

Boletín Advisory*

Julio 2006

Seguridad en redes inalámbricas (wireless networks) Segunda Parte

2 de 2

Prácticas para la detección de
redes inalámbricas

¿Por qué las
redes inalámbricas son tan diferentes?

Principales riesgos de usar
redes inalámbricas

¿Las redes inalámbricas
se encuentran
realmente en riesgo?

Créditos



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 



Prácticas para la detección de redes inalámbricas	¿Por qué las redes inalámbricas son tan diferentes?	Principales riesgos de usar redes inalámbricas	¿Las redes inalámbricas se encuentran realmente en riesgo?	Créditos
---	---	--	--	----------

Prácticas para la detección de redes inalámbricas

Al igual que cualquier otra tecnología de punta, la utilización de redes inalámbricas implica tanto oportunidades y beneficios, como desventajas y riesgos. La era de la red inalámbrica le ha brindado un espacio a una nueva generación de “hackers” quienes se especializan en inventar y aplicar novedosos métodos para penetrar las comunicaciones inalámbricas, y hacer uso de esta infraestructura para vulnerar las redes LAN.

- **Wardriving**

Consiste en localizar puntos de acceso inalámbricos desde un automóvil. Muchos Wardrivers utilizan GPS para detectar la ubicación exacta de la red y publicarla posteriormente en Internet.

Metodología:

- Manejar por los vecindarios.
- Busca cualquier Punto de Acceso.
- Identifica las redes inalámbricas disponibles y las incluyen en mapas por medio de GPS's para la disposición de terceros.

- **Warchalking**

Consiste en dibujar símbolos en lugares públicos para denotar la existencia de redes inalámbricas. (Ver Figura N° 1)

Metodología:

- Caminar por la calle.
- Buscar cualquier Punto de Acceso.
- Dibujar en el piso un símbolo especial indicando el tipo de seguridad.

- **Roadwarrior**




Es una persona que lleva consigo un dispositivo móvil como un Laptop o un PDA y usa conexiones Internet como herramienta de trabajo. Como por ejemplo:

- Conectarse a la VPN de la empresa.
- Revisar y contestar e-mails.
- Enviar documentos.
- Procesar pedidos.

Metodología:

- Camina o maneja por los vecindarios.
- Busca cualquier Punto de Acceso.
- Hace uso de estas conexiones como herramienta de trabajo.

▶ [Haga click en la imagen para ampliarla](#)

Clave	Símbolo
Nodo Abierto	ssid  bandwidth
Nodo Cerrado	ssid 
Nodo WEP (Protegido)	ssid 

Retorno

Figura N° 1: Simbología utilizada en warchalking





Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas

¿Las redes inalámbricas se encuentran realmente en riesgo?

Créditos

¿Por qué las redes inalámbricas son tan diferentes?

1. Medio compartido, no controlado

Tradicionalmente las redes utilizan cables para la transmisión de información. La estructura del cableado representa entonces un medio controlado, protegido a su vez por las localidades o edificios en los que residen. El tráfico externo que penetra a una red “cableada” está protegido por firewalls y tecnologías de detección de intruso. Asimismo, para que un intruso o “hacker” obtenga acceso a una red “cableada”, éste debe traspasar la seguridad física del edificio o hacer uso de alguna brecha presente en el firewall.

Por otro lado, las redes inalámbricas utilizan el espacio aéreo como medio para transferir la información. En este sentido, a diferencia de la estructura del “cableado”, el espacio aéreo es visto como un medio compartido y no controlado. Una vez que un usuario conecta un punto de acceso (Access Point - AP) a la red, su señal puede atravesar paredes, techos y ventanas de cualquier edificio.

Esta característica brinda la posibilidad de que toda la red sea accesible desde otro piso del edificio, o sencillamente desde otra localidad adyacente (estacionamiento, calle, etc). Adicionalmente, los dispositivos inalámbricos

comparten el espacio aéreo por lo que cualquier dispositivo inalámbrico puede “ver” el tráfico de otros dispositivos inalámbricos en la red.

2. Fácil implantación

Los dispositivos inalámbricos son relativamente económicos y fáciles de utilizar. Hoy en día, la mayoría de las computadoras portátiles vienen configuradas por defecto con esta tecnología y aún cuando versiones anteriores no posean estas capacidades, son fácilmente configurables con tan sólo añadir una tarjeta inalámbrica y un software. En este sentido, una computadora portátil puede ser fácilmente configurable en un punto de acceso, por lo que cualquier usuario, empleado, o consultor que instale sus propias estaciones de trabajo inalámbricas sin tomar en consideración los requerimientos de configuración de seguridad adecuados representan una seria amenaza para toda la organización.

Mayor aún es la preocupación en torno a la movilidad de los dispositivos que se conectan a la red LAN, y por consiguiente el gran riesgo que esto representa para la red interna. Los dispositivos inalámbricos pueden entrar y salir de la organización sin ser detectados y pueden estar instalados en cualquier lugar.

3. Blanco fácil de ataque

Debido a que las comunicaciones inalámbricas son transmitidas utilizando ondas de radio compartidas, representan un blanco fácil de ataque por parte de “hackers”.

La única limitación física que posee una señal inalámbrica es la fuerza de su propia señal. Un “hacker” puede fácilmente ingresar a una red inalámbrica desde cualquier localidad circunvecina (calle, carro, edificios contiguos, parques, etc.).

La identificación de las redes inalámbricas que se encuentran activas en una localidad es una actividad bastante sencilla, tanto como que un niño manejando bicicleta con una PDA en su bolsillo pudiera estar identificando las distintas redes inalámbricas que hay en el vecindario.

Además, la presencia en Internet de herramientas especializadas para interceptar el tráfico de información, vulnerar el cifrado y la autenticación, aumenta el riesgo de que la información que viaja a través del espacio aéreo sea fácilmente comprometida por “hackers” no tan expertos.





Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas
1/4

¿Las redes inalámbricas se encuentran realmente en riesgo?

Créditos

Los seis (6) principales riesgos de usar redes inalámbricas

Las redes inalámbricas introducen nuevos retos en el campo de la seguridad de información. Las mismas tecnologías de conexión inalámbrica que operan sin las barreras físicas y lógicas de su contraparte la red cableada, por un lado incrementan la flexibilidad del usuario, aumentan

la productividad y reducen el costo de las redes, sin embargo, por otro lado éstas tecnologías pueden exponer los activos de información de la red a un riesgo alto. En la Figura N° 2 se muestran de manera general las seis (6) principales amenazas de las redes inalámbricas.



Figura N° 2: Principales amenazas en redes inalámbricas

1. Dispositivos no autorizados

Los dispositivos no autorizados, en particular, los puntos de acceso no autorizados, se han convertido en el mayor reto de la tecnología inalámbrica. Su rápida proliferación representa una seria amenaza para la seguridad de los activos de información de una organización ya que por lo general son instalados sin el consentimiento o aprobación del personal de TI o de la Gerencia de Seguridad de la Información, por lo que brindan una puerta de entrada a la red, que pasa por alto los controles de seguridad establecidos para el acceso a los recursos de la organización.

Entre algunos de los dispositivos no autorizados más comunes tenemos: un software AP, un hardware AP, un portátil, un scanner, un proyector u otro dispositivo capaz de brindar y recibir ondas de radio que puedan traspasar todos los esquemas de seguridad establecidos.

2. Visibilidad con otros dispositivos inalámbricos

La presencia de un dispositivo inalámbrico, puede ser identificado (es visible) desde otro dispositivo inalámbrico y viceversa. En este sentido, simplemente al utilizar un cliente de conexión que no esté configurado



Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas
2/4

¿Las redes inalámbricas se encuentran realmente en riesgo?

Créditos

Los seis (6) principales riesgos de usar redes inalámbricas

continuación

adecuadamente (por defecto) se pudiese establecer una conexión accidental a un dispositivo inalámbrico circunvecino. Esto permite que usuarios no autorizados puedan acceder a los equipos y redes de terceros, sin su conocimiento, comprometiendo así documentación sensible. El riesgo de esta situación se ve incrementado si la estación de trabajo o equipo comprometido está conectado a una red LAN.

3. Vulnerabilidades de los dispositivos y redes

Dispositivos de redes inalámbricos inseguros, como AP y estaciones de trabajo, pueden comprometer seriamente la red de la empresa y la información que por ella se transmite. Los dispositivos inseguros son blancos para los "hackers", quienes usando herramientas especializadas logran romper la seguridad y utilizar esas brechas para descifrar toda la información que por la red se esté enviando, bien sea de documentación o de información personal de autenticación.

Un punto de acceso (AP) configurado inadecuadamente puede seriamente comprometer la seguridad de la red de la empresa. Las configuraciones que estos

dispositivos traen por defecto (de fábrica) no incluyen autenticación ni tampoco cifrado de la información.

4. Riesgo cuatro: Amenazas y vulnerabilidades

Las redes inalámbricas introducen múltiples lugares de ejecución para atacar y penetrar aquello que podría ser muy difícil o completamente imposible de ejecutar con una red estándar. Entre las vulnerabilidades y amenazas más comunes tenemos:

- **Reconocimiento**

Los ataques tradicionales requieren una fase de reconocimiento en la que el "hacker" monitorea cuál sistema está disponible para atacar. Para la ejecución del reconocimiento, el "hacker" usa una herramienta de búsqueda (scan tool)

- **Robo de identidad**

El robo de identidad es una seria amenaza. Aunque los SSID y las direcciones MAC actúan como una identificación personal para verificar la identidad de los clientes autorizados, existen estándares de cifrado que no son infalibles. Los "hackers" pueden

eliminar SSIDs autorizados así como las direcciones MAC y robar el ancho de banda, corromper y descargar archivos y de la misma forma "tumbar" los servicios de la red.

Vulnerar el protocolo LEAP (Lightweight Extensible Authentication Protocol) para robar la identidad se ha convertido en una práctica realmente fácil por la disponibilidad de softwares o herramientas de "hackers" que se encuentran disponibles en Internet. Otro esquema de autenticación tal como el EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) y el PEAP (Protected Extensible Authentication Protocol), pueden requerir ataques sofisticados que exploten otras vulnerabilidades conocidas en las redes cableadas.

- **Negación de Servicio (Denial of Service - DoS)**

El objetivo de cualquier ataque de negación de servicio es prevenir el uso de los recursos de la red por los usuarios, perdiendo la conectividad y los servicios mediante el consumo total del ancho de banda de la red y de este modo negar el acceso a los usuarios legítimos. El método usual de provocar



Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas
3/4

¿Las redes inalámbricas se encuentran realmente en riesgo?

Créditos

Los seis (6) principales riesgos de usar redes inalámbricas

continuación

ataques de DoS es inundar una red con paquetes defectuosos excluyendo tráfico legítimo y causando que los sistemas no respondan.

- **Herramientas sofisticadas de ataque**

Las herramientas de “hackers” se encuentran disponibles gratis en Internet y son actualizadas cada semana. Estas herramientas permiten a los “hackers” romper el código y la autenticación, analizar los protocolos, “olfatear” el espacio aéreo y capturar el tráfico, incluir direcciones IP, nombres de usuario y contraseñas.

- 5. **Riesgo cinco: Exposición de las redes cableadas**

Muchas empresas cuentan con una infraestructura cableada para sus redes locales. Los “hackers”, pueden hacer uso de cualquier dispositivo inalámbrico como un punto de entrada para violar la red.

Adicionalmente, APs mal configurados, pueden actuar como un puente para obtener acceso a la red cableada, enviando toda la información posible al medio aéreo donde puede ser interceptado por intrusos y “hackers”. También,

las empresas que usan protocolos de enrutamiento, como HSRP (Hot Standby Routing Protocol), pueden ser presa de hackers a fin de conocer y entender información que les indique el diagrama de conectividad de la red utilizado en la empresa.

Estos tipos de protocolos, revelan información que puede permitir a los “hackers” hacer análisis de tráfico como de los dispositivos en uso, direcciones MAC, direcciones IP y rutas de tráfico.

- 6. **Riesgo seis: Operación de las redes**

Las redes inalámbricas tienen características que determinan la operación de éstas, las cuales pueden comprometer su uso. Estas características pueden impactar la disponibilidad, el rendimiento, la seguridad y el costo. Algunas de estas características se mencionan a continuación:

- **Actividad fuera de hora**

Debido a que los dispositivos inalámbricos no forman parte de las redes cableadas, pueden ser utilizados en cualquier parte y a cualquier hora del día. Por esta razón, muchas empresas limitan el uso de la red inalámbrica

en las horas de oficina e incluso llegan a apagar los APs. De este modo, todo el tráfico inalámbrico que tenga lugar en esas horas, se identificaría como sospechoso.

- **Tasa de transmisión de datos**

Los APs que anuncien una baja de la tasa de velocidad de transmisión de datos, puede ser un indicio de infracción en la seguridad de la red. Por lo que si existe un apropiado despliegue, el estándar 802.11b para redes inalámbricas, pudiera ofrecer una velocidad de transmisión del 5.5 Mbps o de 11 Mbps. Sin embargo, un AP que permita a un usuario conectarse a una velocidad de 1 Mbps o 2 Mbps en una configuración apropiada de la red, indica que existe actividad sospechosa que podría provenir de cualquier parte donde el AP distribuya su señal.

- **Interferencia**

Debido a que las redes inalámbricas usan ondas de radio, las condiciones y eventos externos o ambientales podrían afectar la operatividad de esta. Por ejemplo, pudiera existir una interferencia la cual puede causar la inoperatividad de la red inalámbrica y producir excesiva retransmisión de datos. La ▶



Los seis (6) principales riesgos de usar redes inalámbricas

continuación

fuelle de esta interferencia, puede ser otro dispositivo electrónico operando en el área. Las redes inalámbricas, tienen limitada capacidad de transmisión la cual es compartida entre los usuarios asociados a un AP. Los “hackers”, pueden fácilmente ejecutar una DoS a fin de atacar los recursos limitados y negar el servicio a los usuarios.

APs maliciosos u otros dispositivos pueden interferir con la operación de dispositivos legítimos de la red, lo cual implicaría ofrecer a los hackers una puerta abierta para acceder a la red interna. Un “hacker” puede tratar de acceder a los recursos de la red instalando intencionalmente un AP furtivo a fin de interceptar información sensible o falsificando una conexión legítima.

Adicionalmente, cualquier persona queriendo restringir el uso de una red inalámbrica, podría cerrarla con una fuerza de señal de radio superior.

- **Conectividad**

Existe un gran número de factores pueden incidir en la degradación de las conexiones inalámbricas. Las redes inalámbricas pueden experimentar una pérdida de rendimiento y

los usuarios podrían tener problemas al conectarse cuando las señales de radio encuentren obstrucciones, bien sea naturales o hechas por el hombre, entre los usuarios y los APs o cuando el usuario se encuentre en una distancia muy separada del dispositivo.

El rendimiento puede causar demoras en los usuarios, por ejemplo cuando existe un gran número de usuarios conectados a un AP al mismo tiempo. Un mal funcionamiento o inoperatividad del AP puede prevenir o limitar los accesos a la red.

¿Las redes inalámbricas se encuentran realmente en riesgo?

De acuerdo con la encuesta realizada por PricewaterhouseCoopers en Estados Unidos de América, en noviembre del año 2005, 48% de las empresas y organismos gubernamentales que tienen redes inalámbricas han sido víctimas de un ataque.

De éstas, 85% reportaron pérdidas monetarias. Cualquier dispositivo inalámbrico o AP no autorizado (furtivo) crea un camino abierto a toda la red de la empresa, incluyendo aquella que es cableada aunque se encuentre apropiadamente configurada, asegurada y monitoreada.

Los beneficios de las redes inalámbricas son indudables, pero los riesgos que estas atraen han venido exponencialmente incrementándose. Existen más de diez millones de nuevos dispositivos Wi-Fi que se instalan cada año generando así el crecimiento de señales abiertas o poco robustas a nivel de seguridad, que hacen vulnerables las redes de las organizaciones.

A modo de conclusión, es posible indicar algunos puntos importantes a tomar en consideración para cualquier compañía que cuente con (o esté planeando instalar) redes inalámbricas:





Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas

¿Las redes inalámbricas se encuentran realmente en riesgo? 2/2

Créditos

¿Las redes inalámbricas se encuentran realmente en riesgo?

continuación

Acciones a corto plazo:

- Planificación de la estrategia de implantación de redes inalámbricas y su seguridad.
- Concientización del usuario en el uso de las redes inalámbricas y su seguridad.
- Cambiar las claves de cifrado.
- No utilizar nombres descriptivos para el Punto de Acceso (AP) y el SSID.
- Ubicar los Puntos de Acceso lejos de los límites del perímetro.
- Identificar Puntos de Acceso no autorizados en la red local.
- Utilización del cifrado WEP.

Acciones a mediano plazo:

- Evaluaciones de seguridad de la red inalámbrica.
- Cambios continuos de las claves de cifrado del protocolo WEP.

- Cambiar las direcciones IP por defecto de los Access Points.
- Habilitar el filtrado de direcciones MAC.
- Segmentar la red inalámbrica de la red local.

Acciones a largo plazo:

- Monitoreo y gestión de incidentes de seguridad en redes inalámbricas.
- Implantar Firewalls para la red inalámbrica.
- Prescindir del cifrado WEP e implantar los estándares 802.11i y 802.1x
- Evaluar esquemas alternativos de cifrado y autenticación (VPN).





Prácticas para la detección de redes inalámbricas

¿Por qué las redes inalámbricas son tan diferentes?

Principales riesgos de usar redes inalámbricas

¿Las redes inalámbricas se encuentran realmente en riesgo?

Créditos

Boletín Advisory

El Boletín Advisory es publicado mensualmente por la Línea de Servicios Advisory de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666

Si está interesado en recibir en su correo electrónico este Boletín, por favor envíenos su dirección de e-mail a:
advisory.venezuela@ve.pwc.com



© 2006. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3