Espiando Contraseñas de Hotmail
Con SSL Strip

Created by

Cristian Mutis Caez (M4ST3R)
Administrador de Redes De Computadores.
Crisfechan@hotmail.com
http://n3wb13sh3ll.wordpress.com

Como Funciona SSLStrip ?

Para hablar de algo primero debemos saber su funcionamiento el de SSLStrip es simple, lo que hace es un cambio de todas las peticiones “https://” de una página web por “http://” y luego pone la maquina atacante en el medio de el servidor y la victima (MITM). Esto lo hace con la finalidad de que la víctima y el atacante se comuniquen a través de HTTP, mientras que el atacante y el servidor, se comunican a través de HTTPS . Por este motivo el atacante tendra la facilidad de ver toda la informacion de su victima como password, conversaciones y otras cosas en texto plano.

Manos a La Obra !!!

Esta comprobado que lo mas buscado en google es la famosa frase “como hackear hotmail”, y password de otras web que manejen http “Seguro”, bueno no es mi estilo pero aquí tienen una forma de hacerlo, claro como digo siempre hagan las pruebas con sus propios users, usen esto solo con fines educativos, espero no haber despertado malicia XD.

Tratare de explicar los pasos de la forma mas sencilla posible espero hacerme entender.

Herramientas

Para realizar sus pruebas necesitaran lo sigte:

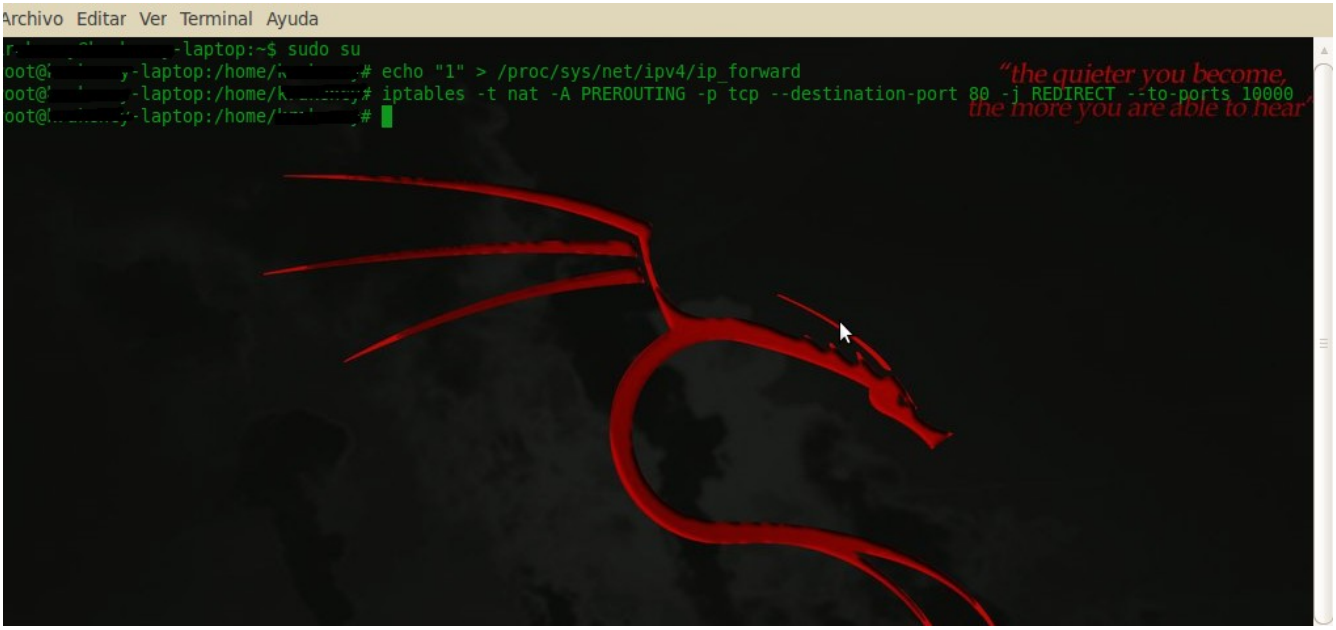
- Su Distro Linux de Preferencia.
- sslstrip
- dsniff

A Lo que Vinimos !!!

Comencemos, una vez descargado sslstrip lo descomprimanlo en el escritorio, asumire que instalaron dsniff (dependiendo su distro pueden hacer asi sudo apt-get install dsniff)...ahhhhhh... Casi lo olvido deben tener python previamente para continuar.

Abrimos una terminal y escribimos lo siguiente:

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



La primera linea es para poner la terminal en modo root.

En la segunda linea habilitamos la redirección por iptables.

Y la tercera redirecciona el tráfico del puerto 80 al puerto 10000.

Ahora nos dirijimos a la carpeta donde se descomprimio el sslstrip, lo ejecutamos y si todo esta bien veremos algo asi...

@python sslstrip.py -w /home/su_user/su_archivo.log -p -l 10000

El paso siguiente sera hacer el **arp-spoofing** , este basicamente es hacernos pasar por otro equipo de la red envenenando la tabla arp del router.

Tipeamos lo siguiente en una nueva solapa :

sudo arpspoof -i eth1 -t 192.168.0.2 192.168.0.1

Les explico que hemos echo, iniciamos el spoofeo ,el parámetro “-i eth1” pondremos la interface por donde saldra el trafico... en caso que no sepasn hagan un simple “ifconfig”.

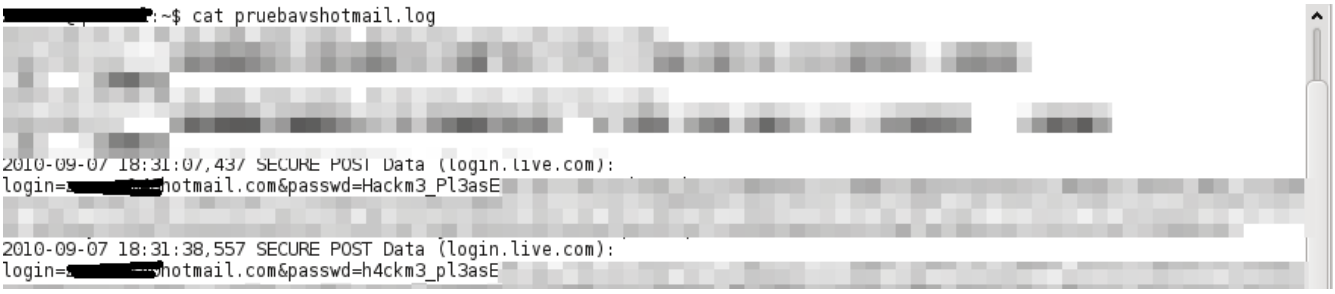
El segundo parámetro indica primero la IP del cliente (víctima) y la segunda IP es la del Router .

Expliquemos un poco el sslstrip como recuerdan le pasamos los parametros “-w nombre_de_su_archivo” y “-p -l 10000”

El nombre del archivo es bastante claro.... y -p -l 10000 que es el puerto a donde estábamos redirigiendo el tráfico

Listo en este momento ya estamos recibiendo todas la contraseñas y paquetes que van dirigidos hacia nuestra victima, solo es cuestion de esperar que se conecte a algun sitio y lo tendremos en nuestras manos....jajaja.

Para verlas abrimos el archivo el cual creamos cuando para guardar el trafico.



ah... vale la pena decir que lo intente con varios navegadores y en todos me sirvio.

Agradecimientos:

Primero que nada agradezco a san Google que es quien me ayuda en mi formacion.

A mi madre por apoyarme en lo que me gusta... me hace mucha falta...jejej.

A mi novia por irse de mi lado mientras escribia (No me dejaba concentrar ....jeje).

Y A mis compañeros de la comunidad que son los que me motivan a aprender cada dia mas.