



UNIVERSIDAD LUTERANA SALVADOREÑA

CÁTEDRA: Sistema Operativo de Redes

CATEDRÁTICO: Ing. Manuel Flores

TEMA : Sistema de autenticación centralizada de usuarios

INTEGRANTES :

Nº	APELLIDO	NOMBRE	CARNET	PARTICIPACION
1	Hernández Hernández	Elsy Maricela	HH01133827	50%
2	Hernández Moreno	Víctor Ulises	HM01132877	50%

San Salvador, 5 de mayo de 2018

INDICE

RESUMEN.....	Pagina 1
PALABRAS CLAVES.....	Pagina 2
INTRODUCCIÓN.....	Pagina 3
OBJETIVOS.....	Pagina 4
MARCO TEORICO.....	Pagina 5
CONCLUSIÓN.....	Pagina 9
GLOSARIO.....	Pagina 10

RESUMEN

El presente trabajo investigo el tema de Sistema de autenticación centralizada de usuario que consiste en tener una computadora con un usuario principal el cual tiene como función estar conectado a varias computadoras y desde la computadora principal y así poder cambiar de contraseñas desde ese usuario principal

Se tocan temas de autenticación y sus diferentes formas también lo que es el LDAP que es un programa fundamental para este proyecto.

Se concluyó que el proyecto es funcional ya que cumple su funcionamiento de cambiar contraseñas de las computadoras conectadas desde un usuario principal.

PALABRAS CLAVE

Autenticación, identidades, centralizado, descentralizado, firewall, repositorio y LDAP

INTRODUCCIÓN

En el presente trabajo daremos a conocer la creación de nuestro proyecto un Sistema de autenticación centralizada de usuario con lo que es el protocolo LDAP para el cambio de contraseña para las computadoras.

Se explicara a lo que nos referimos como autenticación ya que existen tres tipos de autenticación.

También describimos lo que es la autenticación centralizada ya que existen 2 modelos de esta misma para lo cual explicaremos cada una de ellas brevemente.

Y esta explicado lo que es LDAP el protocolo que necesitamos para completar nuestro proyecto, ya que es necesario explicar lo que es y que hace en el proyecto.

Se muestra en el documento un cuadro en el cual se compara nuestro proyecto con otros dos similares donde se muestran las ventajas y desventajas que poseen nuestro proyecto con los de ellos.

OBJETIVO GENERAL:

Crear un sistema de autenticación centralizada de usuario para facilitar el cambio de contraseña desde un usuario en concreto.

OBJETIVO ESPECIFICOS:

- Utilizar el protocolo LDAP para la creación de este proyecto ya que es muy necesario.
- Crear un usuario Principal que lidere todas las otras aplicaciones web.

MARCO TEORICO

Autenticación se refiere al proceso por medio del cual un usuario de una red adquiere el derecho a usar una identidad dentro de la dicha red. Hay maneras de autenticar un usuario, como el uso de claves, smart cards, certificados digitales. La ventaja es que la identidad del usuario en la red no necesariamente tiene que ser igual al nombre de la persona. Una misma persona puede tener muchas identidades virtuales y viceversa.

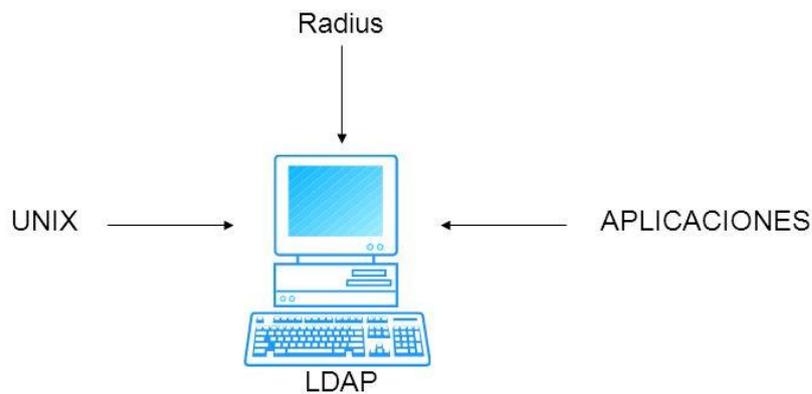
Existen tres tipos de autenticación:

- a. Autenticación por conocimiento específico: El nombre de mi mamá, la clave del cajero, una palabra clave, etc.
- b. Autenticación por posesión: Una tarjeta inteligente.
- c. Autenticación por identidad: La huella digital, la retina, la voz, u otras características físicas.

¿QUE ES AUTENTICACION CENTRALIZADA?

Existen dos modelos de autenticación uno descentralizado y otro centralizado. En el modelo descentralizado, cada servicio de la red maneja sus claves de forma independiente, por ejemplo los usuarios de Oracle, los usuarios de un firewall, los administradores de un sitio Web; cada uno de estas aplicaciones maneja por separado sus claves y las mismas no son compartidas.

En la autenticación centralizada los usuarios y sus claves se ubican en un repositorio central, las diferentes aplicaciones se configuran para identificar este lugar y hacer la autenticación contra el repositorio. Para nuestro caso las claves estarán ubicadas dentro de un servidor de directorio LDAP, pero en general podrían estar almacenadas en un archivo de texto plano o en una base de datos relacional entre otros métodos de almacenamiento de información.



QUE ES LDAP

Lightweight Directory Access Protocol -LDAP-, es un protocolo cliente servidor hecho para acceder a un servicio de directorio en el modelo TCP/IP. Está basado en el protocolo X.500 un protocolo estándar para los servicios de directorio en el modelo OSI.

Un directorio LDAP es similar a una base de datos, pero tiende a contener información más descriptiva. La información en un directorio es consultada muchas más veces de lo que es modificada; como consecuencia, los directorios no tienen esquemas de "roll-back" que las bases de datos usan por el alto-volumen de actualizaciones. Las actualizaciones del directorio son típicamente simples cambia todo o nada.

Los directorios pueden ser afinados para dar una contestación rápida a las búsquedas de grandes volúmenes de datos. Ellos pueden tener la habilidad de replicar la información en varios sitios para aumentar la disponibilidad y la confiabilidad, mientras se mantiene un tiempo mínimo en la contestación.

¿QUE SE NECESITA?

1- UN ORDENADOR



2- ACCESO A INTERNET



3- UNA MAQUINA VIRTUAL



VirtualBox

4- LDAP



CUADRO COMPARATIVO

<i>Tema:</i>	<i>Sistema centralizado de gestión de usuarios para la universidad del tolima</i>	<i>C.A.S. Servicio de autenticación centralizada</i>	<i>Sistema de autenticación centralizada de usuario</i>
<i>Herramienta</i>	<i>Single Sign On (SSO)</i>	<i>Single Sign On (SSO), Java</i>	<i>Lightweight Directory Access Protocol, LDAP</i>
<i>Ventajas</i>	<ul style="list-style-type: none"> • <i>Facilitar la gestión de múltiples contraseñas en múltiples aplicaciones</i> • <i>Simplificar la gestión de cuentas de acceso de múltiples aplicaciones</i> • <i>Preservar la privacidad de los usuarios</i> • <i>Posibilitar la interacción entre organizaciones y sus usuarios</i> 	<ul style="list-style-type: none"> • <i>Software libre.</i> • <i>Facilidad de instalar y usar.</i> • <i>Comunidad amplia y con calidad (JA-SIG).</i> • <i>Excelente librería phpCAS que facilita integración de PHP.</i> 	<ul style="list-style-type: none"> • <i>La herramienta tiene una fuerte documentación y una comunidad establecida.</i> • <i>Es una herramienta muy utilizada en producción.</i> • <i>Se complementa de una forma excelente y cumple las expectativas del proyecto.</i>
<i>Desventajas</i>	<ul style="list-style-type: none"> • <i>Requieren un estudio previo y una investigación extensa.</i> • <i>Al utilizar LDAP, no está claro que aplicaciones web, de escritorio o móviles puedan utilizar el sistema de autenticación sin problemas.</i> 	<ul style="list-style-type: none"> • <i>Construido en Java.</i> • <i>Configurable vía XML.</i> 	
<i>Características</i>	<i>Este procedimiento de autenticación facilita las tareas de acceso a las diferentes plataformas, además cuenta con otras importantes características en aspectos de gestión sencilla, seguridad,</i>		<i>OpenLDAP incluye un número de características importantes: Soporte LDAPv3— OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la</i>

	<p><i>facilidad de uso y transparencia.</i></p>		<p><i>Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL), entre otras mejoras.</i></p> <p><i>Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.</i></p> <p><i>Soporte IPv6— OpenLDAP soporta la próxima generación del protocolo de Internet versión 6.</i></p>
--	---	--	---

CONCLUSIÓN

En el siguiente trabajo se concluye que el Sistema de autenticación centralizada de usuarios es sumamente útil para la organización y la administración de las computadoras enlazadas con el usuario central o la computadora central.

El proyecto es funcional ya que a la hora de querer cambiar o configurar la contraseña de las maquinas solo entra al usuario central y desde ahí cambia la contraseña de las maquinas anexadas a ella en lugar de ir una por una cambiándolas de modo manual.

Se concluyó que al comparar nuestro proyecto con los 2 antes mencionados en el cuadro tiene tanto ventajas como desventajas uno entre otro ya que poseen algunos programas diferentes para poder funcionar.

GLOSARIO

Autenticación: En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Descentralizado: La descentralización tecnológica implica la reestructuración de los siguientes aspectos: distribución y fortalecimiento de la infraestructura de telecomunicaciones y sistemas de información, normatividad, presupuesto operativo y de inversión, procesos de toma de decisiones, estructuras jerárquicas, etcétera, por lo que muchos expertos en gestión tecnológica no apuestan a que la descentralización debe ser total.

Oracle: Es básicamente una herramienta cliente/servidor para la gestión de Bases de Datos. Es un producto vendido a nivel mundial, aunque la gran potencia que tiene y su elevado precio hacen que sólo se vea en empresas muy grandes y multinacionales

Firewall: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

Repositorio: Un repositorio, depósito o archivo es un sitio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente bases de datos o archivos informáticos

- **Protocolo:** Al Protocolo de Internet (*Internet Protocol*), el protocolo de red para la comunicación de datos a través de paquetes conmutados;

