Republica Bolivariana de Venezuela

Ministerio del Poder Polular para la Defensa

Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana

UNEFA Núcleo Tinaquillo

***Ensayo de GitHub***

Profe: Estudiante:

Ing. Jesús Méndez. Carla Romero, CI;29.723.646

Ing de Telecomunicaciones - Semestre 8

Tinaquillo 26 de Noviembre de 2023

GitHub es una página online que se basa en ofrecer un servicio privado en la nube que contiene un sistema de control de versiones, el cual se encarga de gestionar y rastrear los cambios en los archivos en tiempo real a través de un seguimiento del código fuente, que a su vez le permite revirtir dichos cambios sin complicaciones y repercusiones en el archivo. También permite que los usuarios desarrollen varios proyectos a la vez ya que proporciona libertad colaborativa entre los mismos. Es una herramienta de código abierto, que guarda más de 100 repositorios y posee un almacenamiento de 500MB. Gracias a ello, y a sus demás funciones de accesibilidad y gestión desde diversos dispositivos es muy utilizada por profesionales y grandes empresas. Su software presentam ajustes de seguridad y es fácil de manejar incluso para aquellos que no posean conocimiento técnico en el área.

En general GutHub es conocida y utilizada por Ingenieros de Software, pero sus características y funciones hace que diversas empresas y personas la utilicen para diferentes proyectos que requieran alta seguridad y confidencialidad, además de un manejo remoto y gratuito. La plataforma presenta una sección gratuita para el registro o suscripción y el inició de sesión, y también cuánta con una sección paga. Pese a ello, la sección gratuita es accesible a cualquier dispositivo, presenta un desarrollo de procesos fluido y no es nada pesada. Debido a ellos funciona bien con cualquier internet. Además, todas sus funciones están disponibles en el mismo lugar, lo que permite la exploración de todo el contenido que tiene para ofrecer, entre los cuales se encuentra crear repositorios cuyo archivos pueden tener imágenes, texto o cualquier contenido. Permite crear solicitudes de extracción, mediante la cual indicas quien puede generar cambios en el archivo y quien puede verlo. También permite crear ramas, es decir, diferentes versiones de tu repositorio, entre otras funciones que incluyen o abarcan a su vez protocolos SSH y calves RSA y Putty.

El protocolo SSH también conocido como Secure Shell es que básicamente permite el acceso del usuario a servicios y servidores remotos mediante la autentificación. Con esta clave el usuario sé pude conectarse al GitHub e iniciar sesión sin la necesidad y obligación de proporcionar el nombre de usuario la contraseña cada que quería ingresar a su cuenta. De igual manera, sé pude utilizar para generar confirmaciones. Para conectarse mediante SSH se necesita generar la autenticación a través de un archivo clave privado introducido en el equipo local y si se desea se le puede agregar contraseña para doble seguridad. Al generar la denominada llave en el equipo local, está arrojará un texto único y privado con el cual al copiar y posteriormente pegar en el GitHub se podrá ingresar a los datos o repositorios del mismo.Está clave SSH permite también generar nuevas claves públicas y privadas, llaves de acceso para las diferentes funciones del GitHub y para el contenido mismo. Después de generar una llave de acceso SSH se puede guardar en una USB pars acceder al GitHub desde cualquier dispositivo y cómo medida de seguridad al cumplir el año el GitHub inhabilitara la clave SSH automáticamente, cómo medida de seguridad.

Por su parte la clave la clave RSA es un algoritmo de encriptación asimétrica que utiliza una combinación de clave pública y privada para autenticar y encriptar la comunicación, lo cual establece una mejora en la seguridad del contenido y el acceso al usuario . La clave pública se comparte con otros usuarios o servidores para encriptar los datos, mientras que la clave privada se mantiene en secreto y se utiliza para desencriptar los datos y autenticar la identidad del usuario. En el contexto de GitHub, las claves RSA se utilizan para autenticar y encriptar la comunicación entre tu computadora y los servidores de GitHub a través del protocolo SSH, lo que evuts la dependencia de contraseñas. Al generar una clave RSA, se crea un par de claves pública y privada que se pueden utilizar para acceder de forma segura a los repositorios remotos en GitHub.

Por otro lado, Putty es una herramienta que proporciona una interfaz gráfica para gestionar conexiones SSH y generar claves RSA. Putty también permite configurar y administrar claves SSH para autenticarse de forma segura en servidores remotos, incluyendo los servidores de GitHub. En este sentido Putty protege la confidencialidad de los datos que se transmiten y a su vez genera mayor control al usuario respecto al acceso de su cuenta. En resumen, las claves RSA y Putty se utilizan en GitHub para autenticar y encriptar la comunicación a través del protocolo SSH, proporcionando una capa adicional de seguridad y control sobre el acceso a los repositorios remotos.Las claves RSA y Putty son utilizadas para la autenticación y encriptación de datos en GitHub. A continuación se detalla cómo generar estas claves paso a paso:

1. Generar una clave RSA:

- Abre una terminal o línea de comandos en tu computadora.

- Utiliza el comando ssh-keygen -t rsa -b 4096 -C "tu\_email@example.com" para generar una nueva clave RSA. Reemplaza "tu\_email@example.com" con tu dirección de correo electrónico.

- Se te pedirá que elijas la ubicación y el nombre del archivo donde se guardarán las claves. Puedes dejar la ubicación por defecto o especificar una diferente.

- También se te pedirá que ingreses una contraseña para proteger la clave privada. Esto es opcional, pero se recomienda para mayor seguridad.

2. Generar una clave Putty:

- Descarga e instala Putty en tu computadora si aún no lo has hecho.

- Abre Puttygen, una herramienta incluida en la instalación de Putty, que te permitirá generar una clave SSH compatible con Putty.

- En Puttygen, selecciona el tipo de clave RSA y haz clic en el botón "Generate" para generar una nueva clave.

- Sigue las instrucciones en pantalla para generar la clave. Puedes ingresar una frase de contraseña para proteger la clave privada si lo deseas.

Una vez generadas las claves RSA y Putty, puedes agregarlas a tu cuenta de GitHub siguiendo estos pasos: Copia la clave pública generada (generalmente se encuentra en un archivo con extensión .pub) utilizando el comando cat ~/.ssh/id\_rsa.pub en tu terminal o abriendo el archivo con un editor de texto. Después, ve a la configuración de tu cuenta en GitHub, selecciona "SSH and GPG keys" y haz clic en "New SSH key". Luego pega la clave pública en el campo correspondiente y dale un nombre descriptivo a la clave (por ejemplo, "Mi clave personal"). Y guarda los cambios.

En resumen, las claves RSA y Putty son utilizadas para autenticarse de forma segura en GitHub, permitiendo el acceso a repositorios remotos y la interacción segura con los servicios de GitHub a través de SSH.