es.NOG
16/10/2008

RETOS DE CONTROL DE LA INFORMACIÓN EN UN MUNDO MÓVIL

BARCELONA
16 d'Octubre del 2008

"Lo que tu portátil va contando por ahí"

Simon Dyer

simon.p.dyer@gmail.com

Objetivos

- Arrojar luz sobre ataques “nuevos” que afectan potencialmente a todos los que utilizan dispositivos móviles y son usuarios de redes Wifi de acceso público.
- Los presentes en ESNOG II son un demográfico afectado, y en muchos casos con acceso privilegiado a recursos de red conectados a Internet.

ES.NOG
16/10/2008

AGENDA

- Un poco de historia
- ¿Y Qué?
- Mirando paquetes
- Herramientas
- Ataques Activos
- Conclusiones

UN POCO DE HISTORIA

Internet en los '90

- Mucho más sencillo
- “Pocos” usuarios, más confiado
- Seguridad no era una prioridad
- Así tenemos telnet, tftp, ftp, pop, smtp, etc
- O no usan passwords, o peor, en claro

Protocolos confiados

- Pero un nivel de riesgo bajo
- Hacía falta sniffers especializados
- O un PC potente en el segmento, y tráfico bajo, 7Mbps era mucho para un 386 ISA

Pero hoy en día...

- Tenemos SSH, SFTP, TLS, IPSec...
- Certificados digitales establecen identidad de ambas partes
- PFS para evitar replay
- LAN conmutado
- Vigilantes de DHCP/ARP en conmutadores
- Unicast RPF limita el spoofing
- Mucho desarrollo en securizar estas áreas
- Pagar bien a los operadores también ayuda ;-)

Trabajando fuera

- Los portátiles nos dejan trabajar fuera, por ejemplo desde nuestra casa
- Dispositivos móviles están encogiendo, pero sin perder capacidad (excepto pantalla etc)
- Broadband está por todas partes
- Puedo conectar al curro desde casa!

Trucos ADSL - Vigila!

- El portátil, en casa, no está detrás del firewall corporativo, IDS/IDP etc
- Si se le puede penetrar desde Internet, se tendría vía libre a la empresa vía su VPN
- Bloqueos de “split tunneling” por esta razón en clientes VPN

Wifi Corporativo

- Wifi abierto es malo. APs no oficiales son cazados por sistemas de gestión modernas
- WEP no seguro, WPA2 EAP es OK
- Análisis de tráfico, pero no mucho más
- Obviamente la amenaza interna sigue estando presente, igual que con CAT5E

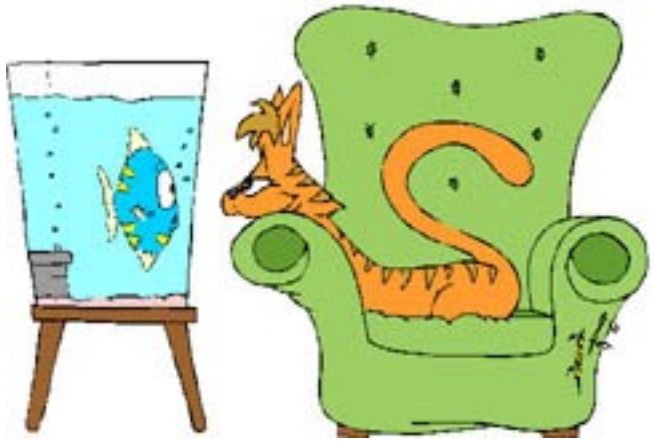
Fronteras Nuevas - Cybercafés

- Wifi abierto (o WEP trivial) por todos los lados; bares, hoteles, aeropuertos, empresas (wifi para los visitantes)
- Vale, hay que autenticar con un proxy para salir, pero la Wifi no está securizada por diseño
- Puedo conectar al curro desde cualquier lado!

¿Y QUÉ?

Ataques – Recogida Información

- Esencial para iniciar un ataque
- Información trivial, combinada, no lo es
- Ping, NMAP, banner discovery, whois
- Ingeniería social
- Cualquier cosa que ayuda a mapear o acceder es información útil



Ataques – Recogida Información

- No limitadas a Wifi, pero la facilidad de captura en una Wifi abierta es un “game changer”
- Ataques completamente pasivas!
- Estudio offline es fácil
- Con mi Netbook PC puedo capturar más de 4h de tráfico a batería con la pantalla cerrada

Plug'n'play

- SO modernos quieren automatizar todo para facilitarnos la vida
- “Es seguro, está a la LAN no?”
- Wifi abierto es una vuelta al mundo de hubs, es radiodifusión!

Información se escapa por la red

- Wifi packets
- DHCP Broadcast
- NetBIOS/SMB Broadcast
- DNS/Bonjour Requests
- ... y más!

Paquetes wifi

- Probe Requests
  - http://www.theta44.org/software/karma.README
  - http://www.nmrc.org/pub/advise/20060114.txt
  - KARMA+Metasploit3 = Karmetasploit
  - Cuando arranca un portátil con wifi, buscará redes conocidas, o donde ha estado antes
  - Esta lista se puede usar para determinar donde ha estado el dispositivo en el pasado reciente

Broadcast NETBIOS/SMB

- Anuncios WKSSVC (Lanman, not Spybot)
- Actividad AD
- Intentos de conexión a discos de red
- Impresoras de red

Solicitudes DNS

- Casi toda actividad necesita una solicitud de DNS
  - Conectar con la intranet
  - Conectar con servidores de correo
  - Casi cualquier aplicación arrancando
    - IM
    - VoIP
    - Juegos

Otros protocolos

- Bonjour (mDNS)
  - Da mucha información!
- Skype
- Herramientas de seguridad
  - Buscando actualizaciones
- OS
  - También buscan actualizaciones
- AIM actualizará el estado de todos tus amigos
  - Divulga quien tienes en tu lista de amigos

¿Pero Que Significa?

- Veamos un ejemplo de información recogida
- La máquina 00-18-f3-57-24-bd es propiedad de John Smith.
- Se ha conectado a la wifi a los aeropuertos de Hartsfield y Heathrow, puntos de T-Mobile, la compañía ABC y la compañía XYZ. Tiene el nombre PrshDude9 en AIM, y XYZ1 en su lista de amigos. Utiliza POP para mirar su correo personal, con la contraseña “porsche911turbo”. Su navegador intenta abrir “internal.abcsoft.com” así que trabaja para ABC. También intenta conectar con “\\internal.abcsoft.com\sales” y “\\internal.abcsoft.com\public” nada más arrancar. Tiene una cuenta de myspace, y mirando allí, hay fotos de la última cena de navidad.

Usando la información

- Si sabemos que ABC y XYZ son competidores?
  - Fusión o compra al horizonte?
- Probar la contraseña contra el servidor de correo de ABC, quizás utiliza la misma
- Conocemos trozos de la estructura interna de la intranet de ABC
  - Permite hacer troyanos más efectivos, o actuar después de una penetración

MIRANDO PAQUETES

MDNS

65 0.261450 69.94.196.132 224.0.0.251 MDNS Standard query response SRV 0 0 9 david-mayno...

```
0000  08 01 2c 00 00 15 c7 aa  d5 30 00 17 f2 41 31 6d   ..,..... .0...A1m
0010  01 00 5e 00 00 fb e0 06  aa aa 03 00 00 00 08 00   ..^..... ........
0020  45 18 01 dc 36 19 00 00  ff 11 99 01 45 5e c4 84   E...6... ....E^..
0030  e0 00 00 fb 14 e9 14 e9  01 c8 05 08 00 00 84 00   ........ ........
0040  00 00 00 09 00 00 00 00  2d 44 61 76 69 64 20 4d   ........ -David M
0050  61 79 6e 6f 72 e2 80 99  73 20 43 6f 6d 70 75 74   aynor... s Comput
0060  65 72 20 5b 30 30 3a 31  36 3a 63 62 3a 64 32 3a   er [00:1 6:cb:d2:
0070  30 37 3a 61 61 5d 0c 5f  77 6f 72 6b 73 74 61 74   07:aa]._ workstat
0080  69 6f 6e 04 5f 74 63 70  05 6c 6f 63 61 6c 00 00   ion._tcp .local..
0090  21 80 01 00 00 00 78 00  21 00 00 00 00 00 09 18   !.....x. !......
00a0  64 61 76 69 64 2d 6d 61  79 6e 6f 72 73 2d 63 6f   david-ma ynors-co
00b0  6d 70 75 74 65 72 2d 33  c0 4c c0 0c 00 10 80 01   mputer-3 .L......
00c0  00 00 11 94 00 01 00 09  5f 73 65 72 76 69 63 65   ........ _service
00d0  73 07 5f 64 6e 73 2d 73  64 04 5f 75 64 70 c0 4c   s._dns-s d._udp.L
00e0  00 0c 00 01 00 00 11 94  00 02 c0 3a c0 3a 00 0c   ........ ...:.:..
00f0  00 01 00 00 11 94 00 02  c0 0c c0 63 00 1c 80 01   ........ ...c....
0100  00 00 00 78 00 10 fe 80  00 00 00 00 00 00 02 17   ...x.... ........
0110  f2 ff fe 41 31 6d 01 44  01 36 01 31 01 33 01 31   ...A1m.D .6.1.3.1
0120  01 34 01 45 01 46 01 46  01 46 01 32 01 46 01 37   .4.E.F.F .F.2.F.7
0130  01 31 01 32 01 30 01 30  01 30 01 30 01 30 01 30   .1.2.0.0 .0.0.0.0
0140  01 30 01 30 01 30 01 30  01 30 01 30 01 30 01 30   .0.0.0.0 .0.0.0.0
0150  01 38 01 45 01 46 03 69  70 36 04 61 72 70 61 00   .8.E.F.i p6.arpa.
0160  00 0c 80 01 00 00 00 78  00 02 c0 63 c0 63 00 0d   .......x ...c.c..
0170  80 01 00 00 00 78 00 50  0a 4d 61 63 42 6f 6f 6b   .....x.P .MacBook
0180  31 2c 31 44 4d 61 63 20  4f 53 20 58 20 31 30 2e   1,1DMac  OS X 10.
0190  34 2e 38 20 28 38 4c 32  31 32 37 29 2c 20 6d 44   4.8 (8L2 127), mD
01a0  4e 53 52 65 73 70 6f 6e  64 65 72 2d 31 30 38 2e   NSRespon der-108.
01b0  32 20 28 41 75 67 20 32  35 20 32 30 30 36 20 31   2 (Aug 2 5 2006 1
01c0  34 3a 35 30 3a 34 38 29  c0 63 00 01 80 01 00 00   4:50:48) .c......
01d0  00 78 00 04 45 5e c4 84  03 31 33 32 03 31 39 36   .x..E^.. .132.196
01e0  02 39 34 02 36 39 07 69  6e 2d 61 64 64 72 c1 1e   .94.69.i n-addr..
01f0  00 0c 80 01 00 00 00 78  00 02 c0 63               .......x ...c
```

MDNS

070213-gatech-balls-ch06a.pcap - Ethereal

File Edit View Go Capture Analyze Statistics Help

```
⊞ Frame 65 (508 bytes on wire, 508 bytes captured)
⊞ IEEE 802.11
⊞ Logical-Link Control
⊞ Internet Protocol, Src: 69.94.196.132 (69.94.196.132), Dst: 224.0.0.251 (224.0.0.251)
⊞ User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)
⊟ Domain Name System (response)
    Transaction ID: 0x0000
  ⊞ Flags: 0x8400 (Standard query response, No error)
    Questions: 0
    Answer RRs: 9
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Answers
    ⊞ David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type SRV, class FLUSH, pr
    ⊞ David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type TXT, class FLUSH
    ⊞ _services._dns-sd._udp.local: type PTR, class IN, _workstation._tcp.local
    ⊞ _workstation._tcp.local: type PTR, class IN, David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._work
    ⊞ david-maynors-computer-3.local: type AAAA, class FLUSH, addr fe80::217:f2ff:fe41:316d
    ⊞ D.6.1.3.1.4.E.F.F.F.2.F.7.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.ip6.arpa: type PTR, class FLUSH, david-ma
    ⊞ david-maynors-computer-3.local: type HINFO, class FLUSH, CPU MacBook1,1, OS Mac OS X 10.4.8 (8L2127), mDN
    ⊞ david-maynors-computer-3.local: type A, class FLUSH, addr 69.94.196.132
    ⊞ 132.196.94.69.in-addr.arpa: type PTR, class FLUSH, david-maynors-computer-3.local
```

MDNS

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

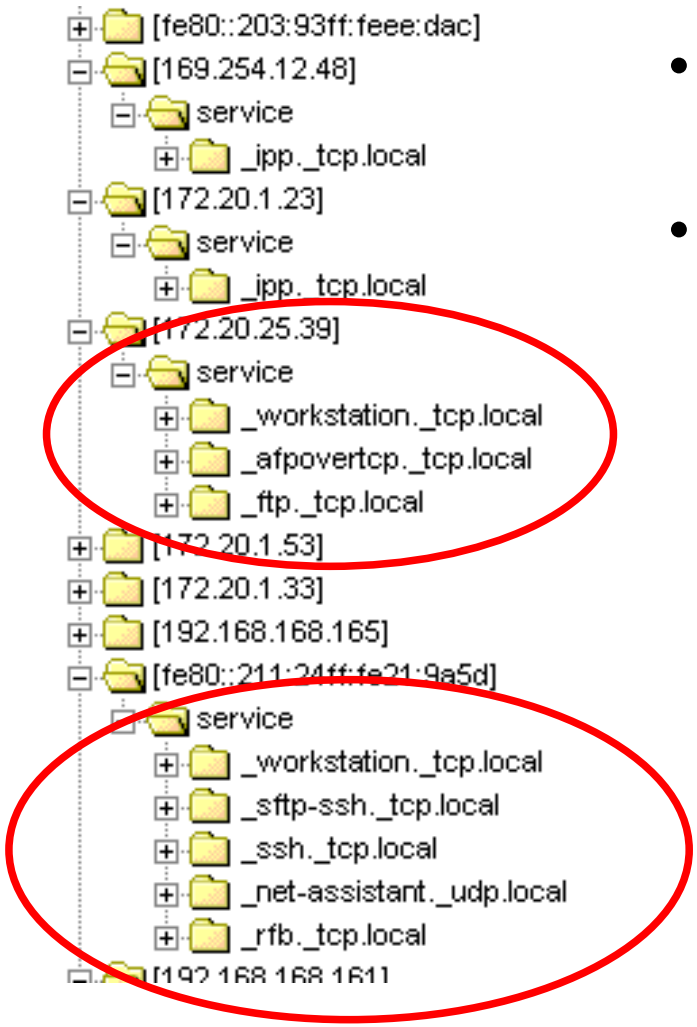
```
Frame 125 (776 bytes on wire, 776 bytes captured)
Ethernet II, Src: Dell_6b:1b:cb (00:13:72:6b:1b:cb), Dst: JetwayIn_77:1b:8a (00:30:18:77:1b:8a)
Internet Protocol, Src: 192.168.2.30 (192.168.2.30), Dst: 216.73.86.52 (216.73.86.52)
Transmission Control Protocol, Src Port: 4046 (4046), Dst Port: http (80), Seq: 1, Ack: 1, Len: 722
Hypertext Transfer Protocol
  GET /adi/N2992.Yahoo__/B2112371.8;dcadv=1281487;sz=728x90;dcopt=rcl;click=http://us.ard.yahoo.com/SIG
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, applicati
  Referer: http://my.yahoo.com/\r\n
  Accept-Language: en-ca\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
  Host: ad.doubleclick.net\r\n
  Connection: Keep-Alive\r\n
  Cookie: id=800000a9c7b526e\r\n
  \r\n
```

HERRAMIENTAS

FERRET

- Como un sniffer de contraseñas, pero recopila más información
- Como IDS, pero esnifando operaciones legítimas, no intrusiones
- Protocolos: DHCP, SNMP, DNS, HTTP, AIM, MSN-MSGR, Yahoo IM, …
- Ferret Viewer: navegador para facilitar la interpretación de los datos recogidos

Ejemplo: Bonjour



- Lista servicios de la máquina
- Usado para buscar vías de ataque

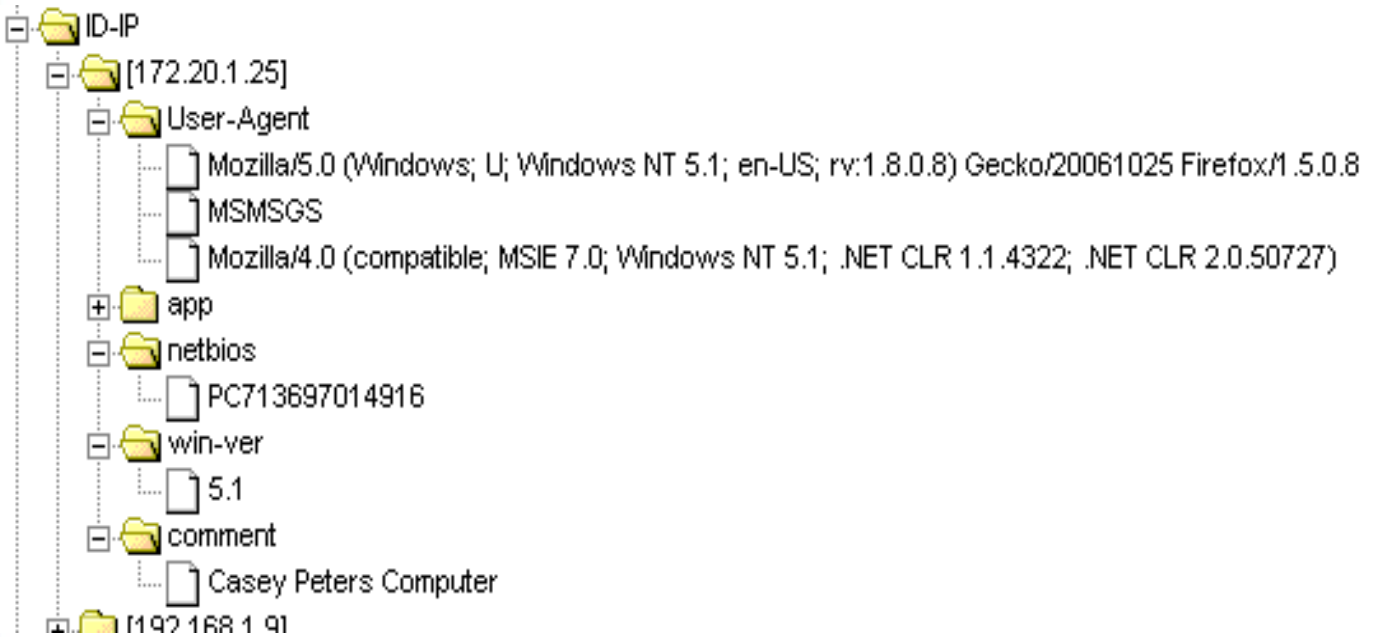
Ejemplo: CUPS

- Impresoras disponibles
- Impresoras vulnerables
- Bugs en los drivers?
  - Son comunes, Microsoft los ha movido a user-mode
- Mapeando la red

- uri
  - d6
  - ipp://169.254.12.48:631/printers/Z600_Series
  - f04e
  - ipp://172.20.1.23:631/printers/hp_LaserJet_1320_series
  - ipp://172.20.1.23:631/printers/Internal_Modem
  - ipp://172.20.1.23:631/printers/jonoprint
  - ipp://172.20.1.23:631/printers/Z600_Series
- location
  - 3
  - Jan Mulder\xE2\x80\x99s Computer (2)
  - Jan Mulder\xE2\x80\x99s Computer
  - Local zone
- info
  - ipp://169.254.12.48:631/printers/raw_on_10_31_59_116
  - Z600 Series
  - ipp://172.20.1.23:631/printers/AdobePDF7
  - hp LaserJet 1320 series
  - Internal Modem
  - jonoprint
  - ipp://172.20.1.23:631/printers/raw_on_10_31_59_116
- model
  -
  - Z600 Series
  - HP LaserJet 1320 series
  - Fax Printer
  - Apple LaserWriter 12/640 PS v2015.105

Identificación

- Datos interesantes sobre el sistema, sacados de diversos protocolos



Identificación (más)

- [172.20.1.39]
  - SERVICE
    - _workstation._tcp.local
    - _afpovertcp._tcp.local
  - mac
    - [00:16:cb:a1:33:57]
  - name
    - EMCMac
  - netbios
    - KKKKATY
  - User-Agent
    - Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)

- [172.20.1.39]
  - name
    - pocketpc.com
    - www.microsoft.com
    - js.microsoft.com
    - www.google-analytics.com
    - www.friendsofpr.com
    - www.oaktrees.org
    - i75.photobucket.com
    - www.speiser.com
    - seweccentric.com
    - www.neoflux.com

Identificación (más)

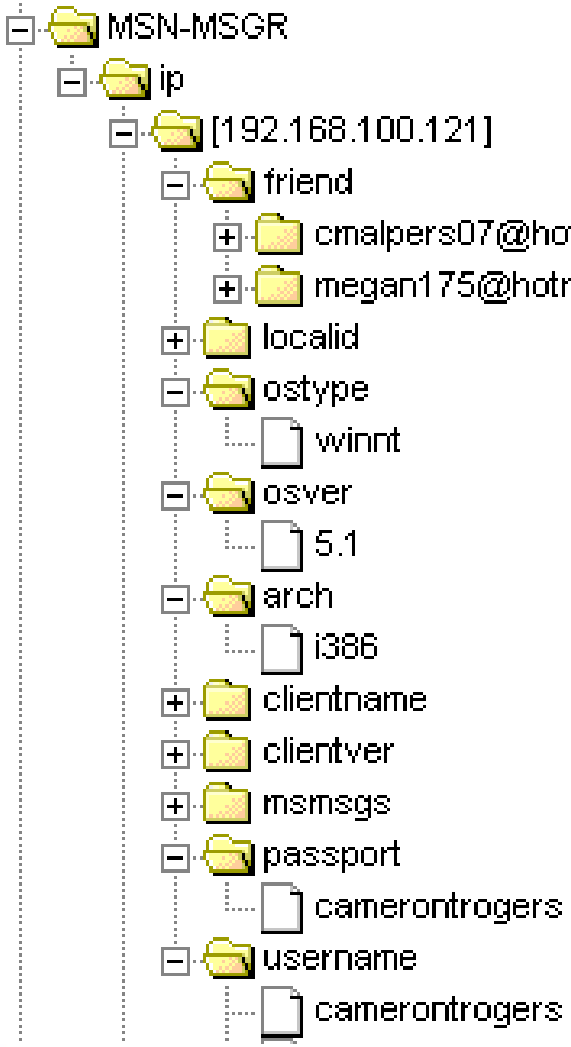
- [172.20.1.12]
  - User-Agent
    - Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8
    - Windows-Update-Agent
    - Mozilla/4.0 (compatible; MSIE 6.0; Win32)
    - Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 1.1.4322.2032)
    - Microsoft BITS/6.6
    - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; CH2M; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
  - netbios
    - PDX31020038
  - win-ver
    - 5.1
  - comment
    - NWR/PDX R[redacted], Andrew (503) 23[redacted]0 x4112
  - name
    - pdx3102003[redacted]m.com

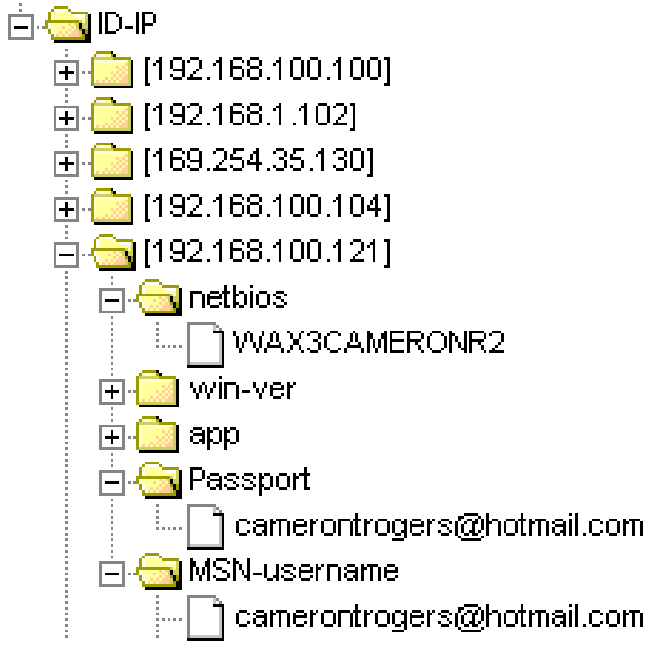
Identificación (más)

- [172.20.1.13]
  - netbios
    - NDC_EMAD
  - win-ver
    - 5.1
  - comment
    - EMAD_
  - User-Agent
    - Microsoft-WebDAV-MiniRedir/5.1.2600
    - Mozilla/4.0 (compatible; Win32)
    - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)
    - Mozilla/4.0 (compatible; MSIE 6.0; Win32)
    - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
    - Industry Update Control
    - Microsoft SUS Client/2.0
    - Microsoft WU Client/2.0
  - name
    - VONGDEUANE-L-N.screen.com

Ejemplo: MSN-MSGR

- Lista de amigos
- Coge el nombre del usuario del PC





es.NOG
16/10/2008

- [00:14:a5:1e:5e:b6]
  - SSID
    - (broadcast)
    - NETGEAR
    - Wireless
    - stayonline
    - concourse
    - guestwifi
    - Internet
    - STSN_Conf
    - ATL-WIFI
    - PBIA_WIFI
    - NH&AWirele$$
    - primnet-916
    - ROC Airport1
    - atlantabread
    - hhonors_Conf
    - hhonors
    - securedemail_Home
    - tmobile
    - comfortinn
    - ROC Airport2
    - tsunami
    - mimecom
    - SJ
    - Connexion1
    - 04Z412566951
    - KudoBeans/ANYWWWWHERE
    - Hilton
    - binz network
    - Stjartrosen
    - securedemail

Ejemplo: Wifi Probe

- Lista de sitios donde el blanco ha estado
- Siempre que el SSID nos da información, “linksys” es ambiguo

Ejemplo:Email

- SMTP va en claro!
- Fingerprinting

- [10.241.0.207]
  - e-mail
  - friend
    - trichmond@totousa.com
    - jfitzsimmons@totousa.com
    - tohtsuka@totousa.com
    - shiro.osawa@toto.co.jp
    - ksako@totousa.com
    - lcampos@totousa.com
    - mabbas@totousa.com
  - X-Mailer
    - Microsoft Outlook CWS, Build 9.0.6604 (9.0.2911.0)
  - X-MimeOLE
    - Produced By Microsoft MimeOLE V6.00.2900.3028
  - netbios
    - SALES-007-WXPJ
  - win-ver
  - pop3-user
    - knojima

ATAQUES ACTIVOS

KARMA

- Responde aceptando los probes de wifi que envían los dispositivos, sean lo que sean
- Actúa de AP falso para todas las víctimas a la vez,
  - linksys para uno, tsunami para otro
  - Intenta ofrecer los parámetros que busca cada cliente, para ser su pareja ideal

KARMA (explicación simplificada)

- Cliente envía probe a broadcast
- Si hay respuestas en sus preferidos los intenta utilizar (si son redes encriptadas fallará)
- Si no, envía probe por cada preferido, por si son de SSID escondido
- Si responde alguno, lo intenta utilizar
- Si no hay nada, se inventa una red ad-hoc con SSID aleatorio y envía probes a este SSID. Si un AP responde, WinXP SP2 se asociará, Vista no.

KARMA
(explicación simplificada)

- En la red aleatoria, si todas las redes preferidas son encriptadas, esta lo será
- Si hay una sola red en las preferidas que no requiere autenticación, se asociará con Karma sin más

KARMA: DHCP++

- Si tenemos cautiva a una víctima
  - Dale IP por DHCP, y somos su DNS
  - Responder con la IP propia a todas las solicitudes de DNS
- El proyecto Karma también responde a :
  - ARPs
  - Solicitudes NetBIOS
  - Conexiones SMB/DCE-RPC
  - Conexiones SMTP
  - Conexiones HTTP

KARMA: HTTP++

- Se usa un proxy transparente para permitir que navega a través nuestro
  - Tenemos otra conexión a la wifi real
  - Podemos modificar e insertar cosas en las páginas que solicita para aplicar exploits
- Otros servicios son simulados. Si intenta autenticación segura, se rechaza. Muchos clientes pasan entonces a enviar la autenticación en claro
  - Email, Chat (IMAP, POP3, AIM, YIM, MSN)
  - Recogida de versiones, posibilidad de iniciar ataques específicas

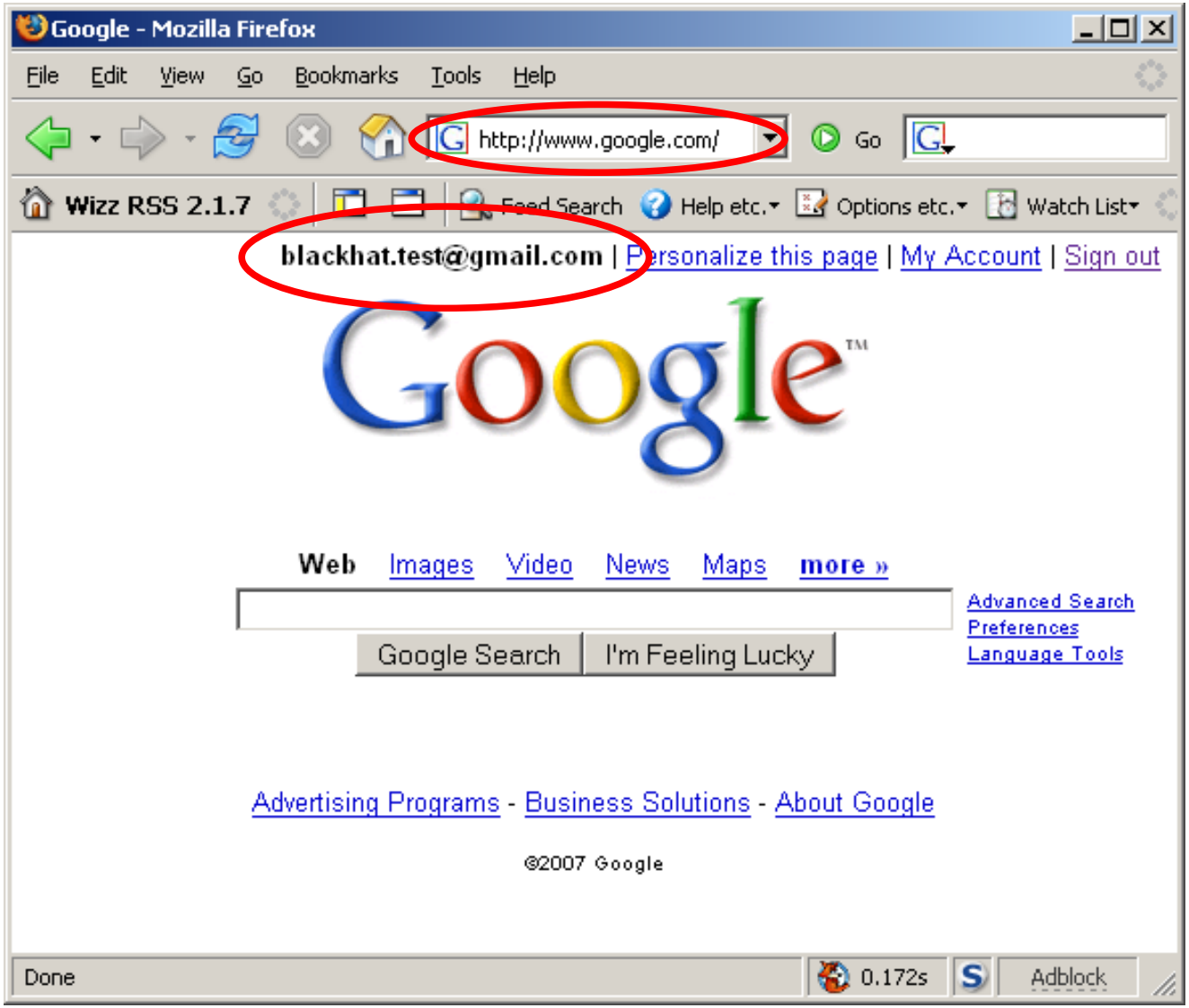
KARMA: Desventajas

- Cualquier ataque activo requiere que estés al radioalcance de la víctima. No es un chiquillo desde China
- Aunque puede ser alguien en un coche aparcado cerca

Robando Cookies

- GMail es vulnerable, pero también Facebook, Amazon etc
- En HTTPS gmail genera un cookie
  - Cookie de autorización: indica login ok
  - Valido 2 semanas
- En HTTP también lo envía
- Puede ser capturado esnifando y aplicado por un tercero
- No divulga el password de una cuenta, pero sí da acceso libre a ella (con restricciones)
- No solo Gmail! Pero es el más fácil de ver

Cookie harvesting

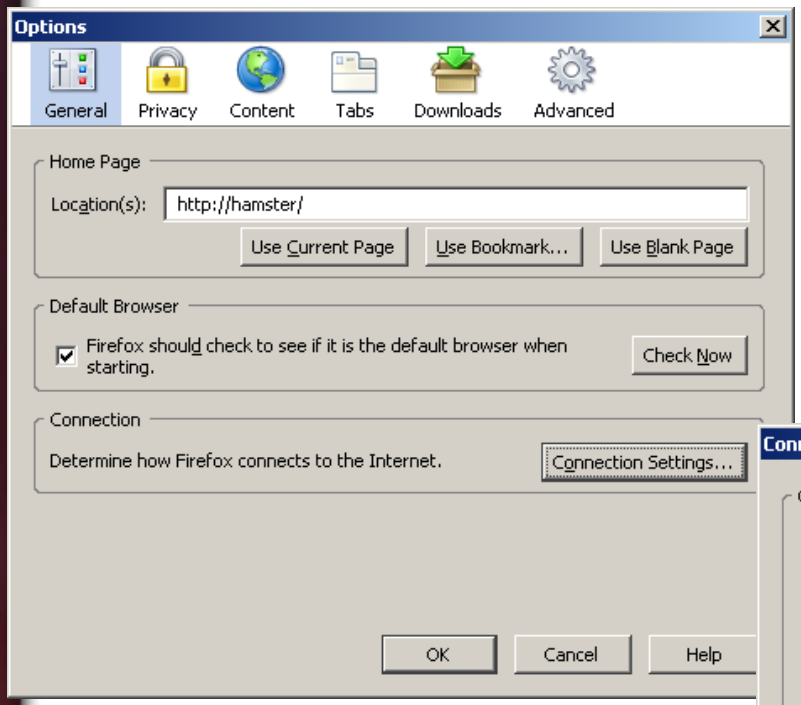


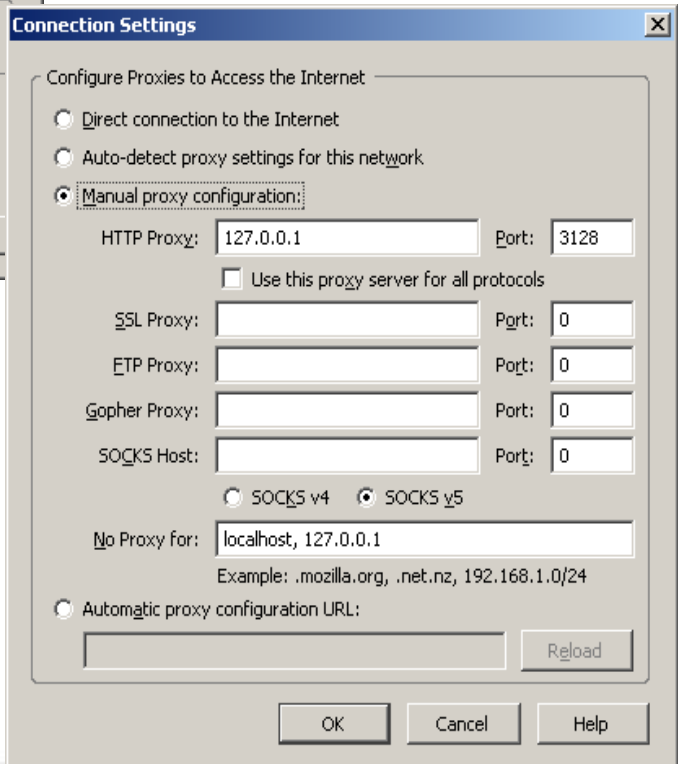
Cookie harvesting

- No es nuevo, pero antes era manual
  - Wireshark
  - Mozilla plugin “Edit Cookies”
- Nuevas Herramientas “point and click”
  - Hamster, utiliza Ferret http://www.erratasec.com/sidejacking.zip
  - SurfJack http://surfjack.googlecode.com/
  - Back Track LiveCD tiene todo organizado y a mano.

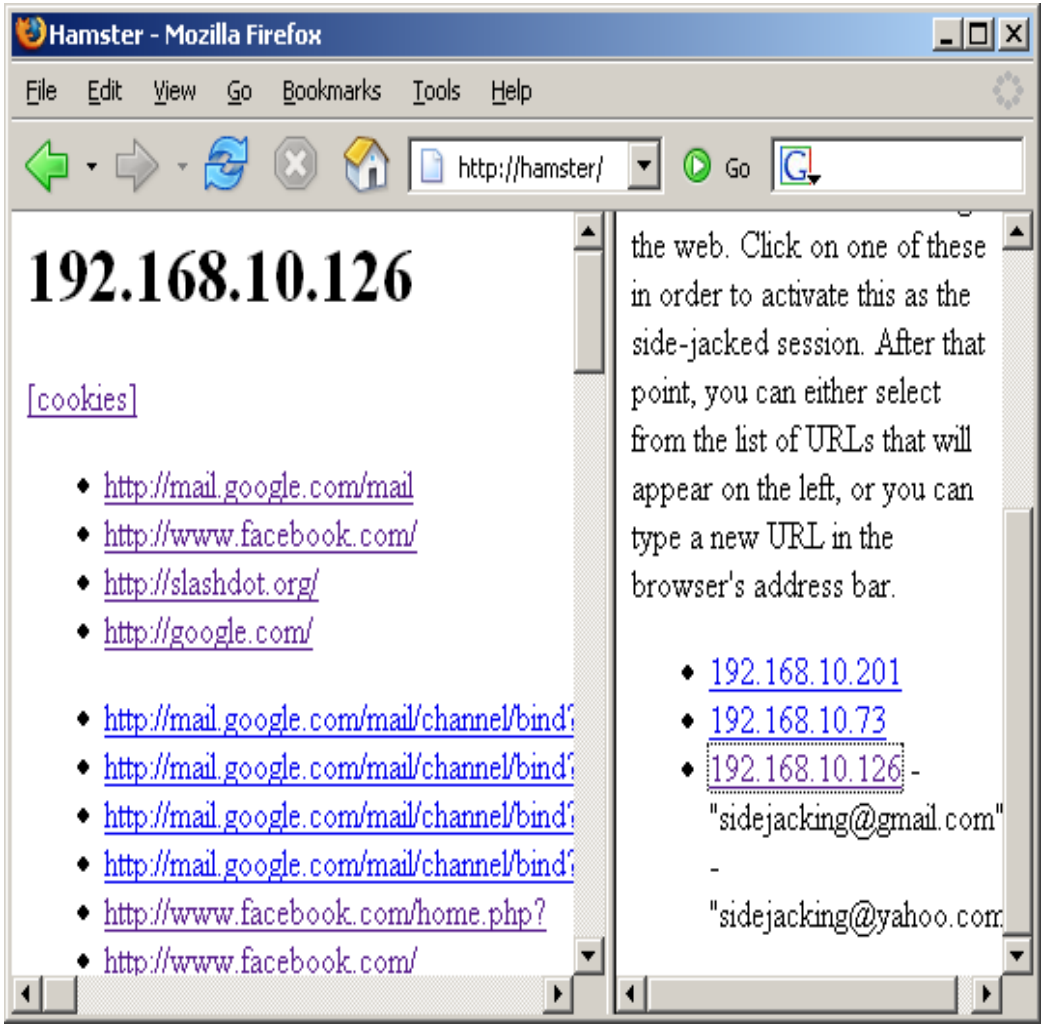
es.NOG
16/10/2008

Cookie harvesting: HAMSTER





Cookie harvesting: HAMSTER



Cookie harvesting: Prevención

- Google ha respondido añadiendo una opción de configuración de la cuenta, anunciado el 24 de Julio de este año, pero por defecto no esta activado.
  - Always use HTTPS

Cookie harvesting: Prevención

Edit labels

Invite a friend
Give Google Mail to:
Send Invite 50 left
Preview Invite

Out of Office AutoReply:
(sends an automated reply to incoming messages. If a contact sends you several messages, this automated reply will be sent at most once every 4 days)
Learn more

- Out of Office AutoReply off
- Out of Office AutoReply on

Subject:
Message:
Only send a response to people in my Contacts

Outgoing message encoding:
Learn more

- Use default text encoding for outgoing messages
- Use Unicode (UTF-8) encoding for outgoing messages

Browser connection:
Learn more

- Always use https
- Don't always use https

Save Changes Cancel

CONCLUSIONES

Conclusiones

- Conocer los riesgos y actuar en consecuencia
  - ¿Hace falta conectarse al CA-Root desde una cafetería?
  - Vigilar en eventos con expertos en comunicaciones, y Wifi de visitantes ;-)
  - Aplicar settings de Gmail si lo usas
  - Limitar salida de tráfico con un FW si no estas en una red conocida
  - Deshabilitar servicios no necesarios
  - Mantener limpia la lista de redes preferidas, borrando entradas temporales

FIN
MUCHAS GRACIAS

Agradecimientos:
Centre de Supercomputació de Catalunya, Cloudmark y Force 10 Networks
Grupo de trabajo del GORE

Atribuciones:
Robert Graham, David Maynor: ERRATA SECURITY: BH_DC_07_Data_seepage.ppt
Dino A. Dai Zovi and Shane Macaulay, autores de KARMA