Laboratorio_08_seguridad_de_sistemas

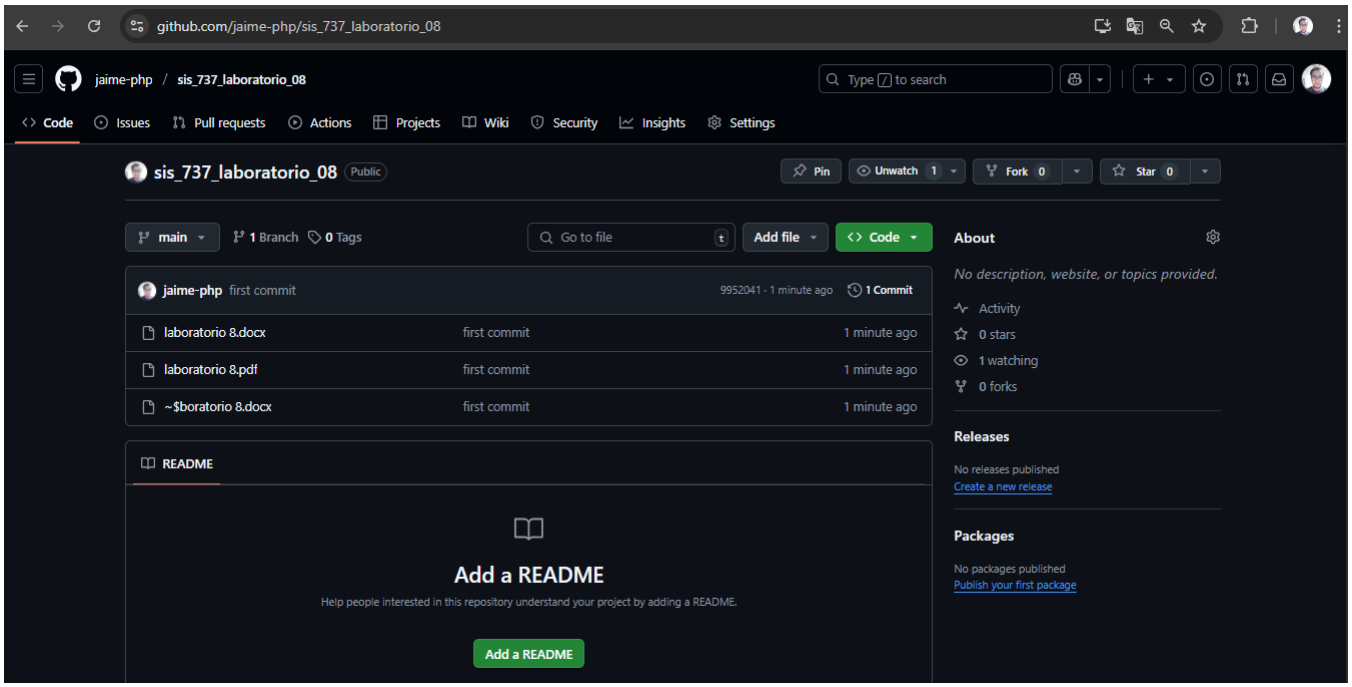
Univ.: **Jaime Mamani Mendizabal**

C.I.: **6672063**

GITHUB

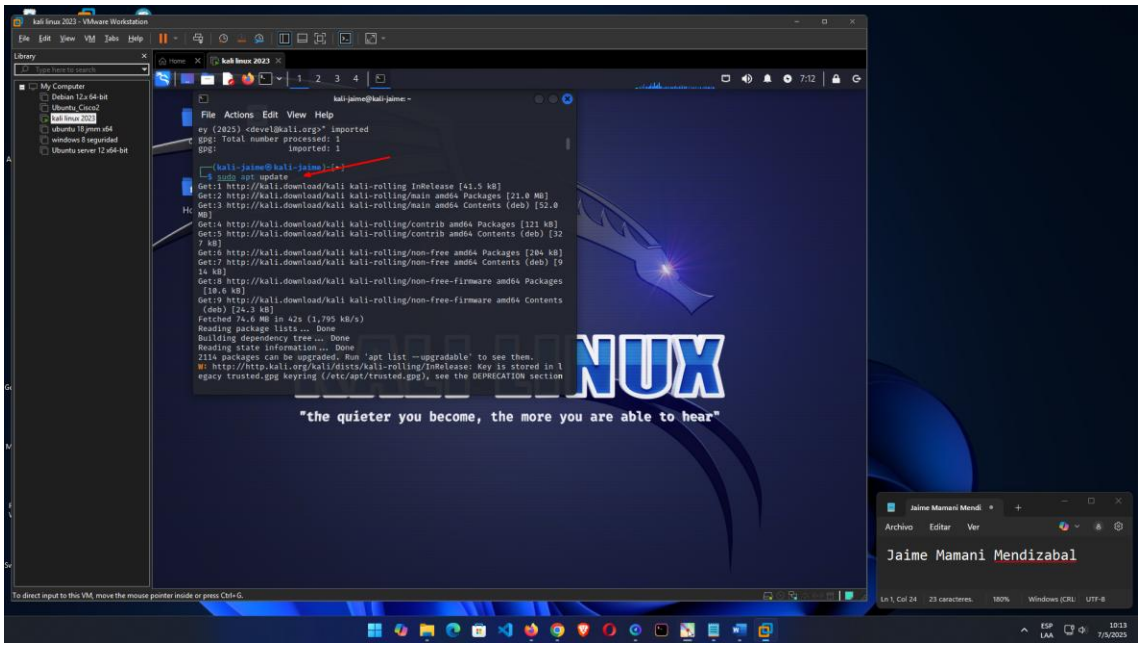
Nombre: **Jaime Mamani | Jaime-php**

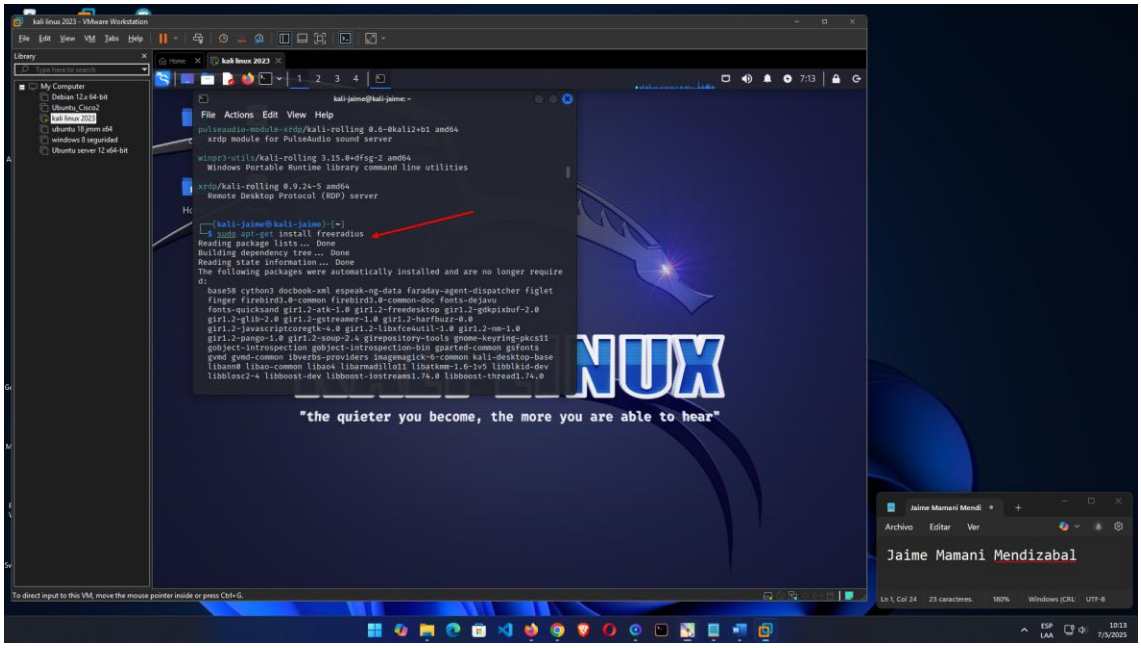
Enlace: **https://github.com/jaime-php/sis_737_laboratorio_08**



Instalación de Freeradius

1.- Inicialmente para la implementación de la Guía es imprescindible contar con la instalación de Freeradius. Por lo tanto, iniciamos con el usuario **kali** y contraseña **sistemas,** procederemos iniciando el proceso de actualización de los paquetes en Kali mediante el comando: **sudo apt-get update**.

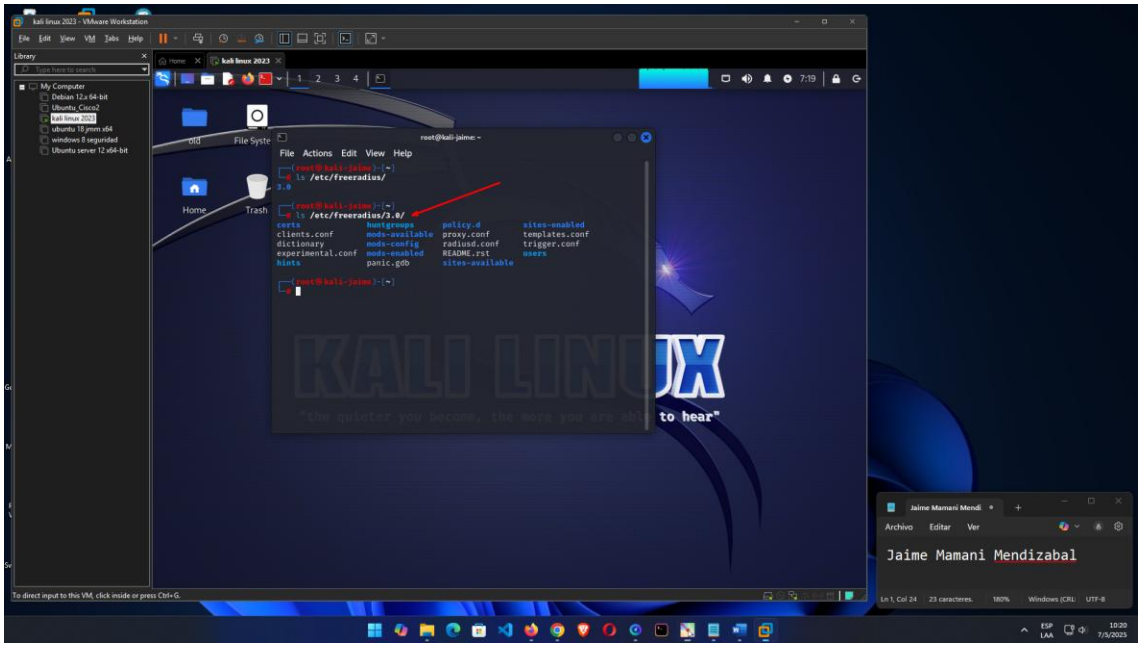




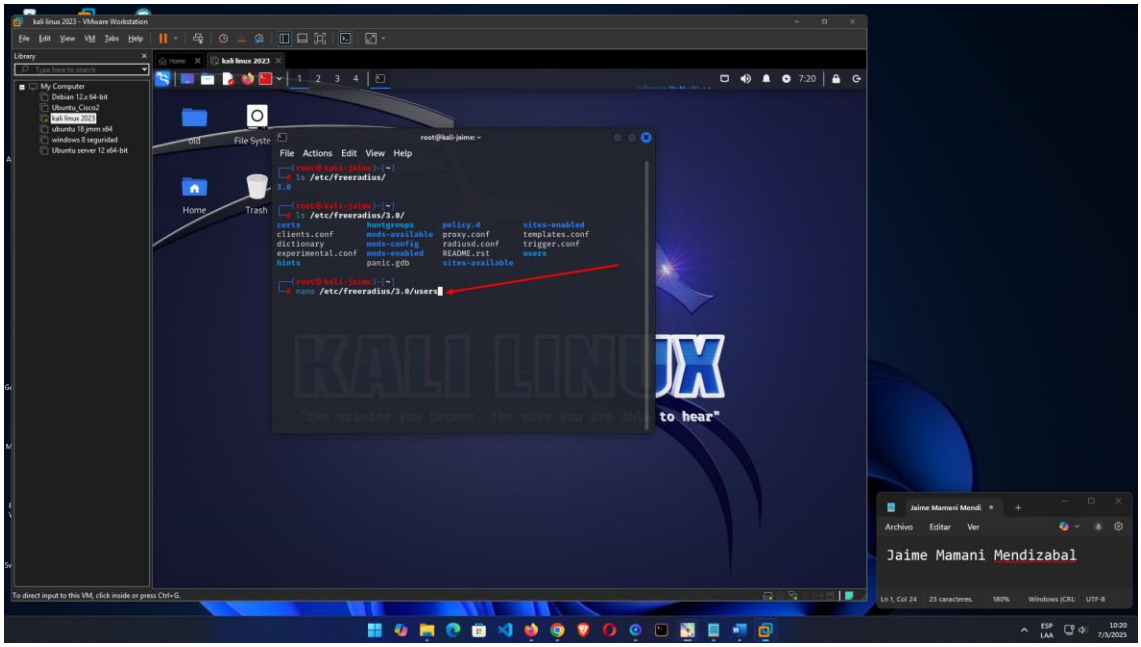
Se requiere inicializar como **Super Usuario** dentro de kali con la constraseña **sistemas**

Nos dirigimos a la carpeta de Freeradius con el comando: **ls /etc/freeradius/3.0/**

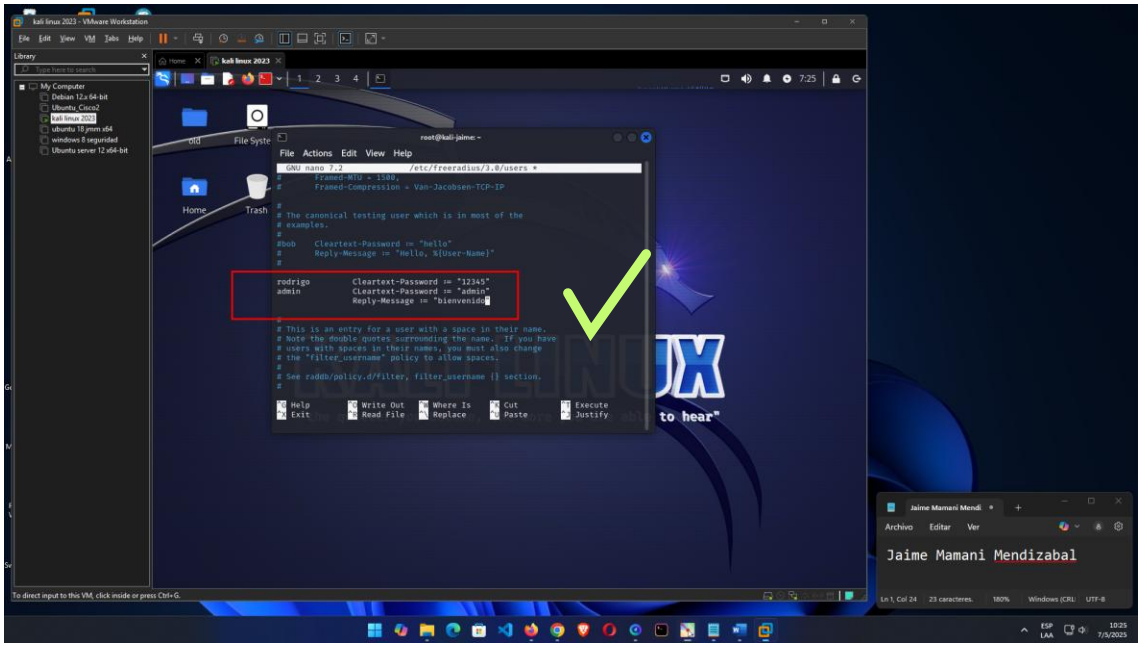
Si la instalación se realizó correctamente tendrían que salir los siguientes archivos



Para comenzar con la configuración, accedemos al archivo de usuarios utilizando el comando **nano /etc/freeradius/3.0/users**



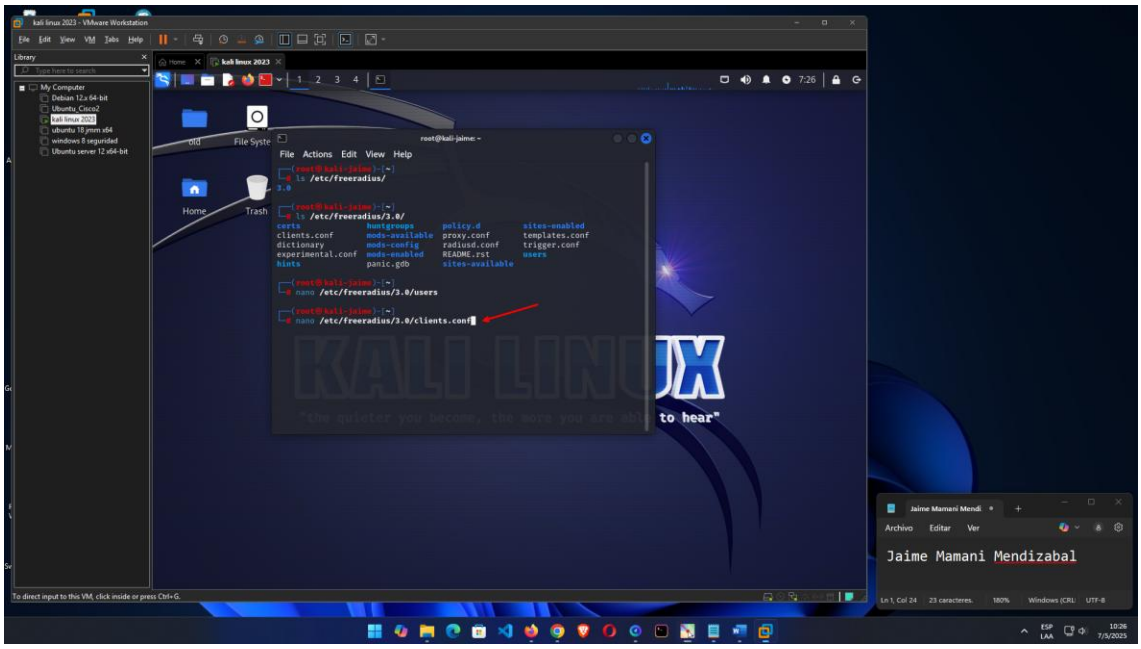
Una vez dentro del archivo, procederemos a la creación de usuarios: un usuario cliente con su contraseña “12345”y un usuario administrado, para el usuario administrador, agregaremos un mensaje de Bienvenida.



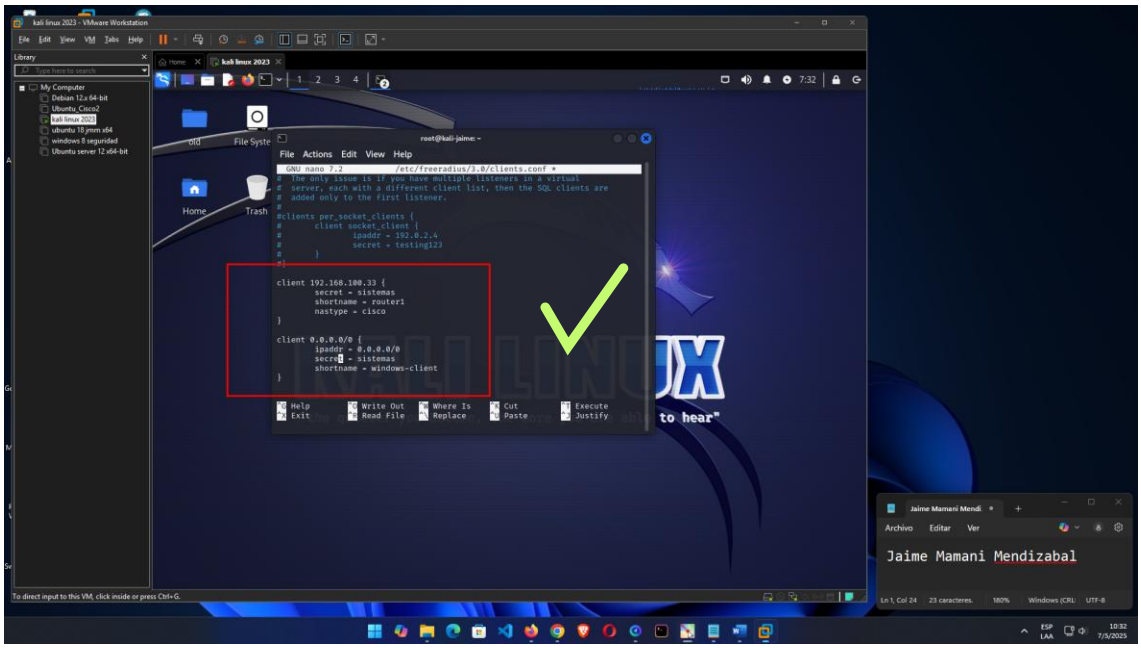
Una vez creados los usuarios guardamos y cerraremos el archivo.

A continuación, procederemos a configurar los clientes, estos son los equipos de red que tienen permiso para consultarnos por los usuarios.

Para ello ingresamos el comando: **nano /etc/freeradius/3.0/clients.conf**



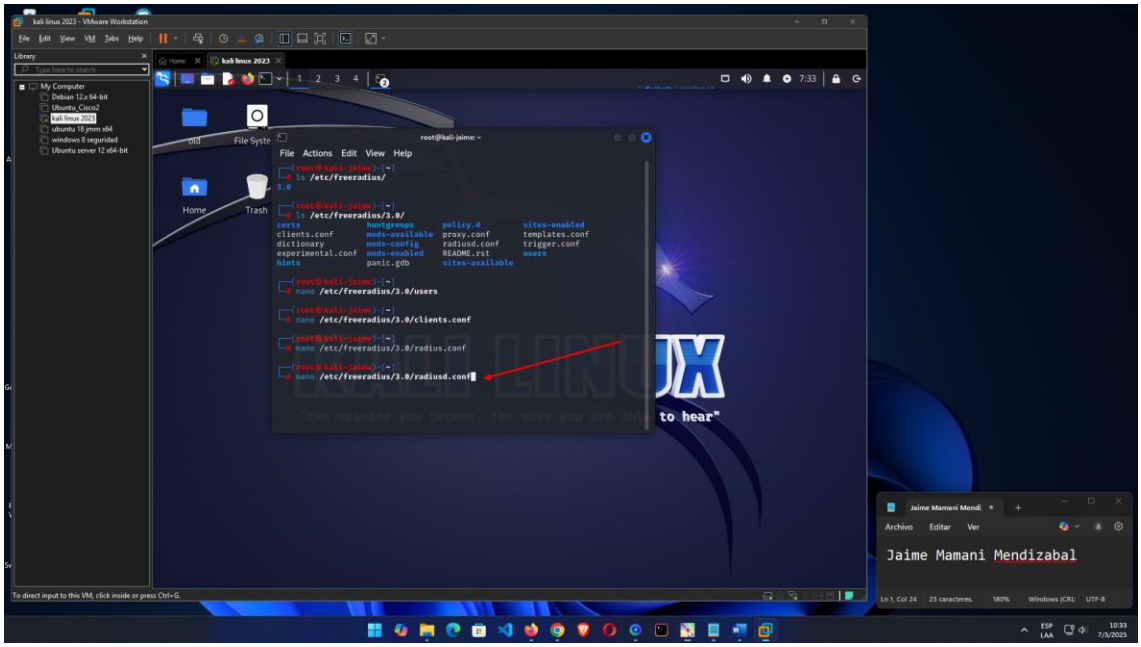
Implementaremos los clientes que pueden realizar la autentificación, en este caso "0.0.0.0/0" nos indica que todas las ip pueden realizar la autentificación, si se quisiera solo en un segmento de red seria de la siguiente manera "192.168.100.0/0"



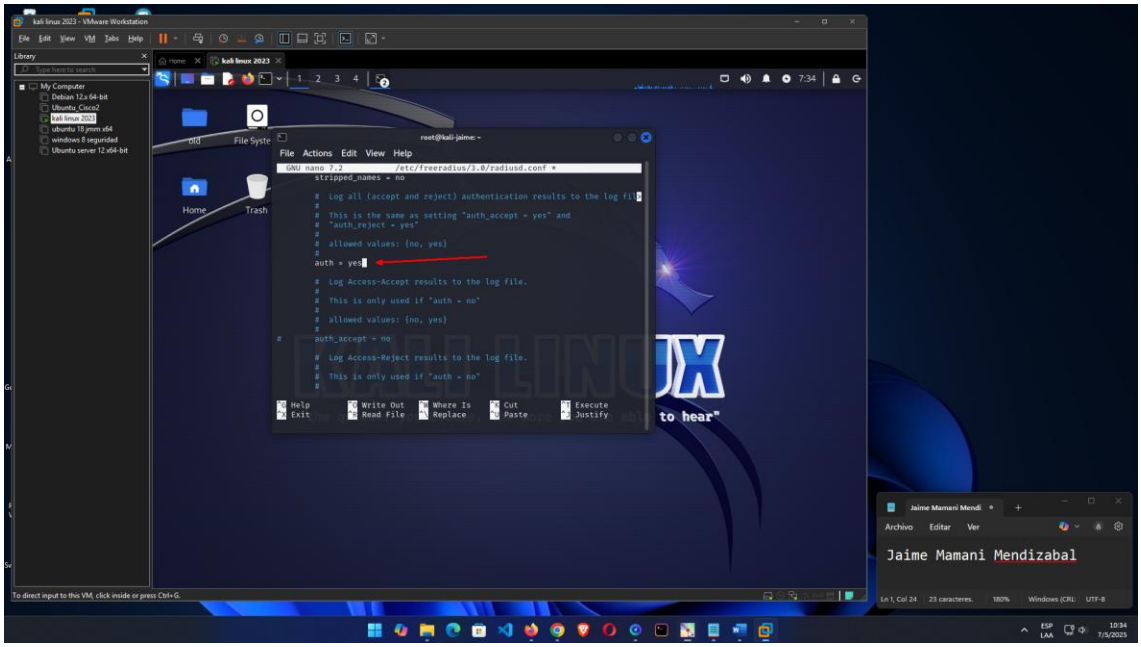
Hasta este punto, Freeradius estaría configurado de forma local, sin embargo, para agregar una capa adicional de seguridad y poder rastrear quien consulta nuestro servicio, habilitaremos la generación de registros (logs).

Para ello nos dirigimos al archivo radiusd.conf con el comando: **nano**

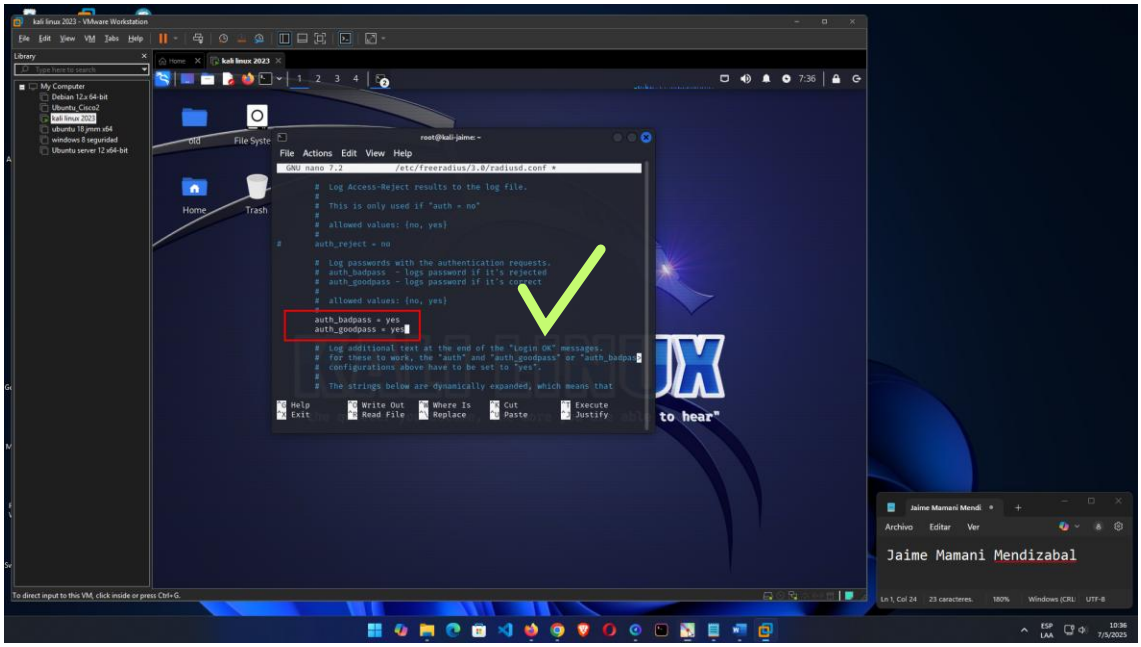
/etc/freeradius/3.0/radiusd.conf



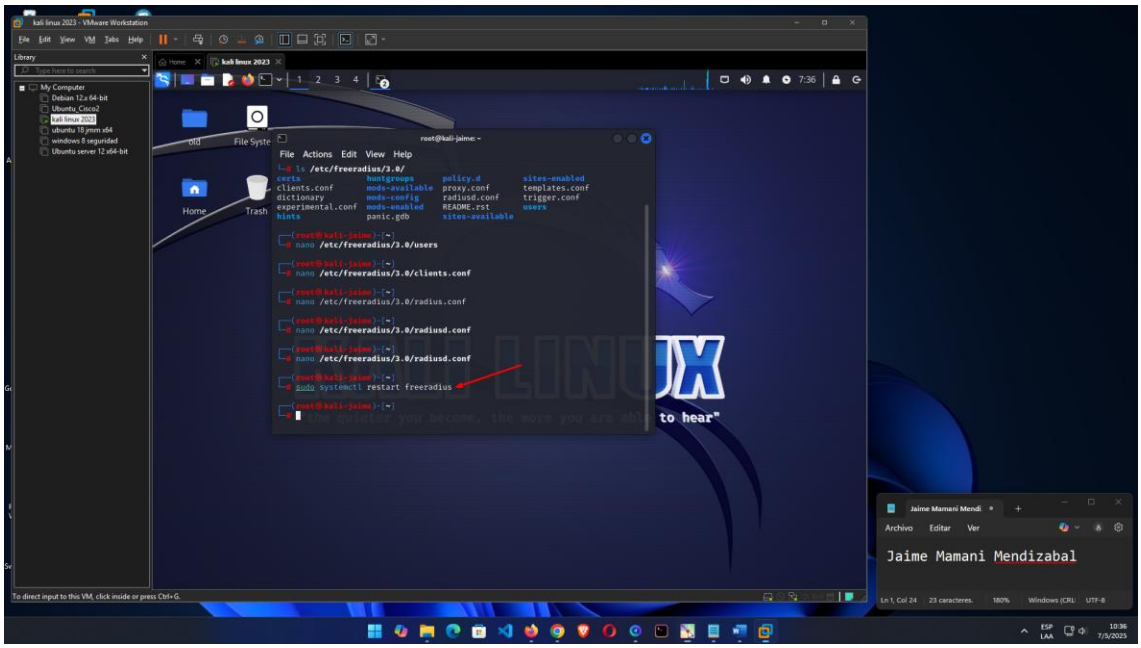
Una vez dentro del archivo, localizamos la línea correspondiente de la autentificación (auth) y modificamos el valor predeterminado “no” a “YES”



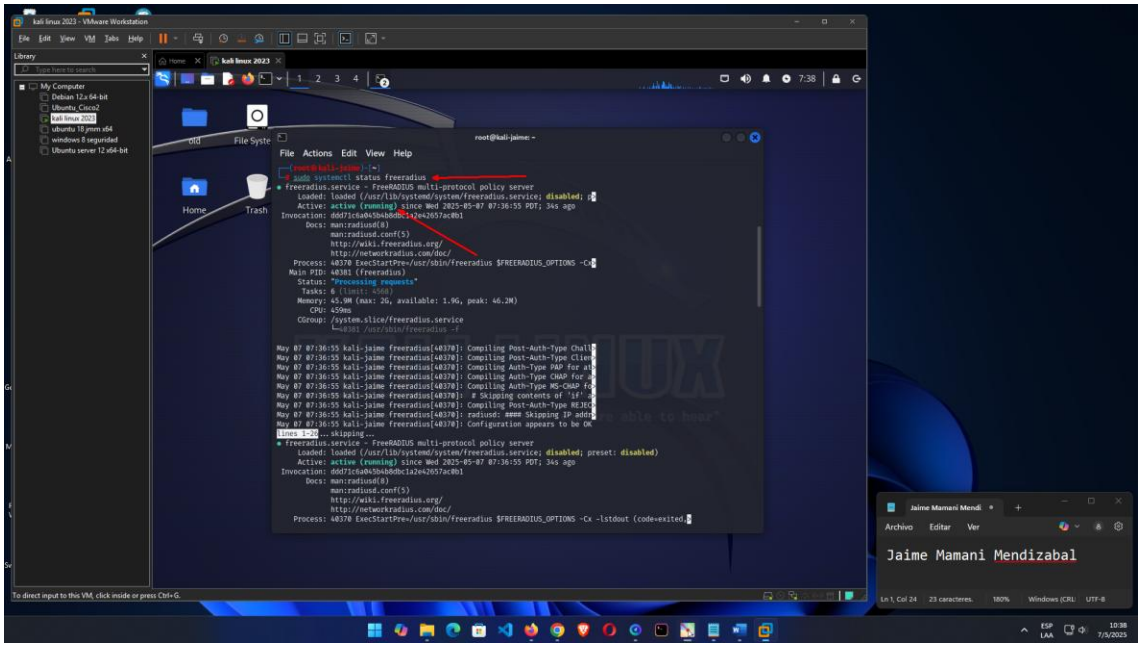
Realizaremos el mismo paso anterior para la generación de logs para eventos como **auth_badpass** y **auth_goodpass**



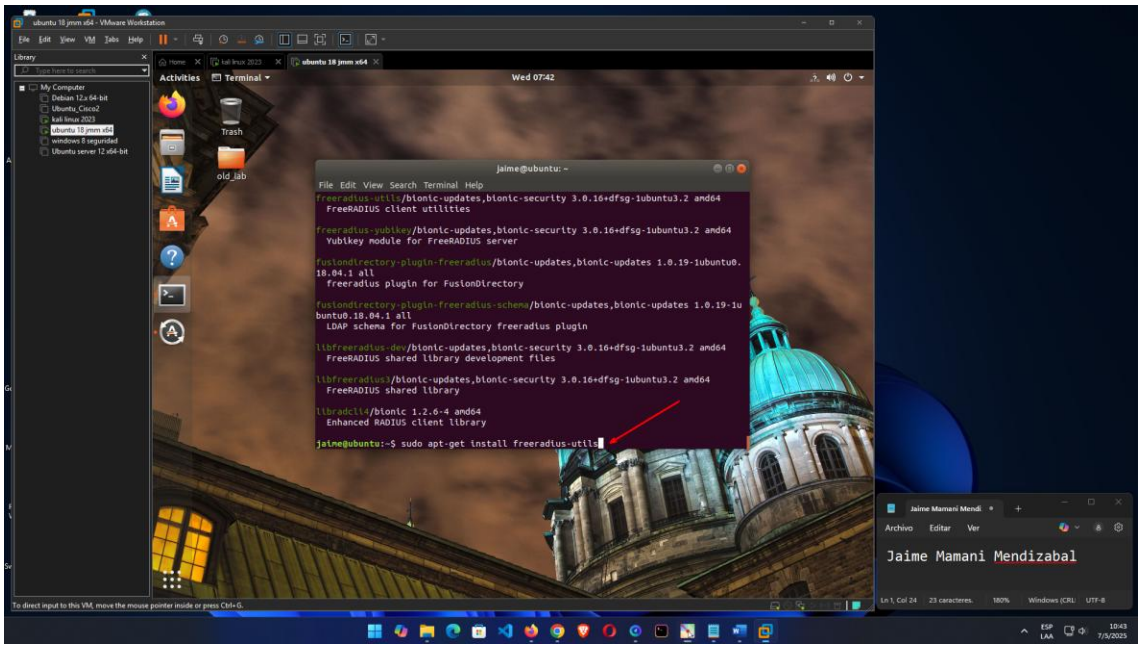
Procedemos a reiniciar el servicio de Freeradius para aplicar todos los cambias realizados con el siguiente comando: **sudo systemctl restart freeradius**



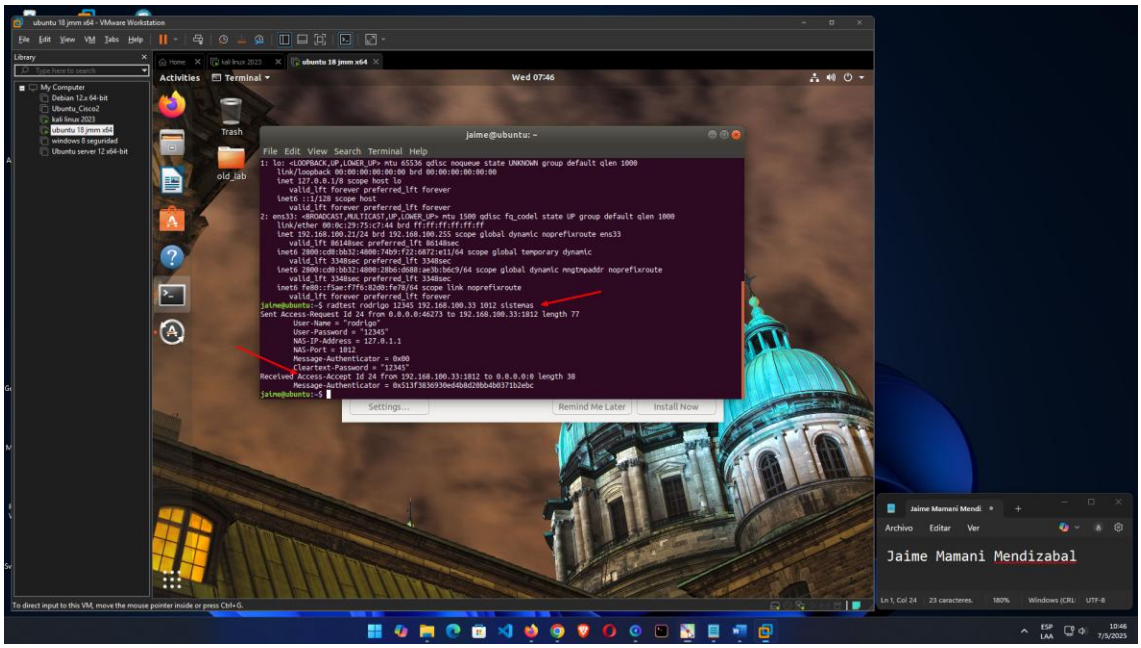
Una vez hecho esto, verificamos que el servicio este activo con el comando **sudo systemctl status freeradius**



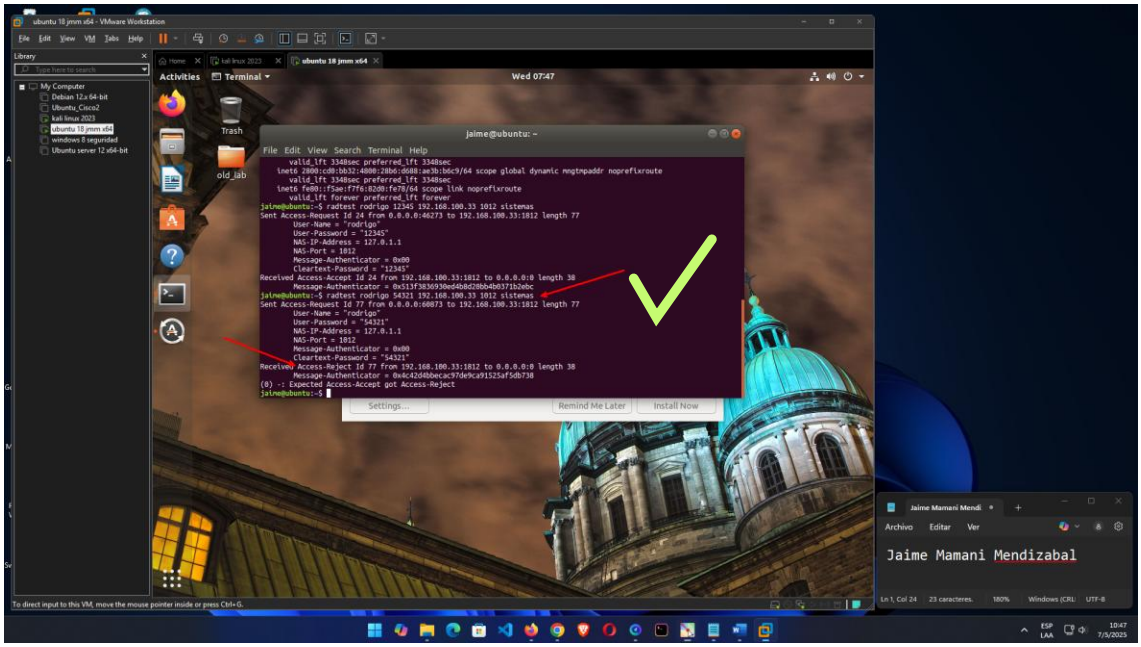
Ya está listo para usarse para ello nos vamos a otro equipo en este caso utilizamos Ubuntu eh instamos la siguiente herramienta



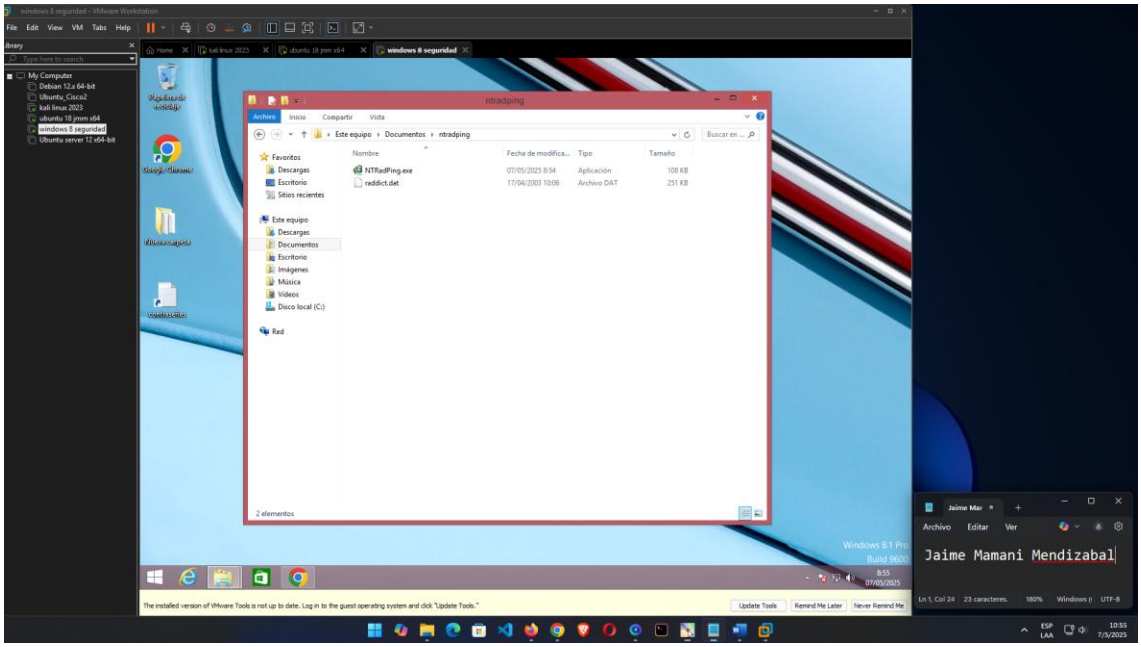
Con el siguiente comando podremos logear en el servidor radius y comprobar que este anda, con el comando **radtest "usuario" "contraseña" "ip_del_servidor" "puerto" "contraseña compartida".**



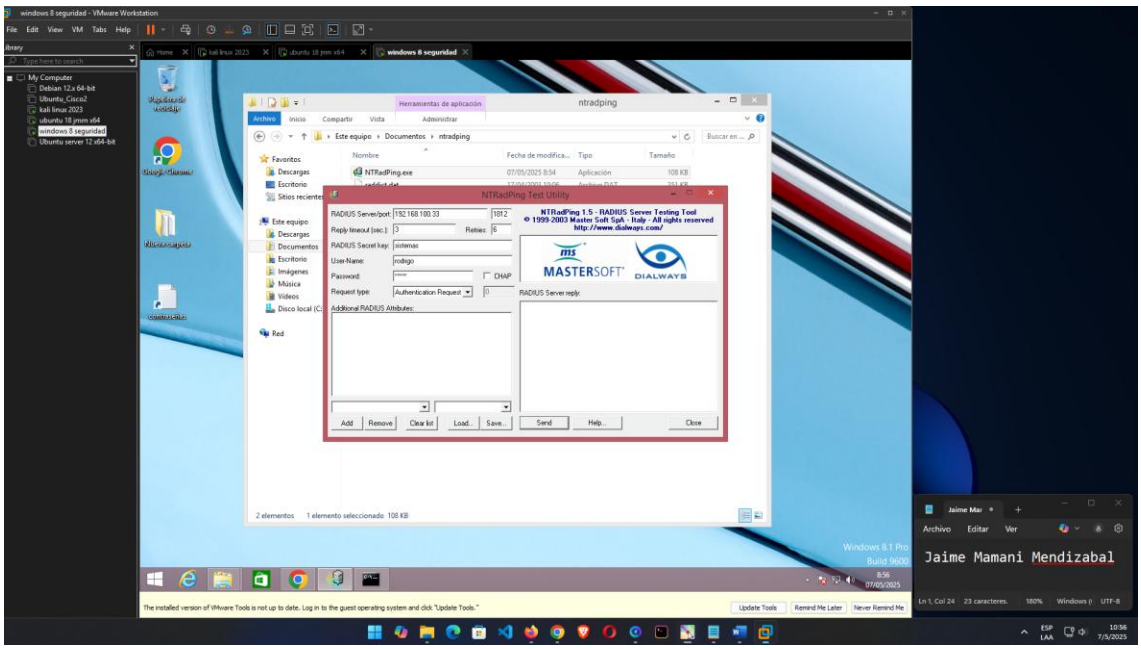
Haremos un logeo correcto y seguidamente se realizará un logeo incorrecto, en ambas logeos nos genera un mensaje de logeo aceptados o rechazado.



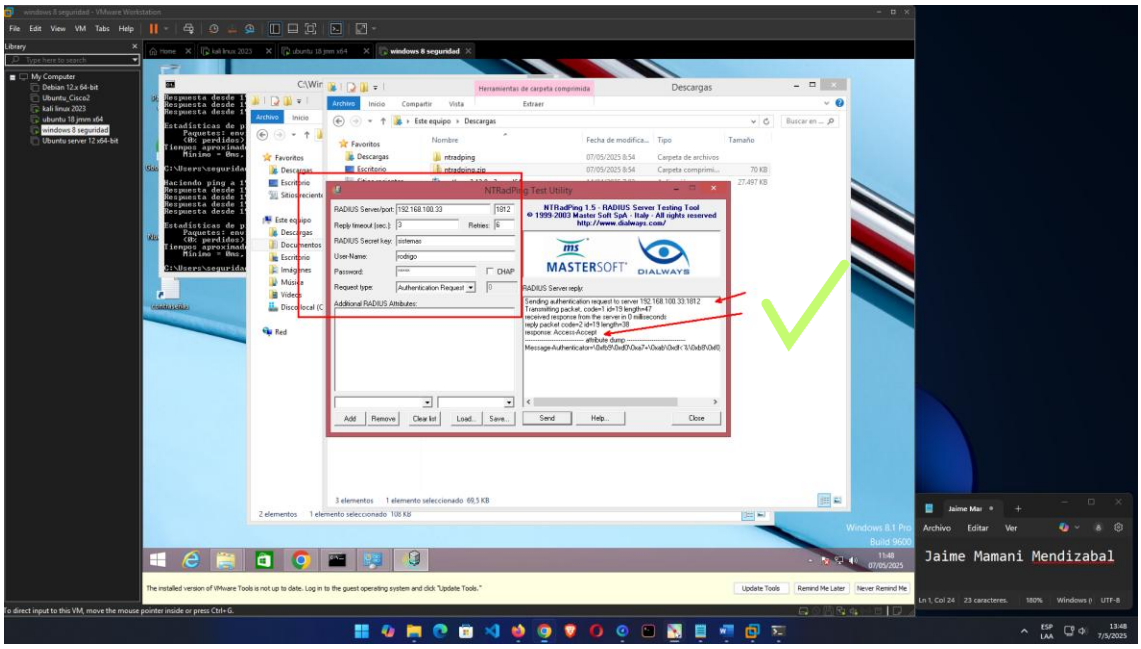
Nos dirigiremos a Windows 8 y abriremos la aplicación de **NTRadPing**, esta se encuentra dentro de la carpeta con el mismo nombre de la aplicación.



Dentro de la aplicación pondremos la ip del servidor radius, puerto lógico, contraseña compartida, usuario, contraseña de usuario, una vez llenado todas las casillas presiona **Send.**



Y este nos mostrara el siguiente mensaje



Evaluación

Pregunta 1

1.- Con que comando se puede ver los logs en tiempo real en el servidor radius.

En tiempo real y modo debug con:

sudo freeradius -X

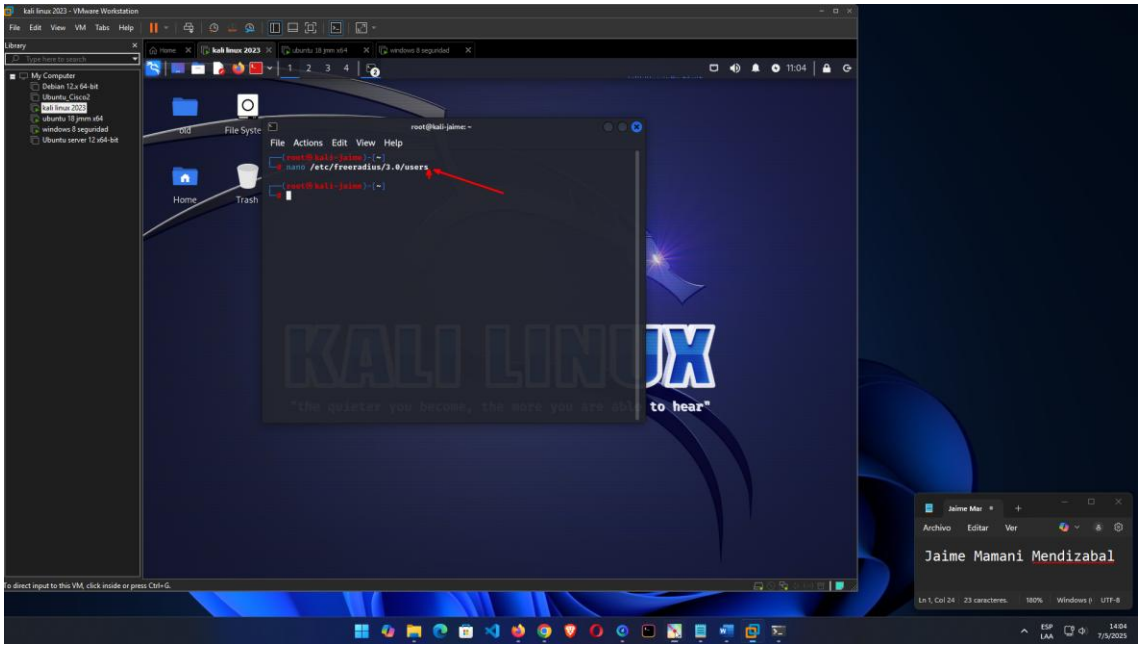
Otra opción es ingresar donde se almacenan los log con el comando:

sudo tail -f /var/log/freeradius/radius.log

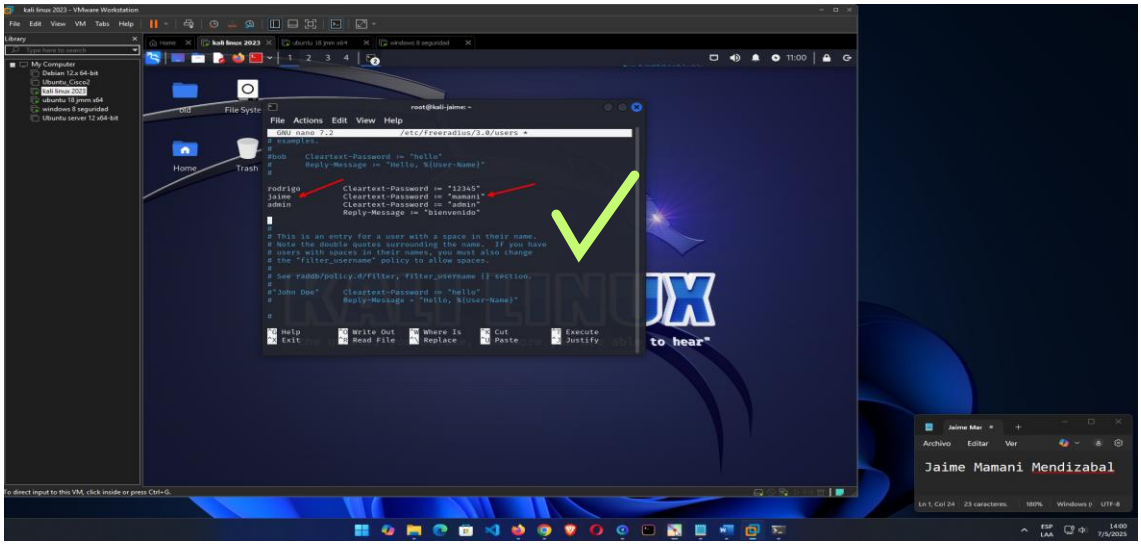
Pregunta 2

2.- Crear un nuevo usuario e logearse tanto desde Linux como desde Windows e indique que datos puede observar en estos logs. Al crear el usuario ponga su **nombre como usuario y su apellido como contraseña.**

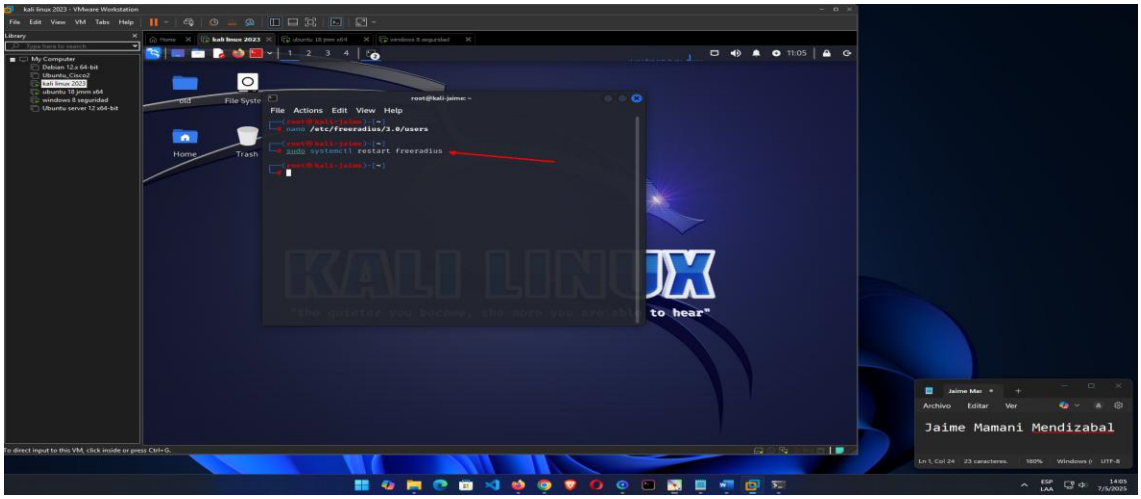
Por lo cual agregaremos un nuevo usuario



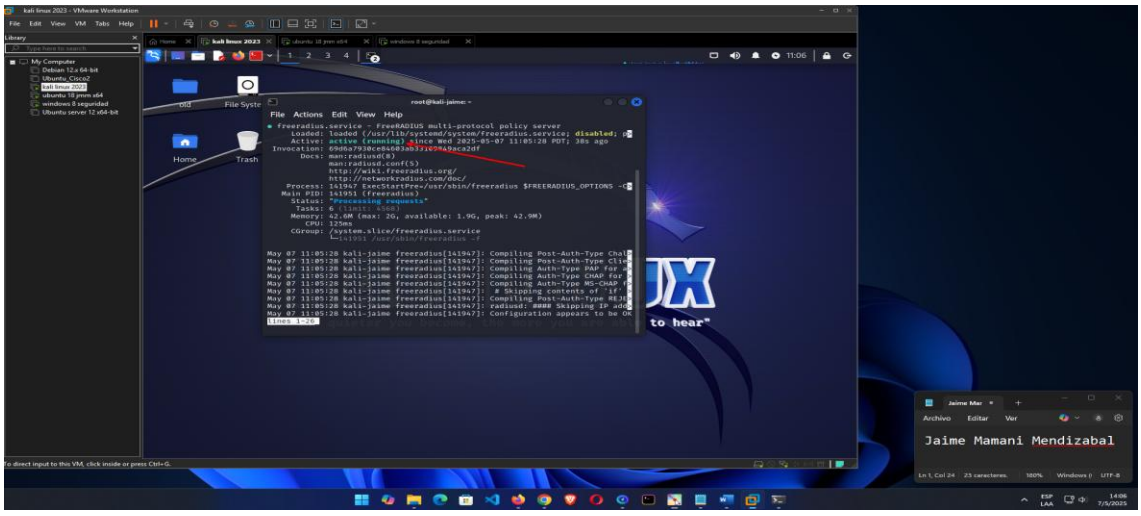
Agregamos el usuario “jaime” con contraseña “mamani”



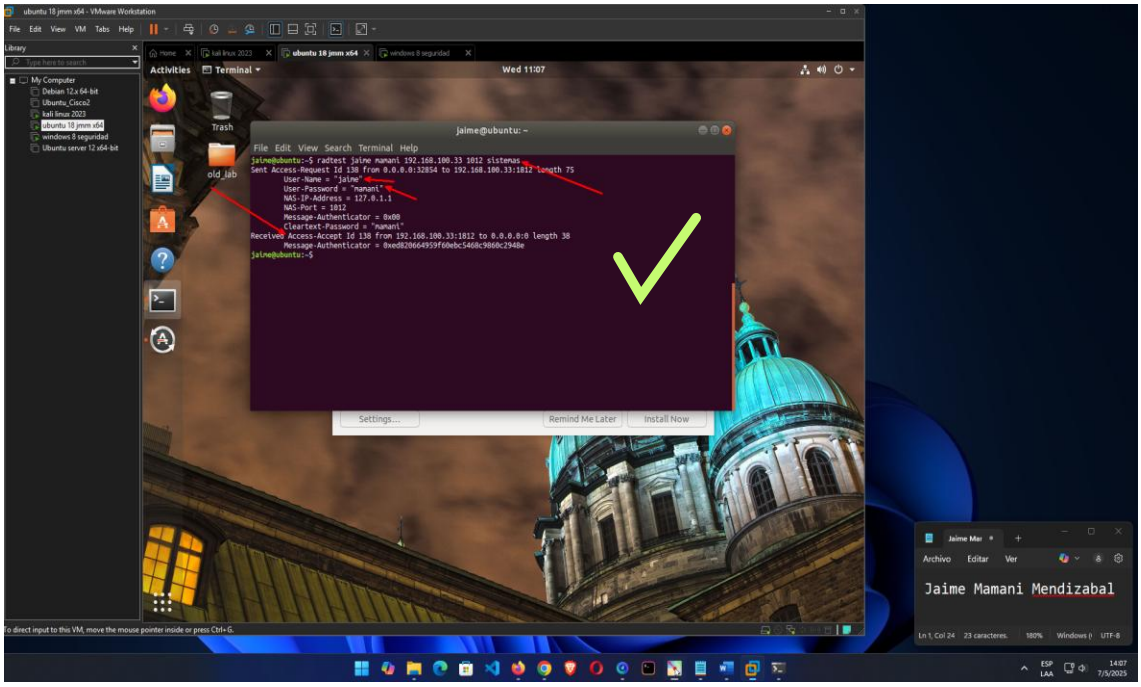
Guardamos el usuario y posteriormente reiniciamos el servicio de freeradius



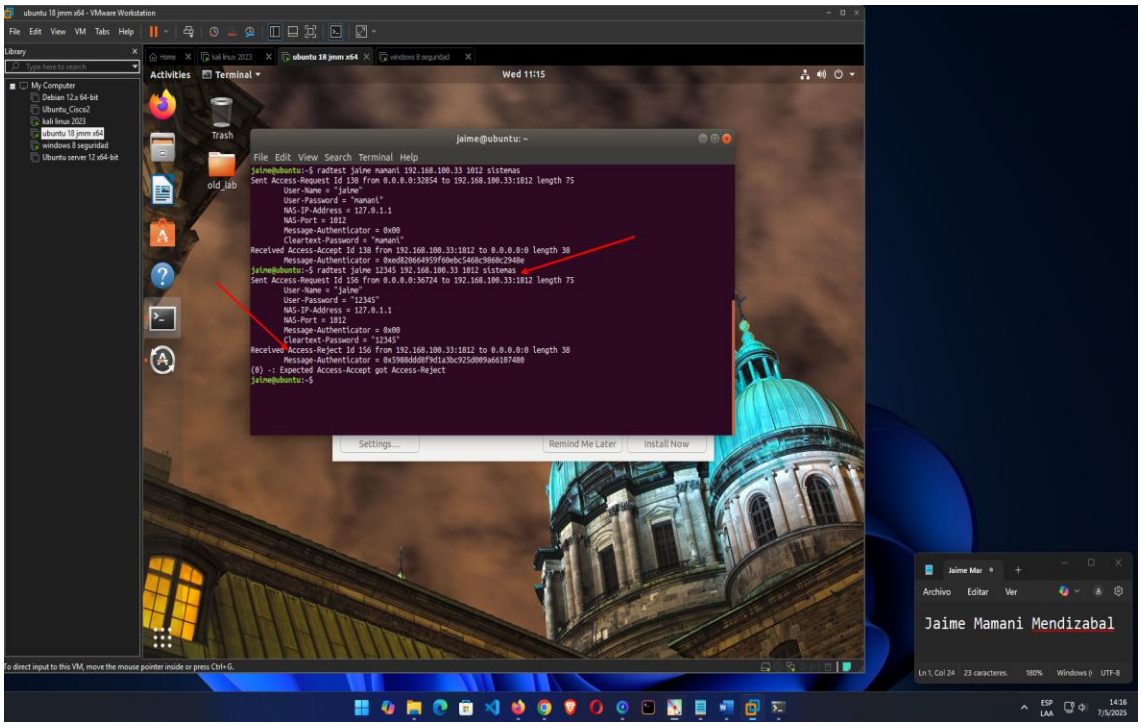
Verificamos que el servicio este levantado



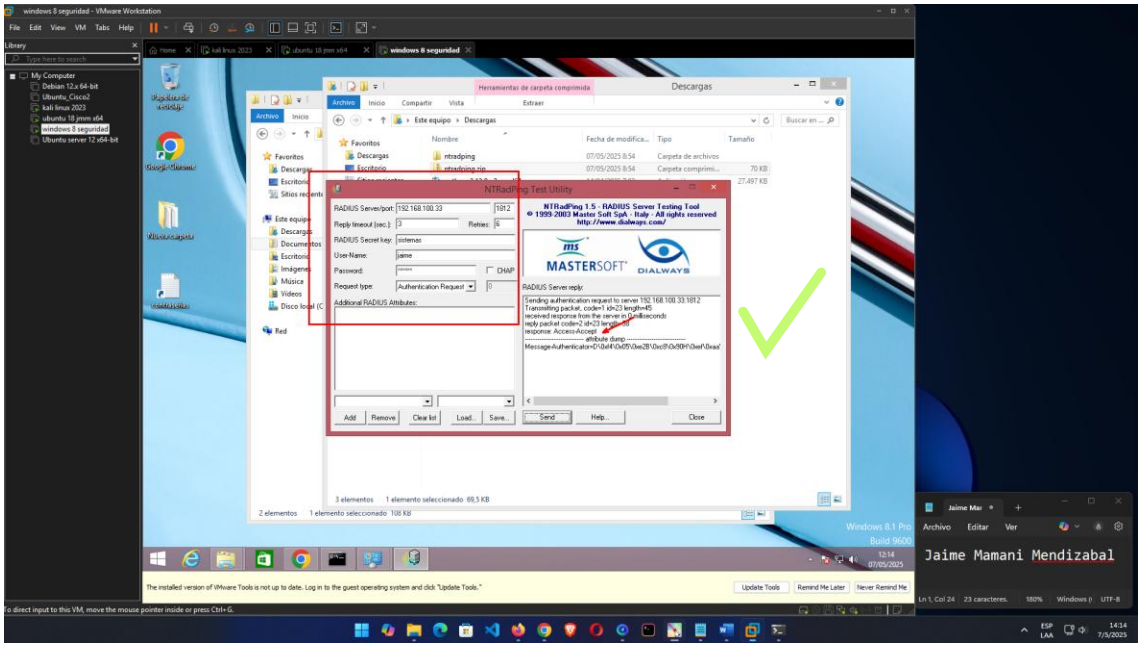
Probamos loguearnos desde Ubuntu 18 con nuestro nuevo usuario



Si realizamos un logue incorrecto, nos genera un mensaje de logueo rechazado.



Ahora realizamos la prueba desde Windows 8, donde nos acepta el logueo



En los archivos LOGS podemos apreciar datos como los nombres de los usuarios que intentan autenticarse, permite ver desde que maquina llego la petición además del tipo de autenticación que se usa, también muestra la contraseña del usuario, también nos muestra quienes tuvieron autenticación exitosa y quienes fallida