

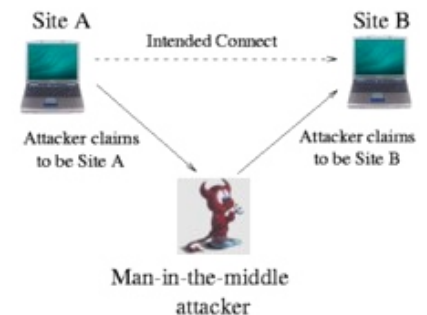
Seguridad Inalámbrica

En la actualidad, las redes inalámbricas proporcionan beneficios tangibles a las empresas como son el ahorro en el cableado de la red y la movilidad de sus usuarios, entre otros. Como bien es sabido las redes inalámbricas trabajan sobre un medio libre, el aire. Como consecuencia, se incrementa la dificultad para administrar la red LAN y a su vez las vulnerabilidades que ésta presente. Esto se debe a que, en la mayoría de los casos, solamente se tiene control de lo que pasa sobre el Access Point al ruteador pero no se puede controlar o ni siquiera monitorear las acciones de los usuarios los cuales guardan la información que es valiosa para la empresa. Ejemplos de la inseguridad existente en las redes inalámbricas son los posibles ataques a los que esta expuesta una empresa con esta infraestructura:

Robo de identidad.- Suponiendo que la red inalámbrica tenga control de acceso por medio de direcciones MAC (que es lo más común en redes bien administradas), es muy sencillo obtener la dirección MAC de un usuario que este dentro de la red y tomar esta dirección para entrar a la red inalámbrica con la identidad de otro usuario. Obviamente si este control de acceso no existe en la red, a menos que se cuente con una llave WEP para entrar a la red, ésta se encuentra abierta para cualquiera que quiera utilizarla.

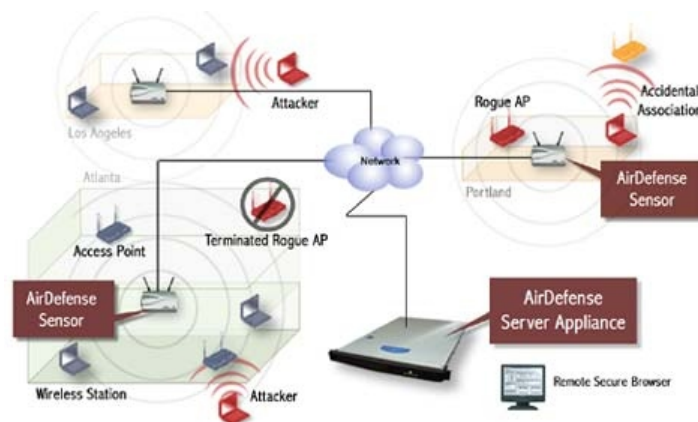
Descifrar el WEP.- Si se tiene un control de acceso mediante una llave WEP existen herramientas que pueden descifrar la llave que se usa tomando texto en claro que pasa por la red y haciendo una operación lógica con el texto cifrado que se ha atrapado. Esta operación puede tomar de uno a tres días con las herramientas adecuadas. Por otro lado, en redes muy grandes la llave WEP pierde su función ya que los usuarios fácilmente la revelan a un desconocido con buena cara o simplemente dejan de ser un secreto.

Ataque de hombre en medio.- Para este ataque se necesitan dos interfaces de red. Consiste en generar una denegación de servicio (DoS) entre el Access Point y la estación que se quiere atacar. Después, rápidamente, el atacante usa la dirección MAC del Access Point (AP) en una de las interfaces y la de la estación atacada en la otra interfaz. Al final el atacante hace creer al Access Point que es la estación y a la estación que es el AP. Con esto el atacante logra que toda la información que la estación mande al AP antes pase por él. En parece más complicado de lo que en realidad es ya que existen herramientas que pueden hacer este ataque con un simple clic del Mouse (Kismet es un ejemplo).



Estos son algunos de los ataques más comunes y más sencillos de efectuar en una red inalámbrica. En su mayoría nos son detectados por los administradores de la red puesto que se tiene un falso sentimiento de seguridad y no se cuenta con las herramientas adecuadas como: detectores de intrusos inalámbricos, reforzadores de políticas en la red y analizadores inalámbricos de protocolos.

Como se ha explicado, es necesario un herramientas que faciliten la administración del desempeño de la red, la seguridad y el monitoreo de estaciones. AirDefense protege la red actuando como un sistema inteligente, observando en su totalidad y correlacionando información proveniente de todos los sensores y recabando información en su bitácora para su futuro análisis.



Mediante monitorear toda la actividad de transmisión sobre el protocolo 802.11 (a/b/g) y correlacionando eventos a través de la red inalámbrica, **AirDefense** proporciona un panorama completo de todo lo que esta sucediendo en su espacio aéreo. Provisto de la ingeniería en detección de Intrusos mas avanzada en la industria, AirDefense realiza detección detallada y protege su red contra todo tipo de amenazas inalámbricas y dispositivos no autorizados.

Defensas Activas

AirDefense fortalece a las empresas con el mas avanzado sistema de protección contra intrusos, no solo dando la habilidad de detectar intrusos y dispositivos sospechosos en su espacio aéreo, sino permitiéndole además determinar protecciones activas manualmente o pre-definidas.

Detección de toda la actividad y dispositivos ajenos a su red

- ⦿ Access Points y estaciones no autorizados.
- ⦿ Dispositivos y Laptops habilitados con Wi-Fi.
- ⦿ Access Point mediante software.
- ⦿ Scaners de código de barras inalámbricos.

AirDefense también identifica conductas sospechosas de:

- ⦿ Asociaciones accidentales
- ⦿ Asociaciones destructivas o maliciosas (ataques como hombre en medio, etc).
- ⦿ Redes punto a punto entre estaciones de trabajo (redes Ad-Hoc)

Terminación Aérea

Después de la detección de un intruso o de algún dispositivo sospechoso, AirDefense tiene la capacidad de mitigar el ataque, mediante terminar la sesión entre una estación intrusa y un access point permitido, o mediante terminar las conexiones entre estaciones permitidas y Access points corruptos (no permitidos) de manera automática o manual.



Para más información acerca de este y más productos contáctenos o visite nuestra página de Internet.

RealNet, S.A. de C.V.
"Administración y Seguridad de Redes"
Guaymas 11bis Col. Roma C.P. 06700
México, D.F.
info@realnet.com.mx
Tel: (01 55) 5219 8656
Fax: (01 55) 5208 8201

www.realnet.com.mx