CAPÍTULO 4
ANÁLISIS DE IMPLEMENTACIONES

En el anterior capítulo se realizaron implementaciones en una red de datos para los protocolos de autenticación Kerberos, Radius y LDAP bajo las plataformas Windows y Unix. Por tal motivo, en base a las implementaciones realizadas a continuación se realizará un análisis más detallado de acuerdo a las siguientes características:

- Administración que se tiene con en el servidor implementado.
- Optimizar recursos del servidor de acuerdo a las necesidades del sistema operativo y del servicio de autenticación instalado.
- Eficiencia del protocolo de seguridad que emplea cada servidor de autenticación implementado.

4.1 ADMINISTRACIÓN DE SERVIDOR

Analizando las distintas implementaciones realizadas de los protocolos de autenticación Kerberos, Radius y LDAP bajo las plataformas Windows y Unix, se puede observar sus características de acuerdo a la complejidad de instalación del sistema operativo, implementación y configuración del servicio de autenticación, facilidad de administración para el usuario y la cantidad de documentación disponible para ayudar en la administración del servidor.

4.1.1 Kerberos, Radius y LDAP para Windows

La implementación de los protocolos de autenticación Kerberos, Radius y LDAP bajo el sistema operativo Windows es similar para los tres casos, ya que la instalación del sistema operativo Windows Server 2008 es la misma para los tres protocolos, donde dicha instalación del sistema operativo resulta intuitiva y fácil de realizar.

Por otro lado, la implementación y configuración del servicio de autenticación que se desea implementar radica básicamente en saber qué servicio de seguridad se desea habilitar en la consola del Administrador de funciones de Microsoft Windows Server 2008. Para comprender esto existe una gran cantidad de manuales en la página de internet de Windows.

Haciendo referencia a la facilidad de administración para el usuario, se considera como una interfaz muy amigable, intuitiva y de gran alcance administrativo para generar usuarios y asignar perfiles por medio de la Consola de Administración de servidor y usuarios Active Directory. Además se cuenta con comandos a nivel consola para realizar cargas masivas de usuarios.

4.1.2 Kerberos, Radius y LDAP para UNIX

La implementación de los protocolos de autenticación Kerberos, Radius y LDAP en UNIX resulta muy distinta al modo del cómo se realizan las implementaciones en Windows. Por tal motivo el análisis de estos tres servicios en UNIX resulta detallado y sin poder generalizar características.

4.1.2.1 Kerberos para UNIX

La implementación de Kerberos en Unix no resulta muy compleja haciendo referencia al sistema operativo dónde se instala el KDC, ya que la instalación del sistema operativo Ubuntu 8.04 es sencilla, sólo se necesita tener conocimientos sobre el tipo de formateo Ext2 que se realiza a la partición del disco donde se instala el sistema operativo y la ubicación del /(root) como punto de montaje.

La parte compleja de esta instalación radica en la implementación y configuración del servicio de seguridad Kerberos, ya que para realizar esto es necesario tener conocimientos en el dominio del ambiente Ubuntu para configurar la tarjeta de red, conocimiento en el manejo de comandos UNIX para el uso adecuado de la consola y para el manejo del editor de texto *vi*. Además los manuales de usuario de la página del MIT para realizar la instalación de Kerberos son insuficientes ya que no contempla muchos puntos para una correcta configuración.

La parte administrativa del servidor es insuficiente para que el usuario pueda realizar una fácil administración, ya que no se cuenta con una interfaz gráfica para realizar esta operación, por lo que la carga de usuarios y asignación de perfiles sólo se puede realizar a nivel consola, aunque se tiene la opción de realizar carga masiva de usuarios por medio de comandos a nivel consola. Es posible instalar Apache y php-myAdmin para tener un ambiente gráfico de administración del sistema, pero es muy complicado y tardado optimizar este recurso al servidor, además que no hay

información al respecto en las página principal del MIT y en Internet tampoco se cuenta con mucha información para realizar esta configuración.

4.1.2.2 Radius para UNIX

La implementación de Radius en Unix es compleja en la instalación del sistema operativo donde trabaja el servicio de autenticación, ya que se tiene una gran desventaja en la instalación y ambiente del sistema operativo, porque Ubuntu Server 8.04 LTS trabaja totalmente a nivel consola.

Se tiene la ventaja que se cuenta con gran cantidad de información en Internet y libros especializados para realizar la implementación, por tal motivo no resulta complicado realizar su respectiva configuración puesto que se cuenta con bastante información para lograr este fin. A pesar de ello el administrador debe tener dominio en el ambiente Ubuntu Server para configurar la tarjeta de red, conocimiento en el manejo de comandos UNIX para el uso adecuado de la consola y para el manejo del editor de textos *nano*. También se puede configurar sin problemas Apache en el servidor para tener un ambiente gráfico para la administración del servidor y con ello poder conectarse a él de manera remota.

La administración del servidor también resulta fácil de realizar, ya que por la basta cantidad de información que se cuenta para realizar este fin, cualquier duda al respecto puede ser aclarada sin mayor complicación por los manuales de usuario que existen en Internet, además el ambiente gráfico proporcionado por Apache facilita la creación de usuarios y asignación de perfiles, además que se cuenta con la opción de realizar carga masiva de usuarios por medio de comandos a nivel consola.

4.1.2.3 LDAP para UNIX

La implementación de LDAP en UNIX es sencilla de realizar para instalar el sistema operativo Fedora y para configurar el servicio de autenticación. Para instalar el sistema operativo Fedora no son necesarios conocimientos de experto, ya que se cuenta con un ambiente gráfico para realizar la instalación y además se pueden seleccionar los paquetes para complementar la instalación y de gran ayuda para la configuración posterior del servicio de autenticación como el Servidor Web Apache y el paquete Java JRE.

La instalación y configuración del servicio de autenticación LDAP no es complicada, puesto que no es necesario editar archivos de configuración y con la instalación de los paquetes de Directory Server se completa gran cantidad de configuración con un test en la instalación. En la página principal de Fedora se cuenta con un manual detallado para instalar y configurar lo necesarios para una correcta implementación.

La administración del servidor es fácil de realizar, ya que la Consola de Administración de Fedora Directory Server tiene interfaz gráfica y es de gran ayuda para crear usuarios y asignar perfiles, además se cuenta con la opción de realizar carga masiva de usuarios por medio de comandos a nivel consola.

4.2 OPTIMIZACIÓN DE RECURSOS DEL SERVIDOR

Dentro de la instalación y adecuación de una red de datos, es determinante, que se cuente con el hardware suficiente o mayor para que la capacidad de la misma no se vea sobrepasada, considerando las necesidades de aplicación y la demanda a la cual será sujeto el servicio, con lo cual se tendrá una eficiencia considerablemente mayor y los problemas de aplicación serán menores.

4.2.1 KERBEROS

En las Tablas 4-1 y 4-2 se muestran los requisitos de hardware para servidores en Kerberos.

Windows Server 2008		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	1.4 GHz (x64 processor) or 1.3GHz (Dual Core)	AMD Athlon XP 3000+ 2.10 GHz
Memoria	512 MB RAM	1.25 GB RAM
Espacio en Disco Duro Requerido	32 GB o mayor	80 GB
Pantalla	Super VGA (800 × 600) o alta	VGA
Otros	DVD drive, Teclado, Mouse, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-1. Requisitos servidor Kerberos en Windows

Ubuntu 8.04 Desktop Edition		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	1 GHz x86 Procesador	Pentium 4 1.60 GHz
Memoria	512 MB RAM	512 MB RAM
Espacio en Disco Duro Requerido	5 GB o mayor	30 GB
Pantalla	Tarjeta gráfica y monitor que soporte 1024x768	NVIDIA
Otros	CD/DVD drive, Teclado, Mouse, Audio, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-2. Requisitos servidor Kerberos en Unix

4.2.2 RADIUS

En las Tablas 4-3 y 4-4 se muestran los requisitos de hardware para servidores en Radius.

Windows Server 2008		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	1.4 GHz (x64 processor) or 1.3GHz (Dual Core)	AMD Athlon XP 3000+ 2.10 GHz
Memoria	512 MB RAM	1.25 GB RAM
Espacio en Disco Duro Requerido	32 GB o mayor	80 GB
Pantalla	Super VGA (800 × 600) o alta	VGA
Otros	DVD drive, Teclado, Mouse, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-3. Requisitos servidor Radius en Windows

Ubuntu Server 8.04 LTS		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	Intel x86 and AMD64 Procesador	Intel Core 2 T7200 2.00 GHz
Memoria	128 MB RAM	3 GB RAM
Espacio en Disco Duro Requerido	1 GB o mayor	100 GB
Pantalla	Super VGA (800 × 600) o alta	NVIDIA
Otros	CD/DVD drive, Teclado, Mouse, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-4. Requisitos servidor Radius en Unix

4.2.3 LDAP

En las Tablas 4-5 y 4-6 se muestran los requisitos de hardware para servidores LDAP.

Windows Server 2008		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	1.4 GHz (x64 processor) or 1.3GHz (Dual Core)	AMD Athlon XP 3000+ 2.10 GHz
Memoria	512 MB RAM	1.25 GB RAM
Espacio en Disco Duro Requerido	32 GB o mayor	80 GB
Pantalla	Super VGA (800 × 600) o alta	VGA
Otros	DVD drive, Teclado, Mouse, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-5. Requisitos servidor LDAP en Windows

Fedora 9 Core		
Componente	***Requisitos (Mínimos)***	***Implementación***
Procesador	X86 o x86_64 Procesador	Intel Core 2 T7200 2.00 GHz
Memoria	256 MB RAM	3 GB RAM
Espacio en Disco Duro Requerido	4 GB o mayor	100 GB
Pantalla	Super VGA (800 × 600) o alta	NVIDIA
Otros	CD/DVD drive, Teclado, Mouse, Internet.	CD/DVD drive, Teclado, Mouse, Internet.

Tabla 4-6. Requisitos servidor LDAP en Unix

Windows server en modo gráfico supone un uso de mayor recursos que cualquiera de los otros sistemas operativos, aunque tiene la posibilidad de instalación en modo consola, que supone menos recursos pero la pérdida de su principal características que es el ambiente amigable.

Ubuntu Server tiene requisitos mínimos debido a que es totalmente modo de consola.

Ubuntu Desktop y Fedora 9 son muy similares en su ambiente gráfico y requisitos por lo cual sus características de implementación son parecidos y menores a los de Windows Server.

4.3 EFICIENCIA DEL PROTOCOLO

Todos los protocolos analizados en este trabajo tienen el mismo reto de seguridad: la autenticación. Al considerar una aplicación de seguridad, la autenticación es un componente clave de cualquier solución de seguridad. La autenticación mutua, donde el cliente y el servidor deben autenticarse entre sí, se utiliza para garantizar que sólo a los usuarios autorizados se les permite el acceso a la red. Como se ha visto, Kerberos, RADIUS y LDAP son las más populares y útiles soluciones de autenticación que hacen frente a este desafío de seguridad en las redes de datos.

4.3.1 Eficiencia del protocolo Kerberos

Kerberos está diseñado para que dos partes puedan intercambiar información privada a través de una red, que de otra manera sería insegura. Kerberos proporciona autenticación mutua entre un cliente y un servidor, así como entre los servidores, antes de que una conexión de red se pueda abrir. Utiliza una técnica que consiste en un secreto compartido, que funciona como una contraseña. Esto sucede mediante la asignación de una clave única, llamada ticket, la cual se asigna a cada usuario que se conecta a la red. El ticket se incrusta en los mensajes para identificar al remitente del mensaje.

4.3.2 Eficiencia del protocolo RADIUS

Los servidores RADIUS son servidores robustos y escalables que proporcionan las funciones de autenticación, autorización y contabilidad (AAA), así como políticas avanzadas y gestión de configuración personalizada para controlar el acceso de usuarios a las redes cableadas. RADIUS y LDAP se utilizan a menudo juntos en algunas aplicaciones.

4.3.3 Eficiencia del protocolo LDAP

El Lightweight Directory Access Protocol (LDAP) es un extensible, un estándar de protocolo de red independiente del proveedor, un sistema de autenticación, y un servicio de directorio que se basa en el modelo de servicios de directorio X.500. LDAP es un repositorio de información, así como un protocolo para consultar y manipular los datos en un directorio LDAP. LDAP es uno de los directorios de autenticación más ampliamente utilizados en las redes modernas. LDAP se basa en las normas contenidas

en el estándar X.500, pero es mucho más simple y compatible con TCP/IP, que es necesario para cualquier tipo de acceso a Internet. Muchos de los dispositivos actuales de seguridad en redes, tienen soporte nativo para clientes LDAP.

En resumen, los tres protocolos cumplen con la tarea de autenticación de manera eficiente, pero cada uno de forma diferente e independiente; sin embargo, son protocolos que no están pelados entre sí sino que por el contrario pueden combinarse para formar sistemas mucho más robustos y seguros. Pero si de optar por uno se trata, se puede decir que el más completo en cuanto a seguridad, menor número de vulnerabilidades, y sobretodo el manejo de interfaces de administración amigables y más facilidades en cuanto a configuraciones se trata, es el protocolo LDAP.

En la Tabla 4-7 se muestra un resumen de las implementaciones realizadas, así como algunas de sus características.

PROTOCOLO	SISTEMA OPERATIVO	COMPLEJIDAD DE INSTALACIÓN	INTERFAZ	ADMINISTRACIÓN DE USUARIOS	CONFIGURACIÓN DE CLIENTE	INFORMACIÓN DE LOGS	CIFRADO
Kerberos	Windows Server 2008 Enterprise	Fácil: La instalación del sistema operativo y los componentes para utilizar el protocolo es muy intuitiva ya que solo es necesario seguir los pasos y confirmar opciones.	Amigable: Los menus y los textos incluidos en el sistema operativo son de facil acceso y uso para el administrador.	Fácil: La consola de administración de usuarios es muy comoda y accesible para agregar a cualquier usuario, ademas de tener varias opciones de configuración según las necesidades del administrador.	**Windows**: Agregar equipo a Dominio, Agregar perfil de usuario con privilegios correspondientes; **Linux**:Instalar Likewise, Configurar cuenta.	Muestran información sobre errores en general que el cliente envia, pueden o no evitar la conexión o ser importantes.	AES 128 y 256
	Ubuntu 8.04	Dificil: La instalación del sistema operativo no es compleja, pero la configuración del servidor requiere de conocimientos básicos en el uso de comandos Unix, ya que toda la instalación del servidor Kerberos es a nivel consola.	Complicada: No exíste una interfaz para manipular y consultar opciones del servidor, por lo que es necesario que el administrador tenga conocimientos básico en Unix.	Dificil: La admnistración de usuarios se hace compleja al no tener una consola dónde se pueda observar la unidad organizacional. Sólo es posible agregar usuarios por medio de comandos y cargas masivas de los mismos en archivos .txt.	**Windows:** Instalar programa MIT Kerberos para iniciar sesión en clientes Windows. Copiar achivo krb5.ini a C:\WINDOWS\system32 y archivos dll de configuración. Agregar IP de servidor kerberos a archivo hosts en ruta C:\WINDOWS\system32\drivers\etc. **Linux:**Copiar achivo krb5.conf y agregar IP de servidor kerberos a archivo hosts en ruta /etc.	Logs con información de inicio, caídas y fin de servicios en el servidor.	DES y 3DES

TABLA 4-7. ANÁLISIS COMPARATIVO

PROTOCOLO	SISTEMA OPERATIVO	COMPLEJIDAD DE INSTALACIÓN	INTERFAZ	ADMINISTRACIÓN DE USUARIOS	CONFIGURACIÓN DE CLIENTE	INFORMACIÓN DE LOGS	CIFRADO
Radius	Windows Server 2008 Enterprise	Fácil: La instalación del sistema operativo y los componentes para utilizar el protocolo es muy intuitiva ya que solo es necesario seguir los pasos y confirmar opciones. Requiere mas configuraciones y referencias sobre el tratamiento que da Windows Server 2008 a RADIUS, ya que lo llama NPS y es necesario realizar configuraciones especificas.	Amigable: Los menus y los textos incluidos en el sistema operativo son de facil acceso y uso para el administrador.	Fácil: La consola de administración de usuarios es muy comoda y accesible para agregar a cualquier usuario, ademas de tener varias opciones de configuración según las necesidades del administrador.	**Windows:** Agregar equipo a Dominio, Agregar perfil de usuario con privilegios correspondientes;	Muestran información sobre errores en general que el cliente envia, pueden o no evitar la conexión o ser importantes.	MD5 (Permite protección adicional configurando Ipsec, ESP y 3DES)
	Ubuntu Server 8.04 LTS	Difícil: Tanto la instalación del sistema operativo como la configuración del servidor Radius tiene un grado de complejidad alto, que requiere de ciertos conocimientos sobre sistemas Unix, ya que todo el proceso de instalación se debe hacer desde la consola o línea de comandos.	Muy complicada: La interfaz no es para nada amigable, ya que todo se realiza desde la consola; sin embargo se puede optar por la opción de configurar un servidor web para poder administrar remotamente desde cualquier otro equipo de la red a través de cualquier explorador de internet.	Difícil: La administración de usuarios se realiza desde la consola por medio de comandos, lo que resulta complicado; sin embargo, es posible instalar y configurar herramientas gráficas mediante las cuales esta tarea se vuelve considerablemente sencilla.	**Linux:** Agregar los usuarios a los archivos *users* y *clients.conf* del servidor.	Logs con información sobre las conexiones tanto exitosas como fallidas con el servidor de autenticación, así como errores en general.	WPA y WPA2.

TABLA 4-7. ANÁLISIS COMPARATIVO

PROTOCOLO	SISTEMA OPERATIVO	COMPLEJIDAD DE INSTALACIÓN	INTERFAZ	ADMINISTRACIÓN DE USUARIOS	CONFIGURACIÓN DE CLIENTE	INFORMACIÓN DE LOGS	CIFRADO
LDAP	Windows Server 2008 Enterprise	Fácil: La instalación del sistema operativo y los componentes para utilizar el protocolo es muy intuitiva ya que solo es necesario seguir los pasos y confirmar opciones.	Amigable: Los menus y los textos incluidos en el sistema operativo son de facil acceso y uso para el administrador.	Fácil: La consola de administración de usuarios es muy comoda y accesible para agregar a cualquier usuario, ademas de tener varias opciones de configuración según las necesidades del administrador.	**Windows:** Agregar equipo a Dominio, Agregar perfil de usuario con privilegios correspondientes;	Muestran información sobre errores en general que el cliente envia, pueden o no evitar la conexión o ser importantes.	SSL (Secure Sockets Layer)
	Fedora Core 9	Fácil: La instalación del sistema operativo es muy sencilla ya que se cuenta con la ayuda de una interfaz gráfica, y lo único en lo que se puede demorarse un poco es en definir bien el tamaño de las particiones. Por otro lado, la instalación del servidor LDAP, en este caso Fedora Directory Server, se realiza desde la consola, sin embargo los pasos son sencillos y no se requiere de configuraciones complejas.	Muy amigable: El sistema dispone de varias herramientas gráficas para la gestión de usuarios y demás configuraciones del sistema.	Fácil: La consola de administración de usuarios es muy comoda y accesible para agregar a cualquier usuario, ademas de tener varias opciones de configuración según las necesidades del administrador, de hecho es muy similar a la de LDAP para sistemas Windows.	**Windows y Linux:** Agregar equipo al Dominio, Agregar usuario y asignarlo el perfil o perfiles correspondientes.	Los logs son muy completos, muestran errores en general, conexiones con el servidor, duración de las sesiones y estadísticas generales sobre los usuarios.	SSL (Secure Sockets Layer)

TABLA 4-7. ANÁLISIS COMPARATIVO