Auditoría de Seguridad en Redes Inalámbricas, Soluciones y Recomendaciones

Javier Antonio Benites Barreiro [(1)]
Diego Andrés Chóez Cajamarca [(2)]
Albert Giovanny Espinal Santana [(3)]
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
jbenite@espol.edu.ec [(1)]; dachoez@espol.edu.ec [(2)]; aespinal@espol.edu.ec [(3)]

Resumen

El presente trabajo tiene como objetivo mostrar las debilidades que se pueden encontrar en una red local inalámbrica, para esto se demostrará como operan algunas herramientas de auditoria de seguridad y la facilidad con que ciertos métodos de seguridad poco confiables pueden ser eludidos o vulnerados. Se analizarán y propondrán algunas soluciones de seguridad más complejas orientadas a optimizar la seguridad y el control de acceso en redes inalámbricas. Finalmente, se mostrará el diseño e implementación de una solución de seguridad basada en VPN + RADIUS EAP-TLS.

Se comienza explicando de manera teórica conceptos de seguridad en redes inalámbricas. Se describe el proceso de un test de penetración y sus diferentes fases. Se muestra el funcionamiento de varias herramientas de auditoría y procesos específicos para vulnerar algunos métodos de seguridad usando un escenario de pruebas. Se da algunas recomendaciones para mejorar la seguridad en un ambiente personal o de hogar y propone algunas de las soluciones más confiables de seguridad a nivel empresarial. Finalmente, se muestra el diseño e implementación de un modelo de seguridad usando VPN para el cifrado y certificados digitales para la autenticación de los usuarios.

Palabras Claves: *redes inalámbricas, seguridad informática*.

Abstract

This paper aims to show the weaknesses that can be found in a wireless local network, it will be shown how they operate some security auditing tools and the ease with which certain unreliable security methods can be circumvented or violated. They will analyze and propose some solutions more complex safety-oriented optimize security and access control in wireless networks. Finally, the design and implementation of a security solution based on VPN + RADIUS EAP-TLS will be displayed.

It begins by explaining concepts theoretically wireless security. Process and penetration test described different phases. The functioning of various audit tools and processes specific to violate some security methods using a test scenario is displayed. Recommendations for improving security on a personal or home environment is given and proposes some of the most reliable security solutions at the enterprise level. Finally, the design and implementation of a security model using VPN for encryption and digital certificates for authentication of users is displayed.

Keywords*: Wireless networks, information security.*

1. Introducción

En los últimos años hemos visto un acelerado crecimiento en el uso de redes inalámbricas, esto se debe al incremento de equipos portátiles y las ventajas en la implementación de estas redes como el hecho de no tener que instalar cableado.

Actualmente, podemos observar que prácticamente en toda empresa, además del acceso por medios cableados, existen puntos de acceso inalámbricos.

A pesar de las múltiples ventajas que ofrece una red inalámbrica, la utilización del aire como medio de transmisión ha creado un nuevo riesgo en la seguridad que puede ser difícil de manejar.

En el caso de las empresas, la falta de conocimiento por parte de los propietarios o el presupuesto para su implementación pueden influir en que la seguridad en estas redes no sea considerada de manera adecuada.

El presente proyecto pretende mostrar los riesgos de seguridad que se pueden encontrar en este tipo de redes y proponer algunas soluciones y recomendaciones para mejorar significativamente la seguridad en el acceso a redes inalámbricas.

1.1. Objetivo General

Identificar las vulnerabilidades existentes en una infraestructura de red inalámbrica e implementar un modelo de seguridad que mitigue estas vulnerabilidades.

1.2. Objetivos Específicos

- Describir la metodología para un test de penetración en redes inalámbricas.
- Implementar un escenario para pruebas y efectuar un test de penetración.
- Detectar e identificar las vulnerabilidades presentes en las redes inalámbricas.
- Mostrar diferentes modelos de seguridad, a nivel personal y empresarial.
- Implementar un modelo de seguridad a nivel empresarial.

2. Seguridad en Redes Inalámbricas

La naturaleza de las redes inalámbricas las hace más susceptibles a ser atacadas que las redes cableadas, debido a que estas usan como medio de transmisión el aire que es un medio compartido. Por esto es importante establecer mecanismos de seguridad al momento de implementarlas.

2.1. Tipos de Autenticación

Para que un cliente tenga acceso a una red o un punto de red, es necesario realizar el proceso de autenticación que consiste en verificar la identidad de un cliente previo a otorgarle dicho acceso. Existen diferentes tipos de autenticación de acuerdo al nivel de seguridad que requiera la infraestructura de red:

- Autenticación Abierta
- WEP
- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

2.1.1. Autenticación abierta. La autenticación abierta permite el acceso a la red a cualquier dispositivo, de esta manera cualquier dispositivo que conozca el SSID del punto de acceso puede obtener acceso a la red.

2.1.2. WEP. WEP utiliza el cifrado para ayudar a evitar la recepción no autorizada de datos inalámbricos. WEP utiliza una clave para cifrar los datos antes de transmitirlos. Sólo los equipos que utilicen la misma clave de cifrado pueden tener acceso a la red y descifrar los datos transmitidos por otros. [1]

2.1.3. WPA-Personal. WPA fue creado para corregir los problemas de seguridad que hacían vulnerable a WEP. Utiliza claves de codificación de 128 bits y claves de sesión dinámica para garantizar la privacidad y seguridad de la red inalámbrica. [2]

2.1.4. WPA2-Personal. WPA2 es una mejora de WPA que corrige algunas vulnerabilidades detectadas en WPA e implementa el estándar IEEE 802.11i completo. Al igual que WPA-Personal requiere una clave pre-compartida (PSK) en el punto de acceso y los clientes. [3]

2.1.5. WPA-Enterprise. La versión Empresarial de WPA, ofrece un control individualizado y centralizado sobre el acceso, cuando los usuarios tratan de conectarse a la red, necesitan presentar sus credenciales de acceso al sistema. WPA-Enterprise verifica los usuarios de red mediante un servidor de autenticación como RADIUS. [2]

2.1.6. WPA2-Enterprise. WPA2-Enterprise es una mejora de WPA e implementa todo el estándar IEEE 802.11i completo. Al igual que el WPA-Enterprise, verifica los usuarios mediante un servidor de autenticación. [3]

2.2. Autenticación 802.1x

El estándar 802.1x es una arquitectura de control de acceso para redes inalámbricas el cual hace uso de certificados digitales para proporcionar a los usuarios los servicios de autenticación y autorización. [4]

Aquí intervienen 3 entidades que son el cliente, el punto de acceso y el servidor de autenticación. Al usuario se le concede un certificado digital que permitirá realizar la autenticación y de esta manera hacer uso de la red.

2.3. Tipos de Cifrados de Datos

Los protocolos de cifrado son usados para producir las claves que cifrarán los datos durante la comunicación entre los dispositivos de una red.

2.3.1. TKIP. Es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas. Debido a que las claves están en constante cambio, ofrecen un mejor nivel de seguridad para la red. [5]

2.3.2. CCMP. Es un protocolo de cifrado de IEEE 802.11i creado para reemplazar a TKIP. CCMP emplea el algoritmo de seguridad AES (Advanced Encryption Standard). [6]

3. Metodología de un Test de Penetración a una Red Inalámbrica

Un test de penetración es un conjunto de metodologías y técnicas que permiten determinar las vulnerabilidades de un sistema. Esto incluye las siguientes etapas:

- Planeación
- Descubrimiento
- Ataque
- Presentación de informe

3.1. Planeación

En esta fase el cliente contrata al auditor de seguridad para definir los parámetros sobre los cuales se realizara el test de penetración. Aquí se definirá la ubicación donde se realizará el test de penetración y el área total de las instalaciones.

3.2. Descubrimiento

En esta fase, vamos a explorar las redes inalámbricas y encontrar diferentes puntos de acceso y clientes en los alrededores.

3.3. Ataque

En esta fase, vamos a explorar las redes inalámbricas y encontrar diferentes puntos de acceso y clientes en los alrededores.

3.4. Presentación de Informe

Una vez que se han encontrado todas las vulnerabilidades de seguridad, se debe informar a la empresa. Los niveles de gravedad es un aspecto importante del informe, ya que son una guía que permite conocer rápidamente la importancia de una vulnerabilidad y el tipo de medidas a tomar para solucionarlo.

4. Vulnerabilidades en Redes Inalámbricas

Una vulnerabilidad es una debilidad en la red que permite violar la integridad, disponibilidad o confidencialidad de la misma.

4.1. Selección de Herramientas para Análisis de Vulnerabilidades en una Red Inalámbrica

Se revisaron algunas de las distribuciones de Linux más reconocidas para la auditoria de redes inalámbricas: Beini, Wifiway, Backtrack, Kali.

En un comienzo se descartó el uso de Beini por no ser una herramienta de uso profesional. Wifiway es un sistema totalmente enfocado en la auditoria de redes inalámbricas, cuenta con todas las herramientas necesarias y sería una elección válida para un proceso de análisis de vulnerabilidades en una red inalámbrica; sin embargo, hemos optado por Backtrack 5 R3 principalmente por contar con un mayor soporte y documentación. En el proyecto realizado no se usó Kali Linux porque al momento de su desarrollo este sistema aún se encontraba en fase de pruebas y por no contar con la sufriente información en los foros sobre su implementación en auditorias de redes.

4.2. Evasión de la Autenticación Inalámbrica

Este tipo de ataques busca obtener acceso a la red inalámbrica de manera fraudulenta evadiendo los esquemas de seguridad más débiles encontrados en redes inalámbricas. El porcentaje de éxito de estos ataques es del 100%, además de tomar unos pocos minutos y ser sencillos de realizar.

Estos ataques están dirigidos al descubrimiento y conexión a una red con SSID oculto, eludir el filtrado de direcciones MAC y la autenticación WEP.

4.3. Ataques a la Infraestructura

Estos ataques están enfocados a los principales protocolos de seguridad en redes inalámbricas, desde los primeros en aparecer como WEP hasta sistemas de seguridad más complejos que incluyen el uso de servidores de autenticación como WPA2-Enterprise con servidores RADIUS.

Estos ataques están orientados a obtener la clave de autenticación en la seguridad WEP, WPA/WPA2 y a obtener las credenciales de usuario en los protocolos WPA/WPA2-Enterprise.

4.4. Resultados del Test de Penetración

Se comenzó probando los sistemas que actualmente se consideran menos seguros como el SSID oculto y el filtrado MAC. En este procedimiento se pudo observar que la información requerida (SSID y dirección MAC) se mostraba en texto plano por lo que no se requiere ningún procesamiento adicional, esto le da un 100% de probabilidades de éxito al ataque.

Para comprobar la seguridad de WEP se realizaron varias pruebas en donde se usaron algunas contraseñas de diferentes longitudes y complejidad como “diego”, “qwertyuiopa”, “municipio2011” y “k5l4d7hal44gw”. En todos los casos se obtuvo con éxito la contraseña en diferentes tiempos que van desde los 2 hasta los 5 minutos.

Las pruebas con WPA/WPA2 fueron realizadas mediante ataques de diccionario, que es el único tipo de ataque posible contra WPA/WPA2 en la actualidad. Se probaron contraseñas sencillas como "qwerty", "12345678", "administrator" y contraseñas que se sabía que estaban dentro del diccionario como "Admin2014". En estas pruebas se pudo obtener las contraseñas en tiempos diferentes desde 1 hasta 15 minutos. Al comprobar otras contraseñas no comunes o más complejas como "k5l4d7ha" no fue posible obtener la contraseña luego de recorrer todo el diccionario.

En el caso de las autenticaciones basadas en RADIUS se hizo pruebas con varias configuraciones de seguridad diferentes en la conexión inalámbrica de los clientes. Cuando la opción de verificar el certificado del servidor estuvo deshabilitada, el cliente se conectó al punto de acceso falso sin problemas permitiendo capturar el hash enviado por el cliente que luego pudo ser usado para realizar ataques de diccionario sobre él. Cuando la opción de verificar el certificado de servidor estuvo habilitada, pero no se especificó la entidad de certificación de confianza, el usuario al intentar conectarse era advertido con un mensaje, sin embargo al aceptar pudo conectarse permitiendo capturar el hash. Cuando la opción de verificar el certificado de servidor estuvo habilitada y se especificó la entidad de certificación de confianza, el cliente rechazo la conexión y no le permitió al usuario conectarse por lo que el hash no pudo ser capturado.

5. Soluciones Propuestas

Las empresas manejan mucha información confidencial y suelen ser el blanco de ataque con mayor frecuencia y por hackers más capacitados que un usuario en una red propia en su hogar. Por esto se han desarrollados métodos de seguridad más complejos que involucran servidores de seguridad y acceso.

5.1. Protocolo EAP-TLS

EAP-TLS está basado en el uso de certificados digitales para la autenticación tanto del cliente como el servidor de autenticación.

Esta implementación requiere del despliegue de una arquitectura PKI, en donde al menos debe existir un servidor de certificación para la emisión y manejo de los certificados, y un servidor de autenticación como un servidor RADIUS.

5.2. Control de Acceso a la Red

NAC combina en una solución la autenticación de usuarios, evaluación de seguridad de punto final y control de acceso. El propósito de NAC se divide en dos partes: permitir el acceso a la red únicamente a usuarios y sistemas autorizados, y asegurar el cumplimiento de las políticas de seguridad de la red.

5.3. Acceso a través de VPN

En este modelo de seguridad la red inalámbrica está separada de la red interna de la empresa por un equipo que cumple el rol de servidor VPN. De esta manera los usuario inalámbricos, luego de obtener acceso a la red inalámbrica, aun no pueden obtener acceso a los recursos que se encuentra dentro de la red interna de la empresa, sino hasta que establezcan una conexión VPN con la misma.

5.4. Comparación de las Soluciones Empresariales

En el caso de EAP-TLS se ofrece un esquema de seguridad en donde su principal fortaleza es el uso de certificados digitales, que brindan un nivel de seguridad muy superior a las contraseñas.

NAC está enfocado no solo a la autenticación de los usuarios, sino a resolver un problema especialmente importante en los equipos portátiles, el ingreso de software malicioso de fuentes externas a la empresa.

El acceso a través de VPN permite dar cierto nivel de acceso, como conexión a internet, a usuarios dentro de la red inalámbrica que son considerados como invitados, mientras que para obtener acceso a recursos dentro de la red interna se requerirá una conexión a través de VPN.

La selección de uno de estos modelos de seguridad dependerá de varios factores específicos del ambiente donde se implementará como el tipo de usuarios y sistemas que accederán a la red, las políticas de seguridad de la empresa, la infraestructura de red actual y el impacto que podría causar en la red su implementación, por lo que antes de optar por una de estas soluciones se deberá hacer un estudio y analizar cuidadosamente estos factores.

6. Implementación de Seguridad Inalámbrica a través de una VPN

Se implementó un modelo de seguridad en donde se combinaron los beneficios del acceso a través de VPN y los certificados digitales para maximizar la seguridad en el acceso a la red inalámbrica.

El uso de un servidor VPN que además funcione como cortafuegos para el acceso de los clientes inalámbricos a la red de la empresa permite, no solo el control de

los usuarios que puedan acceder a la red sino, los recursos específicos a los que pueden acceder dentro de la red interna de la empresa.

Por otra parte, el uso certificados digitales como método de autenticación de los usuarios, proporciona un método más seguro al no depender de la complejidad de la contraseña elegida por los usuarios, ni la confidencialidad con que mantengan esa contraseña.

6.1. Diseño General

Se contó con un servidor VPN/Cortafuegos que fue implementado por medio del Forefront Threat Management Gateway 2010, este permitió crear un túnel seguro para el acceso a la red interna. Para la autenticación de los usuarios este servidor se contactó con un servidor RADIUS, implementado usando el servicio de Network Policy and Access Services de Windows Server 2008 R2. El servidor RADIUS usó como método de autenticación el EAP-TLS y se contactó con un servicio de directorio Active Directory de donde obtuvo el grupo de usuarios que tiene permitido el acceso. Para la emisión y manejo de certificados digitales se implementó un servidor de certificación. Adicionalmente, se instaló un servidor web, este representó los recursos internos de la empresa. La Figura 1 muestra el diseño general.

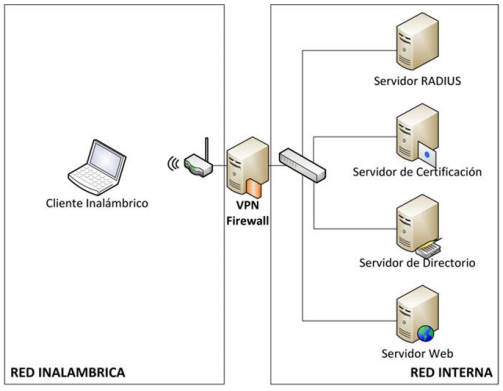

Figura 1. Diseño General

6.2. Descripción del Escenario de Simulación

El hardware constó de dos portátiles y un ruteador inalámbrico. Estos equipos con la ayuda del software de virtualización permitieron recrear los elementos principales de un escenario de red empresarial.

El ruteador inalámbrico fue usado como equipo de acceso a la red inalámbrica. La portátil de menor capacidad fue usada como cliente inalámbrico. La otra portátil ejecutó varias máquinas virtuales que incluyeron los servidores de la red. La Figura 2 muestra los equipos usados para la simulación.

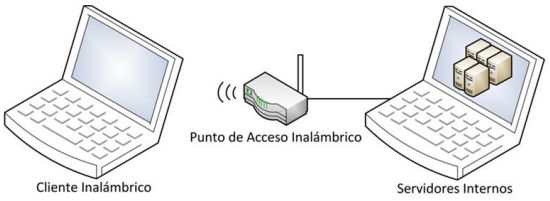

Figura 2. Escenario de Simulación

6.3. Implementación

Se crearon las máquinas virtuales VPN, SERVER y DC-CA-NPS usando el software de virtualización VirtualBox y se instaló en ellas el sistema operativo Windows Server 2008 R2.

Para nuestra implementación al no contar con una red previamente configurada, hicimos una instalación sencilla de un Controlador de Dominio usando Windows Server 2008 R2, en donde creamos el dominio “tesis.com”.

Para el manejo y emisión de los certificados digitales usamos la maquina DC-CA-NPS, en donde agregamos el rol de “Certification Authority”. Debemos tomar en cuenta que para que pueda integrarse con el Active Directory es necesario instalarlo como tipo “Enterprise”.

La máquina DC-CA-NPS también cumplió el rol de servidor RADIUS, para que el equipo pueda cumplir con esta función instalamos el Network Policy Server. Mediante el asistente de configuración de conexiones del Network Policy Server pudimos configurar al servidor NPS como servidor RADIUS.

En la máquina virtual VPN instalamos el Forefront TMG que nos permitió habilitarla como servidor VPN y Cortafuegos. Para su configuración, este equipo debió ser previamente agregado al dominio “tesis.com”.

En nuestro ruteador inalámbrico realizamos las configuraciones básicas para habilitar el acceso inalámbrico, usamos como tipo de seguridad WPA2-Personal con cifrado AES.

Antes de configurar el cliente para el acceso a la VPN necesitamos obtener un certificado digital para autenticarnos. Para ello debimos conectar temporalmente el equipo cliente a la red interna para poder acceder al CA y solicitar el certificado. Otra opción habría sido solicitar el certificado desde un equipo de la red interna, para luego exportarlo e instalarlo en el equipo cliente.
Una vez instalado el certificado en el cliente, y ya estando conectados a la red inalámbrica, agregamos

una nueva conexión VPN y configuramos esta conexión para que use el certificado ya instalado en el equipo para autenticarse.

6.4. Resultados de la Implementación

Al completar de manera exitosa la implementación se pudo constatar lo siguiente.

Los clientes estaban configurados para autenticarse ante el servidor usando un certificado digital y no una contraseña. Esto eliminó cualquier desventaja producida al usar contraseñas de usuario, como la posibilidad que el usuario use una contraseña sencilla, que la tenga anotada en un lugar visible o que sea robada. Al mismo tiempo el equipo cliente comprobaba la identidad del servidor.

La configuración no permitía que el cliente se conecte con ningún servidor a menos que este servidor se identifique usando un certificado digital emitido por la entidad de certificación propia de la empresa, eliminado así la posibilidad de que se conecte con un punto de acceso falso.

La inclusión de un cortafuegos permitió tener un control sobre los recursos a los que podía acceder un cliente inalámbrico. De esta manera, aun cuando llegase a comprometerse la seguridad de la red inalámbrica los recursos que quedarían expuestos ante el atacante serian limitados.

7. Conclusiones

- Deshabilitar la difusión del SSID y el filtrado de direcciones MAC son métodos realmente sencillos de eludir.
- La seguridad WEP está obsoleta. Se puede obtener una contraseña WEP con herramientas sencillas en pocos minutos.
- Una contraseña lo suficientemente compleja con WPA logra que ataque de diccionario pierda sus posibilidades de éxito. Un ataque de fuerza bruta a esta tecnología seria impráctico debido al tiempo que requiere.
- La autenticación del servidor por parte del cliente también es importante ya que ayuda a prevenir ataques de AP falsos.
- Los certificados digitales como alternativa al uso de contraseñas nos ofrecen un método de autenticación mucho más seguro, pero su adopción se ha limitado debido a la complejidad de su implementación.

8. Recomendaciones

- En instalación de puntos de acceso inalámbricos personales se debe evitar dejar ciertos valores predeterminados, como el nombre y contraseña de administrador y el SSID.
- Deshabilitar la opción WPS en los puntos de acceso siempre que sea posible, una vulnerabilidad en esta tecnología permite realizar ataques de fuerza bruta en tiempos relativamente cortos (4-10 horas).
- En un ambiente empresarial, mantener la red inalámbrica en una subred independiente y limitar los recursos a los que se puede acceder a través de ella.
- Antes de seleccionar un modelo de seguridad empresarial debemos tomar en cuenta que este sea compatible con los diferentes sistemas operativos de los clientes inalámbricos.
- Como responsables de la administración de la red de una organización debemos asegurarnos de informar adecuadamente acerca de los riesgos de seguridad en redes inalámbricas a los propietarios de la organización.

9. Referencias

[1] Descripción de la seguridad Wi-Fi. Fecha de consulta enero 2014. Disponible en: http://www.intel.com/support/sp/wireless/wlan/sb/cs-032784.htm.

[2] WiFi Protected Access (WPA). Fecha de consulta enero 2014. Disponible en: http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/665-wifi-protected-access-wpa.

[3] Cuál es la diferencia entre WPA y WPA2-Personal. Fecha de consulta diciembre 2014. Disponible en: http://ordenador.wingwit.com/Redes/network-security/75623.html.

[4] IEEE 802.1X Remote Authentication Dial In User Service Usage Guidelines. Fecha de consulta enero 2014. Disponible en: https://datatracker.ietf.org/doc/rfc3580/?include_text=1.

[5] Diccionario de Informática - Definición de TKIP. Fecha de consulta enero 2014. Disponible en: http://www.alegsa.com.ar/Dic/tkip.php.

[6] AES (Advanced Encryption Standard). Fecha de consulta enero 2014. Disponible en: http://jfherrera.wordpress.com/2010/08/28/aesadvanced-encryption-standard.