Tecnológico Nacional de México

Instituto Tecnológico de Tlaxiaco

Carrera: **Ingeniería en Sistemas Computacionales**

Materia: **Seguridad Y Virtualización**

Tema: **Introducción a la seguridad de la información**

Actividad: **Reporte de Practica 2**

Alumnos: Feria Ortiz Eduardo Tomas **21620095**
Reyes Peña Isaí **21620053**
Zárate Reyes Irving **20620166**

Grupo: **6US**

Catedrático: **Ing. Osorio Salinas Edward**

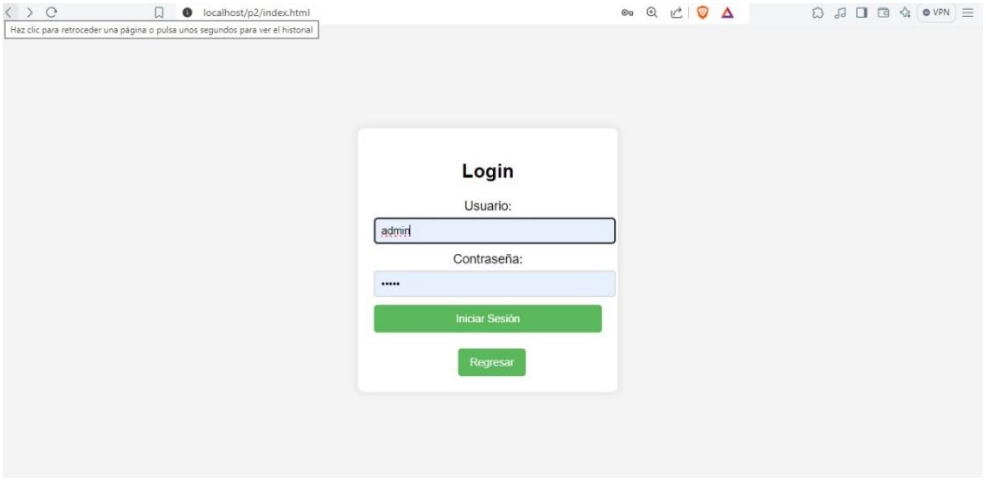
Heroica Ciudad de Tlaxiaco.
Lunes, 09 de agosto de 2024.

índice

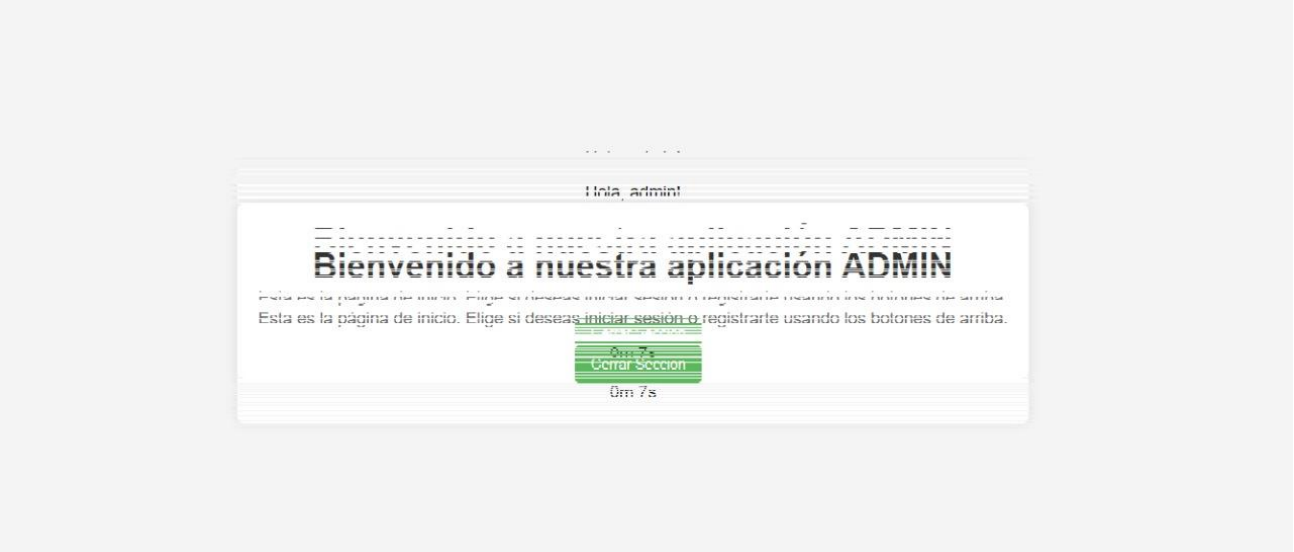
Creación de la aplicación web.

Para comenzar con la creación de esta aplicación diseñamos la interfaz. Una vez completado este paso proseguimos a cumplir cada uno de los requerimientos de la práctica.

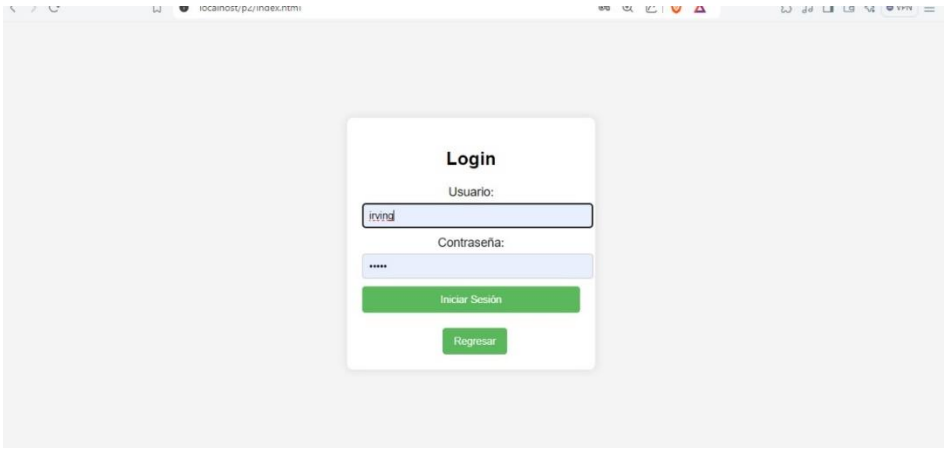
Una vez que algún usuario trate de entra como administrador y no tenga los datos correctos o no exista el registro mandara a esta pagina.



Este es el login que hemos diseñado para el inicio de sección de los administradores.

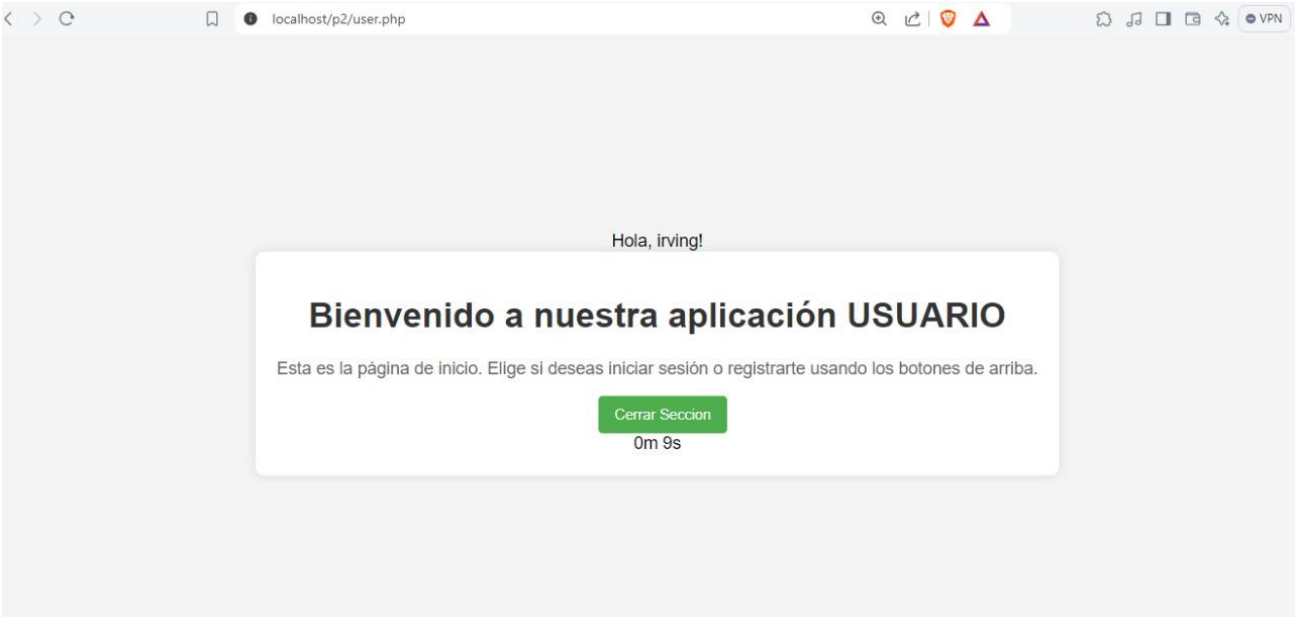


Si el administrador ha ingresado correctamente sus datos será redirigido a esta pagina.



Esta es la pagina de login que hemos diseñado para los usuarios.

Si el usuario intenta ingresar y no existe su registro mandara a esta ventna.



Una vez que el usuario pueda ingresar sus datos correctamente los enviara a una ventana de bienvenida.

Investigación

Investiga y describe los siguientes servicios de autenticación:

LDAP

El protocolo LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos a la que pueden realizarse consultas. LDAP es ampliamente utilizado por cualquier compañía u organización que requiera acceso a una red utilizando información de autenticación. Además de información de contactos o personas, es capaz de acceder a certificados encriptados, punteros a impresoras y otros servicios de una red, y proporcionar un acceso único cuando una contraseña para un usuario está compartida entre determinados servicios. LDAP es apropiado para cualquier información de tipo directorio, donde la norma es acceder de forma rápida a dicha información y actualizarla de manera poco frecuente. En el presente proyecto fin de carrera se diseña un disector de las versiones 2 y 3 de este protocolo, utilizando librerías de código abierto desarrolladas en lenguaje de programación C por el grupo de investigación HPCN de la Universidad Autónoma de Madrid. En primer lugar, se realiza un estudio del estado del arte de dicho código aplicando las funciones básicas de un disector. Posteriormente, se analiza el comportamiento del protocolo con el fin de desarrollar un disector que analice todos sus campos para detectar posibles fallos en la comunicación, así como para encontrar las causas de dichos fallos y estudiar las posibles soluciones. Finalmente, se realizan pruebas de velocidad de procesado, consumo de memoria y efectividad de detección. Esto permite desarrollar un disector altamente eficiente que permite manejar tramas de gran tamaño en poco tiempo y asegurar que se detecta adecuadamente el fallo en la transmisión del protocolo a través de Internet. (Muñoz Mozos, 2014)

RADIUS

RADIUS es un protocolo de red que proporciona servicios de autenticación, autorización y contabilidad (AAA) para gestionar el acceso a la red. Se utiliza principalmente en redes para centralizar la gestión de credenciales y controlar quién puede acceder a los recursos. RADIUS es un estándar abierto, lo que lo hace compatible con una amplia gama de dispositivos de distintos fabricantes. Utiliza el puerto UDP 1812 para autenticación y autorización, y el puerto 1813 para contabilidad. Aunque solo cifra las contraseñas, es ampliamente adoptado por su flexibilidad y compatibilidad (Gómez García, 2009)

TACACS+

TACACS+ es un protocolo desarrollado por Cisco que se emplea para gestionar el acceso a dispositivos de red, tales como routers, switches y cortafuegos. Se destaca por separar los procesos de autenticación, autorización y contabilidad, lo que le permite ofrecer una mayor flexibilidad y control granular sobre cada uno de estos aspectos. A diferencia de otros protocolos, como RADIUS, TACACS+ permite un cifrado completo de todo el tráfico entre el cliente y el servidor, lo que lo hace más seguro para ambientes sensibles. Este protocolo es ampliamente utilizado en grandes redes empresariales donde es esencial un control preciso sobre quién tiene acceso a cada dispositivo. (Moreno Yuste, 2016)

Kerberos

Kerberos es un protocolo de autenticación que utiliza criptografía de clave simétrica para permitir la autenticación segura de usuarios y servicios en una red insegura. Fue desarrollado por el MIT como parte del proyecto Athena y es ampliamente utilizado en entornos como Windows Active Directory y sistemas UNIX. Kerberos opera a través de un modelo de "tercero de confianza" mediante

el uso de un servidor de autenticación centralizado (KDC) que emite tickets de autenticación. Estos tickets permiten a los usuarios acceder a los recursos de la red sin tener que volver a enviar sus credenciales, mejorando la seguridad al minimizar la exposición de contraseñas en la red. La autenticación se realiza en tres fases: obtención de un ticket de autenticación, validación y acceso a los servicios. (Gómez García J. A., 2009)

Investiga y describe los siguientes servicios de autorización:

ACL

Una Lista de Control de Acceso (ACL) es un mecanismo utilizado para definir qué usuarios o sistemas tienen permiso para acceder a ciertos recursos en una red o sistema. Consiste en una lista de reglas que especifican qué acciones (lectura, escritura, ejecución, etc.) pueden realizarse sobre un objeto por parte de un usuario o grupo específico. Las ACLs se utilizan principalmente en sistemas de archivos y en dispositivos de red como routers o firewalls para filtrar tráfico y garantizar que solo los usuarios autorizados puedan acceder a los recursos. Cada regla dentro de una ACL puede permitir o denegar acceso según la dirección IP, el puerto o el protocolo. (Moreno Yuste L. , 2016)

RBAC

El Control de Acceso Basado en Roles (RBAC) es un modelo de control de acceso en el cual los permisos de acceso se asignan a roles en lugar de a individuos. En este modelo, a cada usuario se le asigna uno o más roles, y cada rol tiene un conjunto de permisos que definen lo que se puede hacer en el sistema. RBAC es común en entornos empresariales donde los roles, como "administrador", "usuario" o "invitado", determinan el nivel de acceso a los recursos. Este enfoque reduce la complejidad de la gestión de permisos individuales y facilita el cumplimiento de políticas de seguridad al asignar permisos de forma estructurada y consistente. (Sandhu, 1996)}

ABAC

El Control de Acceso Basado en Atributos (ABAC) es un modelo de control de acceso que toma decisiones basadas en atributos del usuario, el recurso, el entorno y las acciones. A diferencia de RBAC, donde los permisos están vinculados a roles predefinidos, en ABAC las reglas se basan en atributos como la identidad del usuario, la hora del día, la ubicación geográfica, el dispositivo desde el cual se realiza la solicitud, entre otros. Esto permite una mayor flexibilidad y granularidad en las políticas de acceso, siendo útil en entornos dinámicos donde los usuarios y las situaciones de acceso pueden variar considerablemente. (Hu, 2013)

PBAC

El Control de Acceso Basado en Políticas (PBAC) es un modelo de control de acceso en el que las decisiones de acceso se toman según políticas definidas por el administrador de seguridad. Estas políticas son reglas que dictan cómo se deben gestionar los permisos y accesos a los recursos. PBAC permite centralizar la administración de los permisos en base a políticas que pueden adaptarse a diferentes condiciones contextuales. Por ejemplo, se pueden crear políticas que restringen el acceso en función de la hora del día, la ubicación geográfica o el tipo de dispositivo utilizado, proporcionando una mayor adaptabilidad en comparación con modelos tradicionales como ACL y RBAC. (NIST, 2018)

Conclusión.

En esta práctica, hemos logrado comprender y aplicar los conceptos fundamentales de la seguridad de la información, así como su relevancia en el desarrollo de sistemas seguros. Mediante la creación de una aplicación web y el uso de diversos protocolos de autenticación y control de acceso, adquirimos una visión general sobre cómo proteger los recursos y datos de una red. Estos mecanismos no solo nos permiten gestionar quién accede a los sistemas, sino también garantizar que dicha interacción sea segura y controlada.

El análisis de cada protocolo y modelo de control de acceso nos permitió ver las diferencias y fortalezas en cuanto a la seguridad y la administración de permisos en entornos empresariales. Así, reconocemos que la implementación de estos sistemas es crucial para prevenir vulnerabilidades y asegurar la integridad de la información.

Bibliografía

como crear una contraseña segura. (Junio de 2024). Obtenido de Argentina.gob.ar: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-crear-una-contrase%C3%B1a-segura

Cuno, Á. L. (2015). Conceptos de firma digital. *IDENTIDAD DIGITAL*.

Datos., A. E. (2020). *HTTPS: Navegación segura en Internet.* Obtenido de Agencia Española de Protección de Datos.: https://www.aepd.es/charlas/https-navegacion-segura

electrónica, S. (s.f.). *1024 - ¿Qué es la Encriptación o Cifrado?* Obtenido de Real Casa de la Moneda - Fabrica Nacional de Moneda y Tiembre: https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9IeUoAH/content/1024-que-es-la-encriptacion-o-cifrado-

España., I. N. (2018). *SFTP: Transferencia segura de archivos*. Obtenido de Instituto Nacional de Ciberseguridad de España.: https://www.incibe.es/sftp

España., I. N. (2019). *Protocolo TLS: Seguridad en las comunicaciones*. Obtenido de Instituto Nacional de Ciberseguridad de España. : https://www.incibe.es/protocolo-tls

Gómez García, J. A. (2009). *edes de computadores: Un enfoque práctico.*

Gómez García, J. A. (2009). Redes de computadores: Un enfoque práctico. RAMA Editorial.

Hu, V. C. (2013). *Attribute-based access control. Computer.*

Mendoza, J. C. (2008). Demostración de cifrado simétrico y asimétrico. *Ingenius: Revista de Ciencia y Tecnología*, pág. 8.

Moreno Yuste, L. (2016). *Seguridad en redes: Fundamentos y aplicaciones.*

Moreno Yuste, L. (2016). *Seguridad en redes: Fundamentos y aplicaciones.* .

Mozilla., F. (2020). *SSH: Seguridad en las comunicaciones remotas.* . Obtenido de Fundación Mozilla.: https://developer.mozilla.org/es/docs/Glossary/SSH

Mozilla., F. (2021). *¿Qué es SSL y cómo funciona?* Obtenido de Mozilla.org: https://developer.mozilla.org/es/docs/Glossary/SSL

Muñoz Mozos, G. (2014). *Diseño de Protocolos LDAP*. Obtenido de UAM: https://repositorio.uam.es/handle/10486/660546

NIST. (2018). *Policy Based Access Control (PBAC) Strategies.*

Pousa, A. (Diciembre de 2011). ALGORITMO DE CIFRADO SIMÉTRICO AES. . pág. 3.

Rivest, R. S. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

Sandhu, R. C. (1996). *Role-based access control models. IEEE Computer.*

Talens-Oliag, S. (2008). *Introducción a los certificados digitales*. Obtenido de Universidad de Valencia, España: https://www. uv. es/sto/articulos/BEI-2003-11/certificados_digitales. html.[Accessed: 28-Enero-2018].

Technology., N. I. (2002). Secure Hash Standard (SHS). *Federal Information Processing Standards Publication.*

Tejedor-Morales, M. Y. (s.f.). HASHING. UN CONCEPTO. UNA REALIDAD. *Universidad Tecnológica de Panamá*.