CAPÍTULO 3
IMPLEMENTACIÓN DE SERVIDORES DE AUTENTICACIÓN

3.1 KERBEROS

3.1.1 Implementación de Kerberos en Windows

Instalación y configuración de Microsoft Windows Server 2008

-Insertar DVD de instalación de Windows Server 2008, utilizando la versión Enterprise

-Proporcionar contraseña de la cuenta de administrador.

-Configurar fecha, hora y zona horaria. (GMT -06:00) Guadalajara, Ciudad de México, Monterrey. El horario es importante ya que el protocolo no funcionara si los relojes no se encuentran sincronizados.

-Configurar nombre de servidor. WIN-72NP5HN05CF

-Configurar red. Asignando una dirección IP v.4 fija. 192.168.1.88

-Instalar rol de Active Directory Domain Services.

En Administrador del Servidor, ubicar las funciones y agregar el "Servicio de dominio de Active Directory". Esto se puede observar en la Figura 3-1.

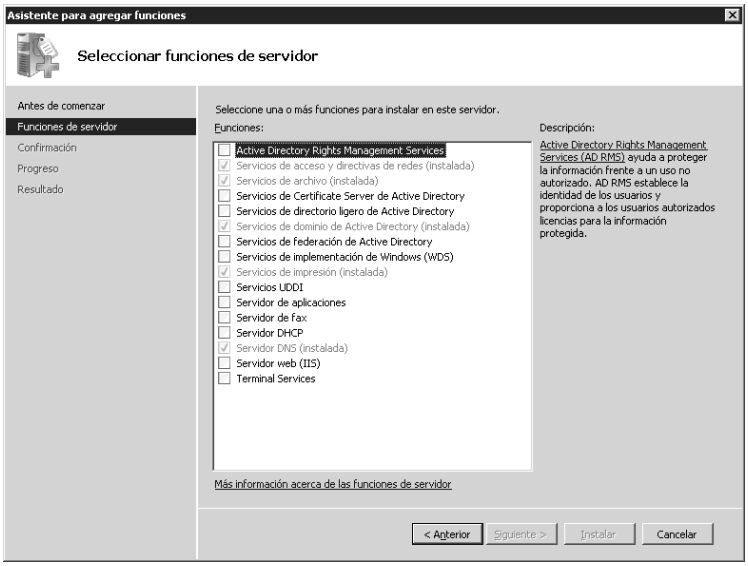

Figura 3-1. Administrador de funciones de Microsoft Windows Server 2008.

-Crear el controlador de dominio.

Para promocionar el rol antes instalado, es necesario, ejecutar el comando dcpromo.exe.

Continuar con las instrucciones y crear un nuevo dominio en un bosque nuevo.

Nombrar el bosque PROTOCOLOSFI.ORG, posteriormente se solicita instalación opcional de un servidor DNS, en este caso, como no se tiene otro servidor que realice tal función, se instala, por default al ser este el primer controlador de dominio de un bosque se instala el Catalogo Global.

-Indicar las ubicaciones de las bases de datos de los archivos log y de la página de Sysvol.

-Asignar la contraseña para la restauración de servicios del Directorio Activo.

-Finalizar y reiniciar el sistema.

-Crear usuarios de dominio y permisos.

Esta consola de administración se puede observar en la Figura 3-2.

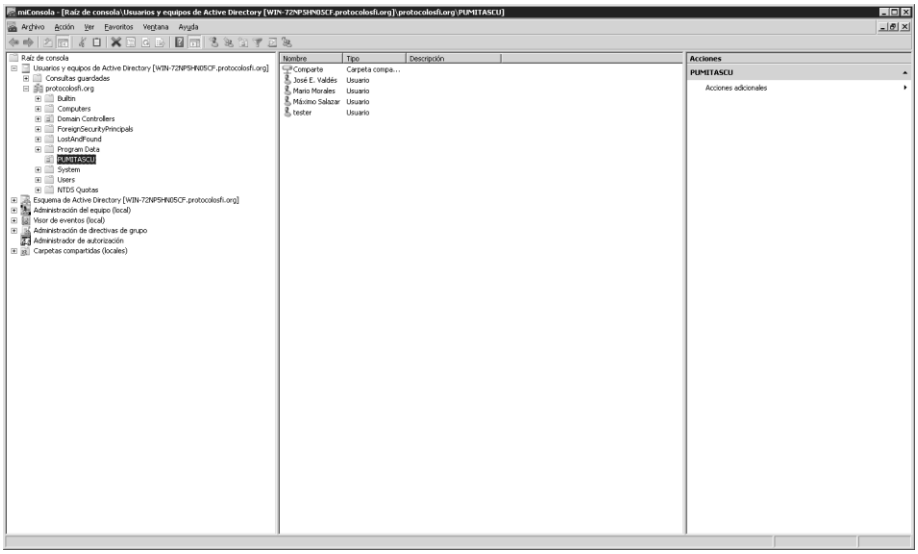

Figura 3-2. Consola de administración de servidor y usuarios.

a) Inicio de sesión de dominio en Windows XP

La configuración de usuario en un equipo con sistema operativo Windows XP, bajo el protocolo Kerberos en Microsoft Windows Server 2008, incluye agregar el equipo al dominio PROTOCOLOSFI.ORG, así como al usuario en caso de proporcionarle permisos de administrador. Esta opción se muestra en la Figura 3-3.

Figura 3-3. Acceso a Windows XP en el dominio PROTOCOLOSFI con la cuenta jvaldes.

Posteriormente, al estar con la sesión iniciada en el dominio, se puede hacer uso de cualquiera de los servicios compartidos por el servidor y con los permisos otorgados por el mismo, en este caso, una carpeta compartida y una impresora. Lo mencionado anteriormente se muestra en las Figuras 3-4 y 3-5.

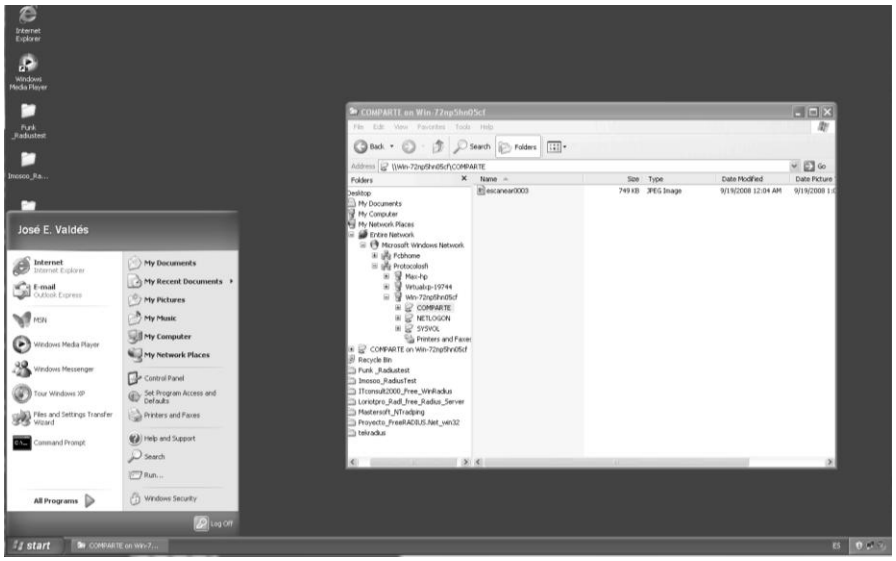

Figura 3-4. Carpeta compartida en el dominio PROTOCOLOSFI.

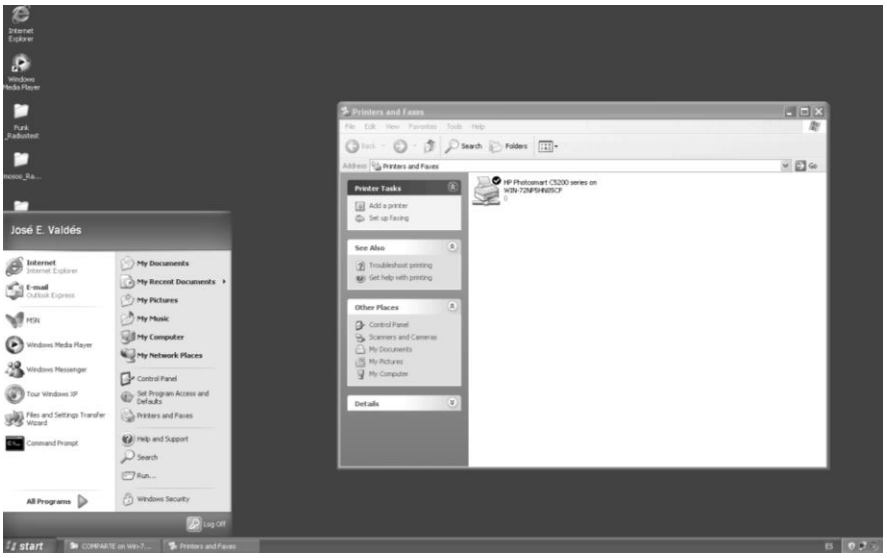

Figura 3-5. Impresora compartida por el dominio PROTOCOLOSFI.

b) Inicio de sesión de dominio en Windows 7

La configuración de usuario en un equipo con sistema operativo Windows 7, bajo el protocolo Kerberos en Microsoft Windows Server 2008, incluye agregar el equipo al dominio PROTOCOLOSFI.ORG, así como al usuario en caso de proporcionarle permisos de administrador. Esto se puede observar en la Figura 3-6.

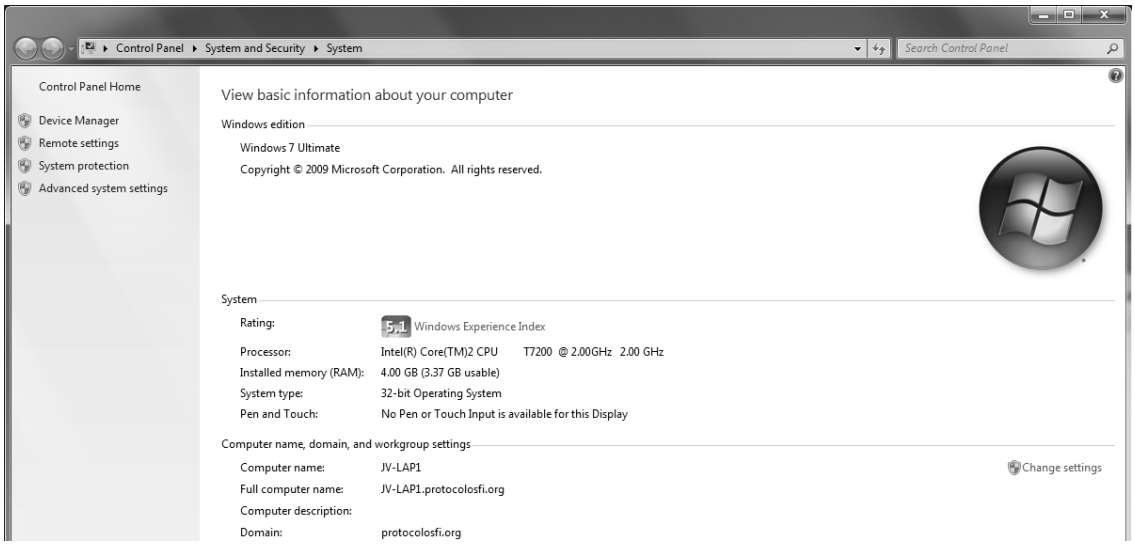

Figura 3-6. Equipo en dominio PROTOCOLOSFI.ORG.

Posteriormente, al estar con la sesión iniciada en el dominio, se puede hacer uso de cualquiera de los servicios compartidos por el servidor y con los permisos otorgados por el mismo, en este caso, una carpeta compartida y una impresora. Esto se puede observar en la Figura 3-7.

Figura 3-7. Carpeta e impresora compartida en PROTOCOLOSFI.

c) Inicio de sesión de dominio en Ubuntu Linux

Para agregar un equipo con sistema operativo Linux, se procede a instalar el programa Likewise, con lo cual es fácil establecer la relación entre el servidor de dominio y el equipo de cómputo, aunque no pertenezcan al mismo ambiente.

Es necesario descargar el paquete LikewiseOpen-4.1.0.1846-linux e instalarlo o simplemente agregarlo por medio de Synaptic.

Finalmente es necesario configurar el programa Likewise con el dominio y la sesión a utilizar. Esta consola de configuración se puede observar en la Figura 3-8.

Figura 3-8. Configuración de Likewise en PROTOCOLOSFI.

Se ingresa al dominio dando clic en "Join Domain" y posteriormente se ingresa la contraseña y se verifica que el equipo se encuentra en el dominio correspondiente. Esto se muestra en la Figura 3-9.

Figura 3-9.Dominio PROTOCOLOSFI.ORG

Una vez ingresado en el dominio, en éste se encuentran los datos del perfil y se puede verificar que el usuario y el equipo pertenecen al dominio. Estos datos se muestran en la Figura 3-10.

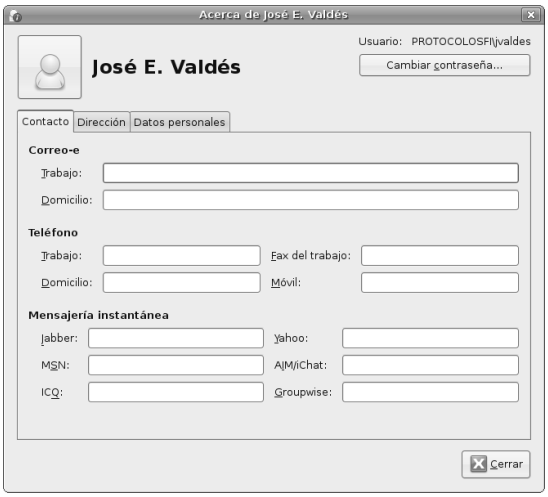

Figura 3-10. Propiedades de usuario en Ubuntu, del dominio PROTOCOLOSFI.

Mediante la consola de Linux, y utilizando el comando kinit y el nombre de usuario, se prueba que el protocolo funciona y se ingresa correctamente recibiendo el ticket de kerberos, esto se muestra en la Figura 3-11.

```
root@jv-lap1:~# kinit jvaldes
jvaldes@PROTOCOLOSFI.ORG's Password:
root@jv-lap1:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: jvaldes@PROTOCOLOSFI.ORG

  Issued           Expires          Principal
Apr  2 23:34:18  Apr  3 09:34:05  krbtgt/PROTOCOLOSFI.ORG@PROTOCOLOSFI.ORG
```

Figura 3-11. Ticket de Kerberos en consola de Ubuntu.

3.1.2 Implementación de Kerberos en UNIX

La instalación del servicio de autenticación Kerberos se realizará en el Sistema Operativo Ubuntu. Para comenzar a levantar este servicio será necesario previamente instalar en un equipo de cómputo el sistema operativo mencionado. La instalación y configuración inicial de Ubuntu 8.04 se precisa con mayor detalle en el Anexo 1.

Instalado el Sistema Operativo Ubuntu en el equipo de cómputo, lo siguiente a realizar es instalar el servidor de autenticación Kerberos.

Si se está estableciendo un nuevo reino Kerberos, se tendrá que empezar por la elección de una implementación de Kerberos para el KDC. Hay muchos KDC disponibles de diferentes proveedores, tanto comerciales como de código abierto. Cada aplicación KDC es diferente, con ventajas y desventajas sobre los demás.

Para este caso la elección del KDC debe ser de código abierto y de distribución libre. Dentro de las distribuciones KDC que cumplen estas características son MIT y Heimdal. Se elegirá como el KDC para instalación y configuración la distribución proporcionada por MIT (Massachusetts Institute of Technology), esto porque el KDC de MIT es la primera y aún la implementación de referencia para Kerberos 4 y 5. Muchas grandes entidades, la mayoría universidades, usan como KDC la autenticación con MIT. Hay una gran base de apoyo para el MIT de Kerberos y se utiliza en muchos ambientes, que ayuda a ejercitar los errores del sistema. MIT Kerberos contiene soporte para los estándares de encriptación de Kerberos, en particular para simple y triple DES. Además, la versión 1.8 (la más reciente) del MIT Kerberos, incluye soporte para el tipo de encriptación RC4 utilizado por el servicio Active Directory de Microsoft Kerberos, así como el nuevo Advanced Encryption Standard (AES).

Kerberos requiere del buen funcionamiento de varios servicios externos. En particular los relojes de todos los equipos participantes deben estar sincronizados a pocos minutos. En primer lugar, el NTP (Network Time Protocol) debe estar instalado en cada servidor y el KDC en la red. El NTP sincroniza los relojes de las máquinas a una fuente central el cual puede ser un recurso de hora local. Si bien es posible configurar para sincronizar todas las máquinas a través de la red, debe haber un servidor de tiempo a disposición del público, donde para los administradores del sitio se recomienda realizar la creación de una fuente de tiempo centralizado en la red y crear otras máquinas en la red para sincronizar con el servidor. La máquina de servidor de tiempo se puede sincronizar a una fuente de reloj de precisión, como un servidor de tiempo público.

Los detalles para implementar el NTP en la red de datos no se contempla en esta explicación de la implementación de Kerberos, pero si se debe contemplar este punto en la implementación ya que relojes mal sincronizados es la raíz de muchos problemas que se generan en el uso de Kerberos a pesar que las implementaciones de Kerberos prevén normalmente unos más o menos cinco minutos de error al comparar los tiempos. Los sistemas Unix no suelen tener NTP instalado y configurado por lo que la configuración de forma manual es necesaria para mantener los relojes de estos sistemas en sincronización. [11]

Dado que la distribución MIT de Kerberos está disponible como código abierto, hay dos maneras de instalarlo: la construcción desde el código fuente o la obtención de una distribución binaria de su proveedor de Unix. Se va a cubrir la instalación por código fuente y dicha distribución del MIT está disponible en la página principal de MIT Kerberos, ubicado en http://web.mit.edu/network/kerberos-form.html.

Una vez descargado el archivo de la página de Internet mencionada, éste está comprimido del siguiente modo krb5-1.8-signed.tar. Para descomprimir este archivo se ejecuta lo siguiente:

```
home/mario# tar krb5-1.8-signed.tar
```

Tras ser descomprimido se obtienen los archivos krb5-1.8.tar.gz.asc y krb5-1.8.tar.gz, el primer archivo mencionado servirá para verificar la versión, esto se obtiene ejecutando lo siguiente:

```
/home/mario# gpg --verify krb5-1.8.tar.gz.asc
```

El resultado que arroja es el siguiente:

```
gpg: Firmado el mar 02 mar 2010 12:24:50 CST usando clave RSA ID
F376813D
```

En este caso como se cuenta con la versión más reciente, no es reemplazado el archivo por alguna otra versión. Lo siguiente a realizar es descomprimir el archivo krb5-1.8.tar.gz. Esto se obtiene ejecutando en *prompt* lo siguiente:

```
/home/mario# tar xzvf krb5-1.8.tar.gz
```

Esto crea un directorio krb5-1.8 en la ubicación donde se descomprimió el archivo, en esta ruta se colocan todos los archivos de la distribución de código fuente de Kerberos. Dentro del directorio krb5-1.8, hay un directorio de nombre /src y otro directorio /doc. Dado que se pretende construir la distribución, ingresar al directorio krb5-1.8/src.

Para compilar la distribución se ejecuta lo siguiente:

```
# ./configure && make
```

Una vez que la compilación está completa, instalar el software:

```
# make install
```

El paso de instalación establece la estructura de directorios bajo su prefijo (/usr/local por default) y en lugares binarios, incluye archivos, bibliotecas y en sus lugares apropiados en el directorio prefijo.

Tener en cuenta que el proceso de instalación no crea el directorio (/usr/local/var por default). Por lo que se tendrá que crear este directorio antes de ejecutar el make install, así como crear un directorio krb5kdc debajo de ella. Además, se tiene que establecer permisos en el directorio krb5kdc para garantizar que los usuarios no autorizados no pueden acceder a datos sensibles del KDC. Para crear esto se ejecuta en prompt lo siguiente:

```
# mkdir /usr/local/var
# mkdir /usr/local/var/krb5kdc
# chown root /usr/local/var/krb5kdc
# chmod 700 /usr/local/var/krb5kdc
```

3.1.2.1 Creación del reino

Ahora se va a realizar una nueva instalación de Kerberos para crear el reino. Este paso sólo se realizará en el KDC principal. Crear los archivos necesarios de base de datos y llenar la base de datos KDC son los principios necesarios. En primer lugar, se necesitan crear algunos archivos de configuración.

Estrictamente la única configuración de archivo que se necesita es crear el archivo krb5.conf. El archivo krb5.conf vive en /etc y contiene los parámetros que se utilizan para las librerías de Kerberos. El archivo krb5.conf tiene una apariencia similar a un archivo Windows del tipo in, con estrofas (o grupos) entre corchetes y los key-value separados por un signo igual. En este punto todo lo que se necesita para este archivo es lo siguiente:

```
[libdefaults]
    ticket_lifetime = 24000
    default_realm = PROTOCOLOSFI.ORG
    dns_lookup_realm = false
    dns_lookup_kdc = false

[realms]
  PROTOCOLOSFI.ORG = {
            kdc = kdc.protocolosfi.org
            admin_server = kdc.protocolosfi.org
            default_domain = protocolosfi.org

  }

[domain_realm]
    .protocolosfi.org = PROTOCOLOSFI.ORG
```

```
        protocolosfi.org = PROTOCOLOSFI.ORG

    [logging]
        default = FILE:/usr/local/var/krb5kdc/krb5lib.log
        kdc = FILE:/usr/local/var/krb5kdc/krb5kdc.log
        admin_server = FILE:/usr/local/var/krb5kdc/kadmin.log

    [kdc]
        profile = /usr/local/var/krb5kdc/kdc.conf

    [pam]
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
```

Otro archivo de configuración que se va a crear es el archivo de configuración del KDC, este archivo tiene el nombre de kdc.conf.

Si no se ha modificado el prefijo o las opciones del localstatedir en el proceso de configuración, este archivo se encuentra en la ruta /usr/local/var. En general los archivo de la las bases de datos KDC viven bajo el directorio krb5kdc. La forma general de archivo kdc.conf es el siguiente:

```
    [kdcdefaults]
        kdc_ports = 88

    [realms]
     PROTOCOLOSFI.ORG = {
        kadmind_port = 749
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        admin_keytab = /usr/local/var/krb5kdc/kadm5.keytab
        acl_file = /usr/local/var/krb5kdc/kadm5.acl
        master_key_type = des3-hmac-sha1
        supported_enctypes = des3-hmac-sha1:normal des-cbc-crc:normal
des-cbc-cr
c:v4
        kdc_supported_enctypes = des3-hmac-sha1:normal des-cbc-
crc:normal des-cb
c-crc:v4
     }

    [logging]
        kdc = FILE:/usr/local/var/krb5kdc/kdc.log
        admin_server = FILE:/usr/local/var/krb5kdc/kadmin.log
```

Con los archivos de configuración realizados se está listo para inicializar la base de datos Kerberos. Para realizar este paso se va a utilizar el programa kdb5_util, incluido con la distribución de Kerberos. Este programa realiza diversas tareas administrativas en la base de datos Kerberos. Por ahora, se utilizará el parámetro create para crear una base de datos y con esto crear el esquema del nuevo reino.

Con la siguiente línea de comandos se crea un nuevo reino:

```
# /usr/local/sbin/kdb5_util create –s
```

La opción -s indica que se estará usando un archivo de contraseñas Kerberos que pide la clave maestra. A continuación se mostrará el cuadro de diálogo que se presenta durante la ejecución del programa kdb5_util cuando se ejecuta el comando create:

```
# /usr/local/sbin/kdb5_util create -s
Initializing database '/usr/local/var/krb5kdc/principal' for realm
'protocolosfi.org',
master key name 'K/M@protocolosfi.org'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

Una vez creado el reino, agregar el archivo kadm5.acl en la ruta /usr/local/var/krb5kdc/kadm5.acl . Este archivo contendrá lo siguiente:

```
*/admin@PROTOCOLOSFI.ORG       *
```

Finalmente indicar el KDC (krb5kdc) del siguiente modo:

```
# krb5kdc
# krb5kdc start
```

Iniciar el kadmin de manera local ejecutando lo siguiente:

```
# /usr/local/sbin/kadmin.local
Authenticating as principal minclan/admin@PROTOCOLOSFI.ORG with
password.
      kadmin.local:
```

Una vez dentro de kadmin.local, se pueden enumerar los *principals* que se tienen actualmente en el KDC:

```
kadmin.local:  listprincs
K/M@PROTOCOLOSFI.ORG
kadmin/history@PROTOCOLOSFI.ORG
krbtgt/PROTOCOLOSFI.ORG@PROTOCOLOSFI.ORG
```

El comando ank sirve para añadir algunos clientes al KDC:

```
kadmin.local:  ank minclan
WARNING:  no  policy  specified  for  minclan@PROTOCOLOSFI.ORG;
defaulting to no
policy
Enter password for principal "minclan@PROTOCOLOSFI .ORG":
Re-enter password for principal "minclan@PROTOCOLOSFI .ORG":
    Principal "minclan@PROTOCOLOSFI .ORG" created.


kadmin.local:  ank jvaldes
WARNING:  no  policy  specified  for  jvaldes@PROTOCOLOSFI.ORG;
defaulting to no
```

```
    policy
    Enter password for principal "jvaldes@PROTOCOLOSFI .ORG":
    Re-enter password for principal "jvaldes@PROTOCOLOSFI .ORG":
        Principal "jvaldes@PROTOCOLOSFI .ORG" created.


    kadmin.local:  ank mwindows
    WARNING:  no  policy  specified  for  mwindows@PROTOCOLOSFI.ORG;
defaulting to no
    policy
    Enter password for principal " mwindows@PROTOCOLOSFI .ORG":
    Re-enter password for principal " mwindows@PROTOCOLOSFI .ORG":
        Principal " mwindows @PROTOCOLOSFI .ORG" created.
```

Para observar los clientes recién dados de alta al KDC se ejecuta nuevamente el comando listprincs:

```
    kadmin.local:  listprincs
    K/M@PROTOCOLOSFI.ORG
    jvaldes@PROTOCOLOSFI.ORG
    mwindows @PROTOCOLOSFI.ORG
    kadmin/history@PROTOCOLOSFI.ORG
    krbtgt/PROTOCOLOSFI.ORG@PROTOCOLOSFI.ORG
    minclan@PROTOCOLOSFI.ORG
```

Una vez vistos en la lista que arroja el comando listprincs los clientes que se dieron de alta en la Base de Datos, se da por terminada la fase de configuración del KCD Kerberos.

En el equipo de cómputo que está actuando como el servidor Kerberos, en su archivo hosts ubicado en la ruta /etc, modificarlo por el editor vi y agregar las siguientes líneas:

```
127.0.0.1 localhost
192.168.1.101 kdc.protocolosfi.org
192.168.1.2 jvaldes.protocolosfi.org
192.168.1.3 minclan.protocolosfi.org
192.168.1.4 mwindows.protocolosfi.org
```

Esto actuará como servidor DNS y el servidor ubicará los equipos de cómputo que tendrá como clientes.[12]

3.1.2.2 Configuración de clientes en Linux

Para llevar a cabo la configuración de un cliente bajo el sistema Linux realizar lo siguiente:

1) Copiar el archivo de configuración krb5.conf del servidor KDC que vive en la ruta /etc a los equipos de cómputo cliente en la ruta /etc.
2) En los equipo de cómputo que estén actuando como clientes, en su archivo

hosts ubicado en la ruta /etc agregar las siguientes líneas:

```
127.0.0.1 localhost
192.168.1.101 kdc.protocolosfi.org kdc
```

3.1.2.3 Configuración de clientes en Windows

Para llevar a cabo la configuración de un cliente bajo el sistema Windows realizar lo siguiente:

1) En el equipo cliente bajo el sistema operativo Windows se descargará el archivo .exe y el archivo .bin para Windows de la página de internet http://web.mit.edu/kerberos/www/.
2) Ejecutar el archivo .exe dando doble clic al icono del programa cliente Kerberos. El archivo .exe es similar al icono que se muestra en la Figura 3-12.

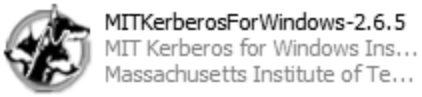

Figura 3-12 Icono ejecutable del programa cliente Kerberos.

3) Pasar los archivos dll del archivo .bin descargado a la ruta C:\WINDOWS\system32. Estos archivos se muestran en la Figura 3-13.

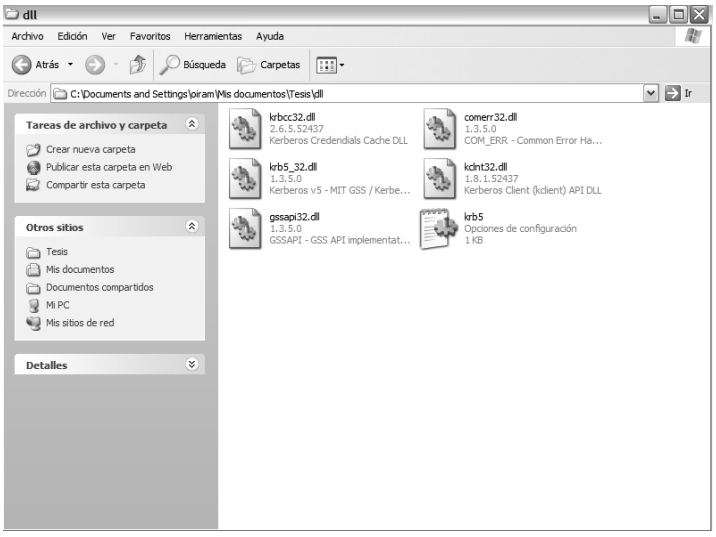

Figura 3-13. Archivos DLL para configuración de cliente Kerberos.

También pasar el archivo krb5.ini con la misma configuración que el archivo krb5.conf que se creó en la ruta /etc en el KDC a la ruta C:\WINDOWS\system32

4) Ir a la ruta C:\WINDOWS\system32\drivers\etc y editar el archivo hosts. En este archivo agregar la dirección IP del KDC. Este archivo de configuración se

muestra en la Figura 3-14.

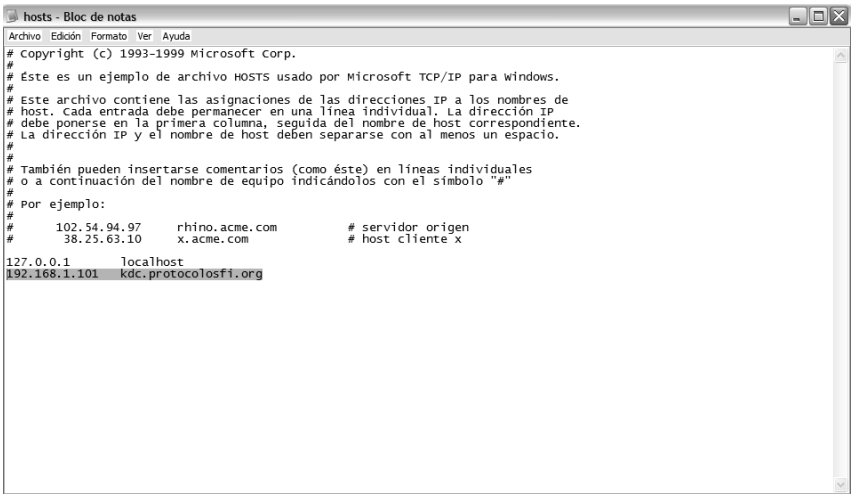

Figura 3-14. Archivos de configuración hosts.

5) Abrir el programa Leash para iniciar el programa de Kerberos para Windows. Éste se encuentra ubicado en la ruta que se muestra en la Figura 3-15:

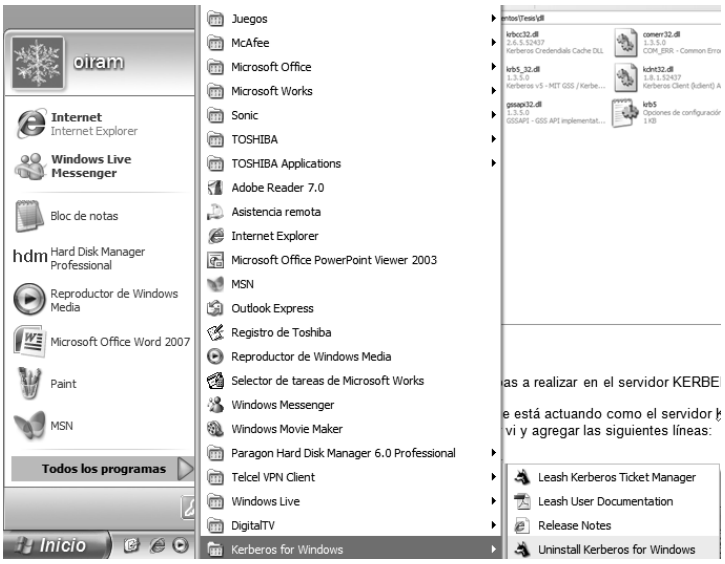

Figura 3-15. Ruta de programa Leash.

Una vez abierto el programa Leash, éste se visualiza de modo que muestra la Figura 3-16:

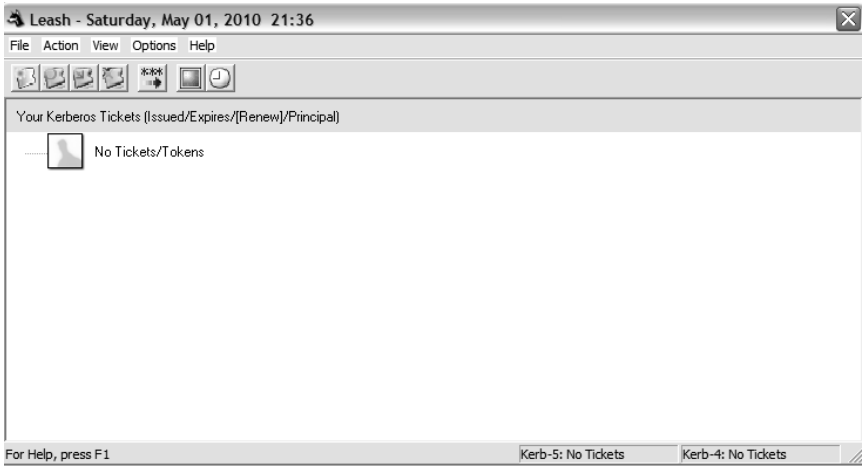

Figura 3-16. Ventana inicial de programa Leash.

6) Configurar las opciones del Leash para que reconozca el reino PROTOCOLOSFI.ORG, esto se hace yendo a la pestaña Options y posterior a la pestaña Kerberos v5 Properties. Esto se visualiza en la Figura 3-17.

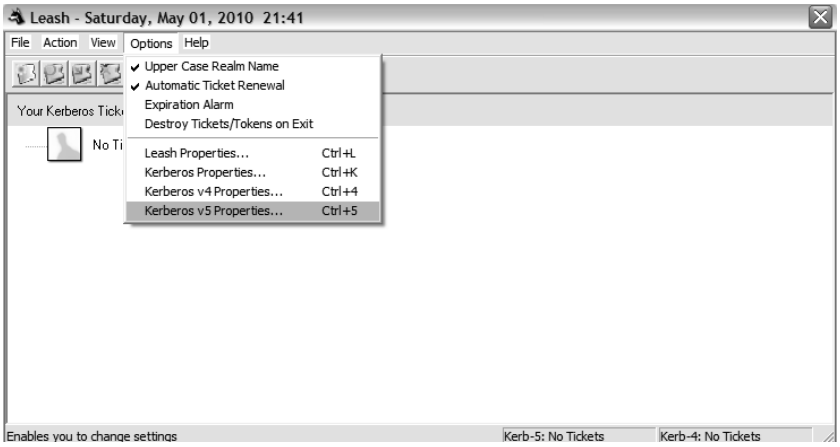

Figura 3-17. Ruta para configurar ruta del KDC.

7) Una vez abierta dicha ventana, cambiar la ruta dada por default por la ruta donde se encuentra el archivo de configuración krb5.ini que se copió en la ruta C:\WINDOWS\system32. Esto se visualiza en la Figura 3-18.

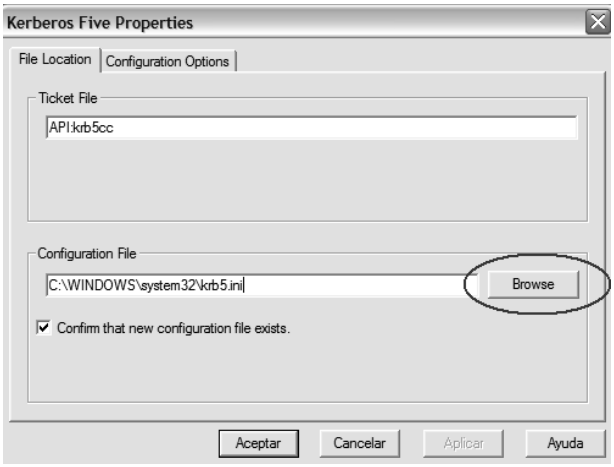

Figura 3-18. Ruta para configurar KDC de Kerberos.

3.1.2.4 Pruebas de conexión con servidor Kerberos

Para hacer algunas pruebas al servidor KERBEROS con clientes bajo sistemas operativos Linux y Windows realizar lo siguiente:

Los clientes que se intenten conectar al servidor Kerberos podrán realizarlo sin necesidad de estar dentro de un DNS. Tener en cuenta que hay que configurar sus respectivas IP en los equipos de cómputo que conforman la red del modo que muestra la Tabla 3-19.

IP address	Hostname	Tipo de Equipo
192.168.1.101	kdc.protocolosfi.org	Servidor
192.168.1.2	jvaldes.protocolosfi.org	Cliente Linux
192.168.1.3	minclan.protocolosfi.org	Cliente Linux
192.168.1.4	mwindows.protocolosfi.org	Cliente Windows

Tabla 3-19. Ruta para configurar KDC de Kerberos.

Una vez configurados los equipos de cómputo clientes con su respectiva IP, se podrán realizar las siguientes pruebas de conexión:

Prueba 1)

Autenticar un equipo de cómputo cliente bajo sistema operativo UNIX con el servidor Kerberos. En el equipo de cómputo que actuará como cliente ejecutar lo siguiente:

```
root@oiram-lap:/etc# kinit minclan
Password for minclan@PROTOCOLOSFI.ORG:
```

Si no se arroja en el prompt algún error, la autenticación pudo realizarse sin ningún problema. Para corroborar esto, ejecutar en el equipo de cómputo cliente lo siguiente:

```
root@oiram-lap:/etc# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: minclan@PROTOCOLOSFI.ORG

Valid starting     Expires            Service principal
04/02/10         21:27:42                 04/03/10         21:27:42
krbtgt/PROTOCOLOSFI.ORG@PROTOCOLOSFI.ORG
          renew until 04/02/10 21:27:42

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

Con esto se observa que el equipo de cómputo cliente ha obtenido los Tickets necesarios para poder autenticarse con el servidor Kerberos.

Prueba 2)

Realizar prueba con un equipo de cómputo bajo sistemas operativos UNIX con un USUARIO NO DADO DE ALTA en el servidor Kerberos. Ejecutar lo siguiente en algún equipo de cómputo cliente:

```
root@oiram-lap:/usr/local/bin# kinit msalazar
kinit(v5): Client not found in Kerberos database while getting
initial
credentials
```

Con esto se observa que algún usuario que no esté dado de alta dentro en la base de datos del KDC, no podrá autenticarse con el servidor.

Prueba 3)

Realizar prueba con un equipo de cómputo bajo sistemas operativos UNIX con un USUARIO EXISTENTE PERO CON CONTRASEÑA DISTINTA A LA DADA DE ALTA en la base de datos del KDC. Ejecutar lo siguiente en algún equipo de cómputo cliente:

```
root@oiram-lap:/usr/local/bin# kinit minclan
Password for minclan@PROTOCOLOSFI.ORG:
kinit(v5): Password incorrect while getting initial credentials
```

Esta prueba demuestra que no puede autenticarse con el servidor Kerberos un

usuario si ingresa de manera errónea su respectivo *password*, a pesar que el usuario exista en la base de datos.

Prueba 4)

Realizar pruebas de usuario bajo el sistema operativo Windows XP utilizando el usuario mwindows. Una vez que se inició sesión en un equipo de cómputo que actuará como cliente bajo el sistema operativo Windows XP y que ya tiene configurado e instalado el programa MIT Kerberos para Windows, se puede observar que tiene instalado dicho programa si se observa el icono del programa cliente Kerberos Leash tal como lo muestra la Figura 3-20.

Figura 3-20. Icono de programa Leash instalado en equipo de cómputo.

Iniciar el programa Leash, una vez abierto ir a la pestaña Action y posteriormente abrir la pestaña Get Tickets(s) para poder iniciar sesión con el principal dado de alta en la base de datos del KDC en el reino PROTOCOLOFI.ORG. Esto lo muestra la Figura 3-21.

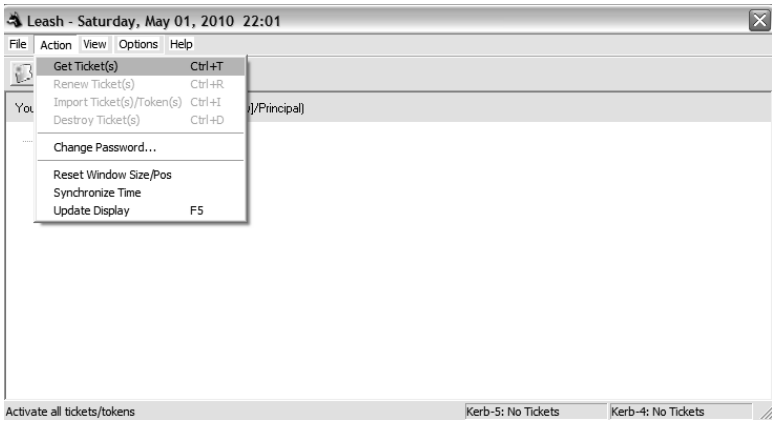

Figura 3-21. Ruta para abrir opción “Initialize ticket”.

Esta pestaña abre la ventana que se muestra en la Figura 3-22.

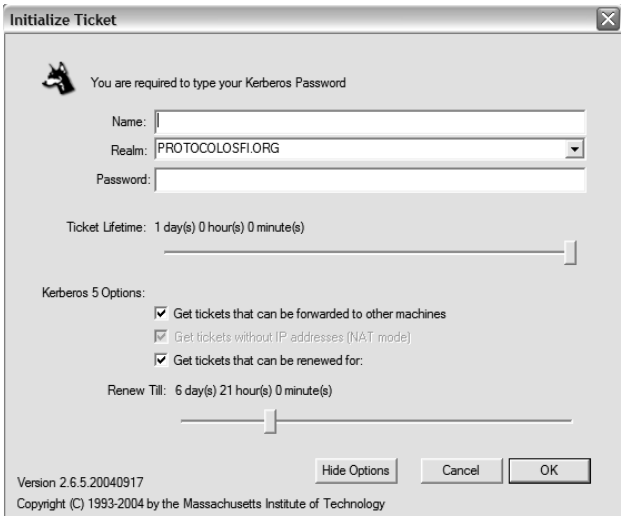

Figura 3-22. Ventana "Initialize ticket".

En esta ventana ingresar los datos del principal para poder iniciar el intercambio de tickets entre el KDC y el cliente, un ejemplo de lo mencionado anteriormente se muestra en la Figura 3-23.

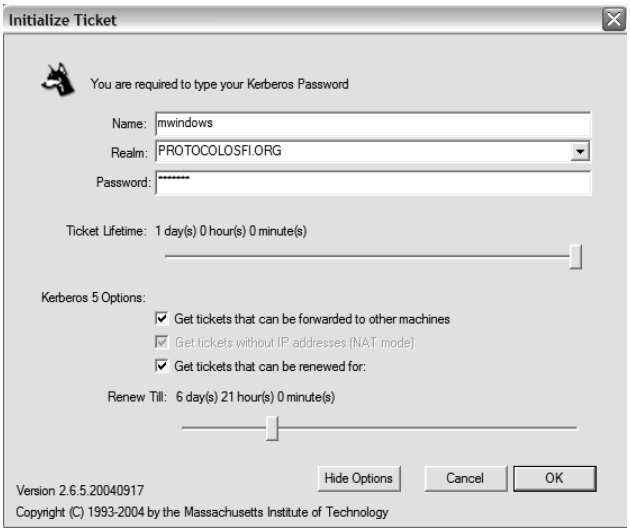

Figura 3-23. Configuración de datos del cliente en ventana "Initialize ticket".

Una vez ingresados de manera correcta los datos del principal, oprimir el botón OK. Observar que el icono del Leash ha cambiado al estatus de conectado tal como lo muestra la Figura 3-24:

Figura 3-24. Estatus de conexión afirmativo con reino Kerberos.

El programa del Leash muestra el intercambio de tickets entre el KDC y el principal mwindows. Esto se muestra en las Figuras 3-25 y 3-26:

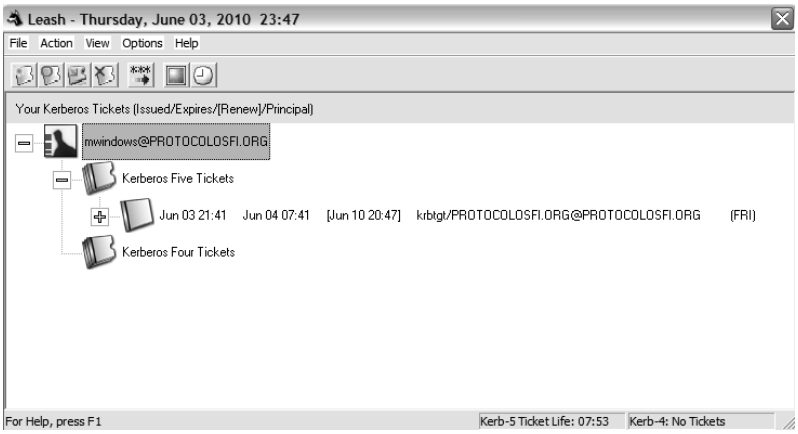

Figura 3-25. Intercambio de tickets con servidor Kerberos.

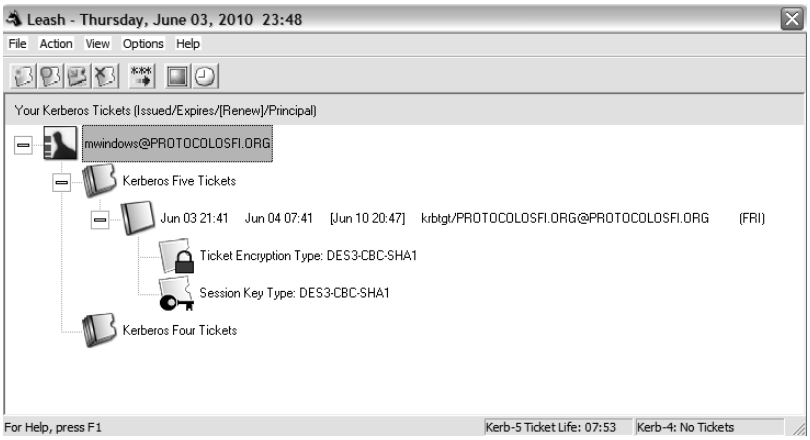

Figura 3-26. Intercambio detallado de tickets con servidor Kerberos.

Para observar el intercambio de tickets a nivel consola teclear desde el prompt de Windows lo que se muestra en la Figura 3-27:

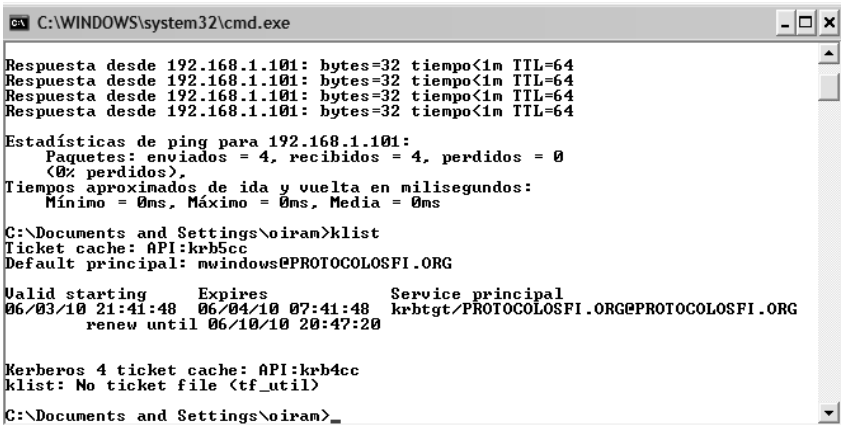

Figura 3-27. Intercambio de tickets desde el pompt de Windows

Cabe aclarar que si se ingresa de modo incorrecto la contraseña con la que se dio de alta el usuario en la base de datos del KDC, se obtiene la ventana de error que se muestra en la Figura 3-28:

Figura 3-28. Ventana de error de conexión con servidor Kerberos.

3.2 RADIUS

3.2.1 Implementación de RADIUS en Windows

Instalación y configuración de Microsoft Windows Server 2008

-Insertar DVD de instalación de Windows Server 2008, utilizando la versión Enterprise

-Proporcionar contraseña de la cuenta de administrador.

-Configurar fecha, hora y zona horaria. (GMT -06:00) Guadalajara, Ciudad de México, Monterrey. El horario es importante ya que el protocolo no funcionara si los relojes no se encuentran sincronizados.

-Configurar nombre de servidor. WIN-72NP5HN05CF

-Configurar red. Asignando una dirección IP v.4 fija. 192.168.1.88

-Instalar rol de Active Directory Domain Services.

En Administrador del Servidor, ubicar las funciones y agregar el "Servicio de dominio de Active Directory". Esto se muestra en la Figura 3-29.

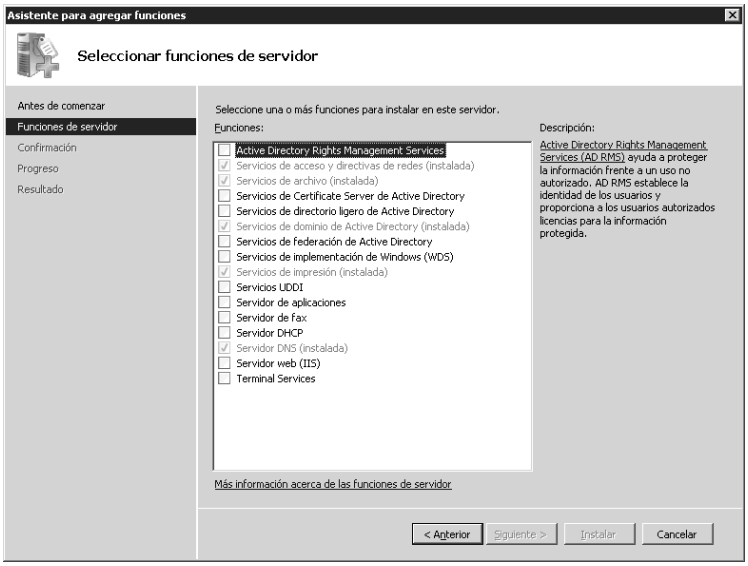

Figura 3-29. Administrador de funciones de Microsoft Windows Server 2008.

-Crear el controlador de dominio.

Para promocionar el rol antes instalado, es necesario, ejecutar el comando dcpromo.exe.

Continuar con las instrucciones y crear un nuevo dominio en un bosque nuevo.

Nombrar el bosque PROTOCOLOSFIR.ORG, posteriormente se solicita instalación opcional de un servidor DNS, en este caso, como no se tiene otro servidor que realice tal función, se instala, por default al ser éste el primer controlador de dominio de un bosque se instala el Catalogo Global.

-Indicar las ubicaciones de las bases de datos de los archivos log y de la página de Sysvol.

-Asignar la contraseña para la restauración de servicios del Directorio Activo.

-Finalizar y reiniciar el sistema.

-Crear usuarios de dominio y permisos.

Esta consola se muestra en la Figura 3-30.

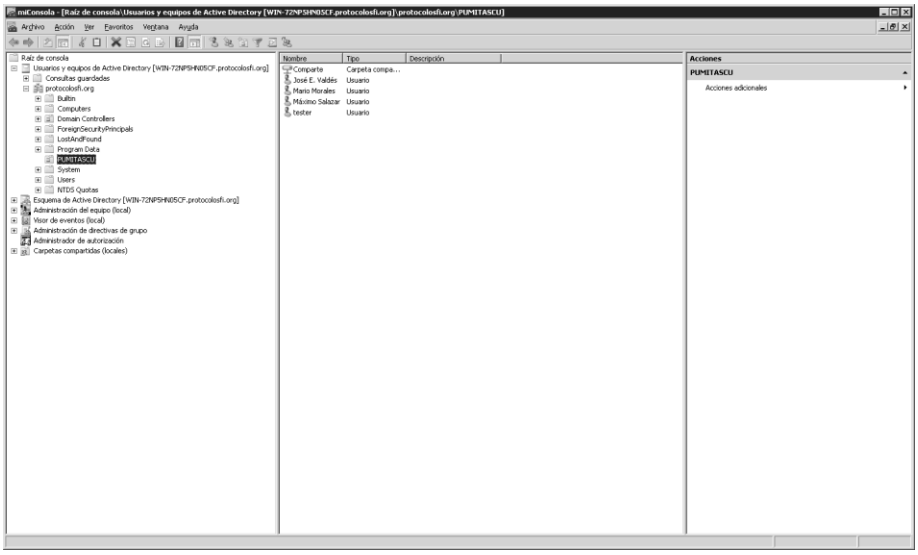

Figura 3-30. Consola de administración de servidor y usuarios.

-Instalar los Servicios de Certificate Server de Active Directory, para activar la Autoridad Certificadora para generar y firmar certificados para el dominio. Agregando la Autoridad Certificadora y la Autoridad Certificadora para el Registro Web.

-El tipo de Autoridad Certificadora será Enterprise y Root CA.

-Creamos una nueva llave privada y la configuración default sha1.

Lo mencionado anteriormente se muestra en la Figura 3-31.

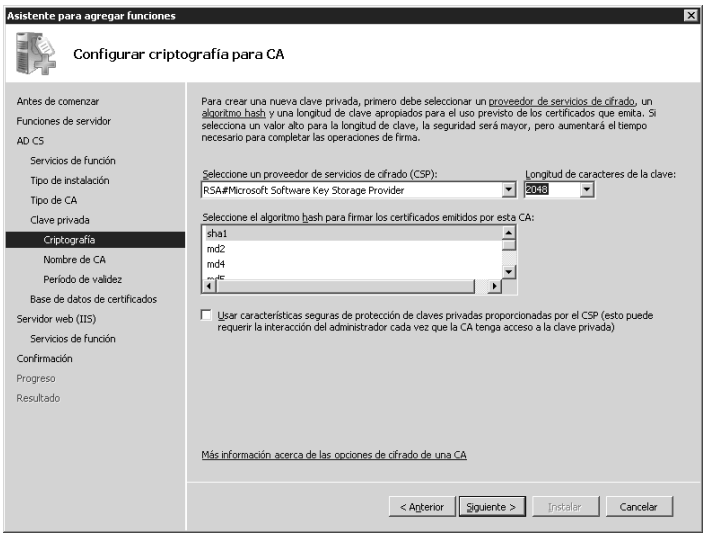

Figura 3-31. Selección de Criptografía para la Autoridad Certificadora.

-Instalar “Servicios de acceso y directivas de redes”, que se encuentra en las funciones del servidor. Seleccionar los servicios de “Servidor de directivas de redes (NPS)”, “Servicio de Enrutamiento y Acceso Remoto”, “Servicio de acceso remoto” y “Enrutamiento” e instalar.

-Ingresar a la consola de "Servidor de directivas de redes (NPS)", a través de comando nps.mmc. Seleccionar "Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X". Esta opción se muestra en la Figura 3-32.

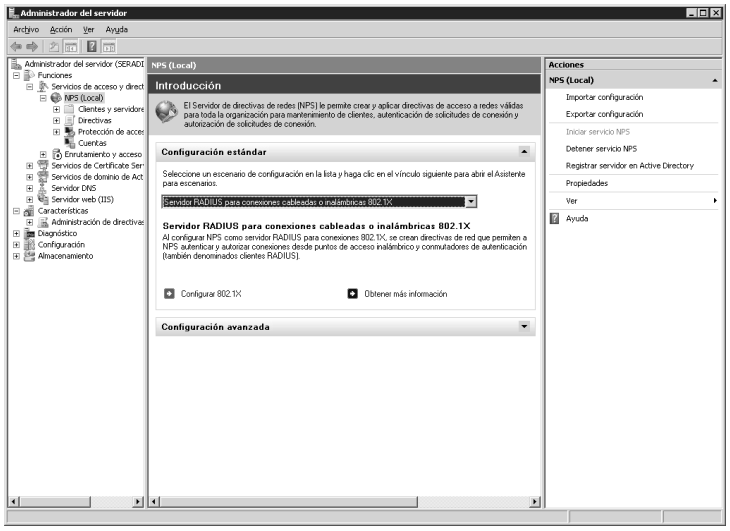

Figura 3-32. Consola NPS.

-Seleccionar "Configurar 802.1X" y elegir la conexión de tipo alámbrico.

-Al "Especificar Switches 802.1X" se agrega la configuración del cliente RADIUS. Utilizando como "Secreto compartido": INGENIERIA2010. Esta opción se muestre en la Figura 3-33.

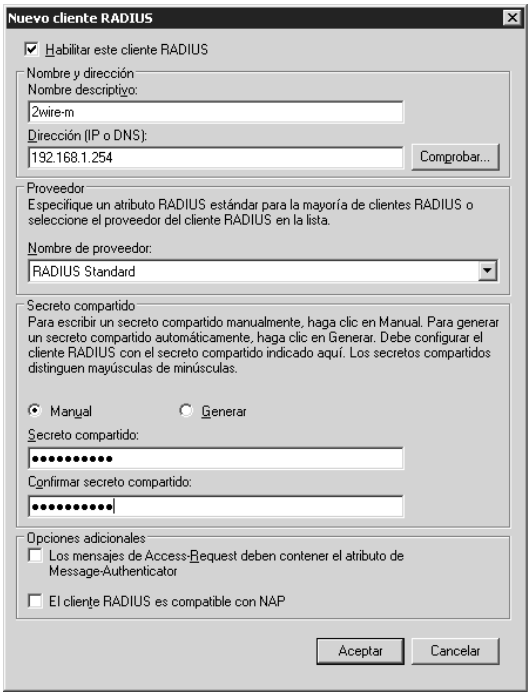

Figura 3-33. Configuración de nuevo cliente RADIUS.

-En la "Configuración del Método de Autenticación", seleccionar "Microsoft Protected EAP (PEAP)" y especificar los grupos de usuarios correspondientes, en este caso serán todos los usuarios del dominio PROTOCOLOSFIR.ORG.

Las pruebas de conexión con el directorio activo se encuentran a detalle en el Anexo 2.

3.2.2 Implementación de RADIUS en UNIX

Para la implementación del protocolo de autenticación RADIUS en el ambiente de UNIX, se instalará y configurará FreeRADIUS en un sistema Ubuntu Server 8.04 LTS.

3.2.2.1 Instalación y configuración de Ubuntu Server 8.04 LTS

La instalación y configuración inicial de Ubuntu Server 8.04 *LTS* se precisa con mayor detalle en el Anexo 3. Una vez instalado el sistema base, como primer paso, se debe cambiar o crear la contraseña del *root*, para lo cual se teclean las siguientes sentencias:

```
msalazar@radius1:~# sudo passwd root
[sudo] password for msalazar: ing110
Enter new UNIX password: rootsecret
Retype new UNIX password: rootsecret
passwd: password updated successfully
msalazar@radius1:~# su -
Password: rootsecret
root@radius1:/home/msalazar# _
```

Una vez probada la configuración de red y el acceso a Internet desde el servidor, lo siguiente a realizar es actualizar todos los paquetes instalados en el servidor (*update*), así como del propio sistema operativo (*upgrade*), esto se hace con los siguientes comandos:

```
root@radius1:~# apt-get update
root@radius1:~# apt-get upgrade
```

3.2.2.2 Instalación de FreeRADIUS

A continuación se listan todas las sentencias, paso por paso, empleadas para instalar FreeRADIUS una vez compilados los binarios y guardados en un CD:

```
root@radius1:~# apt-get install make
root@radius1:~# mount /cdrom
root@radius1:~# dpkg –i cdrom/utils/freeradius_2.0.4-0_i386.deb
root@radius1:~# apt-get –f install
root@radius1:~# dpkg –i cdrom/utils/freeradius-mysql_2.0.4-
0_i386.deb
root@radius1:~# dpkg –i cdrom/utils/freeradius-
dialupadmin_2.0.4-0_all.deb
root@radius1:~# apt-get –f install
```

3.2.2.3 Arranque de FreeRADIUS

Una vez instalado (aunque no configurado) FreeRADIUS, se puede arrancar el daemon (servicio) para ver si se ha instalado correctamente o tiene algún tipo de problema en el arranque. Para esto ejecutar los siguientes scripts para arrancar y parar el daemon *freeradius*:

```
root@radius1:~# /etc/init.d/freeradius start
root@radius1:~# /etc/init.d/freeradius stop
root@radius1:~# /etc/init.d/freeradius restart
```

Otra operación que se realiza muy frecuentemente en FreeRADIUS es arrancar *freeradius* en modo programa y no en modo daemon, además de solicitar que arranque en modo debug (depuración), para observar todas las fases del arranque para cada uno de los módulos de autenticación, autorización y auditoría. Para poder hacerlo, se descarga el daemon de la memoria mediante el script situado en */etc/init.d/* con el modificador *stop*, antes de poder ejecutarlo en modo programa. Los comandos para arrancar freeradius en modo debug trace son los siguientes:

```
root@radius1:~# /etc/init.d/freeradius stop
root@radius1:~# freeradius –X
```

3.2.2.4 Configuración básica de FreeRADIUS

Todos los archivos importantes de configuración de FreeRADIUS se encuentran, como es habitual, en la estructura de directorios de Linux, en el directorio */etc/*, concretamente en */etc/freeradius*.

Mediante el comando *ls* se puede ver cuáles son los archivos de configuración de FreeRADIUS, esto se observa en la Figura 3-34:

```
root@radius1:~# cd /etc/freeradius
root@radius1:/etc/freeradius# ls
acct_users                  dictionary           policy.conf          snmp.conf
attrs                       eap.conf             policy.txt           sql
attrs.access_reject         experimental.conf    preproxy_users       sql.conf
attrs.accounting_response   hints                proxy.conf           sqlippool.conf
attrs.pre-proxy             huntgroups           radiusd.conf         tamplates.conf
certs                       ldap.attrmap         sites-available      users
clients.conf                otp.conf             sites-enabled
```

Figura 3-34. Archivos de configuración de FreeRADIUS.

Los archivos para realizar las pruebas de autenticación contra el servidor, son los archivos *users* y *clients.conf*, los demás se dejaran con su configuración por default. Estos dos archivos serán configurados con la ayuda del editor *nano*.

En el archivo *users* se crean todos los usuarios deseados, con sus atributos relacionados. En este caso, se creará el usuario con el que serán realizadas las pruebas. Este archivo también permite configurar los parámetros o atributos por defecto para la autenticación mediante los campos *DEFAULT*. La configuración de este archivo se observa en la Figura 3-35:

```
mmorales Cleartext-Password := "saeta"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Framed-IP-Address = 192.168.1.101
          Framed-IP-Netmask = 255.255.255.0
          Framed-Routing = Broadcast-Listen,
          Framed-Filter-Id = "std.ppp",
          Framed-MTU = 1500,
          Framed-Compression = Van-Jacobsen-TCP-IP

DEFAULT Auth-Type := Local
         Fall-Through = Yes

DEFAULT Framed-Protocol == PPP,
         Framed-Protocol = PPP,
         Framed-Compression = Van-Jacobsen-TCP-IP

DEFAULT Hint == "CSLIP"
         Framed-Protocol = SLIP,
         Framed-Compression = Van-Jacobsen-TCP-IP

DEFAULT Hint == "SLIP"
         Framed-Protocol = SLIP
```

Figura 3-35. Archivo de configuración *users*.

Ahora, como siguiente paso se agrega el cliente con el que se realizarán las pruebas de autenticación sobre el sistema en el archivo *clients.conf*. El archivo de configuración de clientes o NAS *clients.conf* se observa en la Figura 3-36.

```
client localhost {
        secret = testing123
        shortname = localhost
        nastype = other
}

client 192.168.1.101 {
        secret = saeta
        shortname = mmorales
       nastype = other
}
```

Figura 3-36. Archivo de configuración *clients.conf*.

Con la configuración de estos dos archivos el sistema está listo para realizar pruebas de autenticación contra el servidor.[13]

3.2.2.5 Test de funcionamiento

Detener el servicio *freeradius* para posteriormente ser lanzado en modo programa con la opción de debug trace (depuración completa).

En la consola actual ejecutar lo mostrado en la Figura 3-37 y observar como *freeradius* se queda esperando solicitudes para procesarlas:

```
root@radius1:~# /etc/init.d/freeradius stop
root@radius1:~# freeradius -X
[...]
Listening on authentication address 127.0.0.1 port 1812
Listening on accounting address * port 1813
Ready to process requests.
```

Figura 3-37. FreeRADIUS a la espera de solicitudes.

Ahora abrir otra consola o terminal y realizar una prueba de autenticación con el servidor mediante el comando *radtest*. Esto se muestra en la Figura 3-38.

```
root@radius1:~# radtest mmorales saeta localhost 0 testing123
Sending-Access-Request of id 152 to 127.0.0.1 port 1812
User-Name = "mmorales"
User-Password = "saeta"
NAS-IP-Address = 192.168.1.100
NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=152, length=20
```

Figura 3-38. Prueba de autenticación contra el sistema operativo.

Se ha recibido un paquete de tipo Access-Accept, con esto se demuestra que FreeRADIUS ha sido capaz de leer el fichero de usuarios del servidor. Una prueba de error de una autenticación rechazada se muestra en la Figura 3-39.

```
root@radius1:~# radtest mmorales saeto localhost 0 testing123
Sending-Access-Request of id 19 to 127.0.0.1 port 1812
User-Name = "mmorales"
User-Password = "saeto"
NAS-IP-Address = 192.168.1.100
NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=19, length=20
```

Figura 3-39. Ejemplo de autenticación rechazada por error en el password.

En la consola previamente abierta, en la que se encuentra corriendo *freeradius* en modo debug trace, se puede apreciar la salida de la depuración. Esto se muestra en la Figura 3-40.

```
[...]
++[pap] return reject
auth: Failed to validate the user.
Login incorrect (rlm_pap: CRYPT password check failed): [mmorales/saeto] (from
client localhost port 0)
Found Post-Auth-Type Reject
```

Figura 3-40. Resultado en el modo debug tras una autenticación errónea.

3.3 LDAP

3.3.1 Implementación de LDAP en Windows

Instalación y configuración de Microsoft Windows Server 2008

-Insertar DVD de instalación de Windows Server 2008, utilizando la versión Enterprise

-Proporcionar contraseña de la cuenta de administrador.

-Configurar fecha, hora y zona horaria. (GMT -06:00) Guadalajara, Ciudad de México, Monterrey. El horario es importante ya que el protocolo no funcionara si los relojes no se encuentran sincronizados.

-Configurar nombre de servidor. WIN-72NP5HN05CF

-Configurar red. Asignando una dirección IP v.4 fija. 192.168.1.88

-Instalar rol de Active Directory Domain Services.

En Administrador del Servidor, ubicar las funciones y agregar el "Servicio de dominio de Active Directory". Esto se muestra en la Figura 3-41.

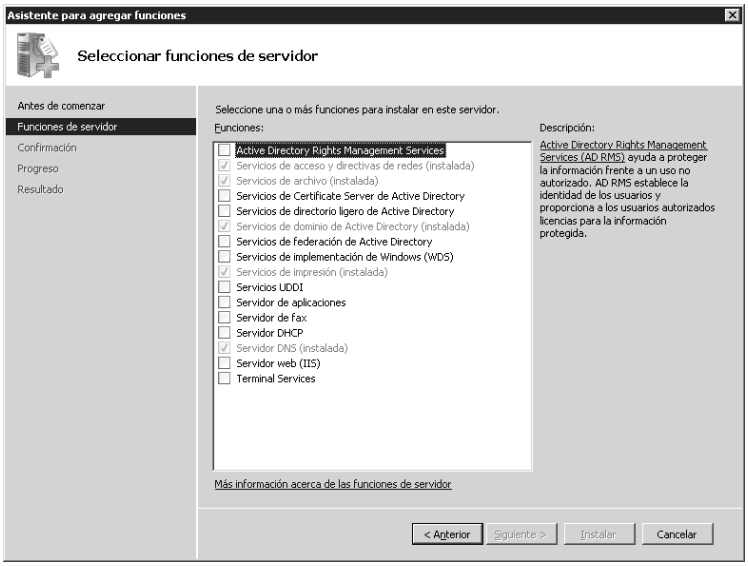

Figura 3-41. Administrador de funciones de Microsoft Windows Server 2008.

-Crear el controlador de dominio.

Para promocionar el rol antes instalado, es necesario, ejecutar el comando dcpromo.exe.

Continuar con las instrucciones y crear un nuevo dominio en un bosque nuevo.

Nombrar el bosque PROTOCOLOSFIL.ORG, posteriormente se solicita instalación opcional de un servidor DNS, en este caso, como no se tiene otro servidor que realice tal función, se instala, por default al ser éste el primer controlador de dominio de un bosque se instala el Catalogo Global.

-Indicar las ubicaciones de las bases de datos de los archivos log y de la página de Sysvol.

-Asignar la contraseña para la restauración de servicios del Directorio Activo.

-Finalizar y reiniciar el sistema.

-Crear usuarios de dominio y permisos.

La consola de administración se muestra en la Figura 3-42.

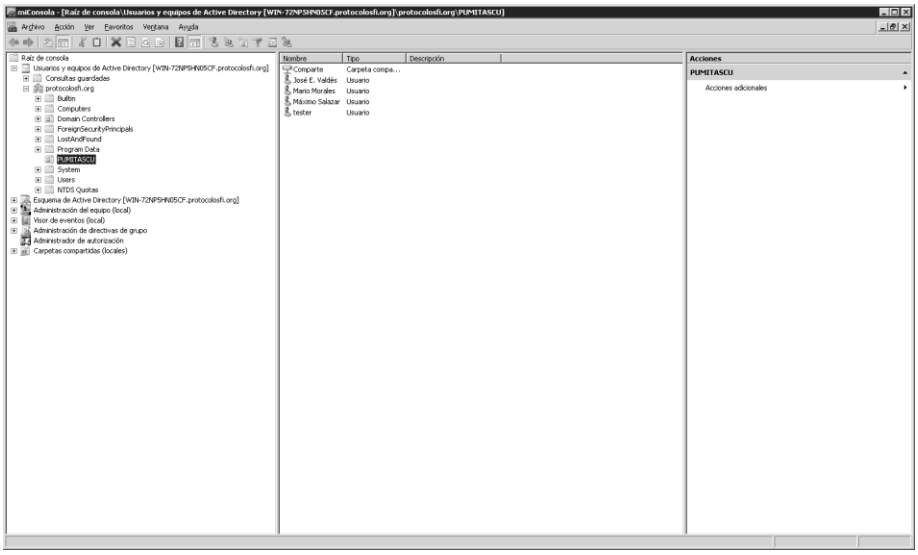

Figura 3-42. Consola de administración de servidor y usuarios.

Las pruebas de conexión con el directorio activo se encuentran a detalle en el Anexo 2.

3.3.2 Implementación de LDAP en UNIX

Para la instalación, configuración y pruebas del protocolo LDAP en el ambiente Linux se han elegido Fedora como sistema operativo y Fedora Directory Server como servidor LDAP.

3.3.2.1 Instalación de Fedora

A continuación se describen de manera breve los pasos necesarios para el proceso de instalación y primer arranque con el sistema operativo Fedora:

1. Descargar la imagen en formato ISO del DVD arrancable, desde la página oficial del proyecto Fedora (http://fedoraproject.org/es/get-fedora-options#formats).
2. Grabar el archivo imagen en un DVD e iniciar la computadora desde el DVD recién creado.
3. Se mostrará una pantalla de bienvenida de Fedora, seleccionar el idioma español y elegir la opción de instalar Fedora.
4. Elegir la configuración adecuada para nuestro teclado.

5. Sólo en el caso de que aplique esta opción, seleccionar y asignar los dispositivos de almacenamiento que estarán disponibles para el sistema Fedora.
6. Inicializar el disco duro donde se instalará Fedora.
7. Configurar el nombre del equipo, para este caso el nombre queda como *ldap.localhost.localdomain*.
8. Las siguientes pantallas son para la configuración del huso horario y para escribir la contraseña del superusuario o root.
9. A continuación siguen las pantallas para configurar la partición o particiones del disco duro donde se instalará Fedora, luego de dar en aceptar se escribirán los cambios al disco.
10. Enseguida se procede a la instalación del sistema base, este proceso puede durar entre 5 y 10 minutos aproximadamente.
11. Seleccionar los paquetes a instalar junto con Fedora, para este caso instalar el Servidor Web Apache y el paquete Java JRE, que son los que se necesitan para el correcto funcionamiento de FDS.
12. Finalmente, reiniciar la computadora la cual ha quedado lista para el primer arranque de Fedora.

3.3.2.2 Instalación y Configuración de Fedora Directory Server

Fedora Directory Server es un servidor LDAP (Lightweight Directory Access Protocol) para Linux desarrollado por Red Hat y la comunidad de Fedora, permite un completo sistema de identidades y una plataforma integral para múltiples servicios de servidor. Enfocado principalmente a instituciones y empresas corporativas, cuenta con múltiples características que lo hace el favorito para implementaciones del mundo real.

Se destaca su capacidad de replicación Multimaster (MMR), compatibilidad con Microsoft Active Directory, Soporte SNMP, Integridad Referencial, Grupos estáticos y dinámicos, Roles, Clases de Servicios, Vistas, Editor Gráfico de Esquema y todo un conjunto de herramientas para un mejor control operacional. En la actualidad está trabajando en una amplia variedad de empresas e instituciones a nivel mundial, principalmente por su alto rendimiento y fácil administración.

La suite Fedora Directory Server consta principalmente de 4 subsistemas:

- Fedora Directory Core
- Fedora Directory Administration
- Fedora Directoty Console
- Fedora Org Chart

El *JRE* es requerido para poder usar la consola de Administración de FDS, una forma de saber si está instalado en el sistema es ejecutando en la consola el comando `java -version` el cuál se encarga de mostrar la versión de java, si al ejecutarlo la salida contiene algo como gcj o GCJ (Gnome Compiler Java) hay que actualizar el JRE pues la instalación del FDS requiere las versiones openjdk o icedtea que se pueden instalar vía yum usando el comando `yum install java-1.7.0-icedtea` o `yum install java-1.6.0-openjdk`, o vía rpm descargando el paquete desde el sitio oficial http://icedtea.classpath.org/download/fedora/.

El Servidor HTTP Apache modelo worker, se encuentra instalado como un demonio del sistema. Para ver el estado del servicio ejecutar desde la consola `/etc/init.d/httpd status`, para correrlo ejecutar `/etc/init.d/httpd start` y para pararlo `/etc/init.d/httpd stop`.

Descargar el archivo fedora-ds-1.0.4-1.PLATFORM.ARCH.opt.rpm desde http://directory.fedoraproject.org/wiki/Download, donde PLATFORM es reemplazado por RHEL3, RHEL4, FC4, FC5, o FC6 y ARCH es i386 o x86_64; es decir, PLATFORM hace referencia a la plataforma sobre la que se va a instalar el FDS y ARCH hace referencia a la arquitectura del procesador. Para este caso de implementación descargar el archivo fedora-ds-1.0.4-1.FC6.i386.opt.rpm.

Para instalar desde la línea de comandos ejecutar:

```
rpm -Uvh fedora-ds-1.0.4-1.FC6.i386.opt.rpm
```

Si no hay problemas en la instalación, la consola nos mostrará:

```
Install finished. Please run /opt/fedora-ds/setup/setup to
complete installation and set up the servers.
```

Para ejecutar el asistente de instalación FDS, ir al directorio de instalación escribiendo en la consola:

```
cd /opt/fedora-ds
```

Antes de continuar, se debe asegurar que el hostname esté apropiadamente registrado en el servidor DNS o en el archivo /etc/hosts, para ello ejecutar el comando `ping ldap.localhost.localdomain` en una consola; si al ejecutar retorna 127.0.0.1 o unknown host esto significa que el hostname no esta registrado correctamente.

Después de haber comprobado el hostname, crear un usuario y un grupo llamados fds para correr el servicio, esto se logra con la ayuda del administrador gráfico para grupos y usuarios que incluye Fedora.

Ahora escribir en el prompt `./setup/setup` para instalar Fedora Directory Server, esto mostrará un asistente que desplegará una serie de preguntas para ir configurando el servicio, como sigue:

1. **LICENSE AGREEMENT AND LIMITED PRODUCT WARRANTY**
   FEDORA(TM) DIRECTORY SERVER
   This agreement governs the use of Fedora Directory...

En este apartado el asistente pide leer la licencia del FDS, al final de la misma se deberá indicar si está de acuerdo y querer continuar.

2. Your system has been scanned for potential problems, missing patches, etc. The following output is a report of the items found that need to be addressed before running this software in a production environment...

El asistente muestra advertencias de problemas que tiene el sistema para que sean resueltas antes de iniciar la instalación, en caso de que puedan ser pasadas por alto se debe escribir *yes* para continuar.

3. Choose a setup type:
   1. **Express**: Allows you to quickly set up the servers using the most common options and pre-defined defaults. Useful for quick evaluation of the products.
   2. **Typical**: Allows you to specify common defaults and options.
   3. **Custom**: Allows you to specify more advanced options. This is recommended for experienced server administrators only.

Se tienen 3 modos de instalación: 1-Express: El más útil para evaluar el producto. 2-Typical: Permite especificar los parámetros comunes y las opciones principales. 3-Custom: Permite especificar opciones más avanzadas.

Por defecto, seleccionar 2 y continuar.

4. `hostname to use (default: localhost.localdomain)...`
   `Computer name [ldap.localhost.localdomain]:`
   `System User [nobody]: fds`
   `System Group [nobody]: fds`

Dejar el hostname que se había configurado con anterioridad, y especificar el usuario y el grupo que se creará para la administración del servicio.

En caso de que aparezca el error:

```
./ns-config: error while loading shared libraries:
libtermcap.so.2: cannot open shared object file: No such file or
directory
ERROR Exiting . . .
Log file is /tmp/lognIfjhl
```

Resolverlo de la siguiente manera:

- ✓ Descargar los paquetes **libtermcap-2.0.8-47.i386** y **termcap-5.5-1.20060701.1.noarch.rpm**
- ✓ Instalarlos con el comando:
  `rpm -Uvh termcap-5.5-1.20060701.1.noarch.rpm libtermcap-2.0.8-47.i386`
- ✓ Después de instalar correctamente, la consola arrojará lo siguiente:

```
Preparando...    ##################################    [100%]
1:termcap    ##################################    [   50%]
2:libtermcap    ##################################    [100%]
```

Ahora hay que volver al paso 1 de la instalación.

5. `Server information is stored in the configuration directory server...`
   `Do you want to register this software with an existing configuration directory server? [no]: ↵`

Como se trata de la primera instalación del Servicio de Directorio, escribir *no* para continuar.

```
6. If you already have a directory server you want to use to
   store your data...
   Do you want to use another directory to store your data? [No]
```

Al igual que en la pregunta anterior, escribir *no* para continuar, pues no se tiene otro Servicio de Directorio instalado.

```
7. The standard directory server network port number is 389...
   Directory server network port [389]: ↵
```

Dejar el puerto por defecto.

```
8. Each instance of a directory server requires a unique
   identifier...
   Directory server identifier:[ldap] ↵
```

El asistente reconoció sin problemas el Identificador del equipo, dar *enter* para continuar.

```
9. Please enter the administrator ID for the Fedora
   configuration...
   administrator ID [admin]:
   Password:
   Password (again):
```

El usuario por defecto *admin* será quien administre desde la consola del FDS, ingresar su password y continuar.

```
10. The suffix is the root of your directory tree. You may have
    more than one suffix.
    Suffix [dc=localhost, dc=localdomain]: ↵
```

El sufijo es usado para almacenar los datos del administrador, esta es la parte del FQDN ldap.localhost.localdomain en la forma dc=localhost, dc=localdomain; siendo dc el acrónimo de Domain Controller.

```
11. Certain directory server operations require an administrative
    user. This user is referred...
    Directory Manager DN [cn=Directory Manager]:
    Password:
    Password (again):
```

El usuario Directory Manager será usado para ciertas operaciones de administración, siendo su uso muy similar al usuario root bajo entornos Unix. Presionar enter e ingresar el password 2 veces, teniendo en cuenta que no debe ser inferior a 8 caracteres.

```
12. The information stored in the configuration directory server
    can be separated...
    Administration Domain [localhost.localdomain]: ↵
```

La información de configuración puede ser almacenada en diferentes Dominios Administrativos, en cuyo caso se ingresan los identificadores de los mismos, esto puede ser útil para algunas empresas con sedes diferentes.

Para este caso se está instalando el FDS para un sólo dominio de administración, por lo tanto presionar *enter* para continuar.

```
13. The Administration Server is separate from any of your web or
    application servers since it listens to a different port...
    Administration port [9830]: 26492
```

Cambiar el puerto de administración HTTP por defecto, el cual es usado por FDS para escuchar el servicio de Administración que monta sobre Apache.

```
14. The Administration Server program runs as a certain user on
    your system...
    Run Administration Server as [root]: ↵
```

Presionar *enter* para continuar, debido a que se usará el usuario root para escribir los archivos de configuración y arrancar el servicio.

```
15. The Administration Server runs on the Apache web server.
    Please provide the directory...
    Apache Directory [/usr/sbin/]:
```

Pulsar enter ya que el binario del demonio de Apache, httpd, se encuentra en la ubicación especificada.

Con estos pasos, la instalación ha sido finalizada satisfactoriamente. Para ejecutar la consola de Administración ejecutar lo siguiente:

```
# cd /opt/fedora-ds
# ./startconsole -u admin -a
http://ldap.localhost.localdomain:26492/
```

Si no hay problemas se obtendrá la ventana de login. Ingresar el password y dar click en OK, con esto se accede a la consola de administración, tal como se observa en la Figura 3-43.

Figura 3-43. Consola de Administración de Fedora Directory Server.

3.3.2.3 Pruebas de autenticación con Fedora Directory Server

Antes de proceder a las pruebas de autenticación de usuarios mediante FDS, es necesario iniciar el servidor Apache, así como los servicios Fedora Directory Core y Fedora Directory Administrator. Los comandos para iniciar estos servicios son los siguientes:

```
# /etc/init.d/httpd start
# /opt/fedora-ds/slapd-ldap/start-slapd
# /opt/fedora-ds/start-admin
```

Una vez inicializados estos servicios, lo siguiente a realizar es agregar un usuario para probar la autenticación mediante FDS. Desde la consola de administración se crea un nuevo registro con los siguientes datos:

Nombre: Mario Morales

Usuario: MMorales

Password: saeta

```
uid=MMorales,ou=People,dc=localhost,dc=localdomain
```

Las pruebas de autenticación con FDS fueron las mismas tanto para ambientes Windows como Linux y se realizaron desde sus respectivos exploradores de Internet, ingresando por HTTP a la URL del servidor LDAP a través del puerto 26492 configurado durante la instalación (http://ldap.localhost.localdomain:26492/).

En las Figuras 3-44 a 3-47 se pueden observar los resultados obtenidos en dichas pruebas.

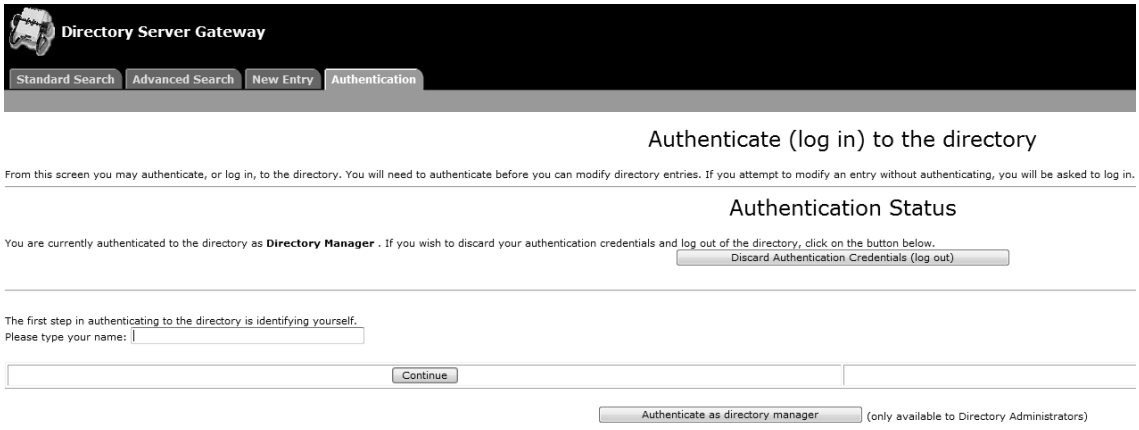

Figura 3-44. Pantalla de login para autenticarse e ingresar al directorio.

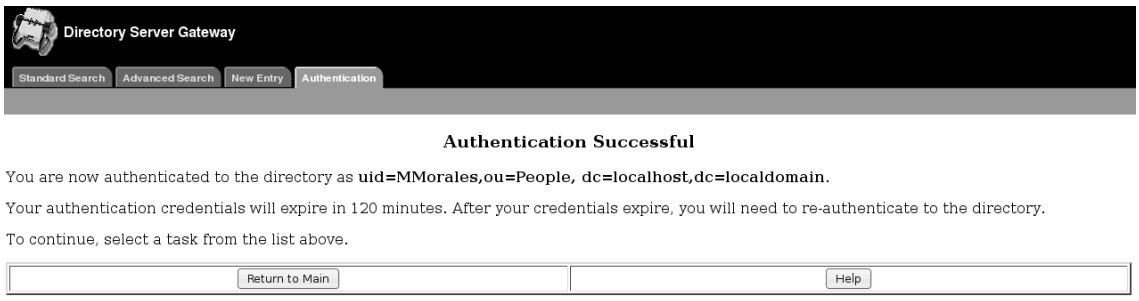

Figura 3-45. Pantalla de autenticación exitosa y obtención de credenciales.

Figura 3-46. Pantalla de autenticación errónea por introducir un password incorrecto.

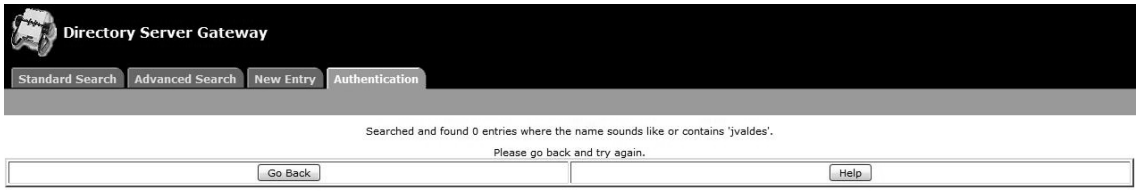

Figura 3-47. Pantalla de usuario no encontrado en el directorio.

Adicionalmente, en las siguientes figuras se observan los resultados obtenidos tras ejecutar el comando *ldapsearch* desde ambientes Unix o Linux, para los casos en que el servidor de autenticación FDS se encontraba apagado (Figura 3-48), y los resultados arrojados una vez que el servidor y los servicios de FDS ya habían sido inicializados (Figura 3-49):

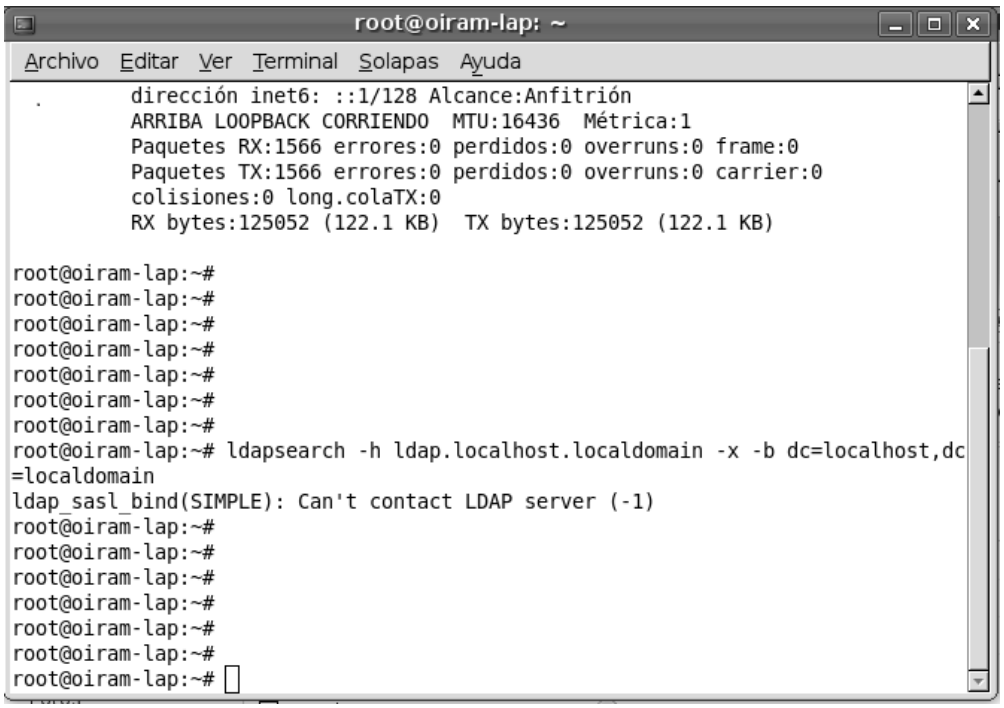

Figura 3-48. Servidor LDAP no encontrado mediante *ldapsearch*.

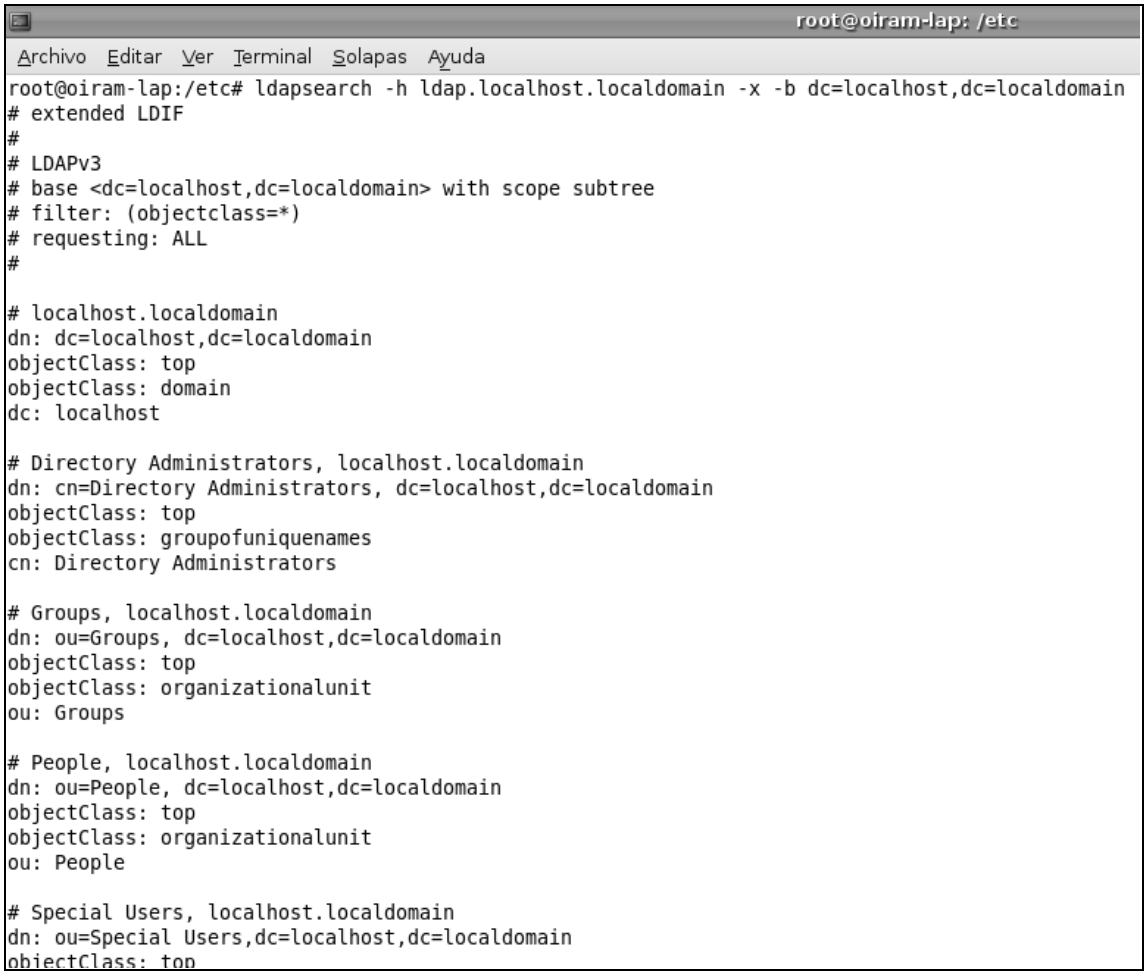

Figura 3-49. Servidor LDAP encontrado mediante *ldapsearch* y obtención de información del directorio.