ANEXOS

ANEXO 1. INSTALACIÓN DE UBUNTU 8.04

A continuación se enumeran de manera general los pasos para instalar Ubuntu 8.04:

1. Insertar el CD con la versión de Ubuntu 8.04 en el CD-ROM del equipo de cómputo. Una vez que éste inicia se indica el idioma con el cuál trabajará la distribución a instalar, en este caso se selecciona español y se continúa con la instalación.
2. Seleccionar el tipo de teclado adecuado para el equipo de cómputo, en este caso se selecciona como tipo de teclado Latinoamérica.
3. A continuación se muestran las opciones para seleccionar la partición dónde se instalará el sistema operativo. Para este caso seleccionar la opción Personalizado, ya que se pretende que vivan en este equipo de cómputo dos o más Sistemas Operativos. Por lo tanto una vez seleccionada la opción Personalizado, se muestran las particiones existentes en el Disco Duro. Se debe seleccionar la partición libre y que fue creada previamente con el programa Hard Disk Manager desde el Sistema Operativo Windows XP. Esta partición libre es aproximadamente del tamaño de 5GB y será formateada al tipo Ext2. Cabe aclarar que en ésta partición se cargará el / (root) como punto de montaje.
4. Una vez configurada la partición dónde será instalado el Sistema Operativo Ubuntu, se muestra un resumen de las configuraciones mencionadas anteriormente. Si todo está debidamente configurado oprimir el botón Instalar.
5. Al terminar la instalación y reiniciarse el Sistema Operativo, se pedirá el nombre de usuario y su respectivo password. Una vez proporcionados estos datos se puede ingresar a la distribución de Ubuntu.
6. Como paso final se recomienda actualizar el Sistema Operativo, esto se hace desde el Gestor de Actualizaciones.

ANEXO 2. PRUEBAS DE CONEXIÓN CON CLIENTES PARA SERVIDORES WINDOWS

Tanto para Radius como para LDAP, Windows Server utilizamos active directory para instalar la red de datos, con lo cual el proceso de inicio de sesión es similar para ambos protocolos.

a) Inicio de sesión de dominio en Windows XP

La configuración de usuario en un equipo con sistema operativo Windows XP, bajo el protocolo Radius o LDAP en Microsoft Windows Server 2008, incluye agregar el equipo al dominio PROTOCOLOSFIR.ORG o PROTOCOLOSFIL.ORG, según corresponda, así como al usuario en caso de proporcionarle permisos de administrador.

Figura A2-1. Acceso a Windows XP en el dominio.

Posteriormente, al estar con la sesión iniciada en el dominio, podemos 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.

b) Inicio de sesión de dominio en Windows 7

La configuración de usuario en un equipo con sistema operativo Windows 7, bajo el protocolo Radius o LDAP en Microsoft Windows Server 2008, incluye agregar el equipo al dominio PROTOCOLOSFIR.ORG o PROTOCOLOSFIL.ORG, según corresponda, así como al usuario en caso de proporcionarle permisos de administrador.

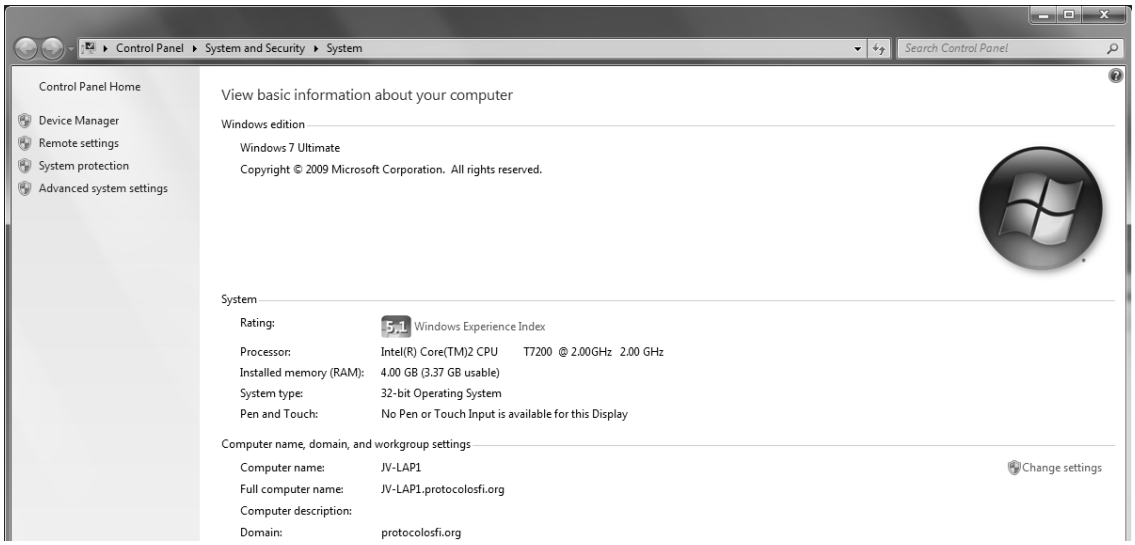

Figura A2-2. Equipo en dominio.

Posteriormente, al estar con la sesión iniciada en el dominio, podemos 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.

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 PROTOCOLOSFIR.ORG o PROTOCOLOSFIL.ORG, según corresponda, y la sesión a utilizar.

Figura A2-3. Configuración de Likewise.

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.

Figura A2-4. Dominio.

Una vez ingresado en el dominio se encuentra, los datos del perfil y se verifica que el usuario y el equipo pertenecen al dominio.

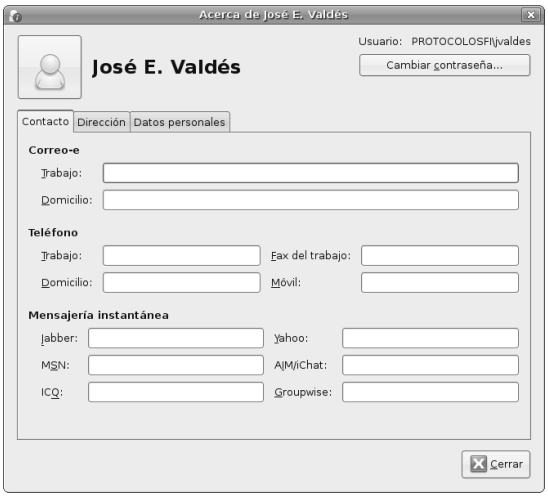

Figura A2-5. Propiedades de usuario en Ubuntu en dominio.

ANEXO 3. INSTALACIÓN DE UBUNTU SERVER 8.04 LTS

A continuación se enumeran de manera general los pasos para instalar Ubuntu Server 8.04 LTS:

1. Descargar y grabar la ISO de Ubuntu. La ISO se puede obtener desde la página oficial de descargas de Ubuntu (www.ubuntu.com/getubuntu/download). En ella se pueden ver las versiones disponibles, en este trabajo se ha optado por la versión 8.04, porque es una versión de tipo LTS (Long Term Support) con soporte hasta 2011.
2. Introducir el CD con la ISO grabada y bootear desde el CD/DVD autoarrancable de Ubuntu Server.
3. En el menú inicial cambiar el idioma de instalación a español y elegir la opción "Instalar en el disco duro". Por tratarse de un servidor, se debe asignar por norma general una dirección IP estática y no dinámica, por lo que es recomendable que antes del siguiente paso, se desconecte el cable de red, por si existiera algún servidor DHCP en la red o un router con el servidor DHCP funcional. De esta manera se evita que Ubuntu reciba una dirección IP de forma automática.
4. Al tener el cable de red desconectado o no haber un servidor DHCP funcional en la red, se dará un fallo de asignación y se debe continuar para llegar a la pantalla de configuración.
5. Ahora se procede a indicarle al instalador que se desea configurar manualmente el direccionamiento IP.
6. A continuación se especifica la dirección IP estática, que se va a utilizar desde este momento para el servidor RADIUS. Se ha decidido utilizar la 192.168.1.100, pero cada uno debe utilizar la que mejor se adapte a sus necesidades.
7. Se indica la máscara de subred que se va a utilizar. En este caso es una subred de clase C, por lo que se utiliza la 255.255.255.0.
8. Enseguida se configura la dirección IP del Gateway, que para este caso es la 192.168.1.254 (el router que nos da acceso a Internet para nuestra red). Esta misma dirección IP será la que se configure a continuación para el DNS.

9. Ahora se procede a asignar el nombre de host y el dominio que utilizará este servidor RADIUS para la red interna o pública. Se asigna el nombre *radius1*, en previsión de que posteriormente se pueda instalar algún otro servidor Proxy RADIUS o de redundancia. El dominio imaginario que se va a utilizar es "protocolosfi.org". Por lo tanto, se establece el nombre de la máquina como *radius1.protocolosfi.org*.

10. Tras la introducción de los datos de red, se continúa con el particionado y formateado del disco duro que va a alojar a Ubuntu Server. Dependiendo de la configuración de cada equipo, existen multitud de posibilidades de particionado a seleccionar, desde asignar el disco duro completo para Ubuntu (utiliza muy poco disco), hasta crear particionados dinámicos LVM o RAID. En este caso se han destinado 4GB del disco duro para instalar Ubuntu Server, por lo que se selecciona el método de partición marcado como "Manual".

11. En el espacio libre de 4GB se crea una partición primaria y se debe formatear como ext3 de Linux.

12. Una vez asignado el espacio y creada la partición, el instalador muestra el resumen de opciones de particionado que se han creado; cuando se tenga completamente claro que no existen equivocaciones en ninguna opción, se procede entonces con la aplicación de todos estos cambios presionando sobre la opción "Sí".

13. Enseguida vienen un par de pantallas para configurar la zona horaria y el reloj.

14. Posteriormente siguen tres pantallas en donde se configuran el nombre y apellidos del usuario principal del sistema, el nombre de inicio de sesión o alias para este usuario, y una contraseña. Luego viene una pantalla para verificar la contraseña asignada y se pide para ello que se vuelva a escribir.

15. En este momento, tras la configuración básica se produce la copia de archivos y la descarga y actualización de las dependencias necesarias. Es necesario que en este momento el equipo disponga de conexión a Internet para comprobar los repositorios de Ubuntu en búsqueda de actualizaciones.

16. Tras la instalación de los paquetes básicos, se procede a la instalación del Kernel de Linux y a su configuración de arranque.

17. Luego el instalador se va a conectar a Internet para la actualización de los repositorios de aptitude (apt), que es uno de los instaladores de paquetes binarios (programas) de Linux.

18. Después de que el instalador actualice y configure el apt, viene una pantalla que pregunta si se desea hacer uso de algún servidor proxy de la organización para el acceso a Internet. En este caso no se reencaminará el tráfico http por un proxy Server, por lo que se deja el campo vacío.

19. En la siguiente ventana se deben seleccionar los paquetes LAMP y OpenSSH para la conexión de sesiones remotas tuneladas.

20. Tras esta selección, comienza el copiado de los paquetes elegidos para su instalación.

21. En otro par de pantallas se debe establecer la contraseña del usuario *root* o superusuario de MySQL.

22. Tras un par de pantallas de instalación de los programas elegidos, se ha finalizado la instalación de Ubuntu Server Linux. Ya se tiene el servidor instalado y preparado para la configuración de todos los servicios que se van a utilizar.

23. Finalmente, se retira el disco de Ubuntu Linux y se reinicia el sistema para el primer arranque.

GLOSARIO

AUTENTICACIÓN – Acción y efecto de autenticar.

AUTENTIFICACIÓN – Acción y efecto de autentificar.

AUTENTICAR – Autorizar o legalizar algo.

AUTENTIFICAR – Autenticar (autorizar o legalizar algo).

BLOWFISH – En criptografía, Blowfish es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado. Toma una clave de longitud variable, entre 32 y 448 bits. Mientras que ningún analizador de cifrados de Blowfish efectivo ha sido encontrado hoy en día, se ha dado más atención de la decodificación de bloques con bloques más grandes, como AES y Twofish.

CHALLENGE RESPONSE – El mecanismo de Challenge/Response (Desafío/Respuesta) tiene como objetivo principal realizar la validación de un usuario mediante su *Nombre de Usuario (username)* y *Password* evitando el traslado de esa información a través de la red. Está pensado sobre todo para redes de carácter público en las que se está expuesto a un ataque de sniffing o Man-in-the-middle.

DES – Data Encryption Standard, Estándar para el Cifrado de Datos. Algoritmo para el cifrado de datos, desarrollado por IBM, que utiliza bloques de datos de 64 bits y una clave de 56 bits.

GNU – Acrónimo de GNU is Not UNIX (o GNU No es UNIX). Sistema operativo libre diseñado por Richar Stallman, basado en programas que pueden ser descargados y modificados de forma gratuita por cualquiera.

GPG – GNU Privacy Guard. Es una herramienta para cifrado y firmas digitales, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

HASH – Es un algoritmo que funciona en base a tomar una cadena y lo convierte en un código numérico. Un hash es un código, calculado en base en el contenido de un mensaje. Se utiliza en criptografía para la búsqueda rápida de datos y códigos de corrección de errores. El algoritmo está diseñado para que el rango de valores sea bastante extendido y las posibilidades de colisiones (dos cadenas que tienen el mismo valor de hash) sean mínimas. En criptografía, una contraseña puede ser enviada a un servidor y compara los valores hash almacenados allí. Esto evita que sean interceptadas contraseña en texto plano.

HDLC – High-level Data Link Control (Control de enlace de datos de alto nivel). Es un protocolo de enlace de datos orientados a bit diseñados para soportar la comunicación semidúplex y dúplex a través de enlaces punto a punto y multipunto.

Todos los protocolos orientados a bit están relacionados con el protocolo de control de enlace de datos de alto nivel (HDLC).

INSTANCE **–** Forma de referirse a la ubicación o directorio de un proceso o archivo.

JRE **–** Subconjunto de Java Development Kit (JDK), que contiene los ejecutables y los archivos del núcleo que constituyen la plataforma Java estándar. JRE comprende Java Virtual Machine (JVM), las clases del núcleo y los archivos de soporte.

LCP – Link Control Protocol (Protocolo de control de enlace). Es responsable del establecimiento, mantenimiento, configuración y terminación del enlace.

LOGIN **–** Forma de referirse al modo de iniciar sesión en un sistema.

LTS **–** Long Time Support, Soporte de Tiempo Largo. Expresa la idea que para las versiones de Ubuntu que tengan asociadas las siglas LTS, éstas tendrán un periodo de tiempo más extenso en cuanto al soporte que prestará Canonical, la empresa detrás de Ubuntu, ya sea en servicios o actualizaciones de seguridad. No todas las versiones de Ubuntu son LTS, esto es así para enfocar los esfuerzos en menos versiones y poder así ser más eficiente con los recursos a largo plazo. Las empresas son las más interesadas en las versiones LTS, el usuario común, cambia con mucha más rapidez entre versiones.

MitM **–** En criptografía, un ataque *man-in-the-middle* (MitM o *intermediario*, en español) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación.

NAS – Un Network Access Server (servidor de acceso a la red) es el primer punto de entrada a una red de la mayoría de los usuarios de los servicios de red que se encuentran protegidos. Es el primer dispositivo de la red para prestar servicios a un usuario final, y actúa como una puerta de enlace para todos los servicios adicionales. Como tal, su importancia para los usuarios y los proveedores de servicios por igual es primordial. El NAS no contiene información acerca de qué clientes pueden conectarse o qué credenciales son válidas. Todos los NAS envían las credenciales suministradas por el cliente a un recurso que sabrá cómo procesar dichas credenciales.

PASSWORD **–** Contraseña de un usuario para acceder a un sistema.

PROMPT **–** Línea de comandos en un sistema operativo.

RFC **–** Abreviatura de *Request For Comments* (Solicitud de Comentarios). Es el nombre que se da a una serie de normas que definen el protocolo TCP/IP, así como sus documentos relacionados.

ROAMING **–** Tecnología que permite que el usuario de un teléfono móvil pueda utilizarlo en una red celular fuera de la cobertura de la red a la que pertenece,

permitiendo así hacer y recibir llamadas, por ejemplo, desde un país a otro. El término roaming significa callejeo o vagabundeo y sólo es posible si hay un acuerdo entre operadores de redes de telefonía móvil.

ROOT – Usuario principal con todos los privilegios de acceso sobre un sistema.

SMART CARD – Una tarjeta inteligente (*smart card*), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay dos categorías principales de TCI. Las Tarjetas de memoria contienen sólo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. Las tarjetas microprocesadoras contienen memoria y microprocesadores.

SNIFFER – Programa que monitoriza los paquetes de datos que circulan por una red, en busca de información referente a cadenas prefijadas. Es un monitor de la red; es decir, un programa que mira todos los paquetes que pasan por la red.

TOKEN – Un token o también llamado componente léxico es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación. Ejemplos de tokens, podrían ser palabras clave (if, while, int,...), identificadores, números, signos, o un operador de varios caracteres (por ejemplo, :=). Son los elementos más básicos sobre los cuales se desarrolla toda traducción de un programa, surgen en la primera fase, llamada análisis léxico, sin embargo se siguen utilizando en las siguientes fases (análisis sintáctico y análisis semántico) antes de perderse en la fase de síntesis.

UNIX – Registrado oficialmente como UNIX®. Es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy. Se utiliza principalmente como programa de control maestro en las estaciones de trabajo y en especial en los servidores.

X.509 – Estándar UIT-T para PKI (Public Key Infraestructure) infraestructura de claves publicas. X.509 especifica, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

802.1X – El protocolo IEEE 802.1X proporciona control de acceso en la Capa 2 de OSI (la Capa MAC). IEEE 802.1X soporta la autenticación de clientes mientras se establece la conexión a la red, antes de que al cliente se le asigne una dirección IP vía DHCP (Dynamic Host Configuration Protocol). Entre otras cosas, el estándar especifica como el protocolo de autenticación (EAP, Extensible Authentication Protocol) se encapsula en marcos Ethernet.