

Practica 5 – Obtener la contraseña de acceso a un Servicio protegido con protocolo seguro HTTPS al que no tenemos acceso autorizado.**Teoría:**

El protocolo HTTPS se utiliza en sitios web que requieren seguridad en el acceso, de forma que se establece una sesión encriptada entre cliente y servidor para que la información crítica (contraseñas) no pueda ser leída por terceros. Esta conexión HTTPS requiere la existencia de un certificado válido de servidor verificado por una CA (Autoridad Certificadora).

El equipo atacante va a situarse como *Man in the Middle* entre el equipo víctima y el router (puerta de enlace) de forma que todo el tráfico circule por él. Cuando el usuario víctima trate de conectarse al sitio web, utilizando protocolo HTTPS, realizará una petición de certificado válido de servidor que será servida por el equipo atacante. Al tratarse de un certificado falseado, es posible que la víctima inspeccione y rechace el certificado, y por tanto, no se produzca el inicio de sesión. Pero también es muy posible que la víctima acepte el certificado falseado, sin siquiera leerlo, y el Sniffer situado en el equipo atacante capture el usuario y contraseña de la sesión segura HTTPS.

Aplicación práctica:

Envenenamiento ARP + Envenenamiento DNS + Sniffado

Escenario:

Atacante: 10.10.0.69

Víctima: 10.10.0.254

Router (Puerta de Enlace): 10.10.0.33

Servidor HTTPS: **Hotmail** y **Yahoo**

Herramientas:

Vamos a utilizar el Sniffer Caín @ <http://www.oxid.it/>

Procedimiento:

1. Instalar, configurar y poner en funcionamiento el Sniffer Caín en el equipo atacante.
2. Envenenar las tablas ARP del equipo víctima y del router (Puerta de Enlace).

Las respectivas tablas ARP

- del equipo víctima:

Interfaz: 10.10.0.254 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.33	00-c0-49-44-b1-d5	dinámico
10.10.0.69	00-05-1c-0a-ab-92	dinámico

- del router (Puerta de enlace):

Interfaz: 10.10.0.33 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.69	00-05-1c-0a-ab-92	dinámico
10.10.0.254	00-20-18-b0-06-df	dinámico

deben ser envenenadas de forma que la nueva configuración sea:

- del equipo víctima:

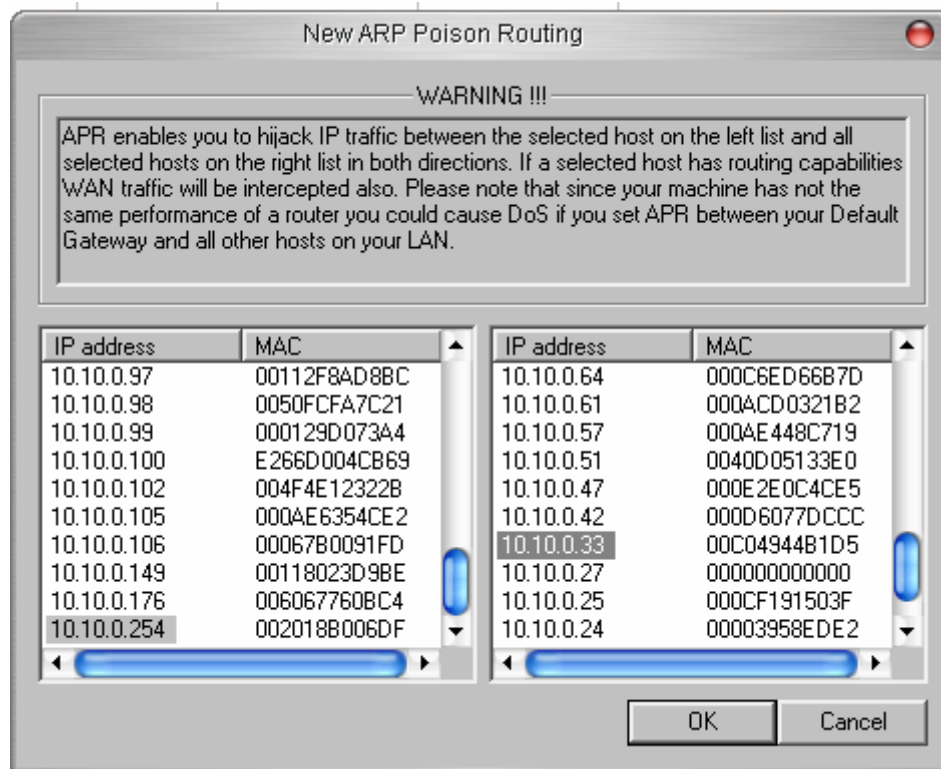
Interfaz: 10.10.0.254 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.33	00-05-1c-0a-ab-92	dinámico
10.10.0.69	00-05-1c-0a-ab-92	dinámico

- del router (Puerta de enlace):

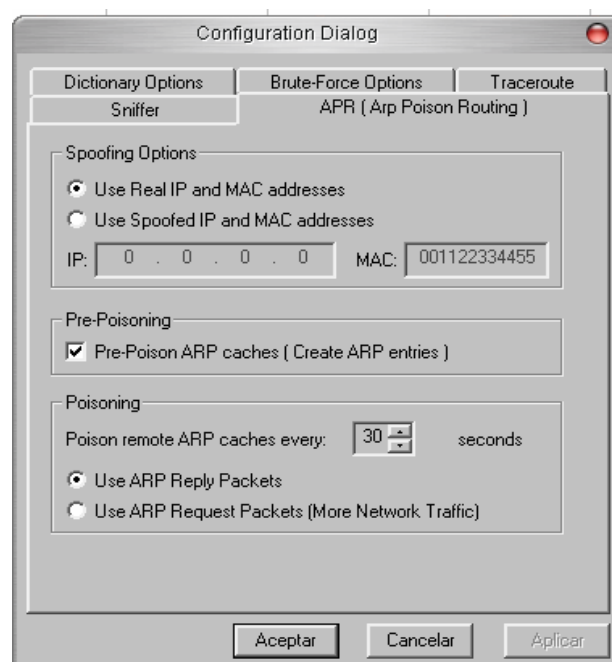
Interfaz: 10.10.0.33 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.69	00-05-1c-0a-ab-92	dinámico
10.10.0.254	00-05-1c-0a-ab-92	dinámico

Esto se puede efectuar de forma manual, generando periódicamente paquetes maliciosos con la utilidad Nemesis y habilitando ip_forwarding en el equipo atacante.

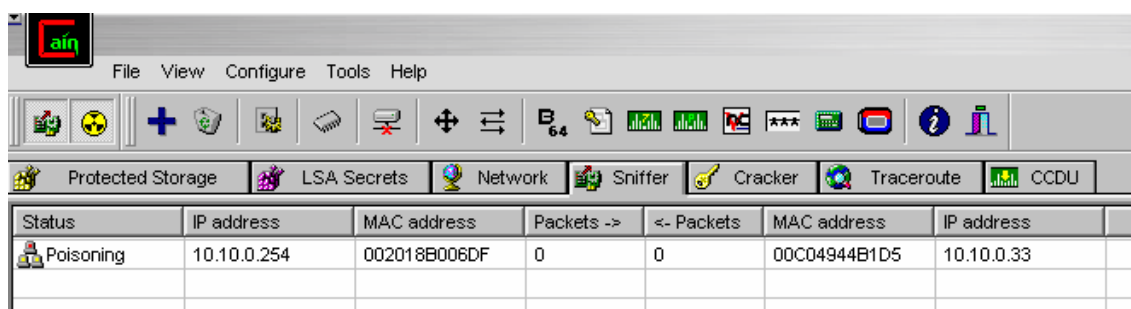
Sin embargo, el Sniffer Caín permite efectuar este proceso de forma sencilla y automática. En la pestaña *Sniffer*, subpestaña *APR*, pulsar el botón **+** y aparecerá el siguiente cuadro, donde podemos seleccionar los dos equipos de la red cuyas tablas ARP van a ser envenenadas:



Es posible cambiar las propiedades por defecto del módulo de Envenenamiento ARP:



Activamos el Sniffer y el módulo de Envenenamiento ARP (*APR*):

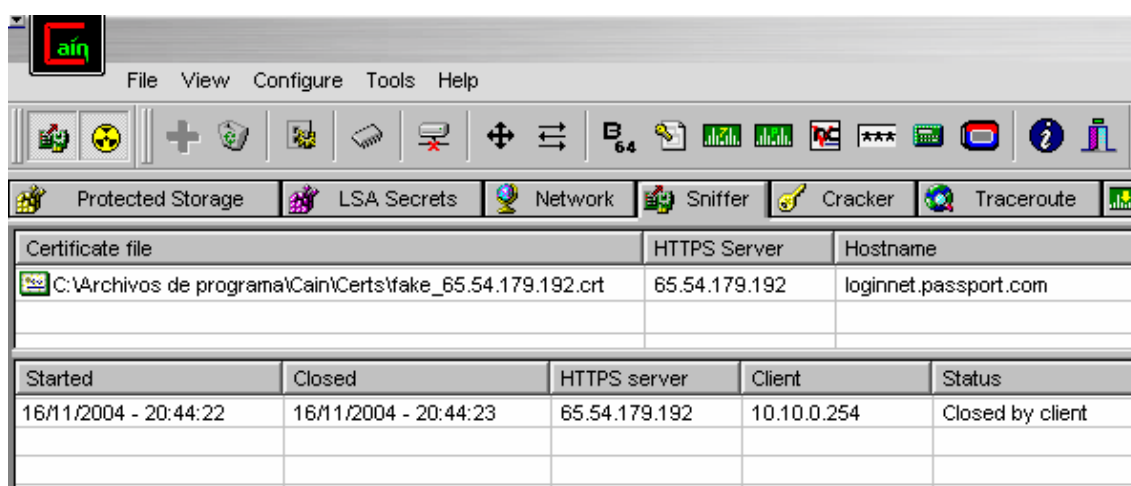


y ya tendremos los dos equipos envenenados de forma que el tráfico que intercambien va a circular por el equipo del atacante.

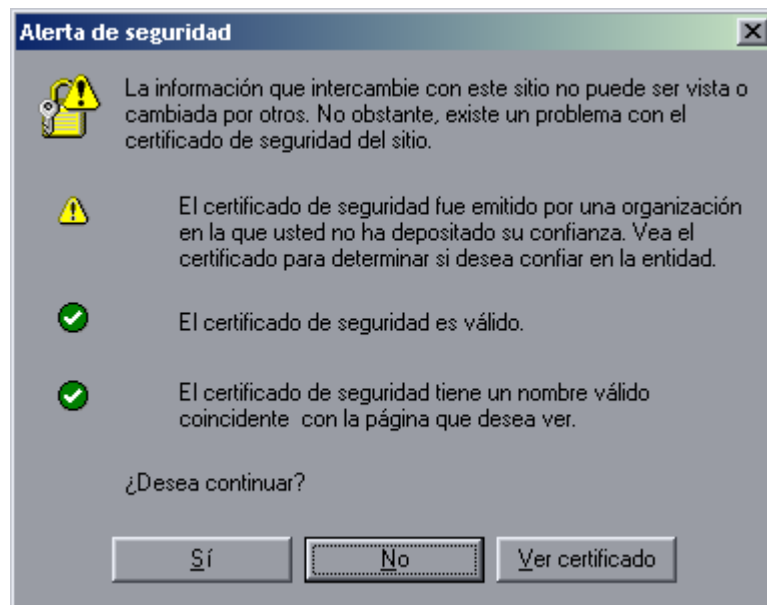
4. Sólo queda esperar a que el usuario víctima intente iniciar sesión en Hotmail para leer su correo. La petición DNS a www.hotmail.com será atendida por el Sniffer Caín (situado como Man in the Middle) de forma que el equipo atacante realiza la petición a Internet en su lugar y luego devuelve al equipo víctima la respuesta a la petición.

El formulario de acceso a Hotmail llega al equipo víctima y el usuario introduce su dirección y contraseña en los campos requeridos. Al pulsar *Iniciar Sesión*, la víctima solicitará el certificado válido de servidor verificado por una CA (Autoridad Certificadora) a hotmail.com, msn.com o passport.net, pero en su lugar, esa petición será procesada por el Sniffer Caín, quien le servirá un certificado falseado.

Podemos comprobar como Caín genera y suministra al equipo víctima su propio certificado falseado. (No hace falta buscar un certificado falso por Internet)



5. En el navegador de la víctima aparecerá el siguiente aviso:



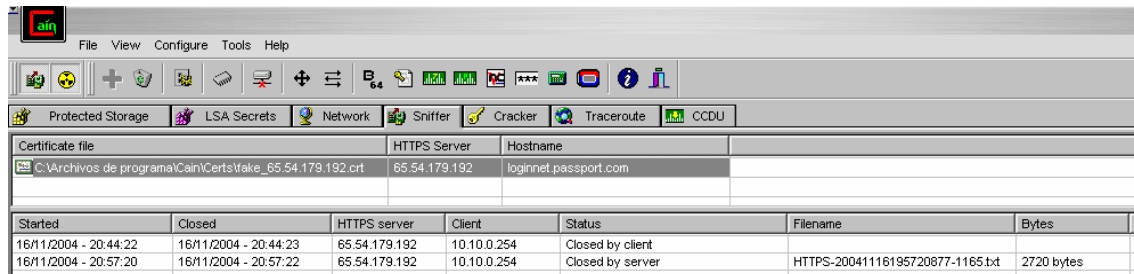
En este momento, entra en juego la astucia del usuario víctima para comprobar que el certificado es de confianza. Puede visualizar el certificado:



y desconfiar de él, cancelando el inicio de sesión. O bien, confiar en el certificado y continuar con el inicio de sesión. Esta alternativa, será la que escojan la gran mayoría de usuarios víctimas.

6. En caso de aceptar el certificado y continuar con el inicio de sesión, el usuario accederá de forma transparente a la zona segura de Hotmail para ver su Bandeja de Entrada de Correo.

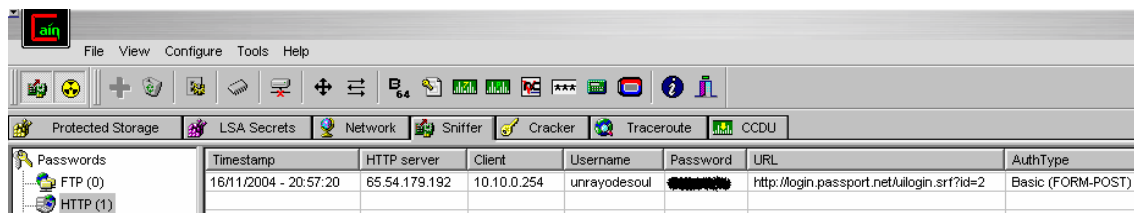
El Sniffer Caín habrá procesado el inicio de sesión HTTPS.



The screenshot shows the 'Certificate file' table in the Sniffer tab of Cain & Abel. The table has columns for Started, Closed, HTTPS server, Client, Status, Filename, and Bytes.

Started	Closed	HTTPS server	Client	Status	Filename	Bytes
16/11/2004 - 20:44:22	16/11/2004 - 20:44:23	65.54.179.192	10.10.0.254	Closed by client		
16/11/2004 - 20:57:20	16/11/2004 - 20:57:22	65.54.179.192	10.10.0.254	Closed by server	HTTPS-20041116195720877-1165.txt	2720 bytes

Y, en consecuencia, habrá registrado el nombre de usuario y contraseña de la sesión.



The screenshot shows the 'Passwords' table in the Sniffer tab of Cain & Abel. The table has columns for Timestamp, HTTP server, Client, Username, Password, URL, and AuthType.

Timestamp	HTTP server	Client	Username	Password	URL	AuthType
16/11/2004 - 20:57:20	65.54.179.192	10.10.0.254	unrayodesoul	[REDACTED]	http://login.passport.net/ui/login.srf?id=2	Basic (FORM-POST)

7. Ahora, la ética del atacante decidirá si esto ha sido un simple experimento científico y educacional para comprobar una debilidad del protocolo HTTPS y, por tanto, olvidarse de la contraseña de acceso a la cuenta de correo de una víctima inocente. O bien, invadir su privacidad accediendo a su Bandeja de Entrada de Correo para ver sus mensajes. **Tú decides!**

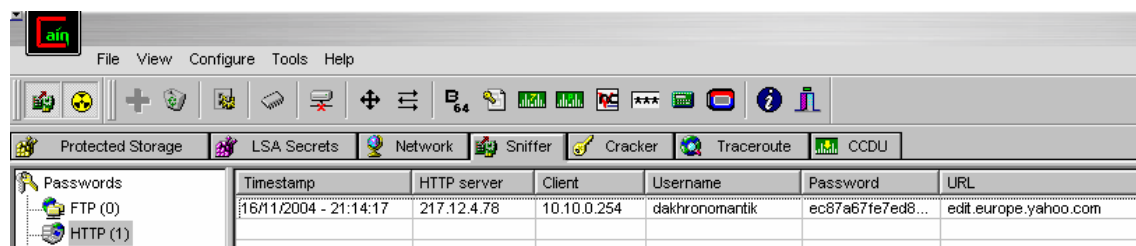
Procedimiento para el caso de Servidor Yahoo:

Se puede aplicar este mismo procedimiento para obtener el nombre de usuario y contraseña de inicio de sesión en el sitio **Yahoo**.

Yahoo ofrece 2 alternativas de acceso:

1) Standard (no protegida)

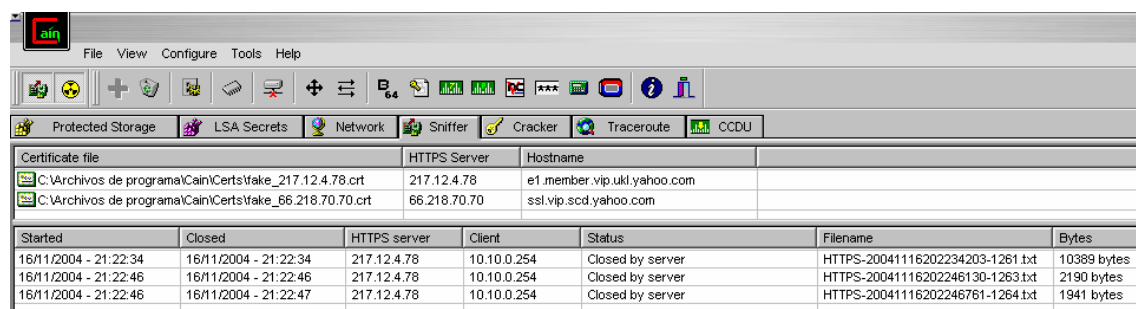
El inicio de sesión no requiere la existencia de un certificado válido de servidor verificado por una CA (Autoridad Certificadora). El Sniffer Caín procesa el inicio de sesión y registra el nombre de usuario y la contraseña. La contraseña aparece encriptada.



Timestamp	HTTP server	Client	Username	Password	URL
16/11/2004 - 21:14:17	217.12.4.78	10.10.0.254	dakhronomantik	ec87a67fe7ed8...	edit.europe.yahoo.com

2) Segura (protegida)

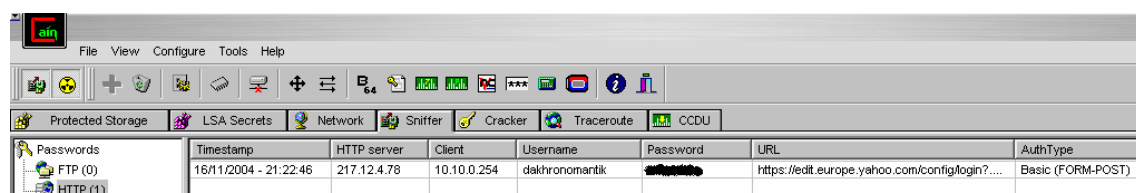
El inicio de sesión requiere la existencia de un certificado válido de servidor verificado por una CA (Autoridad Certificadora). El Sniffer Caín procesa el inicio de sesión y sirve al equipo víctima el certificado falseado.



Certificate file	HTTPS Server	Hostname
C:\Archivos de programa\Cain\Certs\fake_217.12.4.78.crt	217.12.4.78	e1.member.vip.ukl.yahoo.com
C:\Archivos de programa\Cain\Certs\fake_66.218.70.70.crt	66.218.70.70	ssl.vip.scd.yahoo.com

Started	Closed	HTTPS server	Client	Status	Filename	Bytes
16/11/2004 - 21:22:34	16/11/2004 - 21:22:34	217.12.4.78	10.10.0.254	Closed by server	HTTPS-20041116202234203-1261.txt	10389 bytes
16/11/2004 - 21:22:46	16/11/2004 - 21:22:46	217.12.4.78	10.10.0.254	Closed by server	HTTPS-20041116202246130-1263.txt	2190 bytes
16/11/2004 - 21:22:46	16/11/2004 - 21:22:47	217.12.4.78	10.10.0.254	Closed by server	HTTPS-20041116202246761-1264.txt	1941 bytes

Posteriormente, en caso de que el certificado sea aceptado, se registra el nombre de usuario y la contraseña. La contraseña aparece en texto plano.



Timestamp	HTTP server	Client	Username	Password	URL	AuthType
16/11/2004 - 21:22:46	217.12.4.78	10.10.0.254	dakhronomantik	XXXXXXXXXX	https://edit.europe.yahoo.com/config/login?....	Basic (FORM-POST)

Documentación relacionada

- Artículo sobre **INTRUSIÓN EN REDES DE ÁREA LOCAL** publicado por **Moebius** para el número 11 de la revista PC PASO A PASO (HACKXCRACK). En él se explica como llevar a cabo esta misma práctica sobre Linux utilizando el Sniffer DSNIFF.