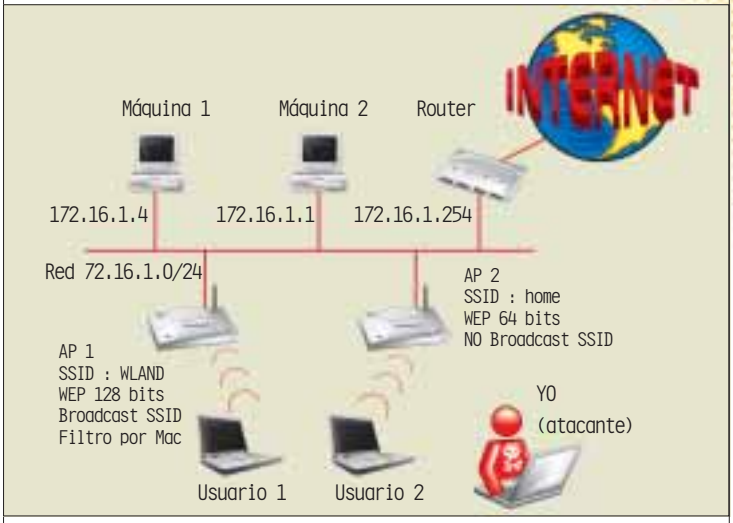
Wireless:
Autopsia de un ataque

Una vez que se conoce el funcionamiento básico de las redes inalámbricas puede entrarse al tema de mayor interés. El punto de partida es una pregunta: ¿por qué las redes implementadas hoy son peligrosas para sus dueños?

Algunas personas creen tener seguridad y en seguida se mostrará la falta de sustento para esa confianza. Para esto es ideal presentar un ataque práctico, no sin antes aclarar que el siguiente artículo de su revista Conthackto mostrará cómo implementar seguridad en una red inalámbrica.

Con ayuda de un laboratorio se tratarán todos los casos y herramientas necesarias para penetrar una red inalámbrica.

EL LABORATORIO



DESCRIPCIÓN DEL LABORATORIO:

Lo que tenemos:

- Red LAN 172.16.1.0/24
- Máquina 1 : 172.16.1.4 sistema operativo XP
- Máquina 2: 172.16.1.1 sistema operativo Linux Fedora Core 3
- Router/Firewall: 172.16.1.254, servidor DHCP para la LAN rango 172.16.1.200-230
- Access Point 1: SSID: WLAN, WEP 128bits, Broadcast SSID permitido
- Access Point 2: SSID: home, WEP 64bits, No Broadcast SSID permitido
- Usuario 1: Usa el acceso a la red a través de AP 1
- Usuario 2: Usa el acceso a la red a través de AP 2
- YO: Sistema operativo Linux Fedora Core 3, tarjeta inalámbrica con chipset PrismGT

Herramientas usadas:

- Wellenreiter [1]
- Kismet [2]
- Weplab [3]
- Aircrack [4]
- Asleap [5]
- WPA passive attack [6]
- Cowpatty [7]
- macchanger [8]
- nmap [9]

Es todo lo necesario para la demostración.

¿CUÁLES SON LOS PASOS A SEGUIR?

Primero, encontrar las redes con sus características:

- SSID
- WEP / WPA / LEAP

Segundo, intentar crackear las contraseñas, es decir, pasar el filtro por MAC.

Al final, ya se está en la red y... todo se puede, excepto que sólo se realizará un escaneo básico con NMAP. En el siguiente número de Conthackto se describirán las técnicas de ataque *Man in the Middle* (hombre en medio) que podrían aplicarse aquí.

PREPARACIÓN DE LA MÁQUINA DE ATAQUE

- Una tarjeta inalámbrica que soporta el modo "monitor" o RFMON, así como sus drivers:

Tarjeta (Chipset)	Drivers
Atheros	madwifi [10]
Prism2/2.5/3	linux-wlan-ng [11], HostAP [12]
PrismGT/Duette/Indigo	prism54 [13]
Hermes	orinoco [14], HermesAP [15]
Aironet (Cisco)	airo-linux [16]

En los últimos kernels (2.6.x) vienen incluidos varios drivers pero si no saben cómo instalar su tarjeta inalámbrica, existen tres soluciones:

1.Consultar el archivo Readme con el driver y aprender a compilar un kernel

2.Bajar un Live-CD de Linux como Auditor [17], Operator [18] o Whoppix [19] que tienen los kernels con los controladores compilados para varias tarjetas (lo más sencillo)

3.Ir a los foros www.Netstumbler.org o www.conthackto.com.mx y ¡preguntar!

UNA VEZ INSTALADA LA TARJETA INSTALADA, SIGUE CONFIGURARLA

Existe una serie de herramientas para configurar las tarjetas y pasar en modo monitor (necesario para varias herramientas). Vea los casos siguientes:

Primero, las tarjetas con controlador Wlan-ng (la tarjeta aparece como wlan0):

```
# wlanctl-ng wlan0 lnxreq_ifstate ifstate=enable
# wlanctl-ng wlan0 lnxreq_wlansniff enable=true channel=<canal AP>
# ifconfig wlan0 up
```

Segundo, si su controlador soporta Wireless Tools (es el caso para Atheros y Prism54, por ejemplo):

```
# iwconfig ath0 mode Monitor
# iwconfig ath0 channel <canal AP>
# iwpriv ath0 monitor_type 1 (hostap only)
# ifconfig ath0 up
```

Finalmente, si usan un Controlador Orinoco:

```
# iwpriv eth0 monitor 1 <AP channel>
```

Ejemplo, para pasar su tarjeta con chipset atheros en modo monitor para el canal 6 (se necesita ser root):

```
# iwconfig ath0 mode monitor channel 6
```

CONFIGURAR LAS HERRAMIENTAS

La mayoría de las herramientas que se usarán no necesitan una preconfiguración; a veces deberá pasarse la tarjeta a modo monitor antes de lanzarla pero uno es sujeto a preconfiguracion: kismet.

Kismet se basa en un archivo kismet.conf que se encuentra en /etc/kismet.conf o /usr/local/etc/kismet.conf

Ahora puede empezarse el proceso.

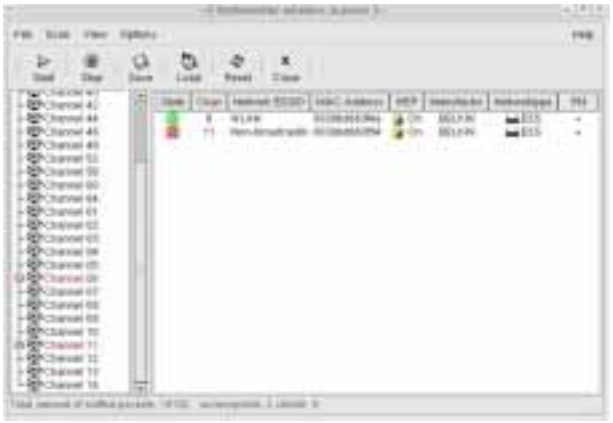
ESCANEO

Existen varias herramientas que implementan un tipo de escaneo un tanto diferente.

La primera familia de escaners calificados de activos pasa de canal en canal escuchando los beacons.

En Windows, puede usarse el excelente Netstumbler [20]. Solamente descubrirá las redes con SSID broadcast permitido.

Con Linux, puede probarse en este lab Wellenreiter [1], aunque se necesita pasar a modo monitor antes de ejecutar el programa. Veamos lo que descubre:



DEDUCCIÓN:

Canal	SSID	BSSID (MAC)	WEP	Equipo	TIPO
6	WLAN	00:30:BD:66:3F:4A	SI	BELKIN	Infra
11	??????	00:30:BD:66:3F:94	SI	BELKIN	Infra

ADVERTENCIA

En algunas versiones Live-cd se preconfigura el kismet.conf; pero en whoppix, por ejemplo, es necesario editar el archivo. Para hacerlo se necesita borrar el symbolic link kismet.conf, copiar el archivo original de /KNOPPIX y configurarlo.

En kismet.conf todo viene bien explicado, solamente debe tenerse cuidado con el tipo de tarjeta (el source).

Ejemplo:

- **tarjeta atheros: source=madwifi_g,ath0,atheros**
- **tarjeta prism54: source=prism54g,eth1,prism**

LINK

Para más información: www.kismetwireless.net/documentation.shtml

Hasta este momento solamente se tienen dos AP y sus BSSID; los dos usan WEP y son de marca BELKIN.

El siguiente paso es usar un escaner pasivo (de hecho, puede ser el primer paso). Este método es muy peligroso porque no manda ningún paquete a la red, al contrario de Netstumbler o Wellenreiter, que pueden ser detectados por sistemas de detección de intrusos (IDS).

ESCANEO PASIVO

El escaneo pasivo solamente "escucha" lo que pasa en la red sin mandar ningún paquete. El mejor para efectuarlo es kismet:

En kismet, se puede presiona "h" a cualquier momento para obtener información sobre la pantalla activa.

A primera vista, proporciona un poco más de informacion, y descubre el SSID del AP 2: ¡home! Aparece en azul como cloaked (invisible). Los SSID en verde usan

WEP, si aparecen en amarillo no usan WEP y en rojo los equipos (AP) están funcionando con la configuración de fábrica (sin WEP).

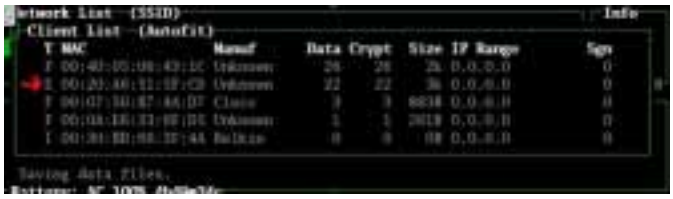
Puede irse llenando esta tabla:

Canal	SSID	Filtro por MAC	WEP	LLave	Equipo
6	WLAN	????????	SI	????????	Belkin
11	home	????????	SI	????????	Belkin

Kismet, proporciona información cada vez que una máquina se asocia con un AP.

De la imagen puede apreciarse que la máquina con la MAC 00:20:A6:51:5F:CD se asoció con el AP1 y SSID WLAN. Tenga cuidado, los SSID son "case sensitive", respetan mayúsculas y minúsculas.

Ahora sería interesante apuntar unas direcciones MAC para saber quién usa cuál AP. Para hacerlo, bajo kismet, presione "s" y "s" otra vez, selecione un SSID y presione "c" para ver a los clientes conectados. Verifique la MAC capturada en la segunda línea.



Pueden verse las direcciones MAC que pasaron por esta red inalámbrica, así como el tipo, la direccion MAC, el fabricante y varios datos más.

Los tipos son:

- T: equipo transmitiendo al AP
- F: equipos en la LAN, ¡sí se ven porque el AP es un puente (bridge)!
- I: Access Point
- E: equipo que se conectó/deconectó al AP (regularmente una máquina cliente a la red inalámbrica), lo que nos interesa.

Por el momento, se guarda esta dirección MAC para el futuro, porque todavía existe un problema: WEP.

Se ha descubierto todo lo que se quería, ahora es tiempo de ver qué se hará con WEP.

CRACKING WEP

Ahora puede pasarse a descifrar el tráfico para crear una asociación con un AP disponible. WEP tiene varias fallas por el algoritmo que usa: RC4. (Lea el artículo anterior para más detalles sobre los métodos para cifrar y autentificar en redes inalámbricas (WPA, familias EAP, WPA2).

Había manera de crackear WEP a través de IV débiles, pero se necesitaban muchos paquetes y hoy en día pocas tarjetas o equipos los dejan pasar. En julio de 2004, un hacker llamado *Korek* presentó una serie de ataques estadísticos sobre WEP ¡basándose en artículos de 10 años atrás!

No se necesitan más IV débiles pero sí una cantidad suficiente de IV únicos, esto cambia todo y definitivamente hay que olvidar WEP, como se verá a continuación.

¿QUÉ SE NECESITA?

Una tarjeta en modo monitor; capturar paquetes (como 500,000 IV únicos para 128bits y 300,000 para 64bits) y lanzar el ataque.

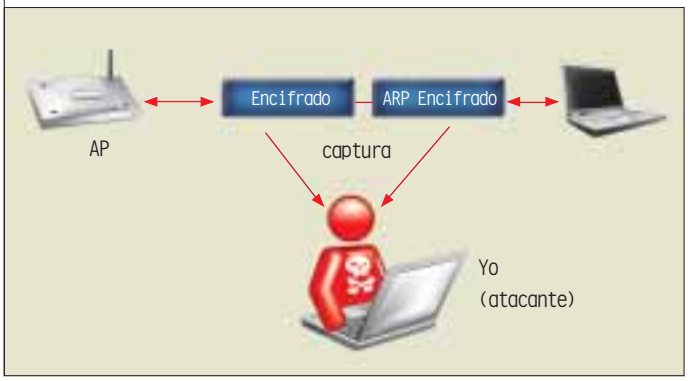
Podrán cuestionar que esos 500,000 IV únicos pueden tardarse mucho tiempo en ser capturados. La realidad es que no hay necesidad de esperar demasiado: en una red con un par de máquinas se capturan 20,000 IV únicos en alrededor de 15 minutos. Todo depende de la cantidad de tráfico que haya en la red.

Si tienen realmente prisa, existe aireplay, parte de aircrack, que permite jugar paquetes cifrados.

¿De qué sirve eso? Hay unos paquetes cortos como request ARP o DHCP que pueden reconocerse aunque cifrados (WEP no cambia el tamaño de los paquetes al cifrar). Si se envían otra vez iguales, aunque cifrados, los equipos blancos van a contestar otra vez al "request" y ¡generarán más tráfico cifrado!

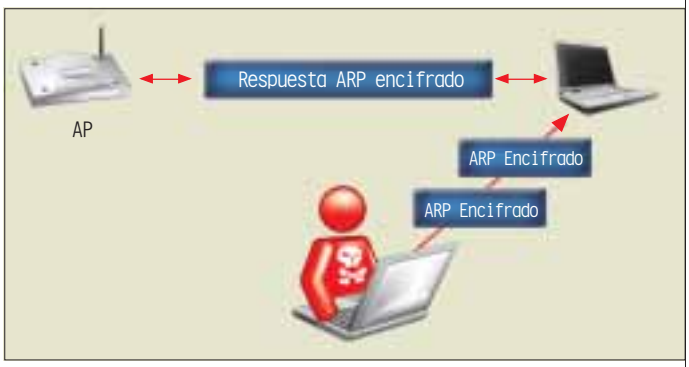
CONCEPTO DE INYECCIÓN:

Fase 1:



Fase 2:

El atacante revisa los paquetes que capturó y va a remitir los paquetes que podrían ser ARP o DHCP.



AIRCRACK AND FAMILY

Aircrack es un conjunto de programas enfocados a crear, inyectar, esnifear y crackear. Vea [4] Aircrack al fin de este artículo. Está en constante evolución (checar www.netstumbler.org para ver el desarrollo. *Devine* es el creador de esta suite, podrán contactarlo en el foro). La revolución es que las tarjetas basadas en Prim2/2.5, Atheros o Prism54 pueden funcionar en modo monitor e inyectar paquetes, lo que significa que una sola tarjeta puede esnifear y reinyectar al mismo tiempo, ¿ven el peligro?

Los programas incluidos en el paquete aircrack son:

- **aircrack**: crackea WPA (desde beta3) con diccionario y WEP con 300,000 IV
- **airodump**: captura los IV mientras se reinyectan los paquetes
- **airforge**: crea paquetes una vez que se tiene el PRGA o para para forzar una reautenticación en WPA/LEAP o vaciar el cache ARP y forzar un nuevo ARP request)
- **aireplay**: puede jugar un paquete (creado con airforge), automáticamente reinyectar ARP request, reautenticar las estaciones, usar el ataque de *Korek* para descifrar un paquete y conseguir el PRGA (cadena usada para cifrar).

No se les enseñará a reinyectar los paquetes por razones obvias (así se crackea una red protegida con WEP en poco tiempo y sin tener tráfico).

Hoy en día mucha gente confía en WEP para estar más o menos protegido y la idea no es hacer que mañana entren en modo pánico. La verdad no es nada difícil ahora que tienen todos los componentes. En la sección software del siguiente foro: forum.remote-exploit.org/ encontrarán lo necesario para poder reinyectar sin problema.

Por ahora no se inyectarán paquetes, pero ya puede intuirse su uso. Solamente se generará una transferencia de archivos entre usuario1 y máquina1 para crackear la llave de 128bits (realmente son 104bits porque cada IV es de 24 octetos).

Se empieza por la captura:

No se necesita capturar los paquetes enteros (solamente puede hacerse si se tiene un disco de 200GB). Para ello se usará weplab (también podría usarse airodump).

Primero se pone la tarjeta en modo monitor, escuchando el canal 6 (el de WLAN). Después se lanza la captura de la siguiente manera:

[root@server ~]# weplab -c -i eth1 —caplen ./captura1

Se presiona Enter <entrar> para ver si se incrementan los unique IV

Las opciones:

c: para capturar

i eth1: la interfaz que se usa

caplen 150: tamaño que capturamos de cada paquete (150 octetos)

./captura1: nombre del archivo donde almacenamos

Para terminar la captura se presiona CTRL+C. Lo hacemos en dos archivos, porque en la vida real, la captura puede hacerse en más de una ocasión para tener suficientes IV.

Capturamos otra vez pero con ./captura2 como nombre.

Al sumar suficientes paquetes puede crackearse la llave WEP con aircrack.

Nota: se podría hacer también con weplab pero para variar:

[root@server ~]# aircrack captura1 captura2

Que devuelve:

Este resultado salió en menos de 15 segundos... y es una WEP de 104bits. ¿Alguna pregunta?

Y si no fuera WEP, sino otra cosa como WPA-PSK o LEAP de Cisco, los dos son vulnerables a ataques de estilo *brute-force* (no implementados en este lab).

LEAP/PPTP

LEAP está basado en un mecanismo de challenge/respuesta vulnerable a *brute-forcing* (pruebe varias combinaciones) o diccionario. Esto porque usa MSCHAPv2 que, a su vez utiliza las credenciales de los usuarios para proceder. El "username" pasa en texto claro (gracias) y el hash NTLM sirve para cifrar un challenge (24 octetos).

Capturar los primeros paquetes de la negociación es necesario para empezar un ataque con un diccionario. Ethereal es suficiente para esto.

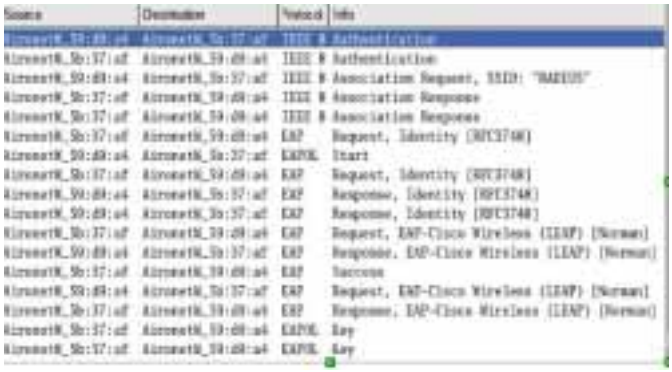
Nota:hay dos formas posibles para capturar paquetes en ambiente inalámbrico:

- estar asociado al AP y usar ethereal o tcpdump
- estar en modo monitor

Ejemplo con ASLEAP:

Asleap

Para usarlo, primero capture una negociación, la que se ve así:



Puede verse el doble challenge/respuesta. Esta captura se llama leap.apc (formato libpcap).

Asleap necesita generar dos archivos:

- una correspondencia hash/contraseña
- una tabla de los índices

Genkeys (incluido en asleap) genera esta tabla desde un diccionario. Lo peligroso de Asleap es que permite escuchar en tiempo real y guardar en un archivo todos los challenge/respuesta que ve para crackear... además puede desasociar los equipos para renegociar (¡se necesita el driver Airjack, no muy estable y para kernel 2.4.X!)

Durante la prueba fue creado un archivo dico con interior blamo, la contraseña de esta conexión.

RESULTADO:

```
[fabien@localhost asleap]$ ./genkeys -f dico -f dico.dat -n index.idx
genkeys 1.4 - generates lookup file for asleap. <jwright@hasborg.com>
Generating hashes for passwords (this may take some time) ...Done.
5 hashes written in 0.04 seconds:  119.25 hashes/second
Starting sort (be patient) ...Done.
Completed sort in 0 compares.
Creating index file (almost finished) ...Done.
[fabien@localhost asleap]$ ./asleap -r leap.apc -f dico.dat -n index.idx
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured LEAP exchange information:
        username:           BSAINI
        challenge:          afe811f2ae948bdb
        response:           5b79dab0bf72ed434ebca8a784466bffb28f6e94280c9184
        hash bytes:         32b6
        NT hash:            13791099d4220065a5813370d4232b6
        password:           blamo
[fabien@localhost asleap]$
```

La conclusión rápida es: si uso LEAP o PPTP, ¡mejor que mis usuarios tengan buenas contraseñas!

LINK

En el link siguiente, puede encontrar lo que dice Cisco en respuesta a este ataque: www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

A final de cuentas, la seguridad de LEAP depende de qué tan difícil sea encontrar la contraseña de los usuarios y, cuando se sabe que la mayoría de las empresas usan LEAP con un servidor RADIUS que autentica contra el Active Directory Corporate, romper LEAP es tener acceso no solamente a la red sino también a Active Directory.

WPA

WPA es vulnerable (en el mismo sentido que LEAP) cuando se usa en modo Pre-Shared-key (WPA-PSK). La idea es la misma, capturar los primeros paquetes intercambiados para la autenticación y correr un ataque *brute-force* basado en un diccionario.

Puede usarse cowpatty (del mismo autor que asleap) o WPA passive attack. No se realizará una demo porque es el mismo mecanismo de ataque que asleap sobre un algoritmo diferente.

DE REGRESO AL LAB...

Ahora se tiene la WEP key de la red WLAN. ¿Qué puede hacerse?

Primero, configurar la máquina con los parámetros siguientes:

iwconfig ath0 mode managed /*regresamos a modo normal*/

iwconfig ath0 essid WLAN key 2222FFFF333344444444444455

Se intenta conseguir una dirección IP vía DHCP. Falla.

Con ethereal se ve que una máquina tiene la dirección 172.16.1.201. Se configura una dirección IP en ese rango; se intenta un escaneo con NMAP, falla; no se puede salir. Hay un filtro por dirección MAC.

Es tiempo de usar la MAC que se capturó antes y ponerla en la máquina.

Para hacer lo anterior es mejor esperar a que se desconecte la máquina que se usurpó, en el lab es fácil hacerlo, en la vida

real se puede hacer con un ataque DoS (Denial of Service) para dejar la máquina fuera y usar su MAC.

¿Cómo cambiar la MAC? Nada hay más fácil con macchanger:

```
[root@localhost macchanger-1.5.0]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0C:55:00:A5:AF
          inet6 addr: fe80::20c:55ff:fe00:a5af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1295272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:528038171 (503.5 MiB)  TX bytes:378 (378.0 b)
          Interrupt:10

[root@localhost macchanger-1.5.0]# macchanger -m 00:20:A6:51:5F:CD eth1
Current MAC: 00:0c:55:00:a5:af (Microlink Communications Inc.)
Faked MAC:   00:20:a6:51:5f:cd (Proxim, Inc.)
[root@localhost macchanger-1.5.0]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:20:A6:51:5F:CD
          inet6 addr: fe80::20c:55ff:fe00:a5af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1295272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:528038171 (503.5 MiB)  TX bytes:378 (378.0 b)
          Interrupt:10
```

Ahora se intenta salir, para lo cual se ejecuta el cliente DHCP:

```
# dhclient eth1
```

o

```
# pump eth1
```

Con eso ya puede salirse con la MAC de la otra máquina. Nos dio la direccion 172.16.1.211/24 con gateway 172.16.1.254. En caso de no obtener una dirección, puede ponerse al azar en el rango 172.16.1.X y correr un escaneo.

NMAP

Un escaneo rápido para verificar que estamos en la red...

```
[root@localhost ~]# nmap -sP 172.16.1.0/24

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-02-17 01:53 CST
Host 172.16.1.1 appears to be up.
MAC Address: 00:40:05:06:43:1C (ANI Communications)
Host 172.16.1.202 appears to be up.
MAC Address: 00:30:BD:4D:B5:5D (Belkin Components)
Host 172.16.1.211 appears to be up.
Host 172.16.1.215 appears to be up.
Host 172.16.1.254 appears to be up.
MAC Address: 00:07:50:B7:4A:D7 (Cisco Systems)
Nmap finished: 256 IP addresses (5 hosts up) scanned in 7.355 seconds
```

Ahora el atacante puede esnifear el tráfico, atacar al estilo *Man in the Middle*, escanear la red por vulnerabilidades, atacar con *brute-force* o *exploits* los servicios encontrados o capturar contraseñas y cifrar para crackeo "offline". Esto se verá en el próximo número de Conthackto.

CONCLUSIÓN

Hoy se necesita monitorear la red inalámbrica y no confiar demasiado en WEP o filtros.

No olvidemos que para alguien malintencionado, las redes inalámbricas son un regalo de Dios, no hay ninguna forma de localizarlos (por lo menos no de forma muy rápida), usan la salida del usuario de la empresa o de su casa. Si alguien quiere atacar un banco o un sitio, ¿qué mejor anonimato que la red inalámbrica, sin proteccion, del vecino?...

LINK:

[1] Wellenreiter: www.wellenreiter.net/
[2] Kismet: www.kismetwireless.net/
[3] Weplab: weplab.sourceforge.net/
[4] Aircrack: www.cr0.net:8040/code/network/aircrack/
[5] Asleap: asleap.sourceforge.net/
[6] WPA passive attack: www.tinypeap.com
[7] Cowpatty: www.c2security.org/tools/
[8] Macchanger: www.mirrormonster.com/gnuftp/pub/gnu/macchanger/
[9] NMAP: www.insecure.org
[10] madwifi: madwifi.sourceforge.net/
[11] linux-wlan-ng: www.linux-wlan.com/linux-wlan/
[12] HostAP: hostap.epitest.fi/
[13] Prism54: prism54.org/
[14] Orinoco: www.nongnu.org/orinoco/
[15] HermesAP: freshmeat.net/projects/hermesap/
[16] Airo-Linux: sourceforge.net/projects/airo-linux/
[17] Auditor (mejor live-cd para hacking inalámbrico): www.remote-exploit.org
[18] Operator: www.ussysadmin.com/operator/
[19] Whoppix: www.whoppix.net
[20] Netstumbler: www.netstumbler.com