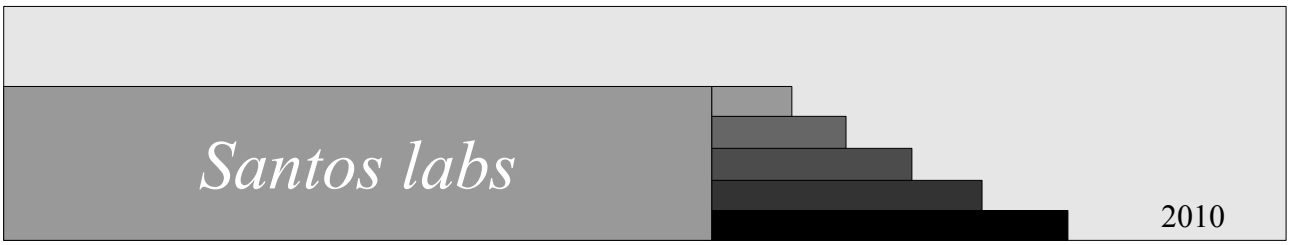


Bueno hoy voy a tratar de explicar de manera sencilla como conseguir password de sitios como facebook, tuenti, …. cualquier site que quieras utilice o no cifrado ssl.

Lo primero de todo esto es lo que necesitas para simular el ataque en tu equipo (ya sabéis, todo esto es tan solo para uso educativo y no para beneficiarte con ello ni para hacer el mal):

1. Un ordenador con conexión a Internet (parece mentira eh?).
2. SSL Strip (versión 0.7 en el momento del tutorial)
3. VMWare o cualquier otro software de virtualmente.

El primer paso es ir a la web de nuestro amigo Moxie Marlinspike (thoughtcrime.org), creador de SSL Strip, para descargarnos la aplicación (de paso si os sentís generosos y la crisis no os esta afectando mucho, le podéis hacer un donativo al chaval, que hasta hace poco estaba en paro) e instalarla en nuestra maquina virtual (el SO de mi maquina virtual era ubuntu a la hora de hacer las pruebas). Aviso, SSL Strip esta escrito en python por lo que es necesario que tengáis en vuestra maquina virtual instalado el interprete de python. Para que el programita este os rule es necesario que también tengáis la siguiente aplicación: twisted-web (que es un modulo de python) para ello si no lo tenéis ya sabéis el mítico sudo apt-get install python-twisted-web (si vuestra versión de ubuntu es nuevecita es muy probable que ya os vengan instalados by default tanto el interprete de python como el modulo twisted web).
Para instalar SSL Strip tan solo hay que descomprimirlo (tar zxvf sslstrip-0.7.tar.gz), movernos al directorio (cd sslstrip-0.7), e instalarlo (sudo python setup.py install).

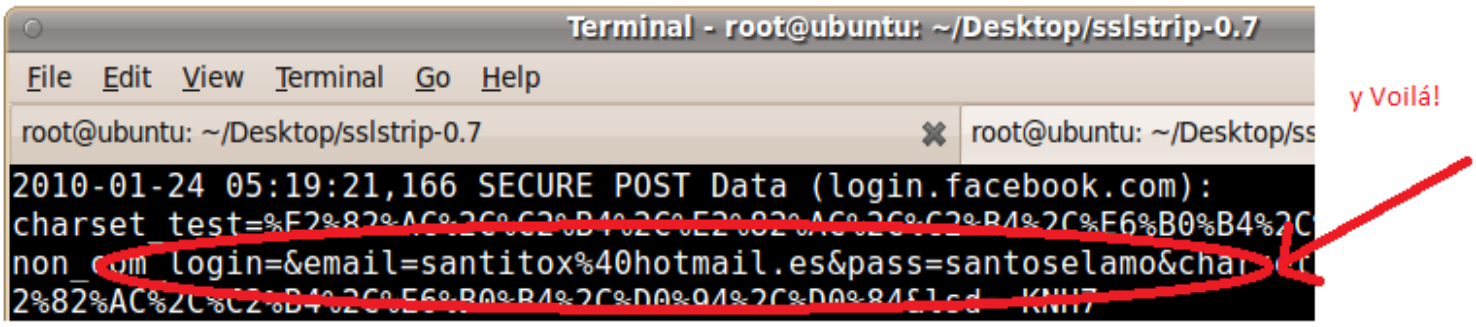
Una vez instaladas todas las herramientas necesarias, vamos a configurar nuestra maquina atacante (aka “evil server”). Lo primero es poner nuestro “evil server” a la escucha, listo para transmitir (echo "1" > /proc/sys/net/ipv4/ip_forward) esta operación es necesaria que la ejecutéis como root; configurar las iptables para que redireccione el trafico HTTP entrante en el puerto 80 hacia el SSL Strip (iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <Puerto que te salga de los güevos>).

Como en este tutorial tan solo voy a explicar como simular el ataque en tu propio equipo, sera necesario que hagamos unos pequeños ajustes en el equipo de la victima (en este caso nosotros mismos). [NOTA: en un próximo tutorial explicare como poder realizarlo en un escenario real, esto es, explicare como realizar el ARP Poisoning]

Abrimos nuestro navegador web (en mi caso Firefox) (OJO! Estos pasos de ahora los realizamos en nuestro SO, no en el del “evil server”) nos vamos a Herramientas – Opciones – Avanzado – Red la mayoría de vosotros tendréis activada la navegación sin proxy, entonces lo que tenéis que hacer es activar la opción de Configuración manual del proxy. En el campo de Proxy HTTP introducimos la Ip de nuestro “evil server” (ya sabéis ifconfig y copy-and-paste) y en puerto el puerto al que en la configuración de las iptables decidimos redireccionar el trafica http; y por ultimo activamos la opción Usar el mismo proxy para todo.

Bueno ya tenemos todo listo para poder ver lo que esta maravillosa herramienta es capaz de hacer.

Para simular el ataque, volvemos a nuestro “evil server” y arrancamos SSL Strip (sudo sslstrip.py -l <el puerto que hubieseis puesto>).
Ahora nos volvemos al papel de la victima y por ejemplo vamos a facebook.com y nos logeamos.
Si en nuestro “evil server” consultamos sslstrip.log (vi ~/Desktop/sslstrip-0.2/sslstrip.log) que nos muestra la captura del trafico y.....

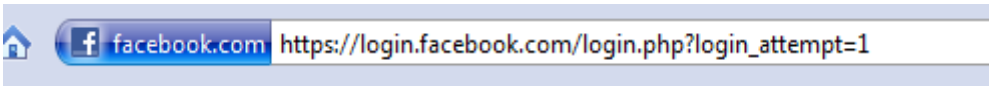


Ahí tenéis los nombres de usuarios y los passwords en texto plano.

[EL PORQUE DE TODO ESTO]

Brevemente os explicare esto a que se debe.
Os estaréis preguntando como es posible que si facebook usa https como es posible que estemos viendo los passwords en texto plano? Pues la verdad es que no os estáis conectando en facebook si no en una pagina muy parecida, tan parecida que solo se diferencia en que una usa cifrado SSL y la otra no. Si así de “sencillo” es, SSLStrip mira si es un link HTTPS y entonces lo redirecciona a nuestro puerto y muestra al usuario una web que parece ser facebook pero no lo es. (Nota si la web no usa https también se registra toda la información en el archivo sslstrip.log).

Sin SSL Strip:



Con SSL Strip:

Saludos y hasta la próxima,
Santos Merino (sant0x!).