MAN IN THE MIDDLE

ATAQUE Y DETECCIÓN

Realizado por:

David Galisteo Cantero
Raúl Moya Reyes

INDICE

Nota1: No nos hacemos responsables de los daños que pueda ocasionar este documento, simplemente pretendemos que sea algo constructivo y educativo.

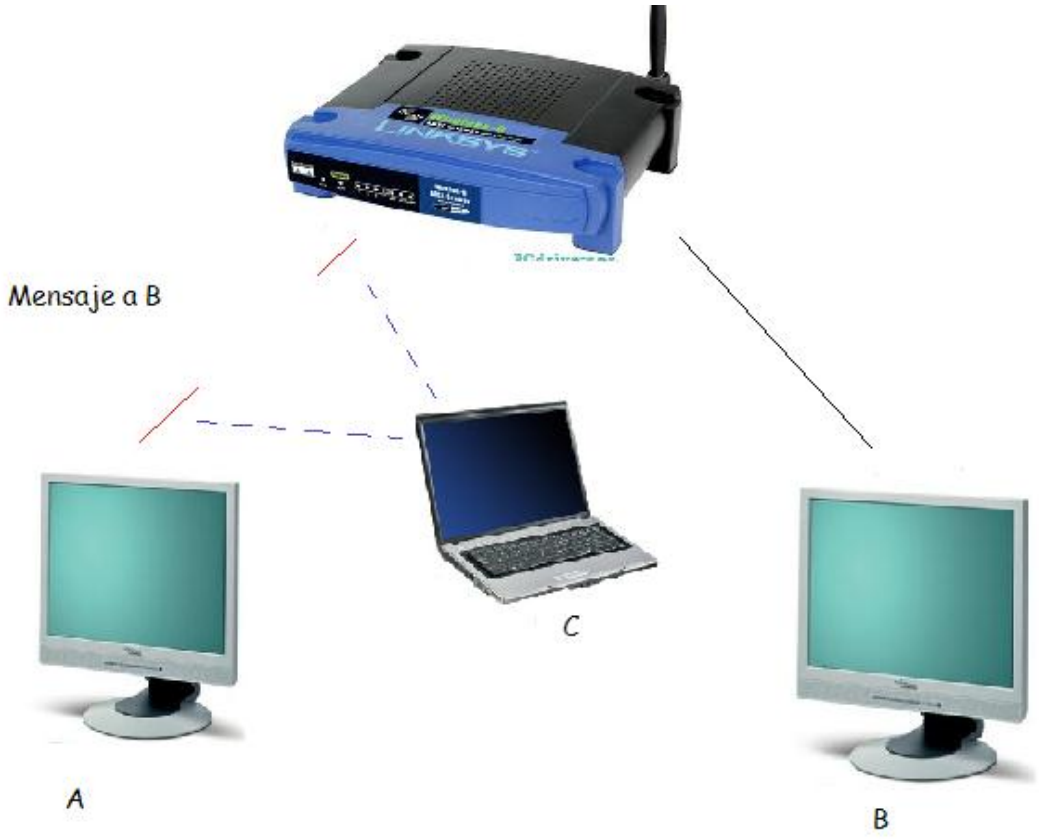
Nota2: Las imágenes tomadas en esta guía han sido recogidas practicando los ataques entre los dos componentes del grupo, no se ha perjudicado a ningún tercero.

INTRODUCCIÓN

El ataque 'Man in the middle', traducido a español como 'El hombre en el medio', es un ataque PASIVO, que se lleva a cabo tanto en redes LAN como WLAN.

Pongamos un simple ejemplo para poner de manifiesto en qué consiste este ataque:

Supongamos que tenemos 3 hosts dentro de una red, host A, host B, y host C. El host A quiere intercambiar información con el host B (éste host puede o no estar en la misma red), para ello, los paquetes deben enviarse a través del router que los dirige hacia B. Ahora, si el host C tiene intención de 'escuchar' el mensaje que A envía a B, sólo tiene que adoptar un papel de puente entre A y el router.



Al ser un ataque pasivo, la víctima no detectaría nada raro, de ahí la dificultad de hacer frente a un ataque de este tipo, como veremos algún apartado más adelante.

En definitiva, este ataque nos permite monitorizar el tráfico que deseemos de una red, tanto de un host hacia el router, como del router hacia un host.

CONCEPTOS CLAVE

A continuación vamos a proporcionar algunos conceptos clave necesarios para comprender y asimilar mejor este documento, algunos de ellos probablemente los conocerás, pero nunca vienen mal.

Protocolos:

No vamos a entrar en detalle en la explicación de los protocolos ya que se saldría de nuestro tema, si quieres más información ojea algún libro sobre redes.

- TCP: Este protocolo está orientado a la conexión, permite la multiplexación mediante puertos (mapeo de puertos), más adelante veremos cómo se capturan paquetes TCP cuando la víctima conecta con algún servidor. También es el encargado de 'fraccionar' la información en datagramas (paquetes) para su envío a través del protocolo IP como partes independientes (muy útil cuando se producen fallos en envíos al reenviar sólo el paquete que ha fallado).

- IP: Es utilizado por los protocolos de conexión (TCP) para el envío y enrutamiento de los paquetes

El protocolo TCP/IP es el que hace posible el 'entendimiento' entre todas las máquinas conectadas a Internet, cada una con un hardware/software diferentes, hablan el mismo idioma, TCP/IP.

- DNS: Este protocolo se encarga de resolver nombres de dominio en direcciones IP, es de gran ayuda ya que es mucho más fácil recordar el nombre de dominio de una web, que su dirección IP.

- ARP: El protocolo ARP es de fundamental entendimiento en este trabajo, ya que si no sabemos cómo funciona no entenderemos este documento. En una red con varios hosts conectados, cada uno con una dirección IP y una dirección física (MAC), el protocolo ARP se encarga de traducir la IP de un ordenador a su dirección MAC, así, a la hora del envío de paquetes, un host comprueba qué dirección MAC tiene la IP a la que quiere enviarle la información.

- ICMP: Es el protocolo encargado de hacer labores de control y error, es utilizado, por ejemplo, para comprobar que un paquete llega a su destino. Cuando hacemos 'ping' a cualquier máquina, estamos enviando paquetes de este tipo.

- Sniffer: Software diseñado para monitorizar la actividad de una red de computadores. Si lo utilizamos de forma ilícita, podemos capturar información de tipo personal (confidencial), y está estipulado como delito(Artículo 1.4 de la Ley Orgánica 15/1999 de protección de datos de carácter personal).

- Modo promiscuo de una interface de red: Aquel en el que una tarjeta de red captura todo el tráfico que circula por una red.

- Arp-spoofing: Ataque que modifica la tabla arp de un host para hacer que resuelva una IP a una MAC que no es la que le corresponde, el Arp-spoofing es lo que hace posible el 'Man in the middle'.

PLATAFORMAS LINUX

A continuación vamos a hacer alguna demostración de este ataque sobre plataformas Linux. Explicaremos el software necesario y unos sencillos pasos para llevarlo a cabo.

SOFTWARE

El software necesario es el siguiente:

- Wireshark (antiguo Ethereal) : Sniffer
- Paquete Dsniff: colección de herramientas para auditoría y test de penetración de redes.
- Arpspoof: Aplicación del paquete Dsniff para hacer arp-spoofing
- SSLstrip: Aplicación que permite capturar contraseñas en páginas https.
- Librerías WinPCap (para Windows) y Libcap (para Linux): Librerías necesarias para la monitorización de redes.

EXPLICACION

Bien, vamos a describir como empezar a monitorizar el tráfico de una red con Wireshark:

- Primero de todo, tenemos que editar el archivo 'ip_forward', esto nos permite redireccionar el tráfico que pasa por nuestra máquina hacia su destino, si no lo hacemos, propiciaremos una denegación de servicio (DOS) al equipo víctima.
    - sudo nano /proc/sys/net/ipv4/ip_forward Cambiamos el 0 por 1
- Después, abrimos el sniffer con una determinada interface de red y con privilegios de root:
    - sudo wireshark –i [interface] -i → Selecciona interfaz
- A continuación, abrimos dos consolas y ejecutamos estos comandos (uno en cada consola):
    - sudo arpspoof –i [interface] –t [ip_objetivo] [ip_router] -t → target(objetivo)
    - sudo arpspoof –i [interface] –t [ip_router] [ip_objetivo]

Ya estaríamos falseando la tabla ARP de la víctima, dada la manera en la que está hecho este ejemplo, capturaríamos todo el tráfico que va desde la máquina víctima hacia el router.

Para ver las direcciones IP que están conectadas a nuestra red, podemos entrar a nuestro router desde el navegador:

Connected Clients

MAC Address	Age(s)	RSSI(dBm)	Type	IP Addr	Host Name
[redacted]	0	0	11g	192.168.0.16	[redacted]
[redacted]	0	0	11g	192.168.0.19	[redacted]
[redacted]	0	0	11g	192.168.0.26	[redacted]

Ahora, en la ventana de Wireshark, vemos que en la barra de herramientas hay 3 botones:

El verde es para especificar las opciones de captura de paquetes, el rojo para empezar una nueva captura, y el azul, para finalizarla, al pulsar este último, nos da la opción de guardar lo que hemos capturado en un archivo para su posterior análisis.

Para más información consulta un manual sobre esta aplicación.

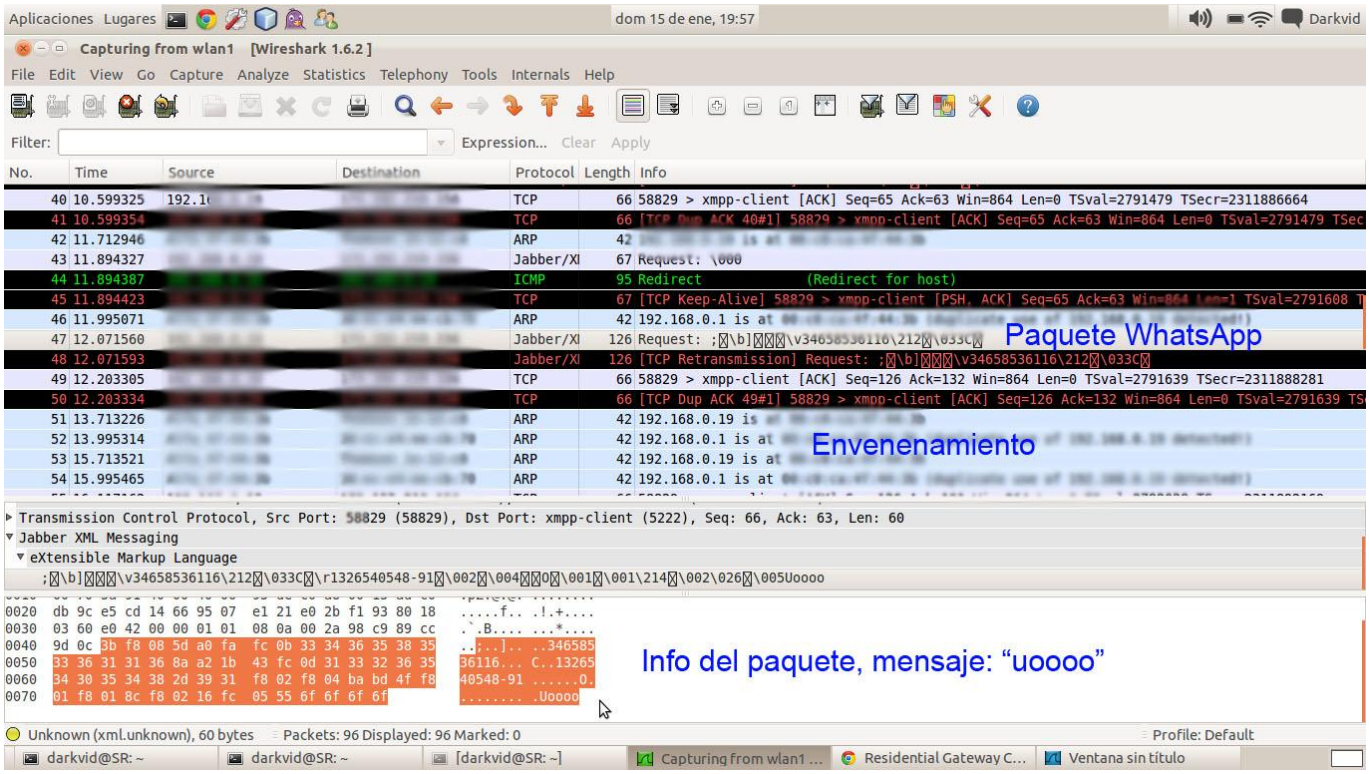
Veamos ahora algunos ejemplos con este sniffer.

ATAQUES DE EJEMPLO

Se van a exponer ejemplos de las diferentes informaciones que hemos conseguido con este ataque:

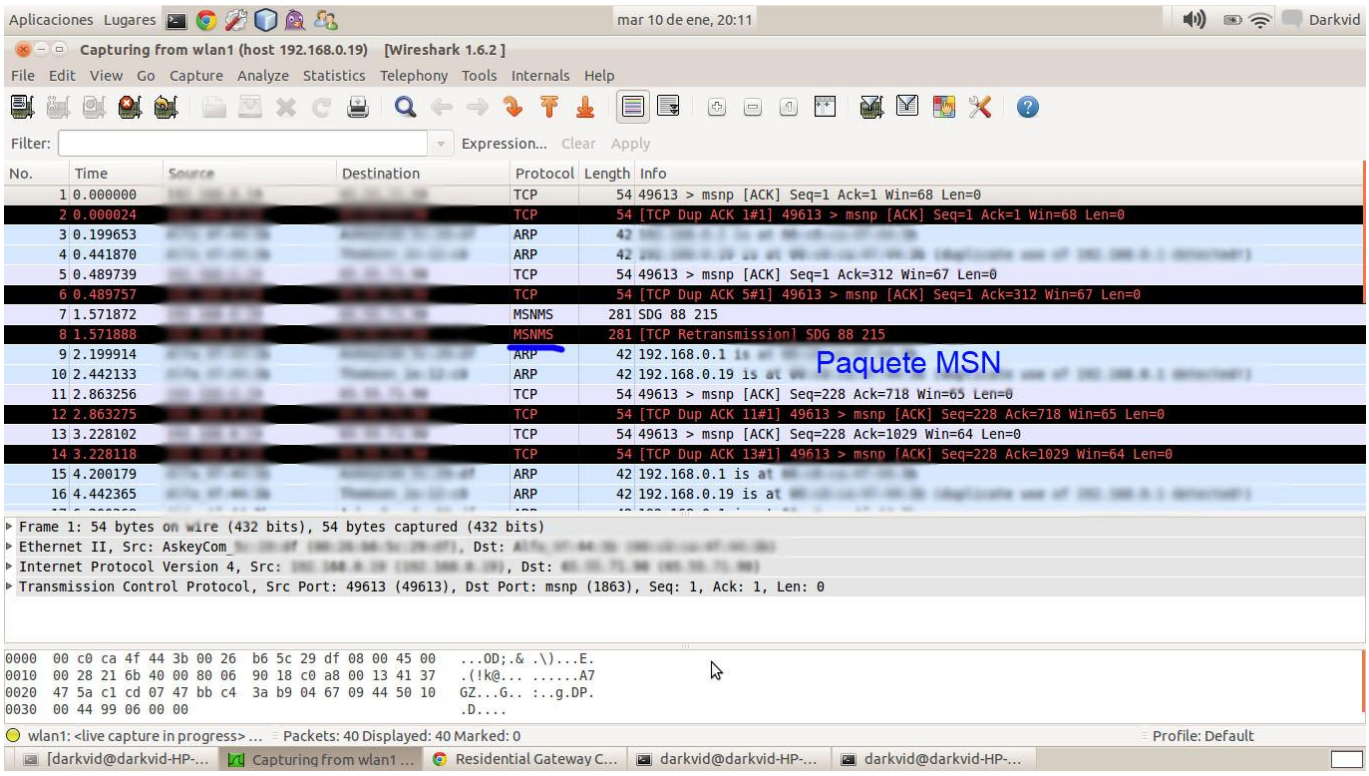
DISPOSITIVOS MOVILES (WHATSAPP)

En aplicaciones móviles como WhatsApp es relativamente fácil capturar los mensajes enviados/recibidos:

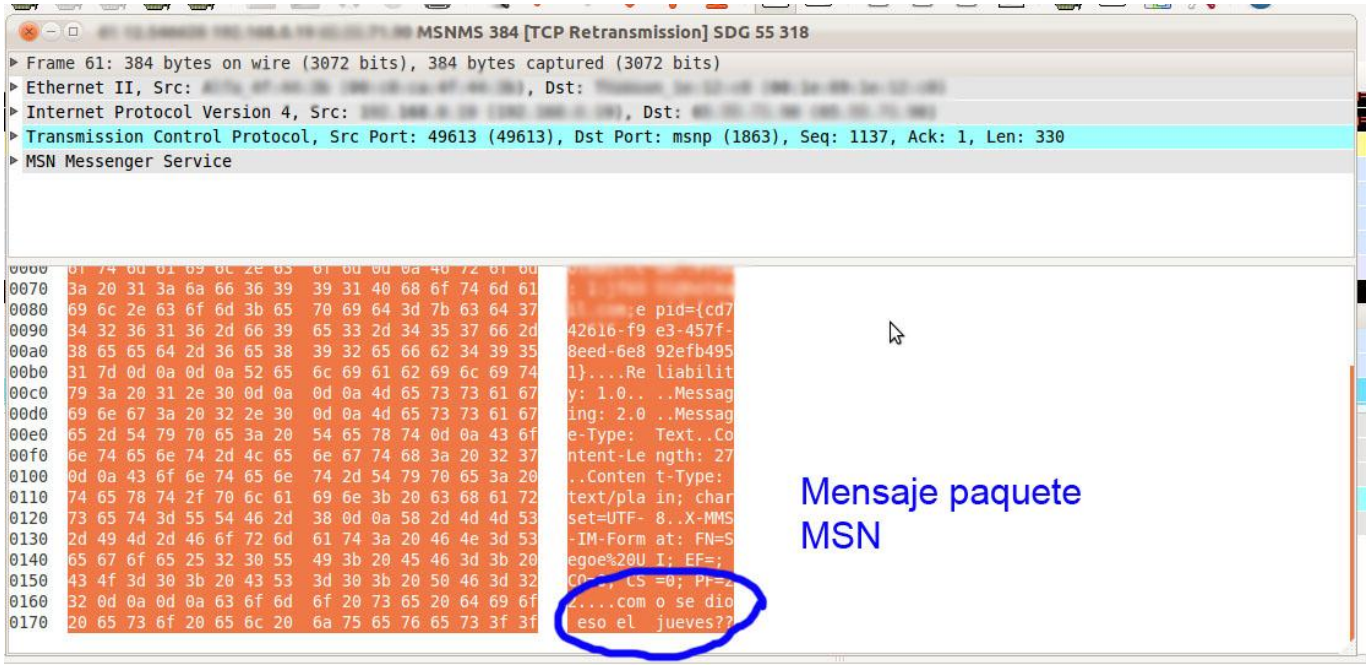


MENSAJERÍA INSTANTÁNEA (MSN)

Igual que el anterior, la información enviada a través de msn, también se puede capturar facilmente:



Veamos lo que contenía el mensaje:



Para este ejemplo, vamos a hacer uso de la aplicación anteriormente mencionada 'SSLstrip'. El protocolo SSL (secure socket layer) es utilizado actualmente por muchas webs para enviar datos de una forma segura.

El funcionamiento de SSLStrip es simple, reemplaza todas las peticiones "https://" de una página web por "http://" y luego hace un MITM entre el servidor y el cliente. La idea es que la víctima y el atacante se comuniquen a través de HTTP, mientras que el atacante y el servidor, se comunican a través de HTTPS con el certificado del servidor. Por lo tanto, el atacante es capaz de ver todo el tráfico en texto plano de la víctima.

Demostración:

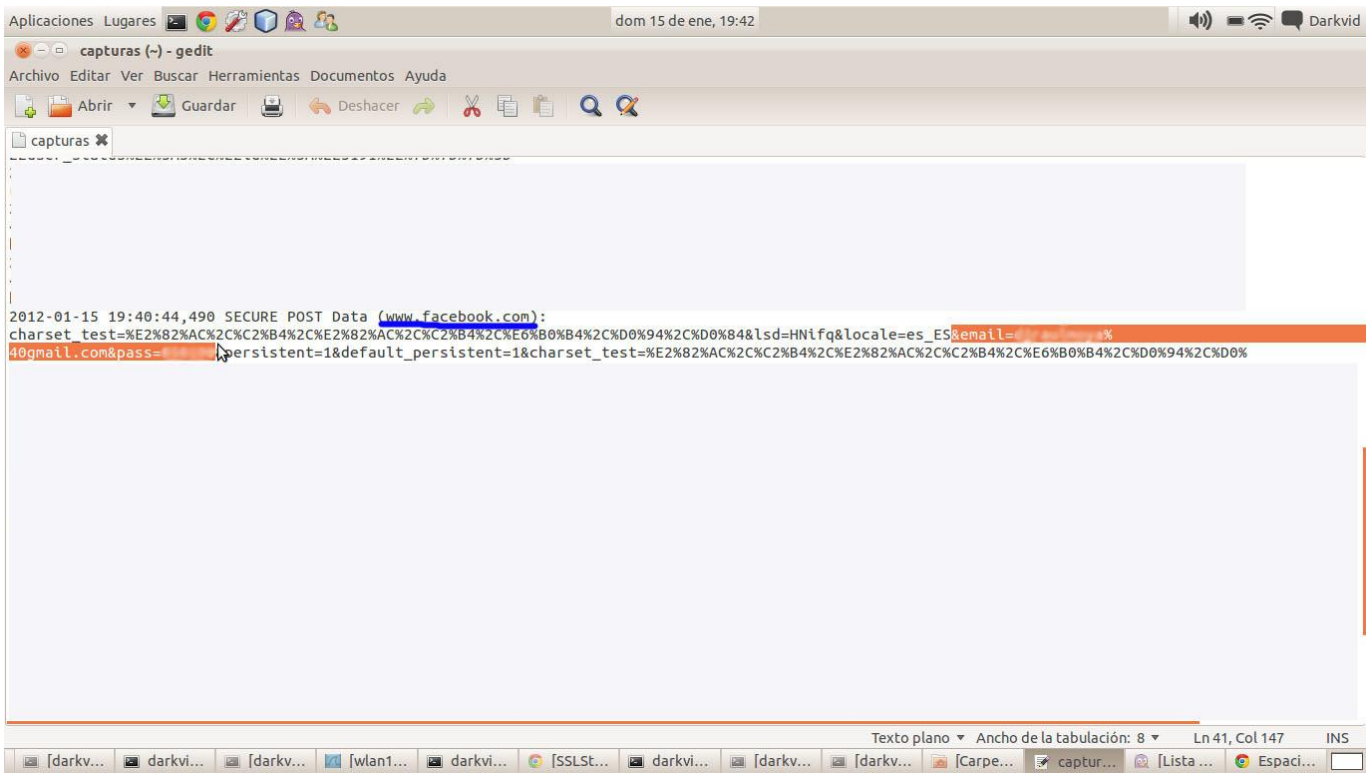
- Empezamos abriendo una consola y escribimos lo siguiente:
  - iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

Con esta línea lo que hacemos es redireccionar el puerto 80 al 10000

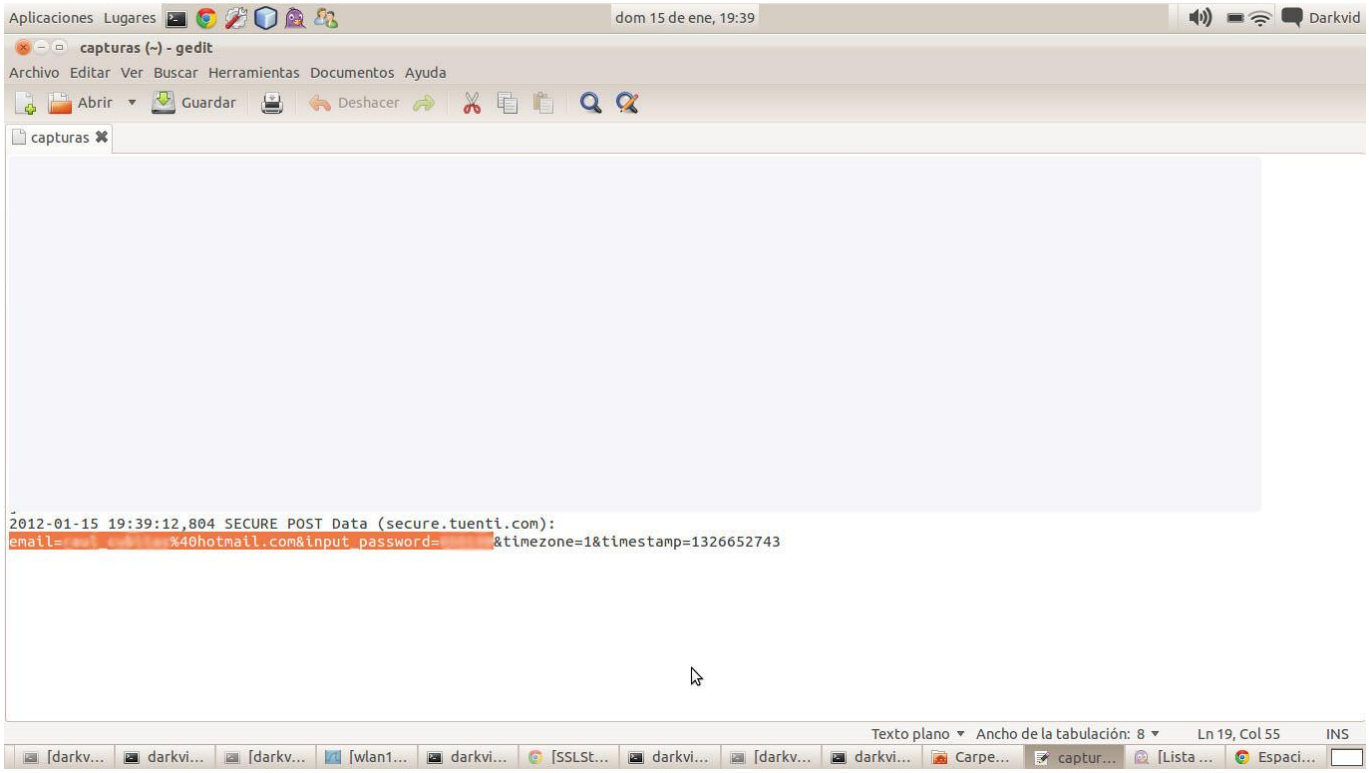
- Ahora abrimos SSLstrip y le decimos que guarde las capturas en un fichero:
  - sslstrip –w capturas.txt

Estos son los resultados:

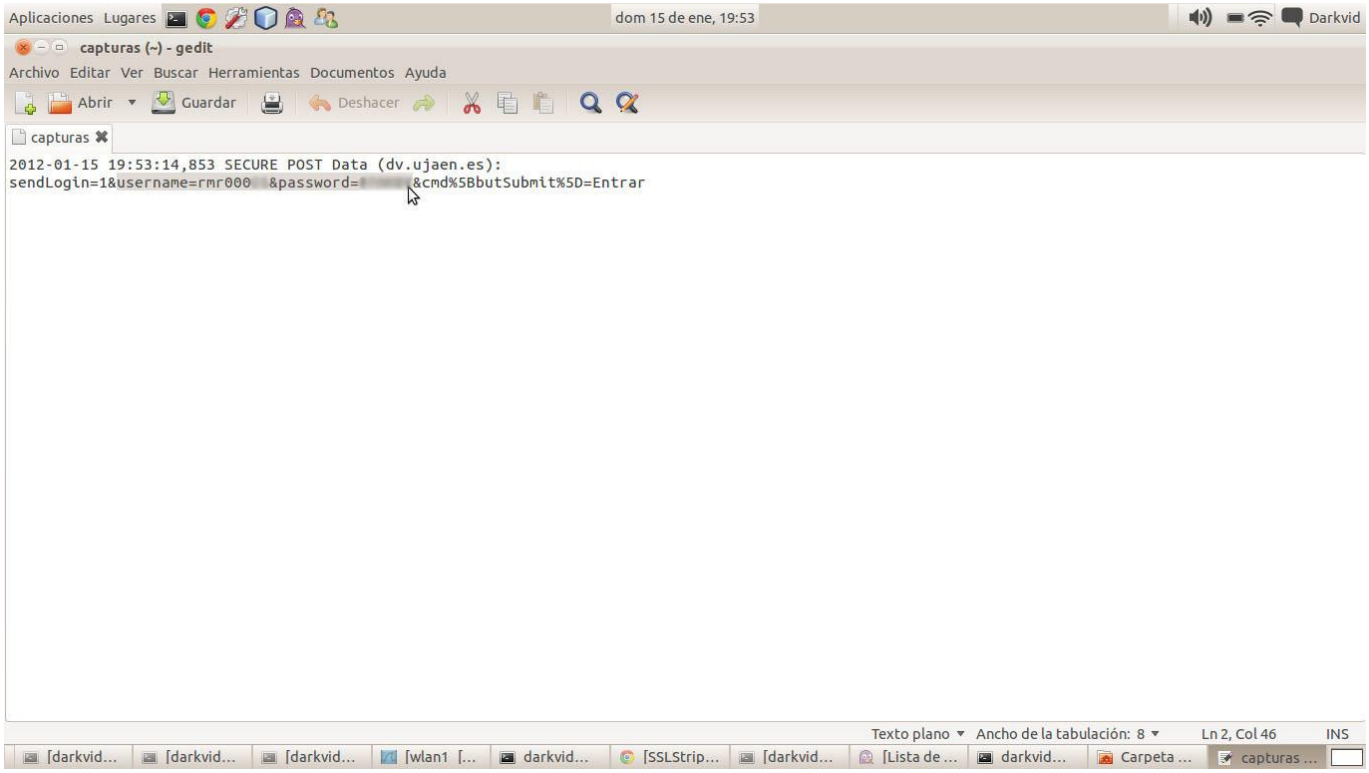
FACEBOOK



TUENTI



Y por último, pero no menos importante, CREDENCIALES DE LA UJAEN

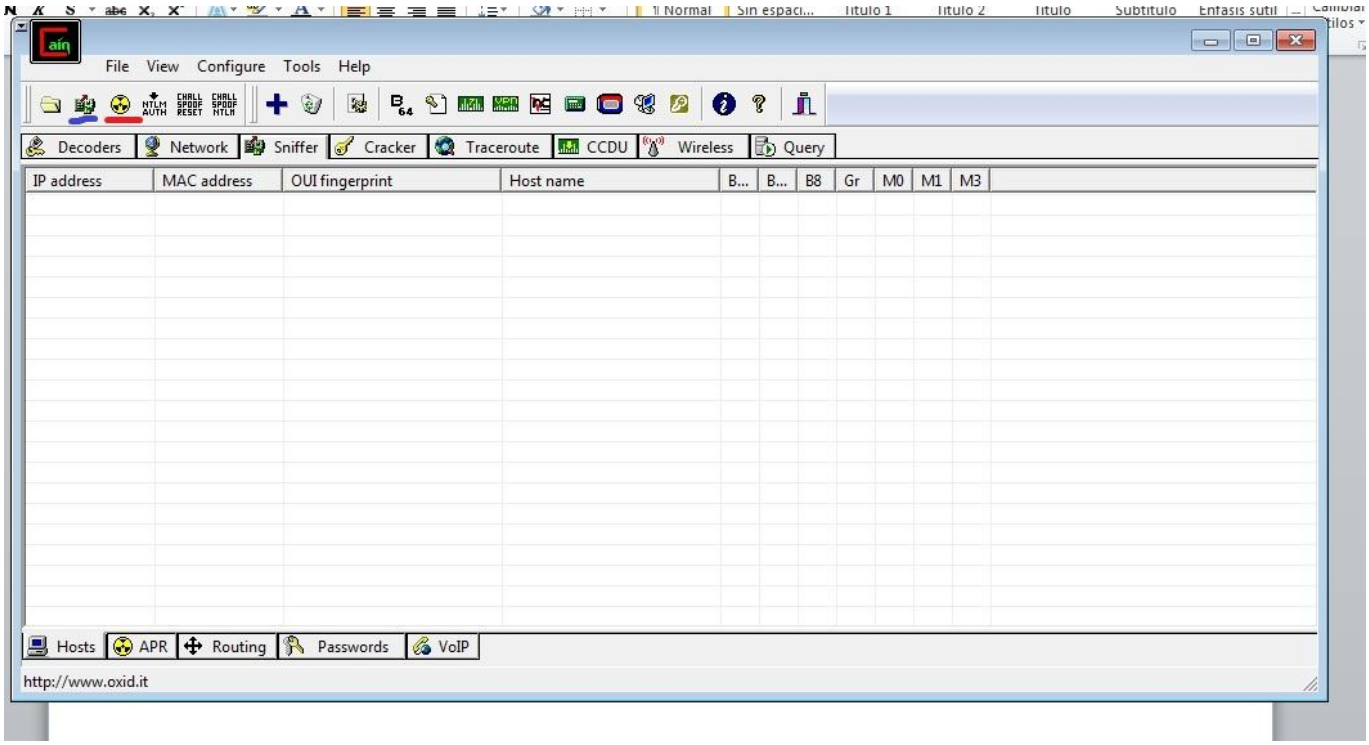


PLATAFORMAS WINDOWS

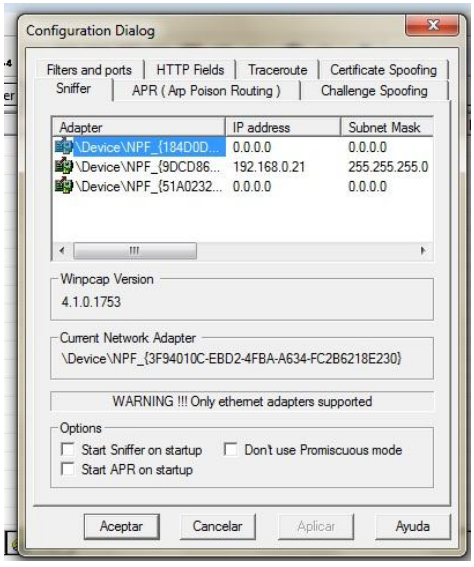
Bien, ahora vamos a realizar el ataque sobre una plataforma Windows, como veremos, es mucho más sencillo que en Linux, solo apretar un par de botones.

SOFTWARE

Para esta demostración solo utilizaremos una aplicación, Cain, que es otro sniffer pero sólo para Windows, que podemos ver en la siguiente imagen:



Para configurarlo, pulsamos en 'Configure' en la barra de herramientas, seleccionamos la interfaz que vayamos a utilizar (aquella cuya ip sea distinta de 0.0.0.0), en la pestaña 'Filters and ports', marcamos todos:



ATAQUES DE EJEMPLO

En estos ejemplos pretendíamos capturar credenciales en páginas https, pero sólo lo hemos conseguido con http, aunque las contraseñas están cifradas.

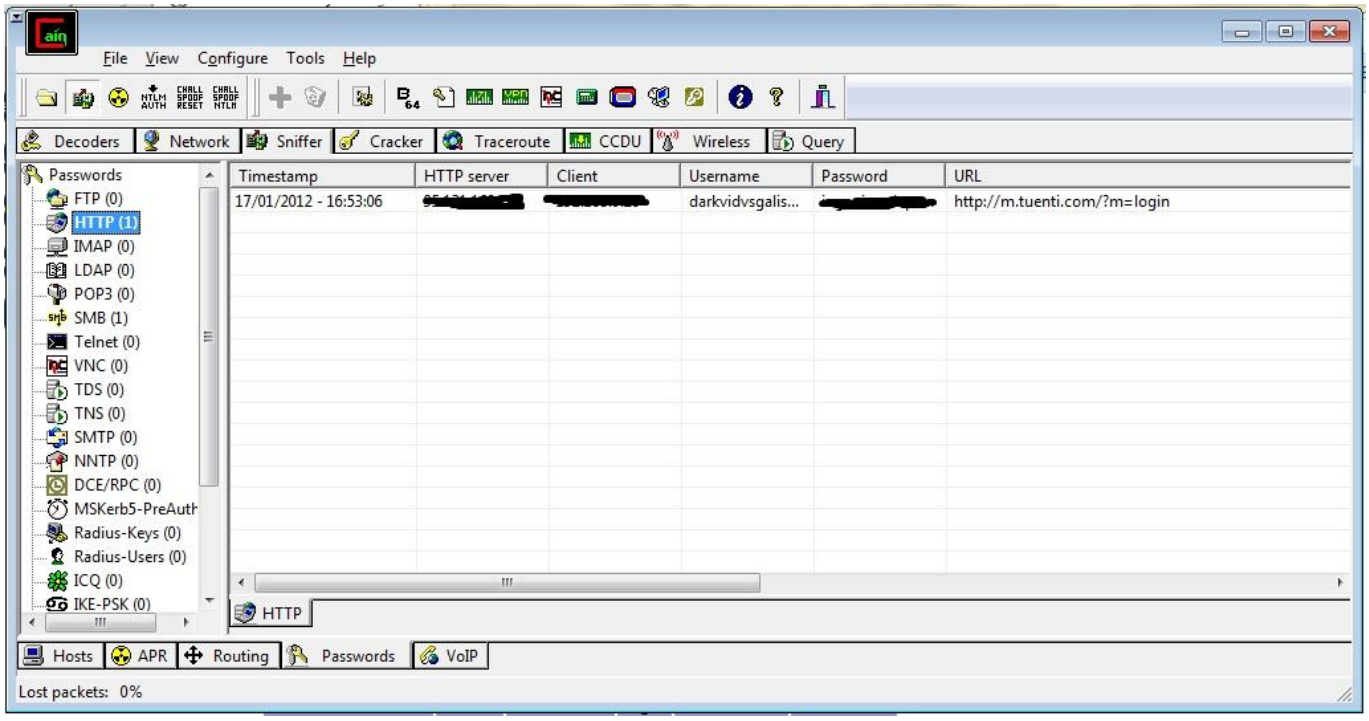
DISPOSITIVOS MÓVILES

Para comenzar con el envenenamiento, vamos a ver los hosts que hay conectados a nuestra red.

Vamos a poner en marcha el sniffer pulsando el botón subrayado de azul, a continuación, pulsamos sobre la cruz (+) y seleccionamos los objetivos (Quizás sea necesario pulsar sobre + varias veces ya que en la primera ocasión pueden no salir todos los hosts conectados).

Una vez tengamos la lista de hosts, pulsamos en la pestaña APR (abajo), pinchamos sobre una casilla vacía y volvemos a pulsar (+), nos saldrán dos cuadros, donde tendremos que elegir la IP de la víctima en el primero, y la IP del router en el segundo, también lo podemos hacer al contrario, dependiendo de nuestros intereses (Podemos seleccionar tantas como queramos).

Una vez hecho esto, pulsamos sobre el botón subrayado de rojo, así comenzará el spoofing, para ver lo que vamos capturando, nos movemos a la pestaña 'Passwords' (abajo), y vemos que… voilà:



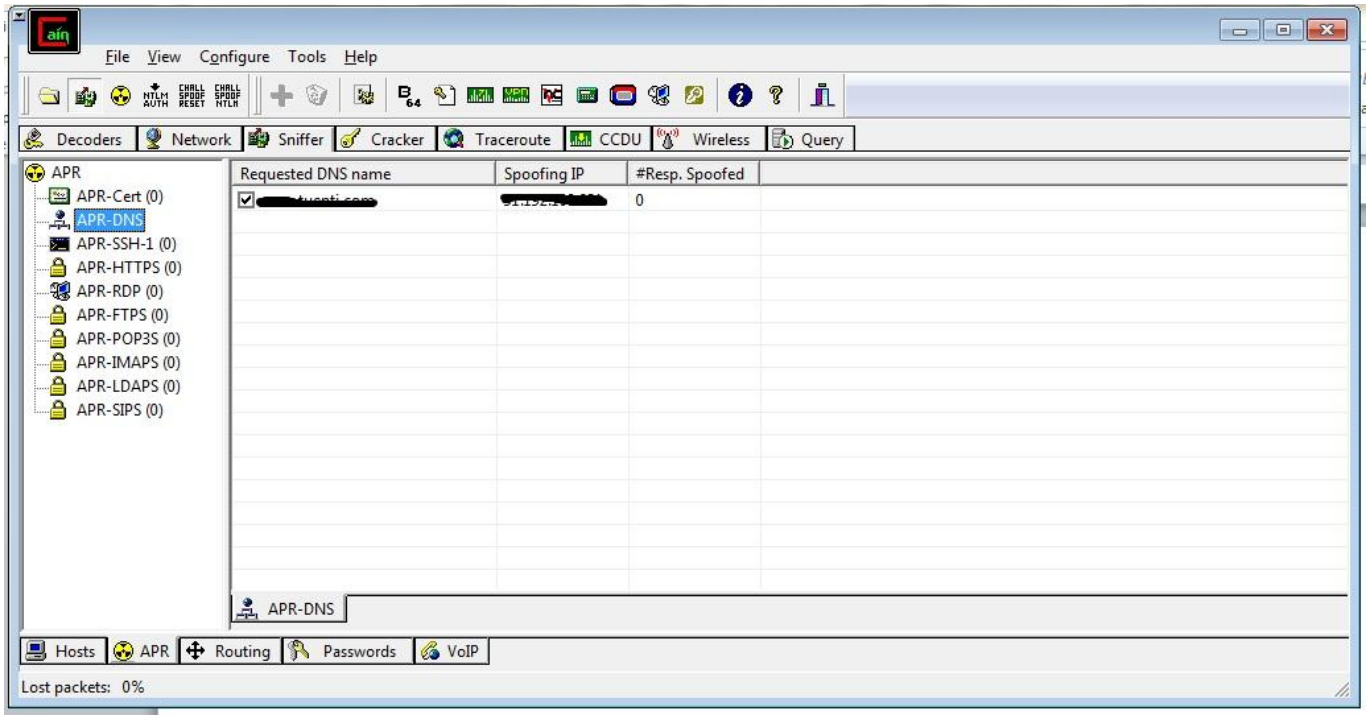
REDIRECCIONAMIENTO DNS

Bueno, hemos incluido este ejemplo debido a que es posible robar información personal complementando un DNS-Spoofing con un Phising dentro de una red.

Cain posee una funcionalidad la cual permite que al teclear una dirección web, en vez de que el protocolo DNS resuelva el nombre de dominio a la IP que le corresponde, lo haga hacia otra (arp spoofing), ¿Qué permite eso además de echarte unas risas viendo como tu compañero de piso, al intentar acceder a www.ujaen.es, es redireccionado a una página de contenido para adultos? (algo un poco infantil, la verdad ☺). Pues bien, podríamos crear en nuestra máquina un servidor http en el cual creemos una web igual (o bastante similar), a alguna otra, como por ejemplo, Gmail, Hotmail, entidades bancarias… etc (PHISING) y hacernos con los datos de algunos usuarios.

Veamos cómo hacer que DNS resuelva a una dirección falsa con Cain:

El método para ver los hosts que están conectados a la red y del envenenamiento es el mismo que en el apartado anterior, sólo que ahora, nos vamos la siguiente pantalla:



Para añadir más direcciones falsas, pinchamos con el botón derecho sobre una casilla vacía y picamos en ‘add to list’.

Por último, pulsamos en el botón de envenenamiento ARP para que se haga efectivo (botón amarillo de la barra de herramientas).

NOTA: Si al practicar el ataque detectamos que dejamos a la víctima sin conexión, vamos a la siguiente ruta del registro de Windows: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, y cambiamos el valor de la variable ‘IPEnableRouter’ de 0 a 1.

DETECCIÓN DEL ATAQUE

Es difícil detectar este tipo de aplicaciones (Wireshark o Cain), ya que son programas que trabajan de manera pasiva, y no dejan casi huellas, por no decir ninguna. Mucha de la información que circula por la red lo hace en texto plano, pudiendo acceder desde cualquier ordenador de una misma red a esa información confidencial mediante un simple sniffer, como hemos ido viendo a lo largo de esta guía.

A continuación vamos a ver algunas de las técnicas para intentar detectar un ataque 'Man in the middle', no son excluyentes una con otra, así que podemos combinarlas como nos parezca.

ACCESO A LA MAQUINA

Este es el más improbable, por decirlo de alguna manera. Si tenemos acceso físico a las máquinas que forman parte de la red y podemos ver para cada una la lista de aplicaciones y procesos activos, podríamos detectar si existe algún proceso que pueda ser de tipo sniffer. A veces estos programas se ejecutan al iniciar la máquina o bien cuentan con alguna entrada en el registro del sistema.

Por ejemplo, Wireshark, en el caso de no estar ejecutándose pero sí estar instalado, podemos comprobarlo en el registro de Windows, en la siguiente ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Uninstall\Wireshark.

PRUEBA DE ICMP

Vamos a realizar un ping a la dirección IP que deseemos para analizar el retardo de los paquetes. Una vez visto el resultado, creamos conexiones TCP falsas en esa red durante un período de tiempo y esperamos a que el posible sniffer procese estos paquetes, incrementando de esta manera el tiempo de latencia. Si cuando volvamos a analizar el retardo del ping vemos que el tiempo en milisegundos aumenta considerablemente, es posible que tengamos un sniffer en nuestra red.

PRUEBA DE ARP

Este test se basa en realizar una petición tipo ICMP echo (ping) a la dirección IP que queramos pero con una MAC errónea. Para esto, podemos agregar a nuestra tabla ARP la dirección que queramos, es decir, incluir la dirección MAC errónea mediante los comandos que nos ofrece ARP, por ejemplo:

Para agregar una nueva entrada a la tabla ARP podemos teclear el comando:

- Arp –s [IP] [MAC]

Se sobreentiende que la MAC es falsa, si posteriormente tecleamos arp -a (muestra el contenido de la tabla) vemos que se añade.

Si la dirección MAC es incorrecta el paquete enviado no debería de llegar a su destino, pero en algunos sistemas, al estar en modo promiscuo debido a la utilización de un sniffer, este atenderá el paquete. Si vemos que el paquete llega a su destino, es que la tarjeta de red está en modo promiscuo, y por lo tanto podemos tener un posible sniffer en la red.

APLICACIONES PARA DETECTAR SNIFFERS

Por último vamos a ver algunas aplicaciones para detectar sniffers:

- Antisnif
- Sentinel
- CPM
- SniffDet
- NEPED
- Promiscan
- Promisdetec
- ProDETECT

Incluso Microsoft sacó su propia herramienta de detección de sniffers llamada PromgyrUI, que trae una interfaz muy sencilla.

La herramiento Antisniff creada tanto para Windows como para sistemas Unix, lo que hace es probar los dispositivos de red para ver si alguno de ellos se está ejecutando en modo promiscuo, usa técnicas de test DNS, ping de latencia y test de ARP. La herramienta no está diseñada para detectar sniffers de investigación o propósito especial, sino más de uso comercial. Es bastante fácil de usar, se introduce el rango de direcciones IP a analizar y la aplicación busca el posible sniffer en la red.

Otra herramienta de detección de sniffers es Sentinel. Hace uso de las librerías Libcap y Libnet. Es parecida a Antisnif, ya que también se encarga de detectar técnicas en modo promiscuo, y usa test de dns, test de ICMP, ping de latencia y test de ARP.

CPM es una aplicación creada por la universidad Carnegie Mellon, que se encarga también de ver si la interfaz de la máquina está en modo promiscuo.

NEPED se utiliza para detectar la intrusión de sniffers, realiza peticiones de ARP para cada dirección IP de la red, destinando los paquetes a una dirección inexistente, no a broadcast. Las interfaces que estén en modo promiscuo contestarán a estas peticiones.

La aplicación SniffDet se basa en realizar pruebas de posibles protocolos que nos pueden llevar a la detección de un sniffer, prueba de ARP, test de ICMP, test de DNS, y test de ping de latencia.

Las herramientas Promiscan, Promisdetec y proDETECT han sido creadas para sistemas Windows y tratan de detectar los hosts que se encuentran en modo promiscuo en redes LAN.

PROTECCION FRENTE A SNIFFERS

La mejor protección frente a los sniffers es proteger la información que enviamos mediante algún tipo de cifrado. Las técnicas de encriptación que cifran y descifran la información hacen posible el intercambio de mensajes de manera segura para que sólo pueda identificar la información el receptor de la misma. Algunas de las técnicas que podemos usar como protección frente a los sniffers son:

- PGP (Pretty Good Privacy): Uso de clave pública y clave privada.
- SSL (Secure Socket Layer): proporciona autenticación privada en páginas web mediante el protocolo https, aunque hemos visto que no es demasiado eficaz ante un ataque como el explicado anteriormente.
- SSH (Secure Shell): Conexión remota a terminales de manera segura.

CONCLUSIÓN

Como hemos podido ver, con unos básicos conocimientos sobre redes y algunas sencillas aplicaciones que cualquiera puede encontrar en la red, se puede comprometer la confidencialidad de la información personal hasta el grado de poder espiar a una persona. ¿Qué queremos decir con esto? , pues que hay que tomarse la seguridad en redes mucho más enserio, tanto los usuarios, como los administradores de las mismas, por ejemplo, las empresas desarrolladoras de las aplicaciones que envían sus mensajes en texto plano, deberían incorporar algún mecanismo de cifrado a las mismas para evitar estas situaciones.

Hablamos de que las compañías deberían implementar medidas de seguridad en sus aplicaciones, pero, ¿y los usuarios con menos formación?, es su responsabilidad asegurarse de que su información se mantiene lo más segura posible en la red, manteniéndose al tanto, al menos de algunas técnicas básicas para aumentar su seguridad. Las grandes empresas de informáticas como Microsoft, ponen a disposición de los usuarios aplicaciones sencillas como PromgyrUI, explicada anteriormente.

Llegando a este punto, se plantea una cuestión, ¿Quién es aquí el ‘delincuente’, aquella persona que demuestra las vulnerabilidades de un sistema o aquellos que no se hacen cargo de ellas? Desgraciadamente, la gran parte de la sociedad en la que vivimos ve con malos ojos a aquellas personas que trabajan por unos sistemas más seguros.

REFERENCIAS

Para la última parte de 'Detección del ataque' y 'protección frente a sniffers', nos ha servido el libro:

Hackers, edición 2009 (Anaya Multimedia).

Para realizar los diferentes ejemplos, webs y foros como, por ejemplo:

http://www.dragonjar.org/ Comunidad de investigadores, estudiantes, profesionales y entusiastas de la Seguridad Informática.

http://foro.elhacker.net elhacker.net es una de las comunidades de seguridad e informática más grandes de habla hispana.

http://www.vidainformatico.com Blog donde se tratan temas relacionados con la informática, tecnología, Internet, aplicaciones, gadgets…

http://casidiablo.net Blog sobre hacking en general y programación

http://www.flu-project.com Flu project es un proyecto que nace de la inquietud de dos mentes por iniciar un proyecto en comunidad sobre la temática de la seguridad de la información y el malware, en el que todos los usuarios puedan participar para compartir sus conocimientos y aprender de otros usuarios.