

Man in The Middle 07

Que es MITM

- Definición y Alcance

- Métodos de Autenticación vulnerados

Métodos para realizar MITM

- Dns Spoofing y Poisoning (local, lan y via wifi)

- Access Point Falso

- Proxy Spoofing

- ARP Spoofing

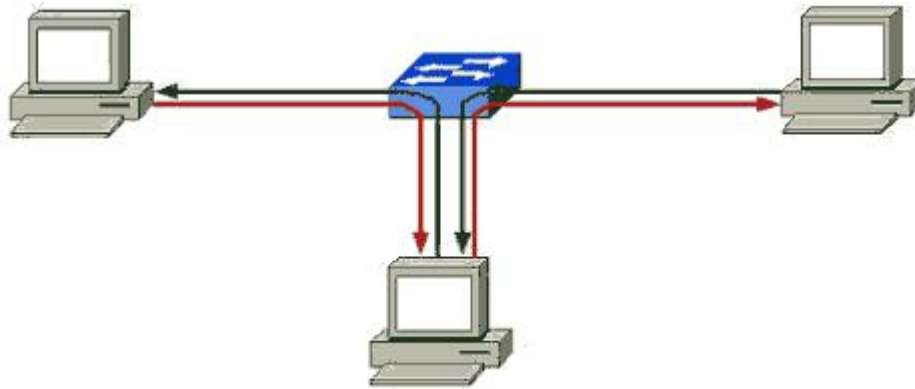
Man in The Browser

MITM con AJAX / cURL

Esto es un texto informativo que da una descripción general de la vulnerabilidad, los ataques previos a MITM, lo que se puede hacer con MITM, los métodos de autenticación que son vulnerados, una variante de esta técnica (MITB) y explica brevemente algunas técnicas y herramientas para realizar este tipo de ataque en Windows y enfocado hacia Web.

Definición y Alcance

“Man in The Middle” traducido al español sería “Hombre En Medio” u “Hombre en el medio” se refiere a que existe alguien en medio de la comunicación entre el origen y el destino.



El atacante puede observar, interceptar, modificar y retransmitir la información, lo que da origen a los siguientes posibles ataques posteriores:

> Sniffing

Leer credenciales enviadas. (Users, Passwords, Cookies, Ccs...)

Leer información enviada. (Archivos, chat, paginas...)

Observar el comportamiento del usuario en base al tráfico de red.

> Spoofing

El atacante puede enviar datos como si fuera el origen.

Realizar operaciones con los datos del cliente.

Mostrar páginas falsas.

Enviar los datos a un destino diferente.

> Negación de Servicio

El atacante puede interrumpir la comunicación.

Bloquear el acceso a ciertas páginas.

Métodos de Autenticación vulnerados con MITM

Metodo de Autenticación	Vulnerada con MITM
OTP / Tokens	El password pasa por el atacante antes del timeout del dispositivo.
IP Geolocalion	El atacante esta localizado en la misma red, usa el mismo ISP o un proxy.
Dispositivo/Hardware	El atacante simula la respuesta original del dispositivo.
Cookie del Navegador / Preguntas secretas	Las cookies pasan por el atacante, o si se pierden, se le solicitan preguntas al usuario que pasan por el atacante quedándose con las respuestas secretas.
Texto personalizado o imagen para identificación personal	Ya teniendo las respuestas secretas también es fácil conocer el texto personalizado o la imagen personal.
Teclado Virtual	La informacion es robada en transito al momento de ser enviada al servidor.
Fuera de banda (por otros medios como SMS o Email)	Después de tener el número de confirmación el usuario lo introduce a la página y este es robado al ser enviado al servidor.

Métodos para realizar MITM

Para poder realizar un ataque de este tipo, es necesario situarse en medio de la comunicación, se pueden utilizar los siguientes ataques que habilitan una comunicación tipo MITM:

- DNS spoofing
- DNS poisoning
- Proxy spoofing
- AP Falso
- ARP poisoning

- STP mangling
- Port stealing
- DHCP spoofing
- ICMP redirection
- IRDP spoofing - route mangling
- Traffic tunneling

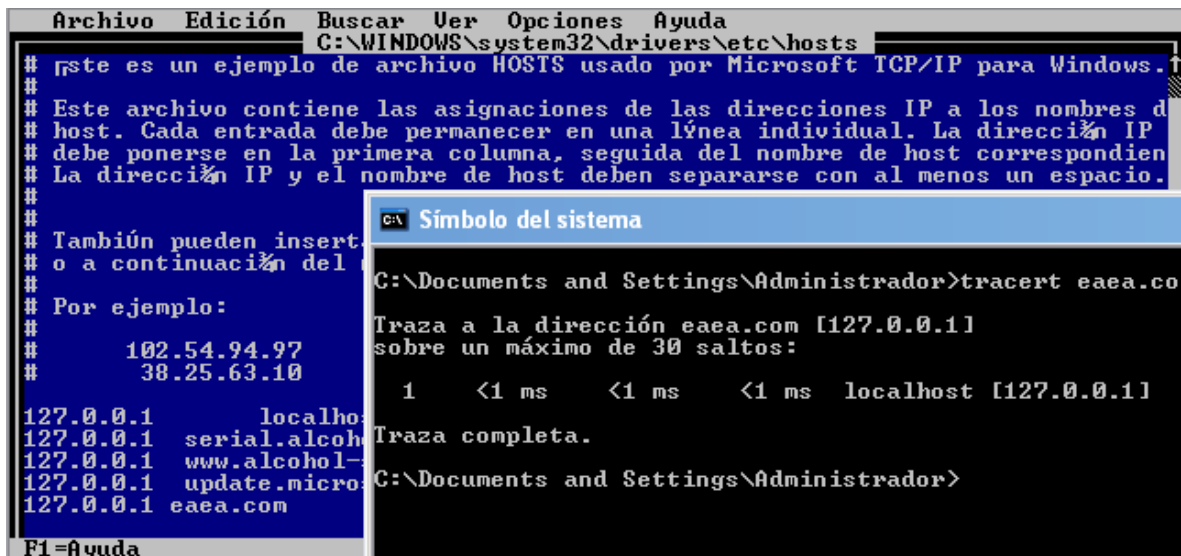
Cuando se realiza este tipo de ataques la velocidad de la conexión se ve afectada ya que aunque la mayoría son para la red local la información tiene que viajar por uno o varios nodos.

DNS Poisoning Local

Consiste en modificar el archivo hosts de nuestro sistema operativo para apuntar un nombre de dominio a una IP. El archivo se localiza en la carpeta de windows\system32\drivers\etc

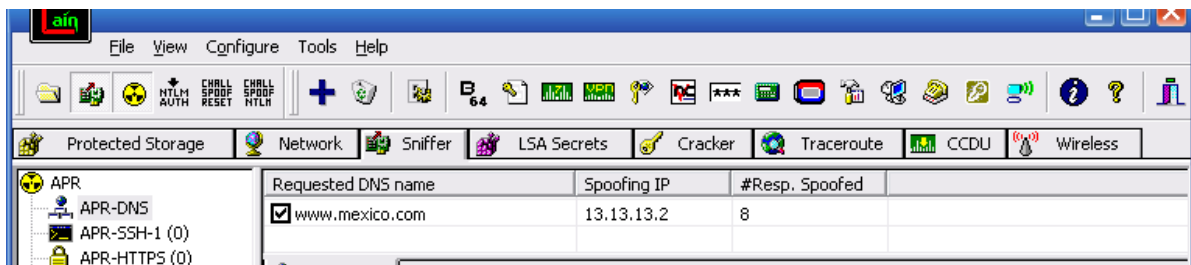
Diferentes tipos de malware utilizan este método para bloquear actualizaciones de antivirus, herramientas y páginas de seguridad.

Se requiere acceso completo al sistema que se quiere envenenar, ya sea físicamente o usando alguna herramienta de administración remota y requiere permisos de Administrador por lo que tiene sus limitantes.



DNS Spoofing usando Caín

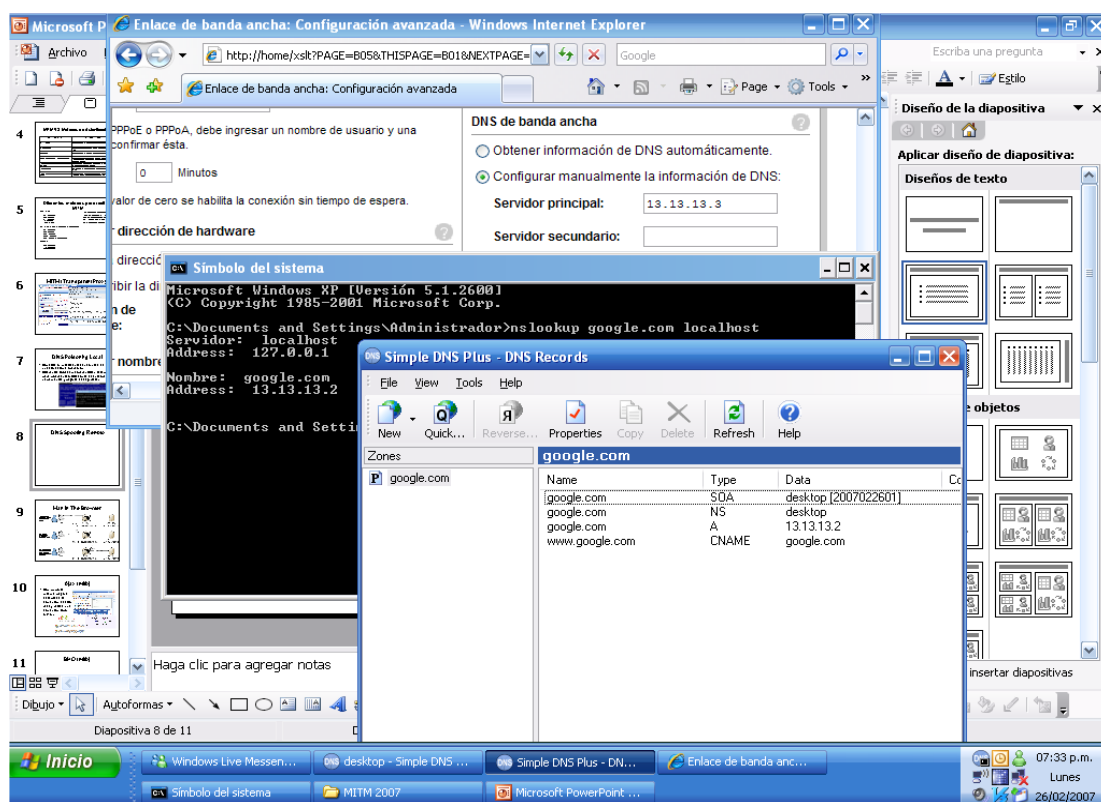
Con Caín es sencillo hacer DNS Spoofing con solo estar en la misma red, dentro del programa habilitamos el sniffer, APR, ahora en APR-DNS podemos agregar el Host e IP al que deseamos redirigir.



DNS Spoofing via insecure WEP

Es trivial crackear la clave WEP default de los modems de Infinitum. Ya se ha hablado mucho de esto pueden ver en los foros de la comunidad existen manuales, ezines y videos que hablan sobre esto.

Ya estando dentro de la red, la mayoría de las personas no tienen password para proteger la configuración de su ruteador. Es sencillo redirigir el servidor DNS a uno propio con direcciones falsas.



Access Point Falso (Evil Twin)

En un lugar con acceso publico a internet podemos poner nuestro access point con el mismo SSID que el publico y las personas que se conecten a el, pasan por nuestra conexión. Es común que esta técnica se realice en aeropuertos o sanborns y usando el SSID default de prodigy "prodigymovil".

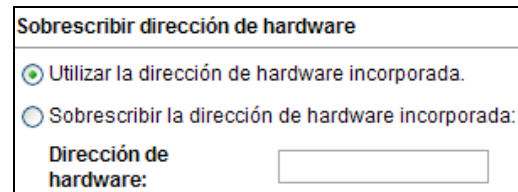


Configuración

Identificar la red

Nombre de red:

Canal inalámbrico:



Sobrescribir dirección de hardware

☒ Utilizar la dirección de hardware incorporada.

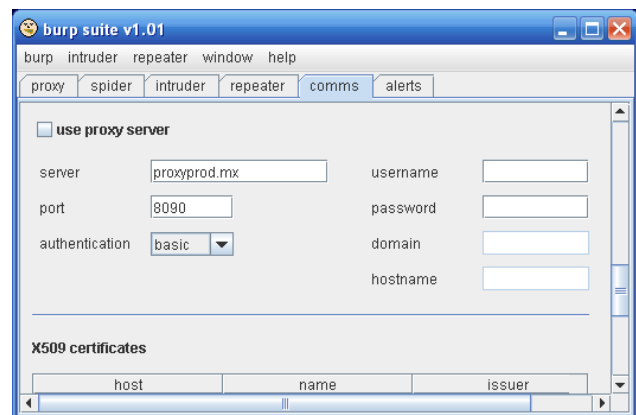
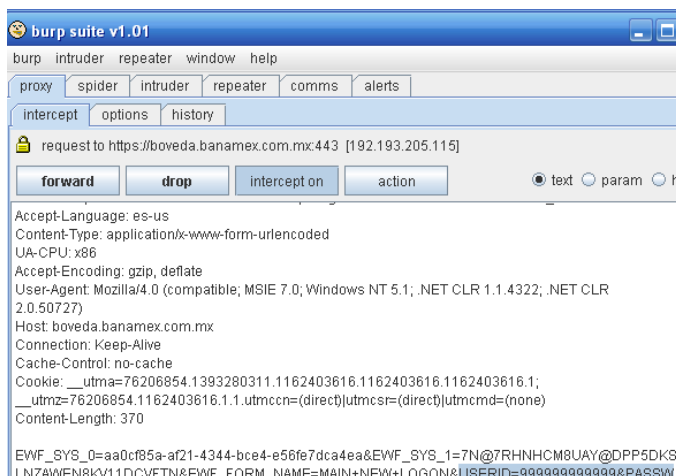
☐ Sobrescribir la dirección de hardware incorporada:

Dirección de hardware:

Existe una vulnerabilidad en el algoritmo de conexión a redes preferidas en windows que permite a un atacante conocer los SSIDs de sus redes preferentes. En Linux esto se puede hacer con una herramienta llamada Karma (<http://www.theta44.org/karma/>) que te permite conocer los -clientes- inalámbricos y falsificar el SSID.

Proxy Spoofing / Transparent Proxy

Es posible apuntar el nombre del proxy a nuestro ip, con alguna de las vulnerabilidades mencionadas y utilizar los servidores proxy: Paros Proxy (<http://www.parosproxy.org/index.shtml>) o Burp Suite (<http://portswigger.net/suite/>) para interceptar la comunicación y poder intervenir incluso ssl.

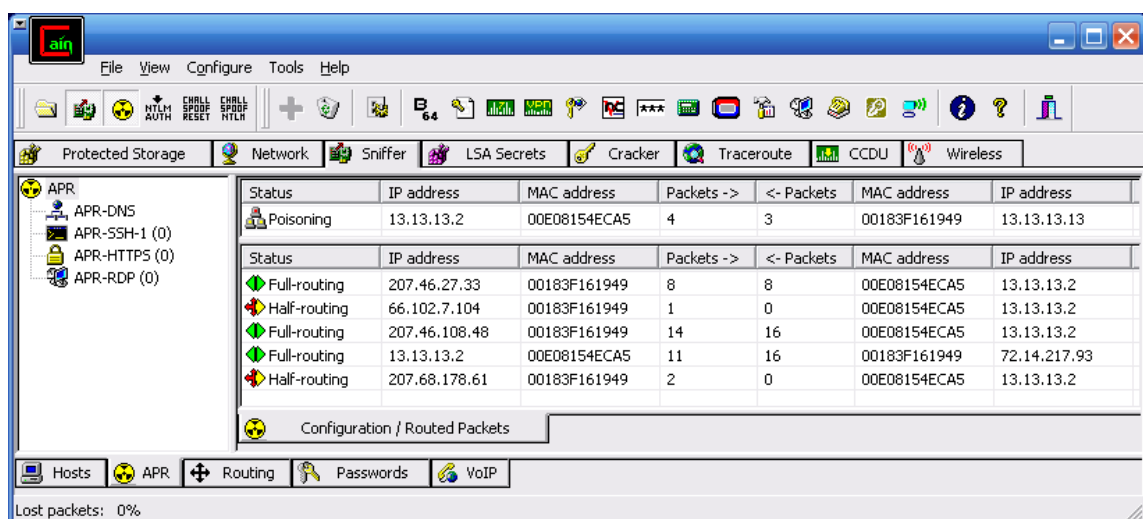
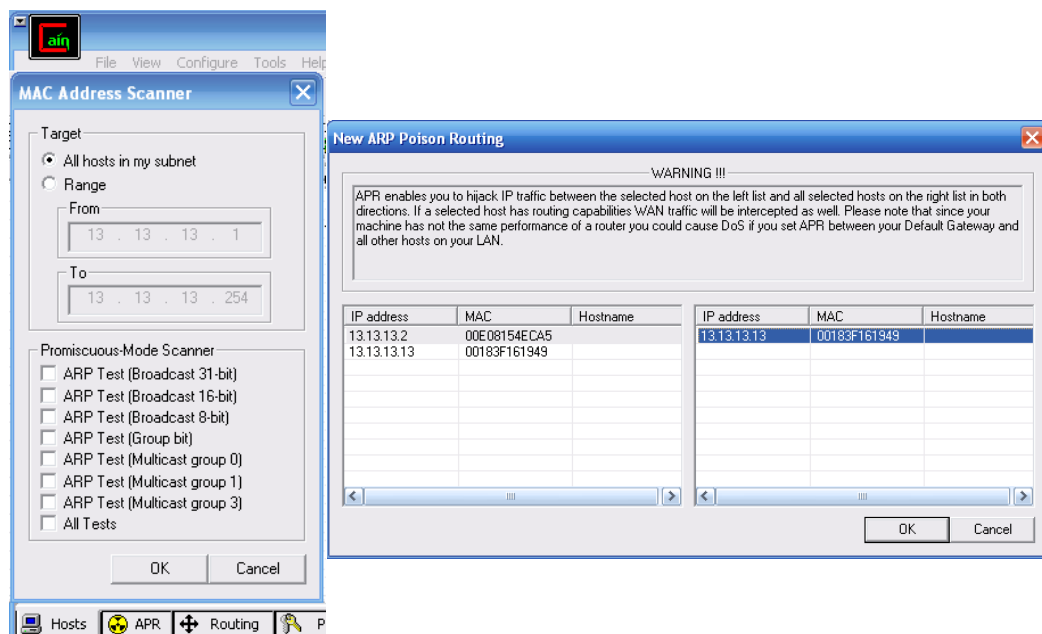


ARP Poison Routing

Se envían mensajes ARP Spoofeados con la MAC de nosotros para envenenar las tablas de ruteo y los paquetes nos lleguen a la dirección que especificamos.

Caín es una excelente herramienta para esto, solamente seleccionamos el Sniffer y dando click en APR en el tab de host seleccionamos Scan MAC ya que tenemos los hosts nos vamos a la parte de Routing y seleccionamos + para redirigir la comunicación entre los hosts que seleccionemos.

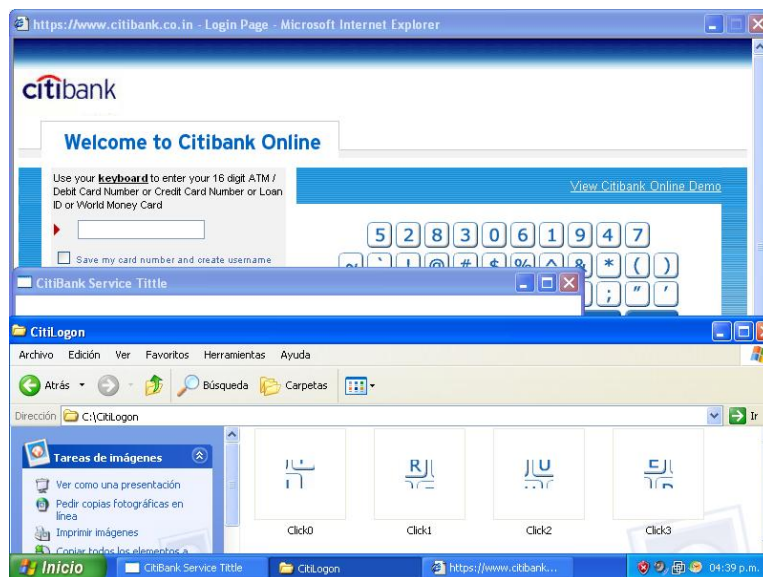
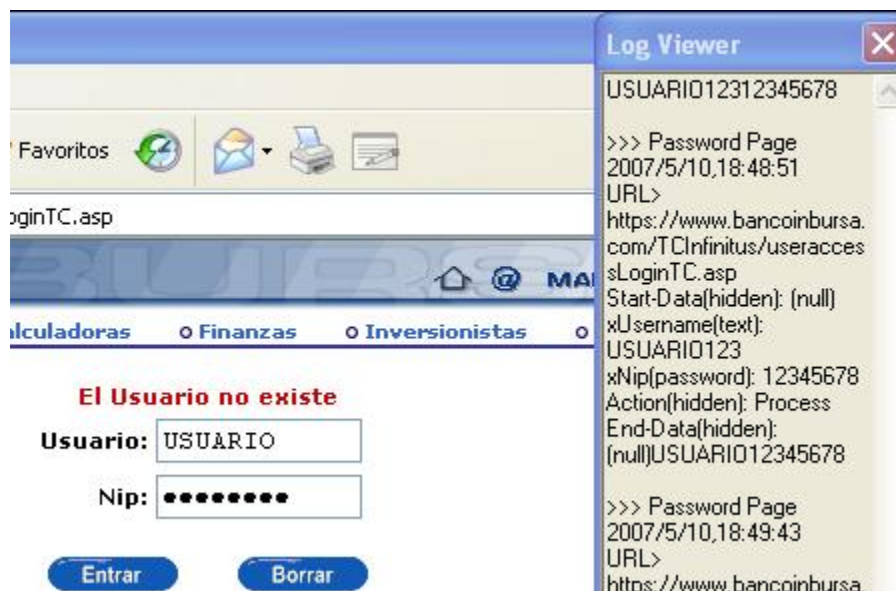
No debemos seleccionar todos los hosts de la lista porque es probable que causemos una negación de servicio.



Man in The Browser

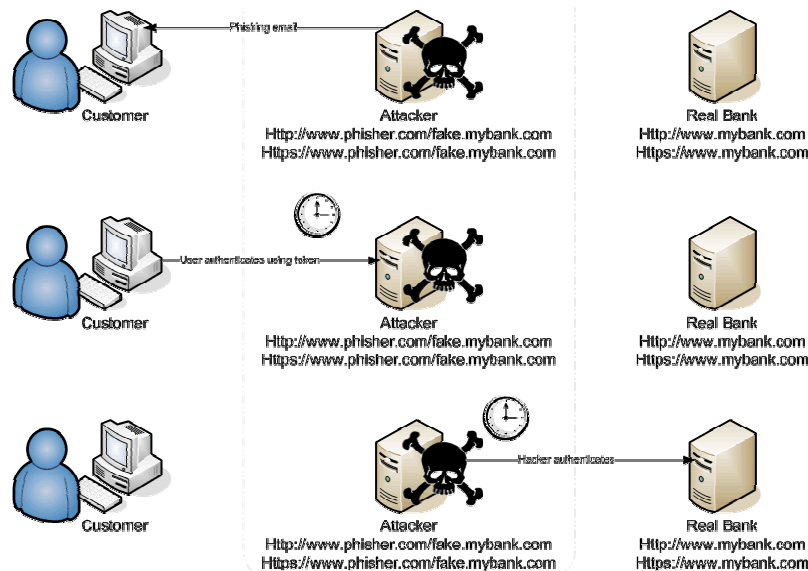
“Man in The Browser” se refiere a cuando no se utiliza un servidor para realizar un ataque de tipo MITM, sino que se utiliza el navegador para interceptar y modificar los mensajes.

Existen los llamados BHOs o Browser Helper Objects para Internet Explorer y los plugins de firefox, así como código que se inserta en el navegador, que cuando la victima ingresa a algún sitio marcado estos programas capturan el tráfico, lo modifican y lo pueden redirigir.



MITM con AJAX o cURL

Existe la posibilidad de utilizar AJAX o cURL para realizar conexiones tipo MITM. La página es quien se comunica con el servidor destino, e intercepta lo que el cliente le pone y lo puede modificar o guardar.



Un ataque similar se utilizo para un portal de phishing que se comunicaba con el servidor original para mostrar los errores correctos o acceder al portal verdadero.

cURL

Automatically get a mirror near you

Front Page
libcurl index
PHP/CURL
Installing
IIS
Apps

Manage Tomcat
Monitor Tomcat, JBoss, MySQL Easy
setup. Download Now!

Rip Curl Beach Wear
Huge Range of Rip Curl
Prices Slashed Rip Curl

cURL ► libcurl ► PHP Binding

PHP/CURL -- using libcurl with PHP

Get libcurl functionality straight from within your PHP
4.0.2, no extra stuff is needed but PHP and libcurl li

http://citibusinessonline.da.us.citibank.com.tufel-club.ru - CitiBusiness Online

citi

CitiBusiness® Online

I am unable to sign you on to CitiBusiness® Online at this time.

7000000008453550 is not a recognized Business Code.
Please close this window and try signing on again.

You can contact customer service at 1 (800) 285 1709.

For hearing impaired call 1 (800) 788 0002

Referencias:

Tipos de MITM

<http://www.contentverification.com/man-in-the-middle/>

Ataque Man-in-the-middle

http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

Ataques MITM: DNS Spoofing, ARP Poisoning, Port Stealing

<http://brsi.blogspot.com/2006/08/ataques-mitm.html>

MITM vs Time Based Tokens

<http://www.securecomputing.com/index.cfm?skey=1574>

Citibank Phish Spoofs 2-Factor Authentication

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

hkm

@hakim.ws

4/2007