CAPITULO VI

VERIFICACIÓN DE LA HIPÓTESIS, CONCLUSIONES Y RECOMENDACIONES

6.1.- Verificación de la Hipótesis
6.2.- Conclusiones
6.3.- Recomendaciones

6. 1.- Verificación de Hipótesis

Hipótesis:

Si implementamos tecnología, mecanismos de control y configuración de la seguridad en una WLAN se optimizará el funcionamiento de la red garantizando mayor confidencialidad, autenticación, integridad y control de datos

Las redes mixtas establecen la comunicación de datos con la movilidad del usuario ampliando su eficiencia y rendimiento.

Verificación:

La hipótesis se ha llegado a comprobar, ya que la seguridad de redes WLAN es el punto mas importante en la implementación de soluciones móviles por su medio de transmisión (ondas de radio). Una vez instalado y configurado los mecanismos de seguridad como son WEP mecanismo básico y WPA como mecanismo avanzado ha mejorado su funcionamiento, al garantizar su confiabilidad en los clientes con la utilización de la red inalámbrica LAN, además autentifica a los usuarios de la red, control de datos e integridad de los mismos.

La combinación de las dos redes como son cableada e inalámbrica LAN establecen la conexión para la comunicación, movilidad y seguridad.

6.1.- Conclusiones

- Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en las empresas, por lo que facilita la implementación, de la red inalámbrica LAN. En este sentido el objetivo fundamental de las redes WLAN es proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde co-existan los dos tipos de sistemas.

- Las redes inalámbricas no podrán desplazar de manera definitiva a la redes alámbricas, ya que dependen de esta para conectarse, son una extensión de las redes cableadas y en conjunto hacen un sistema de comunicación complejo, por lo tanto se soluciona la conexión de los últimos metros hacía la estación proporciona movilidad adicional al equipo. Las redes cableadas siguen teniendo mayor rendimiento y seguridad que las inalámbricas y esto representa un reto para las empresas.

- En una WLAN la capa física y la de enlace es diferente a las redes convencionales debido al medio de transmisión, las frecuencias de 2.40 a 5,40 Ghz limitan la señal, por lo que el medio solo permite la transmisión de cierto ancho de banda. Con respecto a la capa 2 la CSMA/CD y la subcapa MAC utilizan valores definidos para garantizar la compatibilidad con la capa MAC.

- Aunque el estándar inicial tuvo en cuenta los aspectos de seguridad propios de una red inalámbrica, en la práctica ha demostrado que las decisiones que en su día se tomaron no fueron muy acertadas. Al día de hoy es relativamente sencillo encontrar redes WLAN en las que los mecanismos de seguridad brillan por su ausencia. Aunque las empresas suelen alegar que en estas redes no existen datos relevantes o importantes para el negocio, no cabe perder de vista que la máxima seguridad de una red la marca el punto más débil.

- Una red WLAN mal asegurada puede convertirse en un posible punto de entrada o ataque a nuestra red corporativa, donde existan los datos importantes. Además cabe considerar el hecho de que conceptos como wardriving o warchalking se están poniendo de moda. Wardriving significa conducir por la ciudad con un ordenador portátil y una tarjeta WLAN con la finalidad de encontrar redes WLAN instaladas. Mientras que warchalking es un conjunto de símbolos que se realizan en lugares públicos

para dar a conocer la existencia de una red WLAN y los parámetros necesarios para acceder a ella.

- Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores. El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves en un entorno de alto tráfico.

- Viendo que el estándar inicial era demasiado inseguro se opto por otra alternativa, el estándar 802.1x y EAP este es el adecuada para la seguridad en redes empresariales WLAN, con está tecnología se puede usar claves dinámicas con WPA y un servidor RADIUS, que sirve para la autenticación de usuarios, ofreciendo excelente grado de protección.

- Actualmente existe el estándar IEEE 802.11i o WPA2, que permite una seguridad mucho mayor, sumándole las características de 802.1x y una encriptación mas fuerte con la utilización del algoritmo AES. Este estándar trabaja a velocidades de 54 y 108 Mbp siempre y cuando tenga línea de vista y no haya interrupción de la señal, estas interrupciones son realizadas especialmente por microondas, radios, etc.

- Hoy en día el tráfico de información en las redes informáticas es cada vez mas elevado, establecer mecanismo de seguridad en la red física muchas veces es insuficiente, es así que los mecanismos de encriptación dados por los diferentes algoritmos son cada día mas utilizadas para la encriptación de los datos, muy especialmente si son empresas e instituciones que mantienen información vulnerable o de alto riesgo como son: bancos, policía, etc.

- Si bien la implementación de una red inalámbrica es relativamente sencilla que incluso se limita muchas veces a conectar el AccessPoint al concentrador o a al Servidor, su configuración de la seguridad no lo es; en muchas ocasiones por la dificultad que representa esto o por la falta de conocimiento de los administradores de red, las redes inalámbricas quedan abiertas permitiendo el fácil acceso a personas ajenas que deterioran el desempeño de la red.

- Para el funcionamiento de la red espacialmente la inalámbrica se trabajó con los estándares: 802.11b/g y 802.1x con tecnología D-Link, el primero sirve para la velocidad de transmisión que es de 108 Mbs, el segundo para la implantación de la seguridad, todas las tarjetas y Access Point deben tener el mismo estándar, ya que si es diferente trabajaran a diferentes velocidades por Ejemplo. Si el Access Point trabaja a 108 Mbps y la tarjeta inalámbrica a 54 Mbps funcionarán a la menor velocidad que es 54 Mbps.

- El servidor que se implementó para la red mixta en el Municipio del Cantón Sucumbíos fue Windows 2003 por ser mas fácil de utilizar y administrar con respecto a Linux. En lo que se refiere a documentación para la instalación, configuración y administración de Windows 2003 fue más fácil adquirir, lo que no pasa con Linux, que no se encuentra una información completa y especialmente en un solo idioma.

6.2.- Recomendaciones

- La solución de seguridad en redes WLAN en un entorno corporativo depende de las políticas de seguridad que se quieran implantar. No obstante, debe ser teniendo en cuenta que la utilización de excesivas normas de seguridad podría reducir la rapidez y utilidad de la red inalámbrica. Limitando así al usuario final la utilización de la misma.

- Para el ingreso a la red por cada usuario es necesario mantener una política de contraseña adecuada. El administrador deberá prestar atención a las contraseñas, una contraseña debe ser lo suficientemente largo y contener caracteres no alfanuméricos, una desventaja de este método es que los usuarios tienen dificultades para recordarlas y las escriben en el papel en lugar de memorizarlas.

- Las redes WLAN deben ser asignadas a una subred dedicada y no compartidas con una red LAN. Este tipo de instalación se recomienda en caso de que no este configurada la seguridad. Al ser atacada una red los servidores que estén instalados se vuelven vulnerables, por lo tanto los datos, servidor, red, etc. pueden ser desconfigurados, copiado, cambiado o borrado su información.

- Se debe continuar con el estudio de la tecnología WLAN, por el variable cambio de los estándares especialmente a lo que se refiere a seguridades, ya que es una tecnología que va creciendo y que necesita de una constante actualización de conocimientos en lo que es software con la utilización de servidores Windows y Linux.

- Se recomienda realizar el estudio del estándar 802.11i o WPA2, que sirve para la implementación de seguridades en la WLAN, ya que es nuevo mecanismo en las redes inalámbricas seguras, pero hay que tomar en cuenta que lamentablemente los costos de los dispositivos por lo nuevos que son, son elevados, hallar una alternativa de costeo para la implementación se hace imperativo como buscar una entidad que esté en posibilidades de implementar este tipo de red y por ende costearla.

- La seguridad WLAN deben basarse en un tipo de EAP que soporte el tipo de autenticación adecuado. El método de EAP debe proporcionar una autenticación mutua, por lo tanto, no es recomendable utilizar EAP-MD5. En caso de utilización de EAP-TLS, y PEAP se recomienda configurar los clientes inalámbricos con un certificado de un servidor seguro y evitar que el usuario pueda Modificar estos parámetros. Únicamente el administrador debe tener privilegios para poder modificar el certificado empleado. Si no se configura el certificado, los ataques Man in the Middle son posibles.

- A pesar que Linux tiene un sinnúmero de fuentes de información especialmente en el Internet, sigue siendo dificultoso encontrar una completa guía que seguir o adoptar, debido a que se halla manuales de todas las distintas distribuciones que tiene Linux, en algunos casos las configuraciones son muy diferentes entre ellos. Mantener la información de una sola distribución de Linux es lo más recomendable para evitar confusiones entre los distintos manuales que pueden llegar ha hacer que los administradores de red dañen las configuraciones deteriorando el rendimiento de la red o en el peor de los casos dañarla por completo.

- Se recomienda hacer una buena capacitación a todo el personal que use y administre la red para que la información de las empresas o instituciones no este vulnerable, existen buenas alternativas de aprendizaje Online como las que presenta Microsoft con “Profesional Cinco Estrellas”, para el adiestramiento de Windows 2003 que es gratuito e incluso permite obtener una certificación de Microsoft.

- Es recomendable en la implementación de los dispositivos ya sea inalámbricos o alámbricos basarse en estándares y si es posible en una misma marca, para que posteriormente el funcionamiento de la red sea optima. Una vez instalada la red se debe utilizar políticas básicas de seguridad como son: deshabilitar el DHCP para redes inalámbricas, las IPs deben ser fijas, cambiar periódicamente el SSID, inhabilitar la emisión de broadcast del SSID.

- En el Mantenimiento de red WLAN se recomienda realizar copias de seguridad del Servicio de Autenticación de Internet (IAS), por lo que aquí está la configuración del Servidor RADIUS. Los archivos de seguridad de IAS incluyen todos los secretos de los clientes RADIUS. Se trata de una información extremadamente confidencial, por lo que debería tener cuidado y almacenar los datos en forma segura.