del Hotmail, en este caso la maquina victima tiene el sistema operativo Windows Xp, y el navegador Mozilla Firefox, entonces cuando la maquina victima escriba es su navegador http://www.hotmail.com, lo que le aparecerá será algo como la siguiente imagen:




Como se muestra en la imagen anterior, hemos logrado envenenar las tablas ARP de las maquinas que se encuentran en la red LAN, comprobamos que realmente hemos envenenado las tablas de la maquina victima poniendo en la misma el siguiente comando:

**arp –a**

El comando anterior debemos de colarlo en la maquina victima en la consola MS-DOS, cabe mencionar que en un ataque real, no habrá la necesidad de hacer esto, ya que si la maquina victima esta visualizando nuestro scam en su navegador eso es mas que suficiente para nosotros, solo que en este tutorial se muestra de cómo ETTERCAP logra envenenar la tabla arp y es así como redirecciona las peticiones que hace hacia nuestro servidor Web local instalado.




La imagen anterior muestra de cómo la maquina victima tiene envenenada su tabla ARP, ya que todas las peticiones que realice lo hace por la dirección Mac que aparece en la imagen, la cual corresponde a nuestra maquina que esta realizando el ataque que en este caso es Ubuntu.

Bien entonces cuando la victima coloque su cuenta de correo electrónico y su contraseña en los **textbox** presionando la tecla **“enter” o en el boton “iniciar sesión”**, lo que pasará es que se guardará en nuestra maquina virtual, donde tenemos el Xampp instalado, se guardará en la base de datos **“bd_msn”** y dentro de esta en la tabla llamada **“usuarios”.**

## 4.- INGRESANDO A LA BASE DE DATOS:

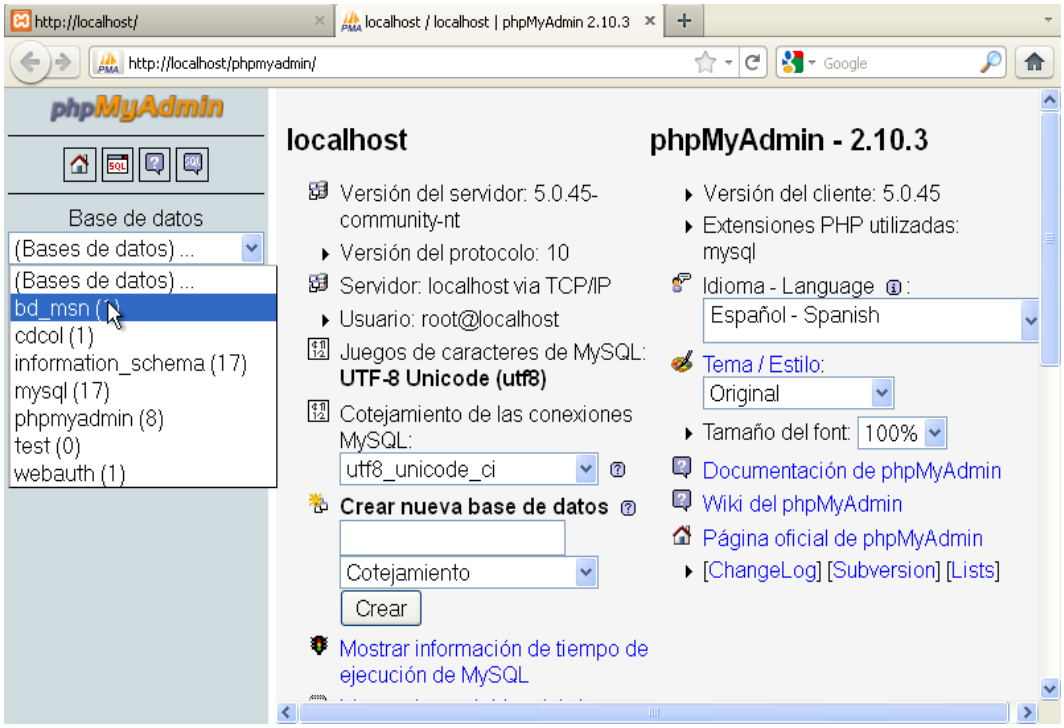
Bien pues en esta parte comprobaremos que realmente los datos de la victima se guardaron en nuestro servidor Web, en nuestra base de datos que tenemos, para esto nos tenemos que dirigir hacia nuestra maquina virtual y comprobar si los datos fueron capturados correctamente.

### 4.1.- Accediendo a Phpmyadmin:

Bien, ahora que hemos logrado capturar el correo electrónico y la contraseña de la victima, el siguiente paso es de entrar al **"PHPMYADMIN"**, de forma resumida les diré que se trata de una interfaz gráfica desde el cual podemos manipular nuestras bases de datos y tablas que hayamos creado en **MYSQL**, pues desde aquí podemos administrar gráficamente nuestro servidor Web, podemos crear bases de datos, tablas, usuarios y todo lo referente a la administración de una base de datos.
Para acceder a la administración de **phpmyadmin** debemos de colocar la siguiente dirección en nuestro navegador, que en este caso será dentro de nuestra maquina virtual en Windows Xp.
Si quieren saber mas sobre el **phpmyadmin** pueden buscar en Internet que hay muchos tutoriales y manuales sobre este servicio.

http://localhost/phpmyadmin

Si queremos entrar desde otra maquina a nuestro servidor Web local, lo único que tenemos que hacer es cambiar la parte donde dice **"localhost"** por la dirección ip de la maquina remota.
http://10.0.0.20/phpmyadmin
Con la dirección anterior podremos ingresar a nuestro servidor desde cualquier parte de la red LAN, bueno una vez que hayamos colocado eso en nuestro navegador deberemos de tener una imagen como la siguiente:




La imagen anterior muestra la apariencia del MYSQL y como podemos crear bases de datos fácilmente sin ingresar a la consola y crearlas desde ahí.

Lo siguiente que debemos hacer es de cargar la base de datos de nuestro scam, que anteriormente copiamos dentro del directorio donde se almacenan las bases de datos en Xampp.

Elegimos el que dice “bd_msn” como muestra la imagen anterior y procedemos a ver las tablas de esta base de datos creada.

### 4.2.- Viendo cuentas de usuario y contraseñas:

Pues bien llegados hasta este punto, lo siguiente que debemos hacer es de ver las tablas que tiene nuestra base de datos y poder observar las columnas o campos que almacenan dicha tabla, en esta base de datos existe solo una tabla la cual se llama “usuarios” y nos sirve para capturar las cuentas de los usuarios de Hotmail y sus contraseñas, entonces una vez ingresado a la base de datos correspondiente, visualizamos la tabla creada, le damos a examinar y nos mostrará la tabla usuarios con sus respectivas columnas.

La siguiente imagen muestra de cómo hemos logrado capturar la cuenta de usuario y contraseña de una victima en nuestra red LAN, para que se entienda mejor deberíamos de tener una imagen como la siguiente una vez examinando los campos de nuestra tabla de usuarios.


Como se puede apreciar en la imagen anterior nos muestra claramente la cuenta de correo de la victima y la contraseña, lo cual quiere decir que logramos nuestro objetivo.

Ahora podemos capturar todas las cuentas de la red LAN de una manera sencilla y rápida, cabe mencionar que esto solo funciona en una red LAN donde los equipos están conectados a un Switch o Hub con salida a Internet y a través de estos dispositivos es posible armar una red de área local.

Por otra parte tendremos en nuestra maquina corriendo con Ubuntu como ettercap nos avisa cuando una maquina se ha conectado al scam, obtendremos una imagen parecida a la siguiente:

Como se puede apreciar en la ultima línea que nos muestra se encuentra la dirección de la pagina del Hotmail con la dirección ip del scam, el cual nos dice que se logro “spoofear” cuando una maquina victima intentó acceder a la pagina de Hotmail.

**5.- DESPEDIDA:**

Bueno hemos llegado a la parte final de este tutorial, espero que haya sido de su agrado, si tienen preguntas sobre el mismo pueden preguntarme por el msn, correo es chester_640@hotmail.com
Les invito a visitar mi blog: http://informaticalive.com.ar
Agradecimientos especiales para las siguientes comunidades de hacking y seguridad informática:

http://www.underc0de.org
http://www.hackxcrack.es
http://www.c-intrud3rs.com
http://foro.infiernohacker.com