TEMA

Tema 7. Seguridad en Redes Corporativas

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 7: Seguridad en Redes Corporativas

¿Qué aprenderás?

- Qué es un Ataque de Denegación de Servicio
- Qué es un Man in The Middle
- Para qué sirve el WireShark
- ¿Cómo puedes hacer tu red inalámbrica más segura

¿Sabías que…?

- Con un ataque MiTM pueden tomar el control de tu cuenta de Facebook

6.1. INTRODUCCION

En este tema vamos a tratar al sistema informático que defendemos, no desde el punto de vista individual, sino desde el punto de vista de la red de una empresa. Por lo tanto, no vamos a hablar de la información que almacenamos y las amenazas que puede sufrir (Malware) sino de cómo transmitimos esa información y cómo se accede a ella, interna y externamente a la red.

Para ello lo primero que hemos de tener claro es el concepto de Comunicación Segura. Un Sistema Informático tiene comunicaciones seguras cuando cumple con:

- Autentificación: Existe un control de usuarios y equipos
- Autorización: Existe una política de permisos clara
- Integridad de los datos: La información que se transmite es comprobada en destino con algoritmos Hash y MD5
- Confidencialidad: La información se transmite cifrada
- No repudio. Se utilizan Firmas Digitales para que el emisor de la información no pueda negar su envio

Si nos damos cuenta, muchos de estos puntos ya los hemos tratado en temas anteriores.

6.2. AMENAZAS PARA UNA RED CORPORATIVA

Vamos a analizar qué tipo de amenazas nos podemos encontrar cuando tenemos un intruso dentro de nuestra red.

6.2.1. Interrupción de servicio.

El Ataque de denegación de servicio **DoS** y su variante mejorada **DDoS**, busca que un servicio de nuestro sistema no pueda continuar trabajando por saturación. Ya hablamos de él y no seguiremos tratándolo.

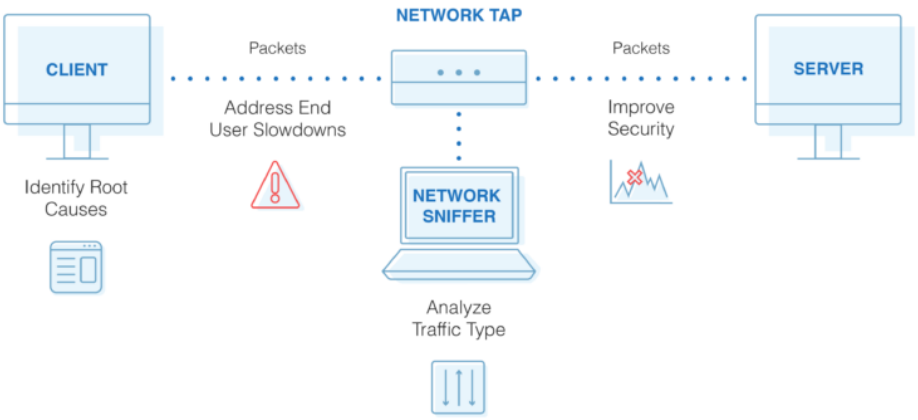
6.2.2. Interceptación de información de la red (Sniffing)

Este es uno de los puntos más interesantes. Se trata de una técnica por la cual se puede escuchar todo lo que circula por una red. Para ello se utilizan aplicaciones que actúan sobre todas las partes que componen el tráfico de la red: usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red.

¿Cómo funciona un Sniffer?

Para que lo entendáis mejor vamos a centrarnos en el caso de una red Ethernet.

El **Sniffer** es un programa que se conecta con la tarjeta ethernet de la red que le digamos, activando el modo promiscuo de esta (este modo hace que la tarjeta no ignore el tráfico que no va destinado a ella), y empieza a leer todo el tráfico que entra y sale por ella. También es capaz de leer la información de broadcast (255.255.255.0) que pase por la tarjeta.

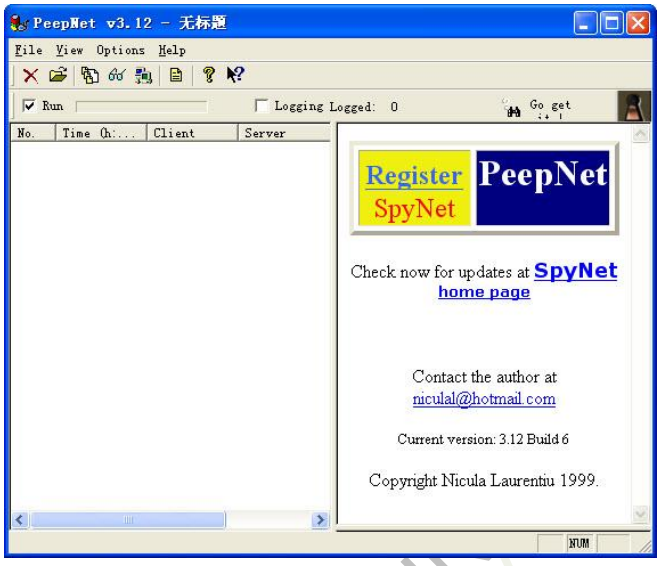


Fuente: 1https://www.dnsstuff.com/packet-sniffers

¿Qué Sniffers son los más conocidos?

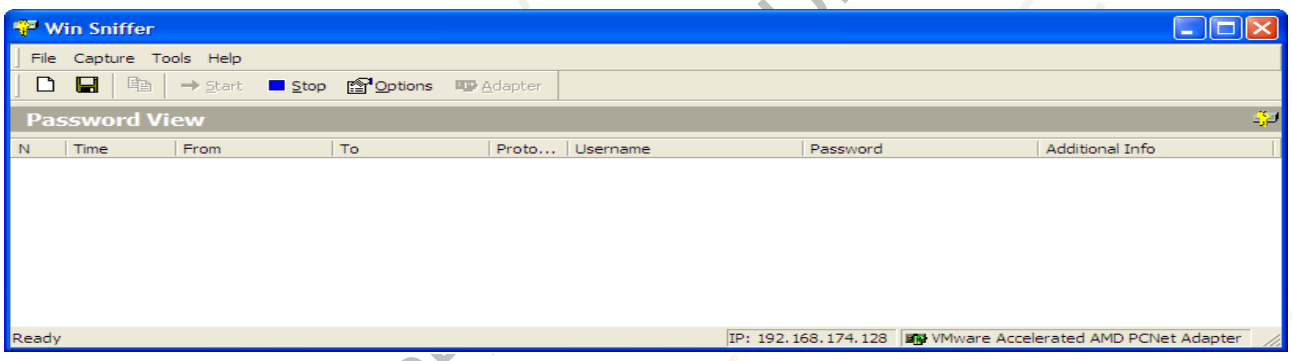
6.2.2.1. **SpyNet**

Está compuesto por dos programas: CaptureNet y PeepNet. CaptureNet se dedica a guardar los paquetes de datos que espía en formato de bytes hexadecimales. PeepNet analiza los datos recopilados, reconstruye los paquetes para obtener: los correos, las contraseñas utilizadas, direcciones de los ordenadores, protocolos, los navegadores utilizados y el sistema operativo.



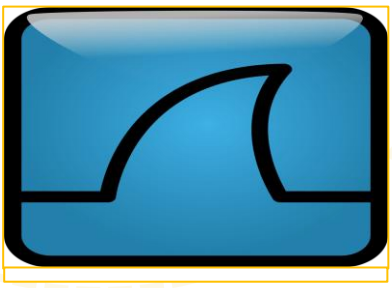
6.2.2.2. **WinSniffer**

Es un Sniffer especializado en obtener contraseñas. Busca en toda la red accesos de usuario/contraseña y los muestra por pantalla.



6.2.2.3. **Ethereal o WireShark**

Este Sniffer se considera "bueno" pues se diseñó para solucionar problemas y monitorizar cambios en las redes. Es capaz de descifrar paquetes de forma inteligente en función de su protocolo. Es muy popular pues funciona en UNIX y Windows y en su web ofrece una gran cantidad de recursos para aprender a utilizarlo.



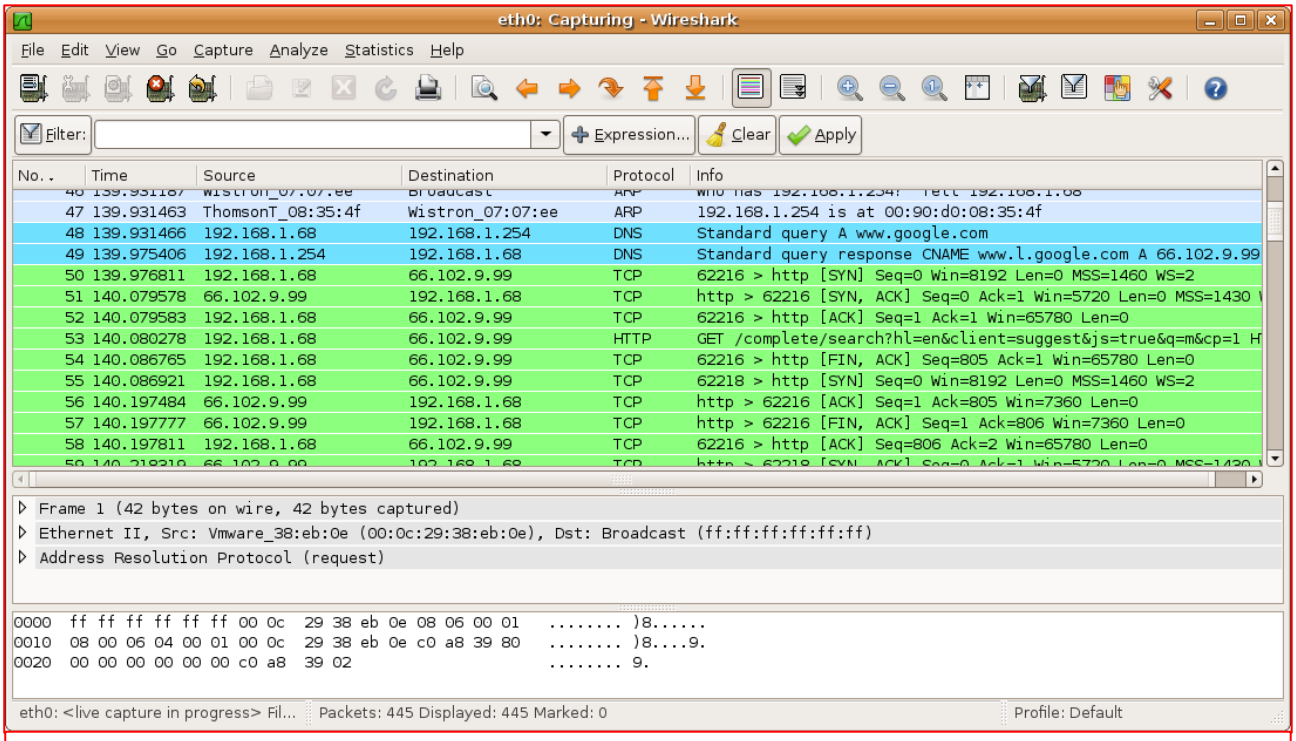


Ilustración 1 Monitoreo de la red

6.2.2.4. **Acrylic WiFi**

Es un Sniffer gratuito que podemos utilizar para analizar las comunicaciones y seguridad de nuestra red Wifi. Nos muestra información sobre los puntos de acceso y los dispositivos conectados a ellos.

6.2.2.5. Otros más profesionales

- SolarWinds Network Performance Monitor
- Paessler PRTG Network Monitor
- ManageEngine NetFlow Analyzer
- Savvius Omnipeek
- Colasoft Capsa

¿Cómo se infiltra un Sniffer en el sistema?

Los Sniffer no son virus, no se propagan por si mismos y deben estar controlados por alguien.

Por ello para su instalación en el sistema:

- Debe instalarse manualmente por el administrador o por cualquier usuario con permisos suficientes. El usuario no tiene conocimiento.
- Vienen con otro malware, virus, troyanos o gusanos

Hablemos también de qué pasa en las redes públicas. Supongamos que estamos en un aeropuerto y llevamos un móvil y un portátil. Como es normal, hay gente conectada a la red wifi del aeropuerto o a la del bar del aeropuerto o buscando una red que no sea lenta (lo que suele pasar a las redes que he comentado ya que hay mucha gente conectada). Lo primero que voy a hacer es crear una red wifi con mi móvil, sin contraseña y que llamaré WIFI_AEROPUERTO. Seguro que con ese nombre y abierta, hay gente que se me conecta. Lo segundo que voy a hacer es abrir mi portátil, conectarme a mi móvil y abrir el Sniffer. Mirando la pantalla podré ver las autentificaciones (usuario/contraseña) de la gente que está utilizando mi red wifi. OJO ESTO ES ILEGAL. NO LO HAGÁIS. ES SOLO UN EJEMPLO EXPLICATIVO DEL FUNCIONAMIENTO DE UN SNIFFER.

¿Cómo evitamos que nos monitoreen?

La medida principal que podemos tomar es cifrar la información. No evitaremos que el tráfico sea capturado, pero al estar encriptada es ilegible. Por ejemplo, si trabajamos con páginas HTTPS estamos utilizando un canal cifrado para que la información circule por ella cifrada.

Otra medida a tomas es trabajar con certificación y claves. Si nos detectan la clave pública o la privada, ya sabemos que por sí solas no sirven para nada.

La tercera medida ya la comenté en otro tema. No os conectéis a redes abiertas.

¿Cómo los elimino?

Ten en cuenta que un Sniffer no es malware, por lo tanto, no pueden ser detectados por lo programas antimalware y por eso necesitamos un programa antispyware bueno o nos toca detectarlos y eliminarlos manualmente. Una forma de detectarlos es ver si una interfaz de red está en modo promiscuo con el comando:

```
$ ifconfig -a

eth0 Link Encap: 10Mbps Ethernet HWaddr: xx:xx:xx:xx:xx:xx
inet addr: a.b.c.d Bcast: a.b.c.f Mask: m.m.m.m
UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1 (OJO: Modo
promiscuo)

RX packets: 0 errors:0 dropped:0 overruns:0TX packets:0 errors:0
dropped:0 overruns:0

Interrupt:15 Base Address:0x300
```

O también podemos utilizar programas diseñados para ello:

- CPM (Check Promiscuous Mode)
- NEPED
- Antisniff
- Sentinel
- SniffDet – Remote Sniffer Detection
- PromiScan
- PromiscDetect

6.2.3. Modificación de la información

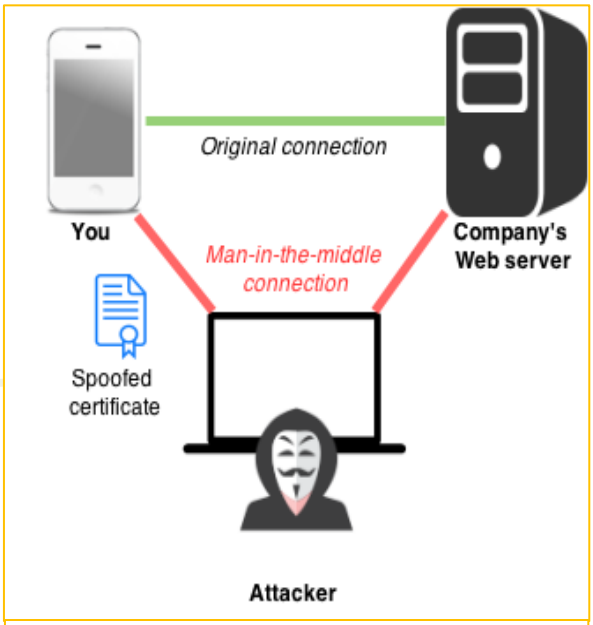
Ya estamos dentro de la red corporativa, podemos monitorear el tráfico que se está produciendo y ahora voy a dar un paso más… Man in The Middle MiTM)

El **ataque Man in The Middle** consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por nosotros y así poder desencriptar sus datos, contraseñas…

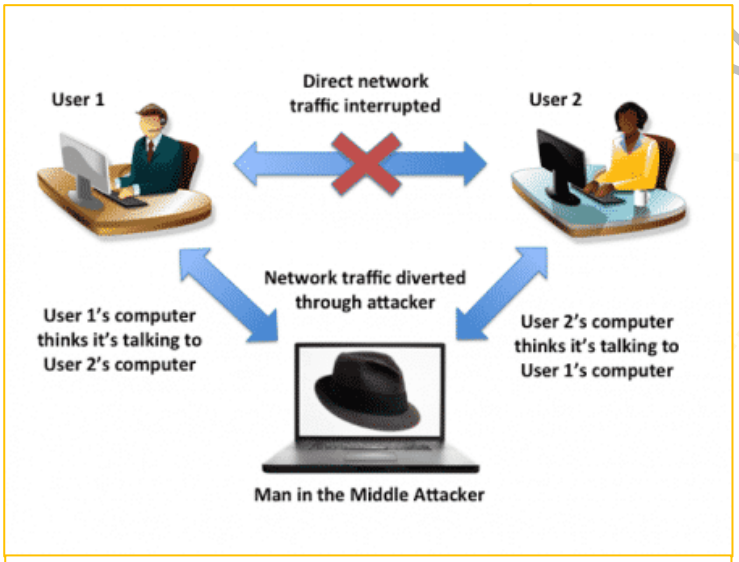
Para este ataque se necesita de dos máquinas que son las víctimas, una podría ser el servidor de la red o el router y el equipo de nuestra víctima real. A parte, lógicamente está nuestra máquina.

Si estamos haciendo un **MiTM** al correo de la empresa, por ejemplo, lo que haremos es desviar todos los correos a una dirección alternativa para leer y alterar toda la información antes de enviarla al destinatario correcto.

Otra modalidad podría ser el crear facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos.



Esta foto de Autor desconocido está bajo licencia



Esta foto de Autor desconocido está bajo licencia CC BY

¿Cómo nos podemos proteger?

Para protegernos de estos ataques, es necesario utilizar siempre sitios web HTTPS, activar la verificación en dos pasos y usar una red Virtual VPN pues la comunicación entre servidor VPN y cliente VPN está cifrada.

6.2.3. Fabricación de un objeto

Sobre este tema nos vamos a centrar en dos tipos de ataques bastante extendidos:

6.2.3.1. **Suplantación de identidad (Spoofing)**

Con el nombre de Spoofing agrupamos una serie de técnicas que tienen como objetivo suplantar la identidad con fines maliciosos o de investigación.

Tenemos diferentes tipo de Spoofing, pero vamos a comentar algunos:

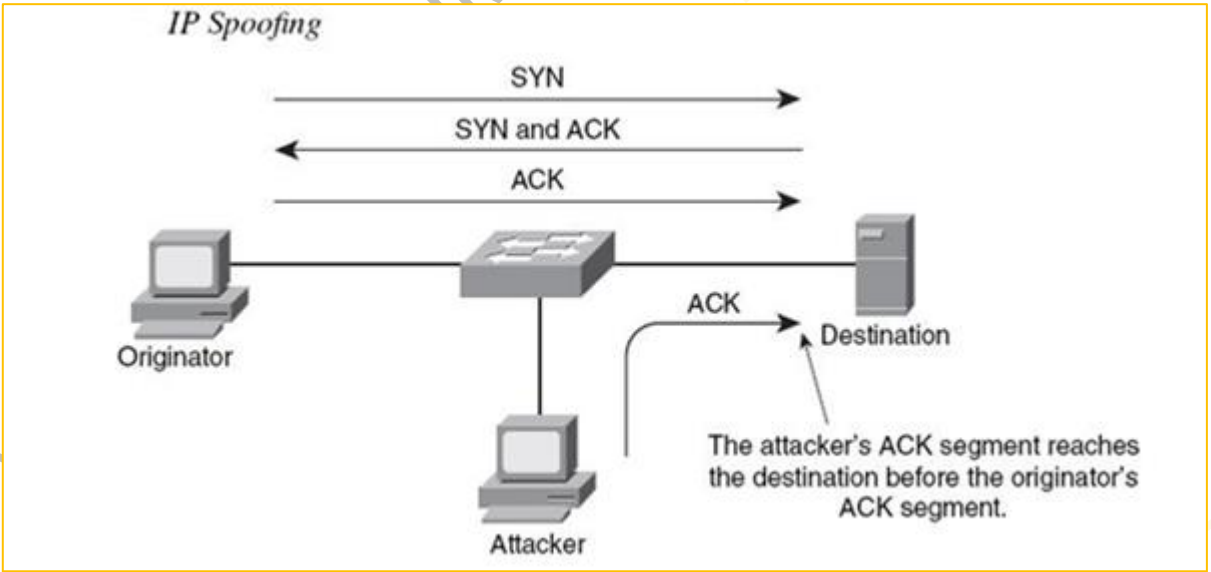
6.2.3.1.1. **IP Spoofing:**

Consiste en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP que se desee suplantar. Las respuestas del host que recibe los paquetes alterados irán dirigidas a la IP falsificada.

Para realizar esto aprovecha un elemento bastante simple. Dentro de cada paquete IP, en su encabezado, encontraremos la dirección de origen y de destino del paquete.

¿Cómo nos protegemos?

Tenemos dos métodos, establecer una solución integral de filtrado de paquetes entrantes y salientes en el router, y utilizar siempre métodos de autentificación cifrados.

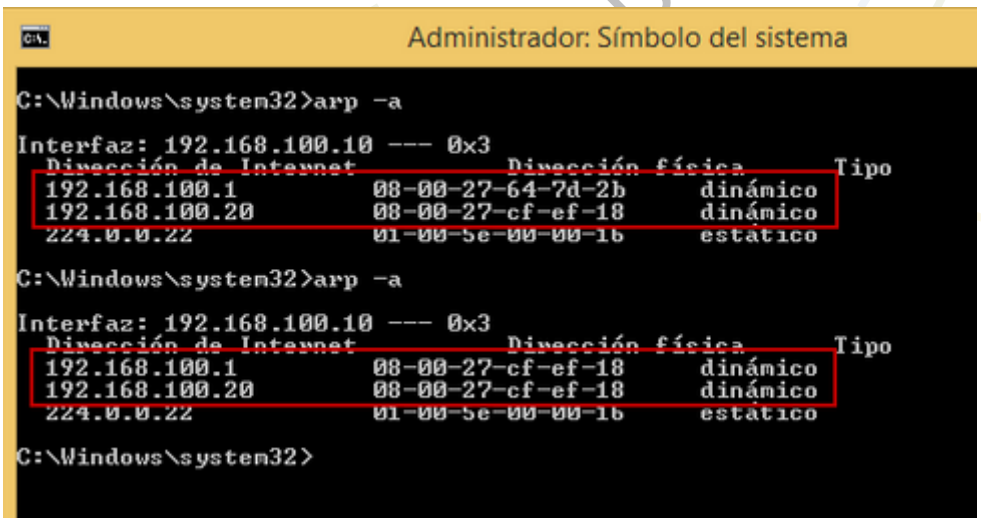


6.2.3.1.2. **ARP Spoofing**

Este ataque se realiza en redes de área local que utilizan el protocolo de resolución de dirección ARP. Con este protocolo la resolución de una IP se realiza con la dirección MAC de la tarjeta. Como sabemos, cuando queremos localizar una máquina en una red realizamos una petición (ARP Request) a toda la red, esperando la respuesta del destinatario (ARP Replay) con su dirección MAC. Estas respuesta se almacenan en una tabla (caché ARP) donde se almacenan temporalmente para no tener que hacer constantemente peticiones. ¿Qué pasa si el que responde antes no es el destinatario sino mi host malo? Pues en esto consiste, en suplantar las tramas ARP. Esto se consigue enviando mensajes falsificados ARP a una LAN. Como resultado, al atacante vincula su dirección MAC con la dirección IP de un equipo legítimo (o servidor) en la red.

¿Cómo nos protegemos?

Lo primero, y más pesado, es utiliza registros ARP estáticos no dinámicos. Otra medida a tomar en una LAN es subdividirla realizando subnetting y así filtrando peticiones de difusión incontroladas. Por último, y como siempre, un software de monitorización de redes.



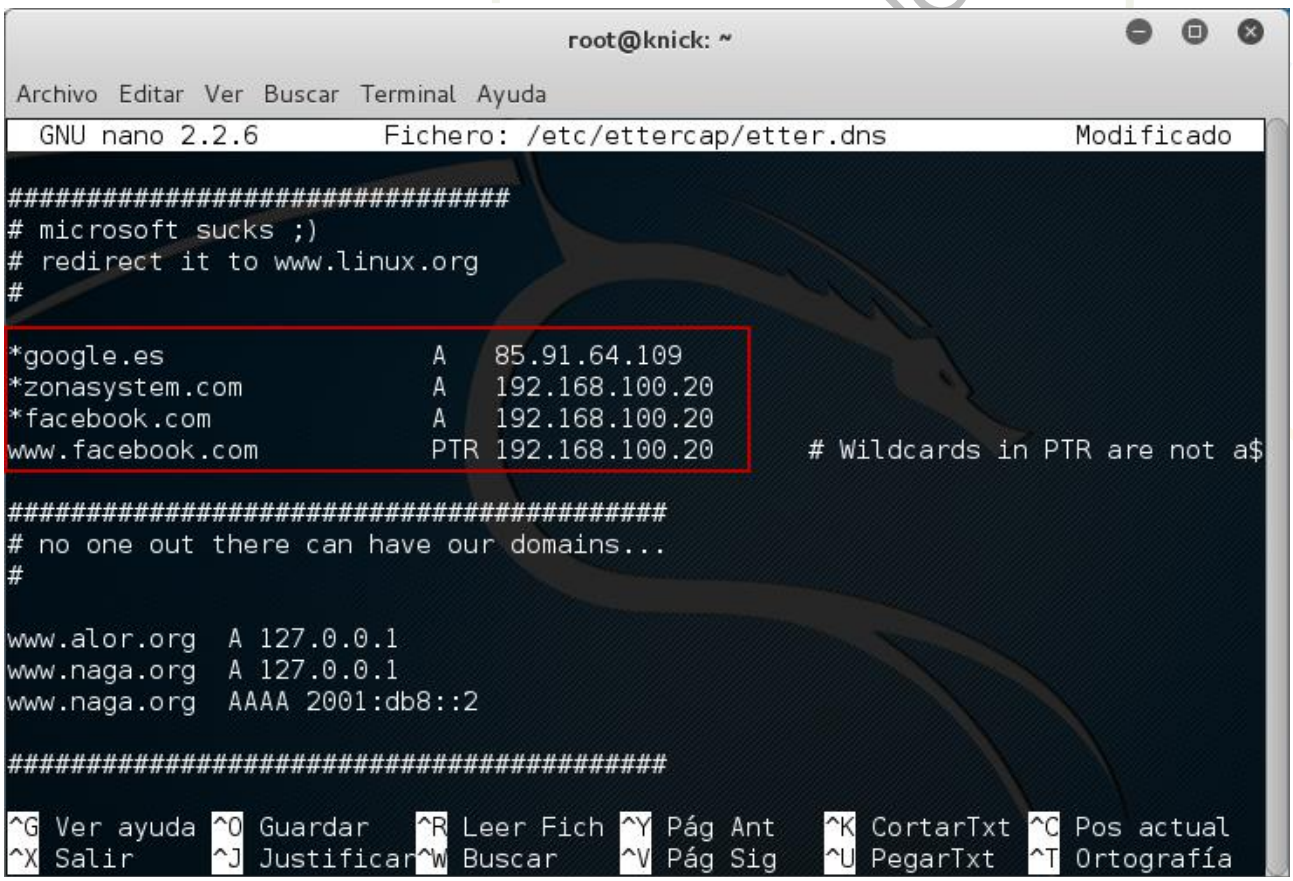
6.2.3.1.3. **DNS Spoofing:**

Consiste en alterar las direcciones de los Servidores DNS que utiliza la víctima, sustituyéndolos por otros servidores maliciosos y de esta forma poder tener el control sobre las consultas que se realizan.

Para ello montaremos un servidor DNS falso que sea una réplica de aquel del que deseamos obtener la información por parte de la víctima. Cuando el usuario quiere acceder al sitio web legal, lo direccionaremos al sitio espejo y así obtendremos toda la información. Aun utilizando sitios web HTTPS funcionará pues también podemos cifrarla.

¿Cómo nos protegemos?

Primero, deshabilitar la opción de gestión remota de los routers o utilizar una contraseña muy fuerte. Después, tener el sistema operativo actualizado, los programas (sobretodo Java) y los navegadores. Y, por último, fijarnos si la web a la que nos conectamos utiliza HTTP cuando debiera utilizar HTTPS.



6.2.3.1.4. **Web Spoofing:**

Consiste en suplantar una página web real por una falsa, para conseguir los datos del usuario. La página falsa actúa como un proxy, y así es posible solicitar información que el usuario a pedido al servidor original sin que la víctima se dé cuenta.

Para poder detectarlos podemos tomar las siguientes medidas:

- Comprobar en la barra de estado la URL a la que apunta el enlace
- Comprobar en la línea de navegación la URL y ver si és demasiado larga
- Comprobar el código fuente de la web

6.2.3.1.5. **E-mail Spoofing.**

Consiste en suplantar la dirección de correo en el campo FROM por una falsa para que cuando contestes la información la reciba otra persona diferente de la que crees.

Se puede hacer esta modificación porque el protocolo SMTP (Simple Mail Transfer Protocol) que utilizamos para enviar correos electrónicos, no incluye ningún mecanismo de autenticación. Se puede entrar en un servidor de correo, y con una serie de comando modificar las cabeceras de los correos.

¿Cómo nos protegemos?

La forma más común es utilizando SPF (Sender Policy Framework), que es un sistema de protección que se aplica a los servidores de correo electrónico.

Cuando recibe un correo el servidor de correo, SPF realiza un buen trabajo, ya que mediante la IP y los registros DNS del Servidor DNS, identifica los servidores de correo SMTP autorizados para enviar mensajes desde el dominio del emisor.

6.2.3.2. **Tablas DNS Falsas (Pharming)**

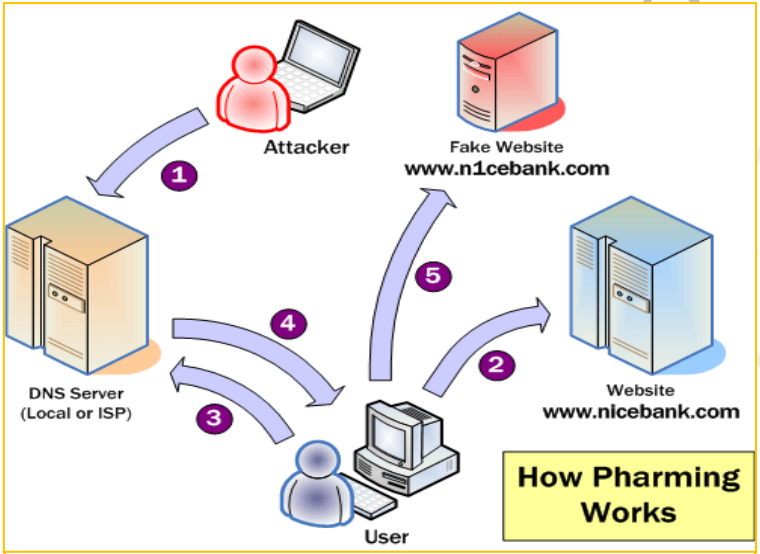
Este ataque consiste en que nos colamos en el Servidor DNS y cambiamos las tablas DNS con la relación entre dirección IP y URL, sustituyéndolas por direcciones IP de servidores web malvados.

Estos sitios web falsos contienen virus o troyanos o recopilarán información del usuario para robarle la identidad.

En este ataque el usuario no puede hacer nada, pues no depende nada de él sino de su servidor DNS.

¿Qué podemos hacer?

Poco podemos hacer. Estar preparados con soluciones anti-malware por si entramos en algunas de estas webs.



6.3. SEGURIDAD EN LAS REDES INALAMBRICAS

Bueno, bueno, llegamos a uno de los quebraderos de cabeza que tenemos los administradores de sistemas, las redes inalámbricas.

¡Qué felices viviríamos si toda la infraestructura de red de nuestra empresa fuera una red cableada! Pero no, con el paso de los años la irrupción de dispositivos móviles ha provocado que tengamos que incorporarlos en nuestro sistema informático. Lógicamente, era inevitable. Todos tenemos alguno de estos dispositivos y era cuestión de tiempo que el responsable de la empresa nos pidiera conectarse a la red de la empresa desde dentro de esta, por ejemplo.

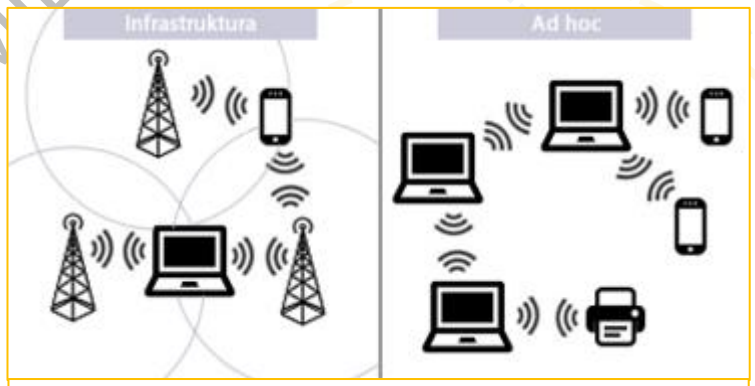
Pero claro, un dispositivo que puedo utilizar fuera de la empresa, que lo conecto a una red abierta de un centro comercial, que se infecta y que una hora después lo tengo en la empresa consultando información, ¡pues nos debe preocupar!

El estándar de comunicaciones más utilizado en la actualidad en redes locales inalámbricas (WLAN) es el llamado **IEEE 802.11, o Wi-Fi.** Este estándar se diseñó para facilitar la conexión entre dispositivos con un protocolo de seguridad llamado **WEP**.

En el protocolo IEEE 802.11 se denomina a los dispositivos como estaciones. En esta estructura dos o más estaciones se pueden comunicar entre sí si están lo suficientemente próximas.

Esta conexión es de dos tipos:

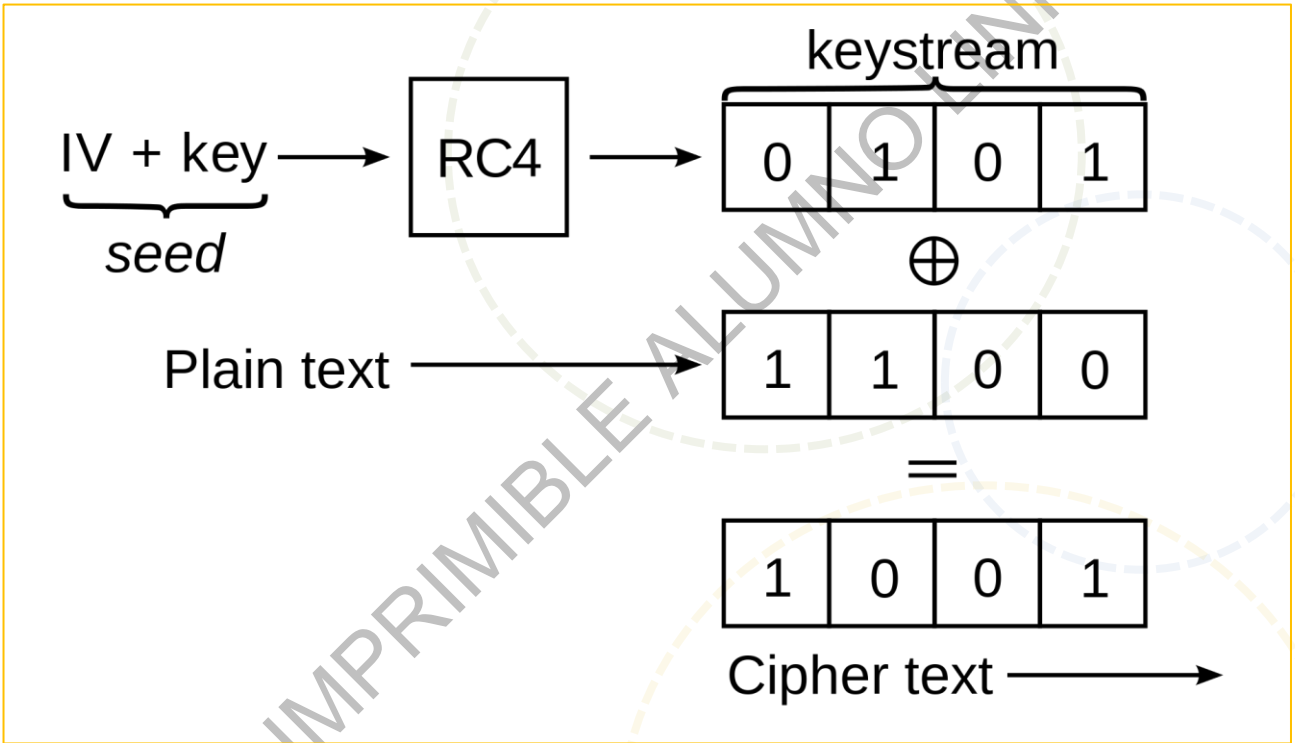
- **Ad-hoc**: Formando una red aislada donde las únicas comunicaciones posibles son las directas de una estación a otra



- **Infraestructura**: Una de las estaciones se denomina **Punto de Acceso (AP)** y permite la interconexión con otras redes, con o sin hilo. Este AP anuncia su presencia enviando periódicamente tramas baliza, cada aprox. 100 ms. En esta trama indica el nombre de la conexión (**SSID**) de la red, su velocidad de transmisión, etc.

Una estación (mi portátil) puede asociarse con el AP que quiera. Pero solo con uno a la vez. Desde ese momento toda la información de la comunicación se realiza a través de ese AP. Pero para poder asociarme al AP debemos antes haber realizado una Autenticación. Esta autenticación puede ser de diferentes formas:

- **Abierta**: El AP se configura para que cualquier equipo se conecte
- **Clave Compartida WEP**: El AP tiene una clave WEP preconfigurada. El AP manda un mensaje (**keystream**) a la estación que se quiere conectar. Esta estación responde con el mismo, pero cifrado con la clave WEP. Esto es un protocolo de clave simétrica.



Este sistema tiene varios problemas:

- El cifrado WEP no es complicado de descifrar para un atacante. Está basado en el **algoritmo RC4**, un algoritmo con poca complejidad de cálculo y bastante simple. Trabaja con claves de 64 a 128 bits. Puede tener preconfiguradas hasta 4 claves secretas para poder trabajar con grupos de estaciones diferentes o ir cambiando periódicamente de clave.
- La respuesta de la estación no incluye información sobre la estación. Por lo tanto, si interceptamos el mensaje cifrado podremos autentificarnos en el AP.

¿Cómo podemos atacar una clave WEP?

Os comento algunas:

- Inyección de tramas. Un capturamos una trama WEP correspondiente a una asociación puede retransmitirla tantas veces como quiera y el AP dará la trama como válida. Pero si cambiamos la dirección del AP de la trama, la estación también la puede dar como válida y conectarse.
- Falsificación de la autentificación. En la autenticación se intercambian 4 tramas: petición de autenticación, reto, respuesta y resultado. En la segunda trama tenemos la clave simétrica, si la capturamos y obtenemos, desciframos la tercera, la respuesta y obtenemos el mensaje. Con el mensaje y la clave, generamos la respuesta y accedemos al AP
- Ataque chopchop. Las tramas WEP tienen un código de integridad (ICV). Este código nos asegura que la información que se envió y la que llegó son iguales. No se han modificado por el camino. Este ICV se genera con el algoritmo CRC-32. Este algoritmo no es criptográfico, por lo que es posible realizar los cálculos inversos. Estos ICV se ubican al final de la trama, por lo que al capturar una trama solo tenemos que generar los 256 valores posibles de 1 y 0, añadirlos al final y enviarlos al AP hasta que demos con el bueno.

¿Y cómo hago estas cosas?

Os comento algunas de las herramientas de que se dispone:

- La herramienta **airmon-ng**. Con esta herramienta ponemos la tarjeta Wifi en modo promiscuo y así podemos capturar todas las tramas de todas las estaciones que tengamos en nuestro radio de acción.
- La herramienta **airplay-ng**. Esta herramienta permite inyectar tramas nueva o previamente capturadas, generando tramas WEP de respuesta para poder sustituir a un AP legal.
- La herramienta **aircrack-ng**. Esta herramienta recupera la clave WEP.
- La herramienta **airdump-ng**. Esta herramienta captura las tramas que detecta y las guarda en un fichero. El fichero que genera puede guardar o la información que necesita la herramienta aircrack-ng o los primeros bytes de keystream de cada trama, consiguiendo al final el mensaje

- **Clave compartida WPA**: Esta modalidad apareció en el estándar IEEE 802.1X. La mejora que respecto a WEP es que la autenticación se realiza en la estación y en el AP, por lo que la estación se autentifica ante el AP pero el AP se autentifica ante la estación. No puede haber un AP falsificado.

  El uso de WPA consiste en el uso de diferentes claves en cada una de las asociaciones y en utilizar claves dinámicas. El sistema de cifrado se denomina **TKIP** y consiste en que generamos:
  - Una clave temporal de 128 bits que cambia cada 10.000 paquetes
  - La dirección MAC
  - La Clave PSK

  Por medio de un Algoritmo RC4 generamos la encriptación.

  ¿Cómo se produce la autenticación?
  - Modo **WPA-Personal**: Se trabaja con una clave maestra prefinida (PSK) y que conocen el AP y la estación.
  - Modo **WPA-Enterprise**: Utilizamos un Servidor de Autentificación (RADIUS).

  ¿Cómo podemos atacarle?
  - Si la clave PSK es una palabra más o menos fácil de recordar, un ataque de diccionario con aircrack-ng la puede descubrir en minuto y medio.

- **Clave compartida WPA2**: Incorpora las siguiente mejoras:
  - Permite el almacenamiento de las claves en las estaciones para que la reconexión sea más rápida
  - El sistema de cifrado es el CCMP, que está basado en **AES-128**, mucho más complicado que RC4.

	WPA	WPA2
Enterprise mode (Business, education, Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal mode (SOHO, home and personal) learncisco	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

No quiero cerrar este apartado sin indicar algunas medidas a todas para aumentar las seguridad de los sistemas inalámbricos:

- Cambiar la contraseña por defecto del AP
- Actualizar periódicamente el Firmware del AP
- Utilizar WPA2 y cambiar el PSK regularmente
- Cambiar el SSID que viene por defecto y ocultarlo

Y añadimos para redes domésticas o con pocos usuarios

- Desactivar DHCP del AP
- Activar filtrado por MAC
- Limitar el número máximo de estaciones conectadas
- Verificar los usuarios que se conectan a la red periódicamente
- Apagar el AP si no se va a usar

6.4. Ataques que puedo realizar con el Ettercap (Una explicación técnica)

6.4.1. INTRODUCCIÓN

Mientras que TcpDump y Wireshark son herramientas indispensables para el administrador de la red a la hora de analizar patrones de tráfico, son también las mismas herramientas que se utilizan para tomar prestada información sensible de las personas al cibercafé y los trabajadores de empresas, en particular las contraseñas de correos y tarjetas de crédito en comunicaciones sin cifrar. La siguiente captura con TcpDump es un buen ejemplo:

Esta foto de Autor desconocido está

En estos paquetes capturados podemos observar la comunicación entre un cliente y un servidor FTP. Si estudias el contenido del paquete en detalle un daréis cuenta de que se ha capturado en el momento que el cliente se valida ante el servidor. Mediante la autentificación normal de FTP, se envía el pedido USER seguida por el nombre de usuario.

Del mismo modo, en el siguiente paquete se envía el pedido PASS seguida por contraseña. Esto puede ser una muestra de la grave consecuencia de tener comunicaciones sin encriptación: cualquier persona que sepa utilizar el Sniffer en redes no conmutadas podrá capturar datos sensibles.

Debemos precisar que esto es un problema de redes no conmutadas, donde existe un Hub como el nodo principal que comunica los hosts mediante la dirección de difusión que en concreto redirige todo el tráfico a todos los ordenadores, sin importarle que el paquete no corresponda. Hoy en día esto se ha solucionado gracias a de introducción de switch. ¡Pero, de todos modos, incluso en redes conmutadas se puede capturar tráfico!

6.4.2. El Ataque MiTM

Para realizar esto se tendrá que buscar la manera de situarse en medio de una comunicación redirigiendo el tráfico deseado en tu interfase. Estos ataques se conocen con el nombre de Hombre en medio o **MITM** (Man in the Middle). La herramienta preferida para realizarlos se llama **Ettercap**.

En su página principal ***http://sourceforge.net/projects/ettercap*** podemos leer:

"Ettercap es una suite de herramientas para ataques hombre en medio dentro de una LAN."

Provee dos métodos para monitorear el tráfico:

- **Unified**, que es el método para capturar todos los paquetes que pasen por el cable. Si el interfaz de red está en modo **promiscuo** y Ettercap recibe un paquete que no está dirigido al host será automáticamente encaminado a su destino.
- **Bridged,** que utiliza **dos interfases de red** y redirige el tráfico de una a otra manera, captura y filtra paquetes. Sería como un hombre en medio en la capa 1, ya que estará en medio de las entidades como si de un puente transparente se trate, efectivamente como parte del cable. Aquí se utilizará el primer método que resulta ser el más útil para el objetivo que se proponga.

Antes de iniciar la captura de paquetes, Ettercap también permite el uso de filtros PCAP. Sólo hace falta seleccionar del menú **Sniff-> Site pcap filter** y aparece un cuadro de dialogo pidiendo introducir el filtro deseado como ha sido descrito

Luego en el mismo menú hay que seleccionar el método de captura, que en este caso será:

Sniff-> Unified sniffing

Ettercap primero preguntará la interfaz para la captura de paquetes. Una vez elegida, aparecerán todas las opciones disponibles para el uso particular que se quiera dar a Ettercap. Antes de iniciar cualquier tipo de ataque, debemos informar a Ettercap de cuáles hosts existan en la red. Se puede dejar esta tarea en el programa, eligiendo el menú **Hosts-> Scan for Hosts** que escaneará toda la red para terminales encendidas y las guardará en una lista accesible mediante la opción **Hosts-> Host list**.

Después de haber descubierto los hosts en la red, se pueden elegir víctimas en concreto o bien dejar que Ettercap tenga como objetivo a todos dentro de la red. Elija la opción **Targets-> Select Target(s).** Aparezca un diálogo especificando el primer y segundo objetivo. En la especificación de objetivos no existe el concepto de Fuente o destino. Los dos objetivos tienen como propósito afectar el tráfico de una víctima a la otra y viceversa. El TARGET se escribe de la siguiente manera:

Dirección MAC / Dirección IP / Ip Puertos

- Dirección MAC: Debe ser única y escrita en hexadecimal como 00: 11: 22: 33: 44: 55
- Dirección IP: Se pueden especificar varias direcciones IP, separándolas con un punto y coma, así como especificando un rango con un guion medio (ejemplo: 192.168.0.1-5)
- Puerto: Se pueden especificar un rango de puertos mediante un guion medio y puertos singulares con una coma (ejemplo: 20-25,80,139)

Algunos ejemplos de Targets:

//21 Significa cualquier MAC, cualquier IP y solo el puerto 21

/192.168.0.1/ Significa cualquier MAC, solo IP 192.168.0.1 y cualquier puerto.

Una vez finalizado, elija la opción **Logging** aparecerán el lugar donde guardar los paquetes capturados y la información de cada host. Escriba la ruta y el nombre del archivo que desea utilizar para luego elegir cualquiera de las opciones del menú MITM para iniciar uno de los ataques MITM. Una vez seleccionado el método de ataque, para iniciar la captura de datos, elija la opción **Start->Start Sniffing**. En cuanto creas que tienes suficientes paquetes elija **Start> Stop Sniffing** y detiene la captura de paquetes.

6.4.2.1. **Envenenamiento del Cache ARP (ARP Poisoning)**

Para los ataques MITM, el método más utilizado es el ARP Poisoning, también llamado ARP Spoofing.

Considere un escenario donde hay tres hosts en una red conmutada. Los ordenadores se detallan de la siguiente manera:

Nombre de host	Dirección IP	Identificador MAC
A	192.168.0.1	AA: AA: AA: AA: AA: AA
B	192.168.0.2	BB: BB: BB: BB: BB: BB
C	192.168.0.3	CC: CC: CC: CC: CC: CC

El host A se comunica con el host B el host C es el atacante que quiere interceptar la comunicación entre los hosts A y B. El objetivo del host C será engañar a las host víctimas en dirigir el tráfico hacia él mismo. Anteriormente habíamos hablado de cómo los hosts intercambiaban su dirección física a través del protocolo ARP. Para evitar tener que constantemente sol • licitar el identificador MAC del ordenador con el que se requiere comunicar el sistema operativo guarda la dirección física junto con la IP que se le relaciona al cache ARP.

Para visualizar esta tabla ARP puede hacerlo introduciendo el pedido ***ARP -a*** y obtendrá una lista de direcciones físicas conocidas. Cada vez que el sistema operativo recibe un paquete ARP-replay guarda la dirección en esta caché, de esta manera simplemente hace referencia a estas tablas en hora de crear un cuadro TCP / IP y llenar el identificador MAC destinatario. La vulnerabilidad reside en el hecho de que el sistema operativo acepta los ARP-replay, aunque nunca solicite el identificador MAC mediante un ARP-request. En el escenario anteriormente descrito entonces el equipo C envía un ARP-replay creado por él mismo que relaciona su propia dirección física con la dirección IP de los otros ordenadores de la red. Es decir, el ordenador A ahora contiene a su mesa ARP el identificador MAC CC: CC: CC: CC: CC: CC relacionado a la dirección IP 192.168.0.2 y B contiene el identificador MAC CC: CC: CC : CC: CC: CC relacionado a la dirección IP 192.168.0.1

Ahora en cuanto A envíe un paquete a B, lo hace con la dirección MAC que contiene el caché ARP. El resultado es que cuando el paquete llegue al switch, este relaciona el identificador MAC con el puerto del ordenador C y lo redirige de acuerdo con esto. C, luego redirige el paquete a B para no interrumpir la comunicación y lo mismo sucede a la inversa.

Al Ettercap sólo hay que elegir la opción del menú ***MiTM-> ARP*** Poisoning y aparece un diálogo para introducir parámetros adicionales. Existen las opciones remote y ONEWAY. Con la opción remote se debe especificar si se quieren capturar los paquetes que provienen de una dirección IP remota, efectivamente envenenando el Gateway de la red, ya que los paquetes deben pasar a través. Muchas veces no es una buena decisión activar esto porque es posible que genere alertas en el momento que el router sea monitorizado. La opción ONEWAY forzará a Ettercap a envenenar sólo los primeros objetivos especificados en Target, capturando el tráfico dirigido al segundo conjunto de direcciones IP.

Si proseguimos sin ninguna opción seleccionada, Ettercap contaminará los caches ARP a los sistemas operativos enviando un ARP-replay a todos los objetivos tanto los especificados en el primer conjunto de direcciones IP como en el segundo. Al realizar esto nos podemos fijar con la tabla ARP y ver que todas las direcciones IP tienen la misma MAC. Para asegurarse de que este valor persista en el caché, Ettercap va enviando periódicamente los mismos paquetes de ARP-replay los sistemas víctima. Para detener el ataque sólo hay que elegir el menú la opción MITM-> Stop MITM attack y Ettercap restaurará las tablas ARP con los valores originales.

6.4.2.2. **ICMP Redirect**

Este ataque implementa direccionamiento ICMP. Mediante Spoofing se envía un mensaje ICMP tipo 5 a los hosts de la red:

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html

Informando a los hosts que el ordenador donde reside Ettercap es la mejor ruta para llegar a Internet. Todas las conexiones a Internet entonces serán direccionadas al atacante que a su vez encaminará los paquetes al Gateway verdadero. De esta manera se obtiene un ataque de hombre en el medio, pero sólo en una dirección. Esto es para que sólo los clientes serán redirigidos, el Gateway enviará los paquetes de respuesta directamente al ordenador víctima. Este método requiere el identificador MAC y la dirección IP del Gateway de red.

6.4.2.3. **DHCP Spoofing**

Este ataque implementa un engaño mediante Spoofing con el uso del protocolo DHCP. Ettercap pretende ser un servidor DHCP y trata de ganar al verdadero servidor DHCP para forzar a los ordenadores cliente que han pedido una dirección IP a aceptar su dirección IP a aceptar su respuesta. De esta manera Ettercap manipula el parámetro del Gateway informando a los ordenadores clientes que, para llegar a Internet, deben hacerlo mediante el atacante. Este resulta también en un ataque de en medio en una sola dirección, ya que los paquetes de respuesta de los servidores remotos serán enviados directamente desde el Gateway al ordenador víctima. Se deben pasar como argumentos el conjunto de direcciones IP, la máscara de red y la dirección IP del servidor DNS. Es importante dar un conjunto de direcciones IP que no estén en uso, ya que Ettercap no sabe distinguir cuáles han sido ya dadas y tienen actividad de las que no

Este método se arriesgado, si especifica una lista de direcciones IP que ya están en uso, podría denegar los servías dentro de la red. Utilice este ataque cautelosamente.

¡En cuanto decidas parar el ataque, los ordenadores afectados seguirán pensando que Ettercap es el Gateway hasta que expire la dirección IP asignada!

6.4.2.4. **Port Stealing**

Port Stealing (préstamo de puerto) es una técnica efectiva en redes conmutadas cuando el envenenamiento ARP no es efectivo. Sucede por el valor asignado a la variable ***port_steal_delay*** a ***etter.conf***., Puesta a 10 milisegundos por defecto. Este valor se puede bajar para obtener mejores resultados. Al interfaz GTK si no se especifica la opción ***Propagate to other switches,*** la red es inundada con paquetes ARP que contienen en el campo identificador MAC destino, la misma que la del atacante. Como estos paquetes son dirigidos de vuelta a Ettercap, los otros hosts de la red no los ven. La dirección MAC original será una de las direcciones físicas en la lista de hosts (obtenida previamente mediante un host scan) Este proceso roba el puerto RJ45 en el switch de cada ordenador víctima en la lista de hosts. Paquetes destinados a direcciones serán recibidos por el equipo atacante. Cuando Ettercap reciba paquetes de los hosts afectados, éste dejará de inundar la red con los primeros paquetes ARP y realizara un ARP-request para el destino real del paquete. Cuando reciba el ARP-Replay esto permitirá que el puerto en el switch ha sido asignado nuevamente a la víctima, permiten a Ettercap reenviar el paquete a su destino original y pueden así reiniciar el proceso de inundación nuevamente. Si utilizamos la opción propágate a otros switches el identificador MAC de cada paquete que envía Ettercap para robar inicialmente los puertos será algún no existente. De esta manera el paquete será propagado a otros switches que existan en la red. Esto genera una cantidad enorme de tráfico y puede ralentizar la red severamente. La opción "remote", al igual que en el caso del envenenamiento del cache ARP, permite capturar paquetes que deben atravesar un Gateway.

Cuando el paquete se detiene, Ettercap enviará un ARP-request cada host afectado devolviéndolo de esta manera a su puerto en el switch. Se pueden capturar paquetes en ambas comunicaciones o simplemente en una sola dirección, dependiendo de la selección de objetivos a Target. Utilice este ataque cautelosamente ya que sobrecarga el tráfico en la red y puede crear efectos inesperados.

Recursos y enlaces

Escanear vulnerabilidades. Nessus

Objetivo: En esta práctica vamos a ejecutar un escáner de vulnerabilidades. Tardará un tiempo, pero nos mostrará información muy interesante. Vamos a realizarlo con Nessus, el cual tiene una versión de prueba:

https://www.tenable.com/try

- https://youtu.be/mnms46baN4U

Escanear redes Windows. NMap

Objetivo: En esta práctica vamos a obtener toda la información posible de nuestra red, mediante el programa Nmap.

- https://youtu.be/wNOypalP85M
- https://youtu.be/-j4ij82DUvs

Escáner vulnerabilidades avanzado. Armitage de Kali Linux

Objetivo: En esta práctica vamos a ver cómo trabaja la herramienta Armitage que tenemos instalada en el Kali Linux. Nos ofrece una interfaz gráfica muy amigable y un listado de ataques bastante interesante.

- https://youtu.be/W2HNKuGF7kQ

Analizar redes. Wireshark

Objetivo: En esta práctica vamos a simular una red aislada compuesta por dos equipos, un W10 y un Ubuntu Server. Vamos a ver el tráfico que se produce con la herramienta Wireshark instalada en el W10.

- https://youtu.be/UhDRbT09qco

Seguridad Router WiFi. TP-Link

Objetivo: En esta práctica vamos a configurar la seguridad de un router WiFi. Para ello utilizaremos uno de los simuladores web que encontramos en: https://www.tp-link.com/es/support/emulator/

- https://youtu.be/5ilbgGf0l50

Servidor Radius Linux. FreeRadius

Objetivo: En esta práctica vamos a trabajar con un servidor FreeRadius y su complemento para web daloRadius.

- https://youtu.be/3jCeZ9wShKY

- WireShark https://www.wireshark.org/

- Suite Aircrack-ng http://aircrack-ng.org/

- WiFI Slax https://www.wifislax.com/

- Ettercap https://www.ettercap-project.org/

- Estandar IEEE 802.11 https://es.wikipedia.org/wiki/IEEE_802.11

Test de autoevaluación

La autentificación WiFi que realizamos con un servidor RADIUS, se denomina:

a) Abierta
b) WPA-Enterprise
c) WPA-Personal
d) WEP

El ataque en el que modificamos las direcciones DNS para poder controlar las máquinas se denomina

a) DNS Spoofing
b) Pharming
c) ARP Spoofing
d) MiTM

Indica cual de los siguientes Sniffer no se considera "malvado":

a) SpyNet
b) Pharming
c) WinSniffer
d) WireShark

Indica la herramienta que nos permite poner la tarjeta de red en modo promiscuo:

a) Aircrack-ng
b) Airdump-ng
c) Airmon-ng
d) Air-play

SOLUCIONARIOS

Test de autoevaluación tema 7

La autentificación WiFi que realizamos con un servidor RADIUS, se denomina:

a) Abierta

b) WPA-Enterprise

c) WPA-Personal

d) WEP

El ataque en el que modificamos las direcciones DNS para poder controlar las máquinas se denomina

a) DNS Spoofing

b) Pharming

c) ARP Spoofing

d) MiTM

Indica cual de los siguientes Sniffer no se considera “malvado”:

a) SpyNet

b) Pharming

c) WinSniffer

d) **WireShark**

Indica la herramienta que nos permite poner la tarjeta de red en modo promiscuo:

a) Aircrack-ng

b) Airdump-ng

c) Airmon-ng

d) Air-play