Seguridad en redes Wireless

Redes Abiertas

En este primer apartado vamos a ver las peculiaridades de las llamadas redes abiertas. Estas redes se caracterizan por no tener implementado ningún sistema de autenticación o cifrado. Las comunicaciones entre los terminales y los AP viajan en texto plano (sin cifrar) y no se solicita ningún dato para acceder a la red.

Los únicos elementos con los que se puede jugar para proporcionar algo de seguridad a este tipo de redes son:

- Direcciones MAC
- Direcciones IP
- El ESSID de la red

Filtrar el acceso a la red sólo a aquellos terminales que tengan una dirección MAC o IP determinada o bloqueando el envío de los BEACON FRAMES, de forma que sea necesario conocer de antemano el valor del ESSID para conectarse a la red, son los medios de los que se dispone para asegurar un poco este tipo de sistemas.

Nótese que estas medidas propuestas tienen en común que todas ellas intentan limitar el acceso no autorizado al sistema, pero no impiden que alguien espíe las comunicaciones. A continuación vamos a ver como saltarse las medidas propuestas anteriormente y otro tipo de ataques a los que se pueden ver sometidas las redes abiertas.

Romper ACL's (Access Control Lists) basados en MAC

La primera medida de seguridad implementada en las redes wireless fue, y sigue siendo, el filtrado de conexiones por dirección MAC. Para ello se crea una lista de direcciones MAC en el punto de acceso indicando si estas direcciones disponen de acceso permitido o denegado. La seguridad que proporciona esta medida es nula debido a la sencillez de cambiar la dirección MAC de nuestra tarjeta por otra válida previamente obtenida mediante un simple sniffer.

Si bien es cierto que el hecho de tener dos direcciones MAC en la misma red puede ocasionar problemas, esto se puede solucionar realizando un ataque de tipo DoS a la máquina a la cual le hemos tomado prestada la dirección MAC.

Ataque de Denegación de Servicio (DoS)

El objetivo de éste ataque implementado en una red inalámbrica consiste en impedir la comunicación entre un terminal y un punto de acceso. Para lograr esto sólo hemos de hacernos pasar por el AP poniéndonos su dirección MAC (obtenida mediante un sencillo sniffer) y negarle la comunicación al terminal o terminales elegidos mediante el envío continuado de notificaciones de desasociación.

Descubrir ESSID ocultos

Siendo fieles a la filosofía de *security through obscurity*, se ha aconsejado desde un principio la ocultación del ESSID de una red como método para aumentar la invisibilidad de nuestra red; una vez más sin embargo se ha demostrado que esta política de seguridad no resulta efectiva.

En casi todos los puntos de acceso podemos encontrar la opción de deshabilitar el envío del ESSID en los paquetes o desactivar los BEACON FRAMES. Ante esta medida de seguridad, un presunto atacante tendría dos opciones:

- Esnifar la red durante un tiempo indeterminado a la espera de una nueva conexión a la red con el objetivo de conseguir el ESSID presente en las tramas PROVE REQUEST del cliente (en ausencia de BEACON FRAMES) o en las tramas PROVE RESPONSE.
- Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque DoS pero sin mantener al cliente desconectado.

Ataque Man in the middle

Este ataque apareció en escena a raíz de la aparición de los switches, que dificultaban el empleo de sniffers para obtener los datos que viajan por una red. Mediante el ataque *Man in the middlese* se hace creer al cliente víctima que el atacante es el AP y, al mismo tiempo, convencer al AP de que el atacante es el cliente.

Para llevar a cabo un ataque de este tipo es necesario obtener los siguientes datos mediante el uso de un sniffer:

- El ESSID de la red (si esta oculto usaremos el método anterior)
- La dirección MAC del AP
- La dirección MAC de la víctima

Una vez obtenidos estos datos emplearíamos la misma metodología que en el ataque de tipo DoS para romper la conexión entre el cliente y el AP. Tras esta ruptura la tarjeta del cliente comenzará a buscar un nuevo AP en los diferentes canales, momento que aprovechará el atacante para suplantar al AP empleando su MAC y ESSID en un canal distinto. Para ello el atacante habrá de poner su propia tarjeta en modo **master**.

De forma paralela el atacante ha de suplantar la identidad el cliente con el AP real empleando para ello la dirección MAC del cliente, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente.

Ataque ARP Poisoning

Al igual que en el caso del ataque man in the middle, el objetivo de este ataque consiste en acceder al contenido de la comunicación entre dos terminales conectados mediante dispositivos inteligentes como un switch. En esta variante de man in the middle se recurre a la alteración de la tabla ARP que mantienen de forma stateless todos los dispositivos de red.

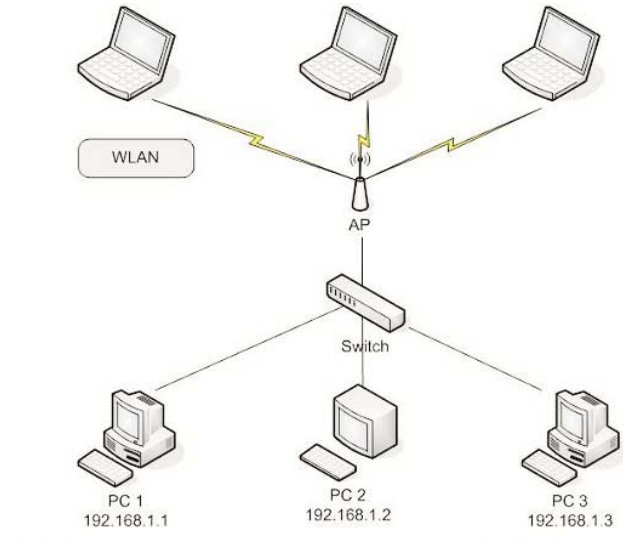

Tabla ARP -PC 1

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 2

Dirección IP	Dirección MAC
192.168.1.1	F1:F1:F1:F1:F1:F1
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 3

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.1	F1:F1:F1:F1:F1:F1

Figura 3 - Red antes del ataque

Para ello el atacante envía paquetes ARP REPLY al PC 3 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue modificar la caché de ARP's del PC 3. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 3 la tiene también su propia MAC (ver figura 4).