Instalación de Kerberos como Controlador de Dominio para Equipos del Centro de Cómputo de la Facultad de Informática Mazatlán

Adriana Hernández García[1], Julián Ontiveros Ramírez[2], José David Santana Alaniz[3], Álvaro Peraza Garzón[4]

[1,2,3,4] *Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa (México)*

Resumen

El presente proyecto documenta la instalación de Kerberos como controlador de dominio, siendo esta la primera fase que sienta las bases para un desarrollo futuro de una aplicación que controle el acceso de ingreso de alumnos al centro de cómputo. En esta fase, el objetivo fue el agregar clientes Windows en un dominio administrado por un servidor Linux, Se presenta una breve investigación sobre el funcionamiento de tecnologías .NET y la secuencia de comandos de red necesarios para lograr una comunicación entre el servidor Linux y el host remoto. Como resultado se logró la instalación y configuración de Samba y su controlador Kerberos, consiguiendo agregar hosts de Windows a un dominio.

Palabras clave: Kerberos, Samba, Active Directory

1 INTRODUCCIÓN

La Facultad de Informática Mazatlán (FIMAZ) da sus inicios en el mes de septiembre de 1992 y seis años después comenzó la construcción de lo que es ahora el edificio principal de la facultad que cuenta con seis laboratorios de cómputo; CISCO el cual está equipado para realizar prácticas y actividades relacionadas con la telemática, cuenta con 18 equipos de cómputo, SOFTWARE cuenta con 20 equipos de cómputo, MAC este laboratorio está montado para realizar múltiples tipos de programación como el desarrollo de aplicaciones IOS y Android cuenta con 20 equipos, MAESTRÍA cuenta con 16 computadoras, EDUCACIÓN CONTINUA se utiliza para diseño gráfico y el desarrollo web cuenta con 24 equipos de cómputo y DR. CESAR GONZÁLEZ BELTRÁN cuenta con 40 equipos de cómputo, siendo estos dos últimos los más grandes laboratorios con los que cuenta la facultad. De tal forma que por la dimensión y la necesidad de llevar un control del ingreso de los alumnos al laboratorio se incorporó una bitácora para poder controlar el acceso y poder conocer los motivos por los cuales ingresan al laboratorio.

Haciendo un conteo de todos los equipos de cómputo con los que cuenta la FIMAZ da un total de 138 equipos de cómputo distribuidos por todos los laboratorios de cómputo.

Actualmente se tiene la necesidad de administrar remotamente equipos de cómputo por lo que se desarrollaron múltiples aplicaciones dedicadas al servicio remoto con el fin de dar soporte a equipos a distancia o de manera local. Con base a los conocimientos previos de estas aplicaciones y teniendo en cuenta las necesidades que el centro de cómputo de la FIMAZ necesita, se decidió implementar un software con la finalidad de dar soporte a los equipos de cómputo en segundo plano, y aprovechando las ventajas que ofrece se decidió crear un control de acceso para el ingreso de usuarios por medio de una matrícula y un lector de código de barras el cual permitirá a la Facultad de Informática llevar un control de ingreso preciso y una mejor organización en sus pasillos.

Sin embargo, para la implementación de dicho software, fue necesario tener como primera instancia un canal de comunicación entre el host y el servidor. Por lo tanto, se realizó una búsqueda acerca de los sistemas operativos que soportan el modo servidor, dando como resultado que la arquitectura Linux, específicamente la distribución de DEBIAN, era la más apropiada para llevar a cabo una conexión remota entre un servidor y un host, dadas las condiciones del lugar. Además, se configuró el servicio SAMBA el cual permite una interconexión de archivos compartidos entre dos sistemas operativos en este caso Windows y Linux.

En este orden de ideas, el objetivo del presente proyecto fue la configuración de un canal adecuado de comunicación para la incorporación de hosts (clientes Windows 8.1) a un dominio. Por lo tanto, se necesitó de un controlador de dominios (KERBEROS) que se encargue de dar acceso mediante un usuario y contraseña a equipos agregados a un dominio maestro y este ser administrado mediante AD (Active Directory).

2 METODOLOGÍA

Instalación de una máquina virtual (Virtual Box) y la familiarización con el entorno gráfico de la distribución Debian y así conocer todas las funcionalidades de ese S.O (Sistema Operativo)

Se hizo la elección de un servidor público (fimaz.uas.edu.mx).

Se investigó sobre la instalación y configuración del funcionamiento del servidor SAMBA. Dentro de la instalación de SAMBA se instaló un protocolo de redes de ordenadores llamado Kerberos el cual sirve para autenticar usuarios, máquinas y servicios. Donde el servidor SAMBA se ejecuta como un controlador de dominio (DC) de Active Directory (AD) que es una herramienta que proporciona servicios ubicados en uno o varios servidores, administrar las políticas de toda la red en la que se encuentre como por ejemplo la gestión de permisos de acceso de usuarios.

2.1 Instalación y configuración de Samba

Para realizar la instalación de SAMBA se tiene que actualizar el servidor con las últimas versiones de seguridad usando

 # apt update

 # apt upgrade

Se edita el archivo /etc/hostname, esto para configurar el nombre del servidor. Una vez instalado y actualizado Debian se tiene que configurar la interfaz de red para que esta tenga una ip estática; (IP, máscara de red, servidores dns, puerta de enlace) a través del servicio DHCP, para esto se utiliza el siguiente comando para editar el archivo:

nano /etc/network/interfaces

Una vez configurado el servidor con una dirección ip fija, activamos la interfaz de red con el siguiente comando:

 # Ifup enp0s3

La herramienta resolvconf actualiza automáticamente el archivo de configuración de *resolución de nombres (DNS)*, el servidor y los clientes del dominio deben usar un servidor DNS que sea capaz de resolver zonas DNS de AD. Esta herramienta por defecto re-escribe en cada arranque el archivo **/etc/resolv.conf**, por lo tanto, se usara la resolución de DNS en el archivo **/etc/hosts** aquí se añaden las DNS para permitir las búsquedas por nombres DNS, en este caso el archivo quedaría de esta forma:

127.0.0.1 localhost

127.0.1.1 Server

192.168.1.200 Server.fimaz.uas.edu.mx fimaz.uas.edu.mx Server fimaz

Kerberos requiere una hora sincronizada en todos los miembros del dominio, para esto se debe instalar el servidor de hora NTP. Usando el comando:

 # apt install ntp

Ahora se obtienen los paquetes necesarios para SAMBA 4 AD DC, para poder instalar el controlador de dominio de Active Directory instalaremos SAMBA y todos los paquetes que sean necesarios con el siguiente comando:

 # apt install samba smbclient attr winbind libpam-winbind libnss- winbind libpam-krb5 krb5-config krb5-user

El instalador requiere de algunas preguntas para la configuración del controlador de dominio. Lo primero que pide es que escribamos el nombre que se usará en el dominio para el valor predeterminado de Kerberos en mayúsculas.

Ahora se necesita un nombre de host del servidor para el dominio, se utiliza el mismo nombre que para el dominio, pero esta vez en minúsculas.

Para finalizar, el nombre de host para el servidor administrativo del reino Kerberos, se usa el mismo nombre del dominio y con esto se finaliza la instalación.

Aprovisionamiento de Samba AD DC para el dominio

Antes de comenzar a configurar Samba para el dominio tenemos que detener y deshabilitar todos los demonios de samba, usando los comandos:

 # systemctl stop samba-ad-dc smbd nmbd winbind

 # systemctl disable samba-ad-dc smbd nmbd winbind

En el aprovisionamiento se cambia el nombre de smb.conf o eliminar la configuración original de samba (smb.conf). Este paso es obligatorio antes de aprovisionar Samba AD ya que en el momento de la provisión, Samba crea un nuevo archivo de configuración desde cero y genera algunos errores en caso de que encuentre el antiguo archivo smb.conf. Para cambiar el nombre de smb.conf a smb.conf. Original con el siguiente comando

 # mv /etc/samba/smb.conf /etc/samba/smb.conf. Original

Cambiado el nombre, ahora si se inicia con el aprovisionamiento de dominios de forma interactiva, aceptando las opciones predeterminadas que ofrece:

 # samba-tool domain provision --use-rfc2307 --interactive

Además, se tiene que introducir la dirección IP del servidor DNS o de un servidor externo. También se requiere de una contraseña segura para la cuenta de Administrador.

Preguntas que nos hace el asistente:

Realm: introduce el nombre del dominio.

Domain [usuariodebian]: ya lo pone por defecto con respecto al dominio introducido en Realm.

Server Role (dc, member, standalone) [dc]: por defecto este seleccionado Controlador de Dominios [dc].

DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIN9_DLZ, NONE) [SAMBA_INTERNAL]: por defecto esta seleccionado DNS interno de SAMBA [SAMBA_INTERNAL].

DNS forwarder IP address (write 'none' to disable forwarding) [ip_de_nuestro_servidor]: por defecto esta seleccionado los DNS.

Administrator password: Introducir la contraseña de administrador, se recomienda usar una contraseña con la siguiente estructura: no inferior a 8 caracteres y tiene que contener al menos un carácter en mayúscula, uno en minúsculas y un número.

Retype password: reescribir la misma contraseña anterior, esto se hace para asegurarnos que la hemos escrito correctamente ambas contraseñas.

Ahora se habilitan los demonios de Samba Active Directory Domain Controller. [1]

 # Systemctl unmask samba-ad-dc
 # Systemctl start samba-ad-dc
 # Systemctl enable samba-ad-dc

2.2 Unir cliente Windows 8.1 al dominio fimaz.uas.edu.mx

Configuración de red del cliente, tenemos que pertenecer al mismo rango, dicha ip que utilizaremos es: 192.168.10.36, como servidor DNS usaremos la ip de nuestro servidor samba: 148.227.227.5

Para agregar un equipo a un dominio iremos a Propiedades del sistema > Nombre del equipo, pulsamos Cambiar y en la ventana que nos aparece seleccionamos Dominio, colocamos el nombre de nuestro dominio (fimaz.uas.edu.mx) y pulsamos aceptar.

Al conectar al dominio fimaz.uas.edu.mx nos pide el nombre del usuario y contraseña que dimos en el servidor samba.

Una vez autenticado el usuario y la contraseña, da el mensaje que el equipo se unió correctamente al dominio: fimaz.uas.edu.mx. Pulsar en Aceptar. Ahora pide reiniciar el equipo para que se apliquen los cambios y pulsar Aceptar. [2]

Instalar RSAT (Remote Server Administration Tool)

Una vez instaladas las herramientas de administración remota del servidor, se procede a habilitar aquellas que necesitemos. Para esto ir a Panel de control > Programas > Programas y características > Activar características de Windows.

Activar herramientas necesarias de administración básica de AD:

Herramientas de administración remota del servidor

Herramientas de administración de características

Herramientas de administración de directivas de grupo.

Herramientas de administración de funciones.

Herramientas de servicios de dominio de Active Directory y Active Directory Lightweight Directory Services (AD LDS)

Centro de administración de Active Director y Herramientas de línea de comandos y complementos de AD DS. [3]

Como siguiente paso del proyecto se utilizaron comandos de red para hacer las primeras pruebas de acceso remoto mediante las herramientas ya mencionadas.

Apagar PC (shutdown)

Shutdown -m \\nombre del host –s ejecutándose desde cmd. [4]

Encender PC (wake on LAN)

Wolcmd [mac address] [ip address] [subnet mask] [port number]. [5]

Bloquear PC

Al usar la herramienta PsExecs puedes ejecutar programas o procesos remotamente en los equipos cliente conectados a la misma red. Esta herramienta forma parte de un conjunto de herramientas de red conocidas como PsTools. Para esto se descarga un archivo comprimido de https://docs.microsoft.com/en-us/sysinternals/downloads/psexec se descomprimen y se pegan los archivos en c:/Windows o c:/windows/system32 con esto ejecutaremos cualquier aplicación desde cualquier directorio estando en la consola. [6]. Al estar en un dominio no es necesario especificar usuario o contraseña, ya que en el dominio nuestro usuario es el administrador de red. [7]

Psexec –accepteula –i 1 –s \\nombre del host C:\ nombre del archivo

3 RESULTADOS

Los resultados de la presente investigación, se dividen en dos partes principalmente, la primera consta de la instalación del servidor Kerberos, el cual nos permite el control del dominio y de las políticas de seguridad para cada host, y un servicio SAMBA (Figura 1), totalmente funcional.

Figura 1 Servicio en ejecución de SAMBA

Además, se llevó a cabo de manera exitosa, el control básico del host desde el servidor Linux, los comandos aplicados fueron:

- Psexec: Para suspensión y bloqueo del host.
- Shutdown: Para apagar o reiniciar el host.
- Wolcmd: Para encender el host vía remota (wake on lan).

4 CONCLUSIONES

Como primer acercamiento a proveer una solución basada en Linux, para el control de acceso remoto a los hosts de Windows, se encontró que, Kerberos es un protocolo funcional y se adapta a las necesidades del presente proyecto y desde el punto de vista del cliente(Windows 8.1), agregarlo al dominio no generó ningún problema, finalmente y dando cumplimiento a la primera fase en donde se especificó que era necesario tener un sistema donde los clientes con SO Windows pudieran ver a un servidor Linux, se puede decir que el entorno se encuentra listo para la siguiente etapa (desarrollo del sistema controlador de clientes).

Trabajo futuro: Desarrollo de la base de datos y del software.

REFERENCIAS

[1] J. D. S. Alaniz, «http://dsantana.uas.edu.mx,» [En línea]. Available: http://dsantana.uas.edu.mx/index.php/2019/08/15/samba-4-como-controlador-de-dominios-ad-dc-en-debian-9/. [Último acceso: 12 Noviembre 2019].

[2] J. D. S. Alaniz, «dsantana.uas.edu.mx,» [En línea]. Available: http://dsantana.uas.edu.mx/index.php/2019/08/15/unir-un-cliente-windows-8-1-a-nuestro-dominio-fimaz-uas-edu-mx/. [Último acceso: 12 Noviembre 2019].

[3] J. D. S. Alaniz, «dsantana.uas.edu.mx,» [En línea]. Available: http://dsantana.uas.edu.mx/index.php/2019/08/15/habilitar-herramientas-de-active-direcory/. [Último acceso: 12 Noviembre 2019].

[4] darkygame, «CCM,» 28 Agosto 2019. [En línea]. Available: https://es.ccm.net/faq/5040-encender-apagar-un-pc-de-manera-remota. [Último acceso: 12 Noviembre 2019].

[5] depicus, «depicus,» [En línea]. Available: https://www.depicus.com/wake-on-lan/wake-on-lan-cmd. [Último acceso: 12 Noviembre 2019].

[6] M. Russinovich, «Microsoft.com,» 29 Junio 2016. [En línea]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec. [Último acceso: 12 Noviembre 2019].

[7] linuxsysymas, «linuxsysymas,» 21 Enero 2015. [En línea]. Available: https://linuxsysymas.wordpress.com/2015/01/21/psexec/. [Último acceso: 12 Noviembre 2019].