ANÁLISIS DE LAS PRINCIPALES TÉCNICAS DE HACKING PARA LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ

AUTORES: Ing. Ángel Pisco Gómez[1]
: Ing. Yanina Holanda Campozano Pilay[2]
: Ing. Jimmy Leonardo Gutiérrez García[3]
: Ing. Javier Marcillo Merino[4]
: Ec. Robards Javier Lima Pisco[5]

DIRECCIÓN PARA CORRESPONDENCIA: (angelloc456@yahoo.com)

Fecha de recepción: 10/11/2018

Fecha de aceptación: 12/12/2018

RESUMEN

La investigación realizada presenta una perspectiva de Análisis de las principales técnicas de hacking para la Universidad Estatal del Sur de Manabí. Actualmente las universidades, organizaciones y compañías están expuestas a numerosas amenazas que violan sus sistemas informáticos, ya que esto pone en riesgo la integridad de la información. Un hacker es una persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos. Ya que uno de los métodos para lograr mitigar eficazmente los impactos provocados por un ataque informático, es precisamente tener conocimiento de la manera como estos atacan y conocer los posibles puntos débiles de un sistema comúnmente explotados y en los cuales se debe hacer especial énfasis al momento de concentrar los esfuerzos de seguridad propensos a la prevención de los mismos. La metodología que se utilizo fue la cualitativa la cual nos ayudó a describir de forma minuciosa los hechos, situaciones, comportamientos, interacciones que se observan mediante la investigación realizada. Ya que la

[1] Ing. Ángel Pisco Gómez - Master en Gerencia Educativa - Docente de Carrera Tecnologías de la Información en la Universidad Estatal del Sur de Manabí Jipijapa-Manabí-Ecuador- angelloc456@yahoo.com.
[2] Ing. Yanina Holanda Campozano Pilay- Master en Gerencia Educativa - Docente de Carrera Tecnologías de la Información en la Universidad Estatal del Sur de Manabí Jipijapa-Manabí-Ecuador- yanicam@yahoo.es
[3] Ing. Jimmy Leonardo Gutiérrez García - Master en Gerencia Educativa - Docente de Carrera Tecnologías de la Información en la Universidad Estatal del Sur de Manabí Jipijapa-Manabí-Ecuador- jileguga@hotmail.com
[4] Ing. Mario Javier Marcillo Merino Master en Docencia Universitaria - Docente de Carrera Tecnologías de la Información en la Universidad Estatal del Sur de Manabí Jipijapa-Manabí-Ecuador- mario_marcillo_merino@hotmail.com
[5] Ec.. Robards Javier Lima Pisco Master en Administración ambiental - Docente de Carrera Tecnologías de la Información en la Universidad Estatal del Sur de Manabí Jipijapa-Manabí-Ecuador- robardslima@gmail.com

© Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador.

información representa un papel muy importante dentro de las instituciones pues es la parte más primordial y día a día se encuentra expuesta a sufrir modificaciones y en muchos casos a ser hacheada en su totalidad y es por eso importante asegurar la integridad de la información. Por lo tanto, es necesario determinar que herramientas utilizar, y las técnicas fundamentales para probar la vulnerabilidad de los sistemas de información y de las redes instaladas.

PALABRAS CLAVE: herramientas; información; seguridad; técnicas; vulnerabilidades.

ANALYSIS OF THE MAIN HACKING TECHNIQUES FOR THE SOUTHERN MANABI STATE UNIVERSITY

ABSTRACT

The research carried out presents an analysis perspective of the main hacking techniques for the State University of the South of Manabí. Currently universities, organizations and companies are exposed to numerous threats that violate their computer systems, as this puts the integrity of the information at risk. A hacker is a person with great knowledge of computer science that is dedicated to illegally accessing foreign computer systems and manipulating them. The methodology that was used was the qualitative one which helped us to describe in a thorough way the facts, situations, behaviors, interactions that are observed through the research carried out. Since one of the methods to achieve effectively mitigate the impacts caused by a computer attack, is precisely to have knowledge of how they attack and know the possible weaknesses of a system commonly exploited and in which special emphasis should be made at the time to concentrate security efforts prone to the prevention of them. Since the information represents a very important role within the institutions because it is the most fundamental part and day to day is exposed to undergo modifications and in many cases to be hacked in its entirety and it is therefore important to ensure the integrity of the information . Therefore, it is necessary to determine which tools to use, and the fundamental techniques to test the vulnerability of the information systems and the installed networks.

KEY WORDS: techniques; tools; vulnerabilities; information; security

INTRODUCCIÓN

La criminalidad informática no es más que una forma de quebrantar los sistemas de seguridad de una institución, de modo que se pueda acceder a unos recursos u obtener una información deseada. Esto ha hecho que se incremente la necesidad de platear esquemas claros de protección sobre la información y demás recursos críticos de las empresas. Como si fuera poco, el hecho de prestar servicios que estén basados en interconexiones con diferentes redes, exige contar

con políticas de seguridad robustas adicionales, que garanticen la prestación confiable de dichos servicios. Tales políticas deben enmarcase dentro del contexto de una metodología de seguridad que trabaje sobre los principios básicos de seguridad: Autenticación, Confidencialidad, integridad, disponibilidad, Control de acceso y Auditorias. La seguridad informática es un área que día a día exige la presencia de un equipo capacitado y dedicado a esta labor, lo que conlleva a la especialización de las personas en diversos campos de la seguridad informática. Los hackers crearon Internet, Unix, Linux, la World Wide Web etcétera, además de la mayoría de elementos que las componen; ellos fomentan la libertad en el uso de herramientas, sistemas y lenguajes no privativos con copyleft; desarrollaron los lenguajes y técnicas de programación, las telecomunicaciones y siguen luchando en un mundo cada vez más globalizado y abierto. (Nazareno, 2010)

DESARROLLO

TÉCNICAS DE HACKING

MONITORIZACIÓN

Esencialmente es un conjunto de métodos de ataque que comprenden unas etapas de observación, donde se indagan las vulnerabilidades de la víctima y un posible acceso.

SCANNING (ESCANEO DE PUERTOS)

El Escaneo de puertos es el precursor de muchas intrusiones y ataques. En ausencia de información privilegiada o de información pública sobre una red de destino, estas exploraciones son el primer paso en la obtención de información básica sobre la red.

Objetivo del ataque

Indagar por el estado de los puertos de un host conectado a una red, y si éstos puertos están abiertos analizar posibles vulnerabilidades.

Modo operacional

TCP connect: La forma básica de escaneo de puertos, intenta establecer conexión con varios puertos de la máquina.

Si el puerto está escuchando, devolverá una respuesta de éxito y se establece la conexión. Cualquier otro evento significará que el puerto está cerrado. Esta técnica se caracteriza por ser rápida y no precisar ningún permiso de usuario sobre la máquina víctima. Sin embargo, es una técnica que se detecta fácilmente ya que los intentos de conexión queda registrados en la máquina. (Suarez A. , 2011)

TCP SYN: Este escaneo usa la técnica de "la media apertura". Consiste en mandar un paquete TCP SYN al puerto. Si este puerto está abierto contestará con un paquete ACK y si no es así responderá con un paquete RST. Si el puerto está abierto se responderá al paquete ACK con un paquete RST para no establecer la conexión y no dejar rastro en la máquina objetivo. Es una técnica poco ruidosa y muy sutil ya que no se llega a establecer conexión en ningún momento.

TCP FIN: Consiste en el envío de un paquete FIN a un puerto. Si éste responde con un RST el puerto estará cerrado. Sin embargo, si no se obtiene ninguna respuesta significa que el puerto está abierto. Esta técnica es la más efectiva para no ser detectados, sin embargo sólo funciona en sistemas LINUX/UNIX ya que en Windows siempre responde con un RST a los paquetes FIN.

Escaneo fragmentado: Este procedimiento consiste en fragmentar los paquetes de sondeo dirigidos a la máquina víctima. Con esto conseguimos provocar menos ruido en las herramientas de protección (firewalls) del sistema.

Consecuencias

- Constantes avisos del firewall.
- Utilización maliciosa de puertos abiertos por parte de intrusos.

Cómo detectar el scanning: La detección de estos escaneos iniciales puede permitir a los defensores bloquear posibles atacantes antes de que puedan ser peligrosos. Sin embargo, los análisis en los puertos son aleatorios y rápidos y los métodos de detección de Escaneo no son tan eficientes para detectarlos y predecirlos.

Modo operacional: Se establecen conexiones activas con el sistema y se llevan a cabo consultas dirigidas. Se puede obtener información en lo que respecta a máquinas, recursos de red, aplicaciones, y hasta información referente al sistema operativo. También se recolectan datos sobre los recursos del sistema que se encuentren mal configurados y vulnerabilidades del sistema que se tiene por objetivo.

Casi siempre los datos que se obtienen con esta herramienta es información pública, como direcciones de DNS.

Consecuencias: Con el conocimiento de cualquier sistema el intruso puede preparar un ataque y acceder a todos los recursos informáticos. Este tipo de intromisión es el punto de partida para llevar a cabo ataques de Validación y de Modificación.

Medidas de prevención

Estos son algunos consejos para protegerse de ataques de enumeración:

• Corregir los protocolos que contestan de diferente modo si el usuario existe o no.

• Configurar correctamente los servicios para que no muestren más información de la necesaria.

• No usar nombres por defecto para archivos de configuración.

• Desactivar puertos de administración http y snmp.

• Cambiar el password por defecto de todos los lugares.

(Marcos, 2018)

SNIFFING (OLFATEO)

También llamada "Robo de información". Con esta técnica "se escucha la información cuando esta no va dirigida a la máquina que está capturando el tráfico"

Objetivo del ataque

Obtener información de todo el tráfico que pasa por una red, no importa si los datos están encriptados.

Modo operacional: En esta técnica "se usan analizadores de protocolos (packetsniffers), que son programas que permiten monitorizar y analizar el tráfico de una red". Las aplicaciones descifran los paquetes de datos que viajan por la red y los almacenan para luego analizarlos. Entre toda esta información se pueden distinguir contraseñas, mensajes de correo electrónico, datos bancarios, y otros datos confidenciales de usuario.

Un sniffer es un programa que trabaja dentro de la red en conjunto con la tarjeta de interfaz de red (NIC, Network Interface Card), para atraer todo el tráfico que está a su alcance, incluso más allá de los routers y dispositivos similares.

Consecuencias: Al detectar toda la información que circula por la red se ponen en evidencia elementos confidenciales tales como números de tarjetas de crédito, nombres y contraseñas de usuarios y más información sensible.

Cómo prevenirla y/o detectarla: Existen dos técnicas esenciales para lograr la detección de los sniffers. La primera se basa en el host, y es determinando si la tarjeta de red del sistema está funcionando en modo promiscuo. La segunda se basa en la Red. Hay que resaltar la importancia que cobra el hecho de enviar la información de manera encriptada con algún tipo de tecnología de encriptación como lo son PGP ó GnuPG. Para evitar ataques en las redes se recomienda utilizar encriptación WPA, debido a que la protección WEP es demasiado vulnerable al software Sniffer.

Si sólo se cuenta con WEP, la contraseña debe ser cambiada con regularidad. Por otra parte, los routers deben estar bien protegidos con contraseñas.

Fuerza bruta: El ataque por fuerza bruta se define como el procedimiento por medio del cual se intenta acceder por medio de la obtención de la clave. Los tipos de ataque por fuerza bruta son: Objetivo ataque, Trawlingattack. (Jose, Dragon.JAR, 2014)

SPOOFING (SUPLANTACIÓN)

El Spoofing es un tipo de técnica de camuflaje online donde se suplanta la identidad de un dispositivo en una red informática para obtener información restringida. Este ataque tiene algunas variedades entre las que se destacan el IP Spoofing (enmascaramiento de la dirección IP), que es el genérico y que "consiste en generar paquetes de información con una dirección IP falsa"38, y por ende, falsificar la cabecera de los paquetes enviados a un determinado sistema informático, donde el paquete pareciera que viene de otra persona. Con esto, la persona que realiza el ataque selecciona una dirección IP que pertenece a un equipo legítimo y así puede acceder a cualquier otro sistema.

Las distintas técnicas de Spoofing se basan en los protocolos ARP (protocolo de resolución de direcciones), ICMP (protocolo de mensajes de control de Internet),

RARP (protocolo de resolución de direcciones inversa).

Objetivo del ataque

En relación a que son diversos los ataques con Spoofing, también varían los objetivos en estos tipos de ataques. Entre ellos tenemos:

- Falsificar datos.
- Adquirir información de una determinada máquina
- Simular la identidad de otro.

Modo operacional IP SPOOFING: Esta variedad de Spoofing tiene ciertas desventajas iniciales, como es el hecho de que la host víctima puede cortar la conexión o que los routers actuales no admiten paquetes cuyos remitentes no corresponden con los que administra en su red, lo cual acortaría el engaño a la red gestionada por un routers. Otro tipo de Spoofing es el DNS Spoofing; también llamado Pharming. Se trata del cambio de la relación de un nombre de un dominio por una IP falsa. Este ataque se realiza si el servidor DNS no es muy seguro, ó si confía en otros que sí son

inseguros. Por otro lado, una vez se haya realizado el cambio, otros servidores DNS que se fíen de este, podrán añadir a sus cachés la dirección falsa, denominándose DNS poisoning.

Modo operacional de arp spoofing: El ARP SPOOFING introduce una dirección IP falsa a la asignación de direcciones MAC en la tabla ARP. El envenenamiento ARP se puede hacer mediante la actualización de una entrada ARP existente. Lo que se busca con esta técnica es que la víctima envíe los paquetes al destino del atacante en lugar de remitirlos al destino legítimo.

Consecuencias: El riesgo más conocido es el de Phishing, donde una persona es timada y se le hace creer que ha entrado a su entidad financiera de confianza.

Medidas de defensa IP SPOOFING: Existen algunas medidas que se pueden utilizar para contrarrestar esta técnica que van desde el uso de IPsec para reducir los riesgos hasta la utilización de filtros que permitan asociar una dirección IP al tráfico que sale de la red en cuestión.

Cómo evitar el ARP SPOOFING: Existen dos casos. Para una red pequeña la utilización tanto de IP estáticas como tablas ARP estáticas puede ser la solución. Para otro tipo de redes la solución debe estar asociada a la dirección MAC y cómo impedir que ésta pueda ser modificada en los host; ya que si se piensa en la primera solución sería imposible actualizar las entradas de nuevas máquinas en la tabla ARP.

HIJACKING (ROBO DE SESIÓN)

El Hijacking es una técnica por medio de la cual se intercepta y se roba una sesión de algún usuario para apropiarse de algún servicio, después de que el usuario autorizado que se quiere suplantar se identifica ante el sistema remoto. Los servicios de los que se apropia van desde módems, routers, las conexiones TCP/IP, dominios, páginas web e inicio de sesión.

Objetivo del ataque

Secuestrar una conexión ya establecida de manera legal por otro usuario con un servidor.

Cómo se hace: El atacante por medio de un software sniffer husmea los paquetes que están circulando por la red y envía paquetes al servidor, y con esto simula y se adelanta al usuario autorizado que ahora lo único que ve es como su conexión se ha colgado. A partir de este momento, el atacante tiene el control y continuará con su tarea de enviar datos.

¿Cómo protegerse? Como primera medida de protección se debe usar la encriptación, para que los datos que viajen por la red se encuentren codificados. Esto es fundamental ya que el Hijacking se basa en Sniffing que tiene como peor enemigo la información encriptada. Tampoco se puede dejar de lado el firewall, el antivirus, el antispyware y la utilización de programas como el Anti-

Hijacker que tienen como finalidad resguardar las máquinas, las páginas webs, y hasta los módems de algún secuestro. Los protocolos de seguridad tales como https son importantes también para evitar el robo de sesión y, por ende, de información. (Suarez M. J., 2013)

D.O.S (DENEGACIÓN DE SERVICIO)

Técnica de ataque donde se consigue que los servidores y redes informáticas colapsen y de esta manera ya no puedan brindar sus servicios como lo hacen habitualmente. Estos ataques pueden ser enviados desde uno o varios computadores. Cuando son enviados desde servidores, se denominan ataques distribuidos. A los servidores que cumplen con esta tarea se les conoce como zombies, y es el atacante quien se ha apropiado de ellos. Los ataques de denegación de servicio (DoS) no se limitan sólo a los sistemas finales. También incluyen routers de núcleo de red, switches y servidores de nombres de dominio.

Jamming (interferencia): Jamming se refiere al bloqueo de un canal de comunicación con la intención de impedir el flujo de información. Esta es una de las formas más temidas de los ataques en las redes inalámbricas. Esto es así porque, con la arquitectura de red existente, es muy poco lo que se puede hacer para superar un ataque de bloqueo. Son muy comunes las noticias de ataques D.o.S dentro de las entidades gubernamentales. En 2007, los sitios Web del Parlamento, los bancos y los organismos de radiodifusión en Estonia fueron víctimas de ataques de denegación de servicio.

Objetivo de jamming

El objetivo del ataque es inundar con pedidos falsos, saturando los recursos (disco duro, la memoria y el procesador) de las máquinas destino para que estos equipos sean incapaces de proporcionar los servicios normales.

Medidas de prevención: Algunos elementos importantes para tener en cuenta a la hora de prevenir y descubrir ataques de Jamming son:

- La eliminación de las vulnerabilidades conocidas en los comportamientos del protocolo y la configuración del host.
- Filtrar el tráfico. - La detección de ataques. (Rouse, 2012)

SYN FLOODING (ATAQUE POR SINCRONIZACIÓN)

Consiste en mandar paquetes SYN a una máquina y no contestar a los paquetes ACK produciendo en la pila TCP/IP de la víctima una espera de tiempo para recibir la respuesta del atacante

Modo de operación: Se inicia una sincronización de conexión con un servidor a un determinado servicio que proporcione. Posteriormente esta petición formará parte de la pila TCP/IP del servidor (ocupando desde aquí un espacio); luego el servidor esperará la respuesta del usuario (sobre aceptación de la conexión).El servidor puede esperar de 1 a 3 minutos a que el usuario responda; en caso que se sobrepase el tiempo, el servidor rechaza la conexión y libera el espacio de la pila. Mediante aplicaciones maliciosas o de auditoría de red, se pueden falsear (spoofear) las dirección IP de origen, haciendo múltiples intentos de conexión desde un mismo equipo, así mismo el servidor espera las respuestas de direcciones falseadas (spoofeadas). Esto realizado en mayor escala llega a saturar el ancho de banda y colapsar los servicios que brinda el servidor

Consecuencias

- Saturación de los recursos de memoria.
- Incapacidad de establecer conexiones adicionales.
- Inundación de puertos, como Smtp (correo electrónico) y http (contenido web) con conexiones.

Medidas:

- Blindar el servidor con un firewall del tipo stateful.
- Disponer de un sistema operativo actualizado.
- Habilitar la protección SYN Cookie

Modificación: Este tipo de técnicas tienen como objetivo la modificación no autorizada de los datos y ficheros de un sistema. También pueden modificarse programas que se ejecutan en el sistema cambiando su funcionamiento.

BORRADO DE HUELLAS

Consiste en modificar los ficheros log del sistema operativo de la máquina asaltada, donde queda constancia de la intrusión, para borrar el rastro dejado por el atacante

Se le llama “huellas” a todas aquellas tareas que ejecuta el atacante dentro del sistema. Estas tareas ó procedimientos son guardadas en archivos logs.

¿Cómo se hace? El intruso puede borrar sus rastros de muchas formas. La más grotesca es haciendo un simple rm –rf /var/log, ya que así podrían ser recuperados fácilmente con técnicas forenses simples. Diferente es si utiliza una herramienta de borrado seguro como Wipe, pero así se despiertan las sospechas del administrador. Puede hacerlo de manera más sutil si programa un zapper adecuado al objetivo y al modo de gestionar registros que existe en el servidor (que puede

no estar por defecto). A su vez, debe borrar todos los logs que éste modifica tras su paso y sólo eliminar las entradas que corresponden a dichas sesiones.

Consecuencias

- Posibilidad de ataque futuro, al no detectarse la intrusión a tiempo.
- Pérdida de información de la mano del borrado de archivos.

Medidas de detección: Es difícil guiarse por los logs después de una intrusión, ya que casi siempre han sido borrados. Pero si se detecta al intruso pueden ocurrir tres cosas importantes. Lo primero es que sabiendo dónde está el hueco de seguridad, éste puede ser cubierto. Lo segundo es que con el conocimiento obtenido se pueden evitar ataques posteriores, y algo que, incluso, se puede llevar a cabo es el rastreo del atacante. (Heidegger, 2011)

Resultados de análisis de la seguridad de la red (WIFI)

Tabla:1

FUNCIÓN	**WEP**	**WPA**	**IIS**
Encriptación	Débil	Soluciona debilidades	Inhabilite protocolos como ftp si no se utilizan.
Claves	40 Bits	128 Bits	Habilite el registro en la herramienta de configuración.
Claves	Estáticas	Dinámica	Inhabilite el servicio de datos remotos si no es necesario.
Claves	Distribución Manual	Automática	Establezca permisos de acceso para la clave de registro winreg. Sólo los administradores requieren acceso a esta clave.
Autentificación	Débil	Fuerte, según 802.1x y EAP	Elimine aplicaciones de ejemplo como \\IISSamples, \IISHelp y \MSADC.

Tabla:2

Métodos recomendados de seguridad para el servidor web.	**Para Apache, métodos recomendados:**

Elimine los directorios virtuales no utilizados.	Habilite sólo los módulos necesarios.
Elimine o inhabilite los scripts ASP o cgi-bin predeterminados de ejemplo proporcionados con la aplicación del servidor web. Por ejemplo: Apache: cgi-bin/printenv.pl.	Asegúrese de que la instalación de Apache oculte la información de versión y otra información confidencial.
Cree un directorio raíz para el servidor web. En Apache, esto se conoce como chrooting.	Desactive el examen de directorios.
Elimine las correlaciones predeterminadas no deseadas, como las de las aplicaciones con las extensiones de archivo .htr, .idc, .stm, .printer y .htw.	Configure el servidor web para restringir el acceso por dirección IP.
Habilite SSL (secure sockets layer) en el servidor web.	Asegúrese de que el registro de errores y el registro de acceso estén habilitados.

CONCLUSIÓN

El trabajo describe sobre la importancia de la seguridad informática como es el tema de hacking ya que ha venido ocurriendo en algunas Instituciones, organizaciones por motivo de que no tienen políticas de seguridad.

La información recogida en el artículo explica sobre las diferentes técnicas de Hacking que permite abordar el problema del acceso sin autorización tanto desde una perspectiva de prevención como desde un ámbito de detección con las correspondientes medidas. Con el conocimiento adquirido se dispone de cierta ventaja para afrontar muchos de los retos que surgen cada día en materia de seguridad informática.

Ya que los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

Ciyi, C. G. (2010). *Hablemos de Spoofing.* Hacking Ético.

Gonzales, M. (2018). *Monitorización.*

Heidegger, Z. (20 de 08 de 2011). *Blackploit*. Obtenido de https://www.blackploit.com/2011/08/eliminar-rastro-y-huellas-post.html

Jose, T. (07 de 05 de 2014). *Dragon.JAR*. Obtenido de https://www.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-sniffing-i.xhtml

Jose, T. (s.f.). *Dragon.JAR*. Obtenido de https://www.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-sniffing-i.xhtml

Marcos, Q. (8 de 11 de 2018). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Esc%C3%A1ner_de_puertos

Nazareno, G. (2010). *DocPlayer.es*. Obtenido de http://informatica.gonzalonazareno.org

Rouse, M. (5 de 11 de 2012). *TechTarget*. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

Silva Castro, L. A. (2011). *Bliblioteca de Información Cientifica*.

Suarez, A. (21 de 06 de 2011). *Buenas tareas*. Obtenido de https://www.buenastareas.com/ensayos/Amenazas-L%C3%B3gicas/2453279.html

Suarez, M. J. (18 de Noviembre de 2013). *Con la Tecnologia Blogger*. Obtenido de https://mjesussuarez.blogspot.com/2013/11/ataque-mediante-hijacking-robo-de-sesion.html