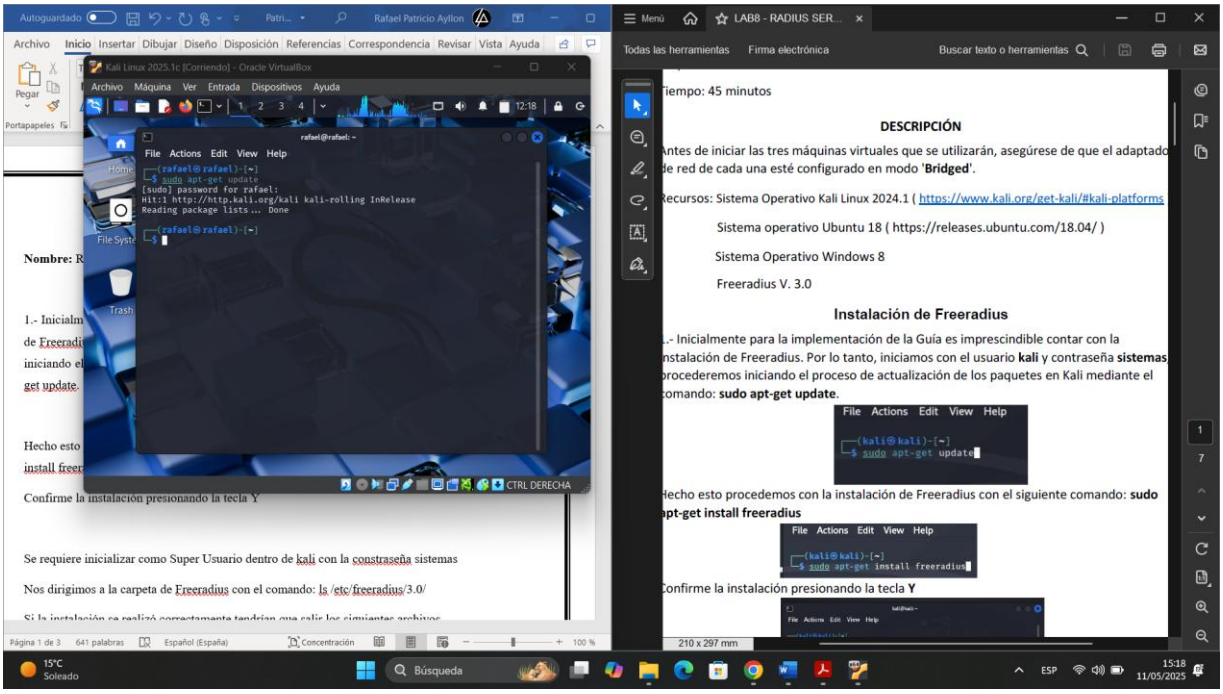
Laboratorio 8

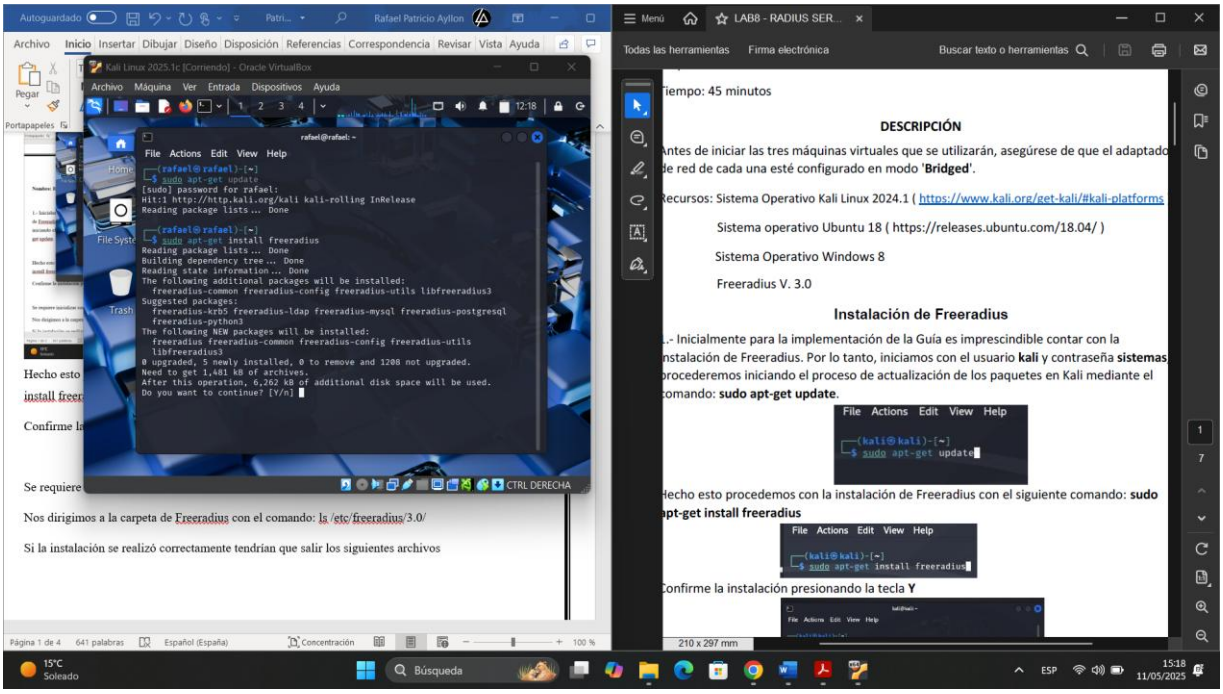
Nombre: Rafael Antonio Patricio Ayllón **CI:** 10473854 **RU:** 108771

Instalación de Freeradius

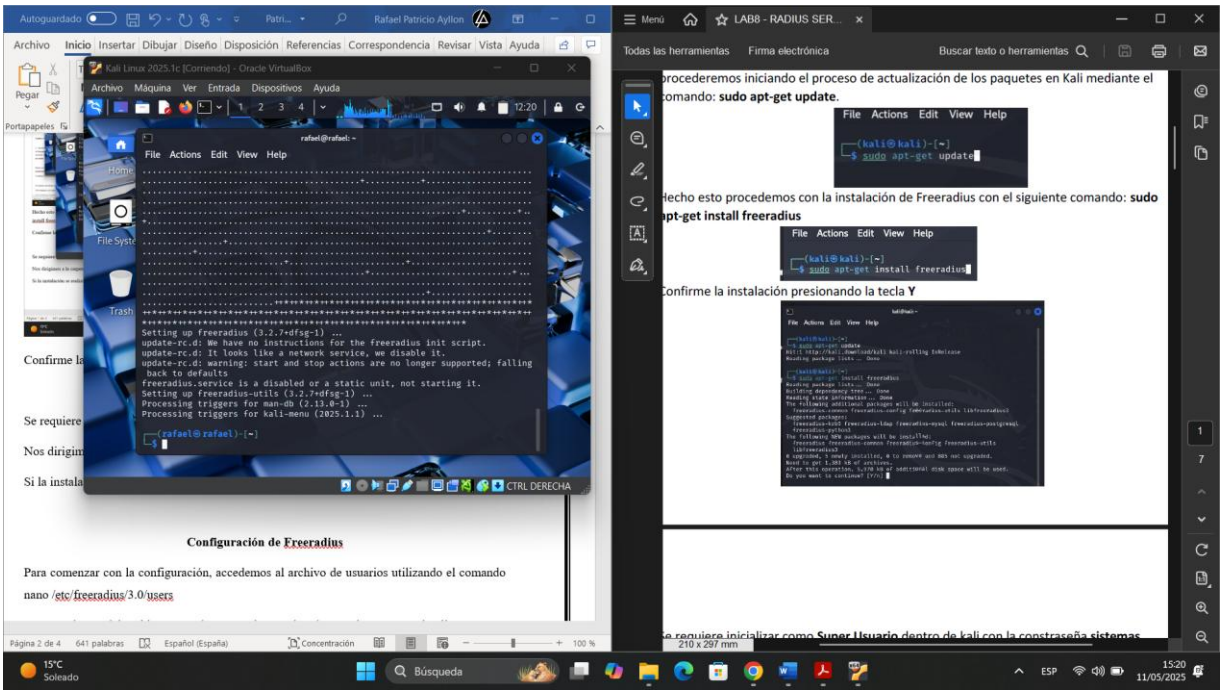
1.- Inicialmente para la implementación de la Guía es imprescindible contar con la instalación de Freeradius. Por lo tanto, iniciamos con el usuario kali y contraseña sistemas, procederemos iniciando el proceso de actualización de los paquetes en Kali mediante el comando: sudo apt-get update.



Hecho esto procedemos con la instalación de Freeradius con el siguiente comando: sudo apt-get install freeradius



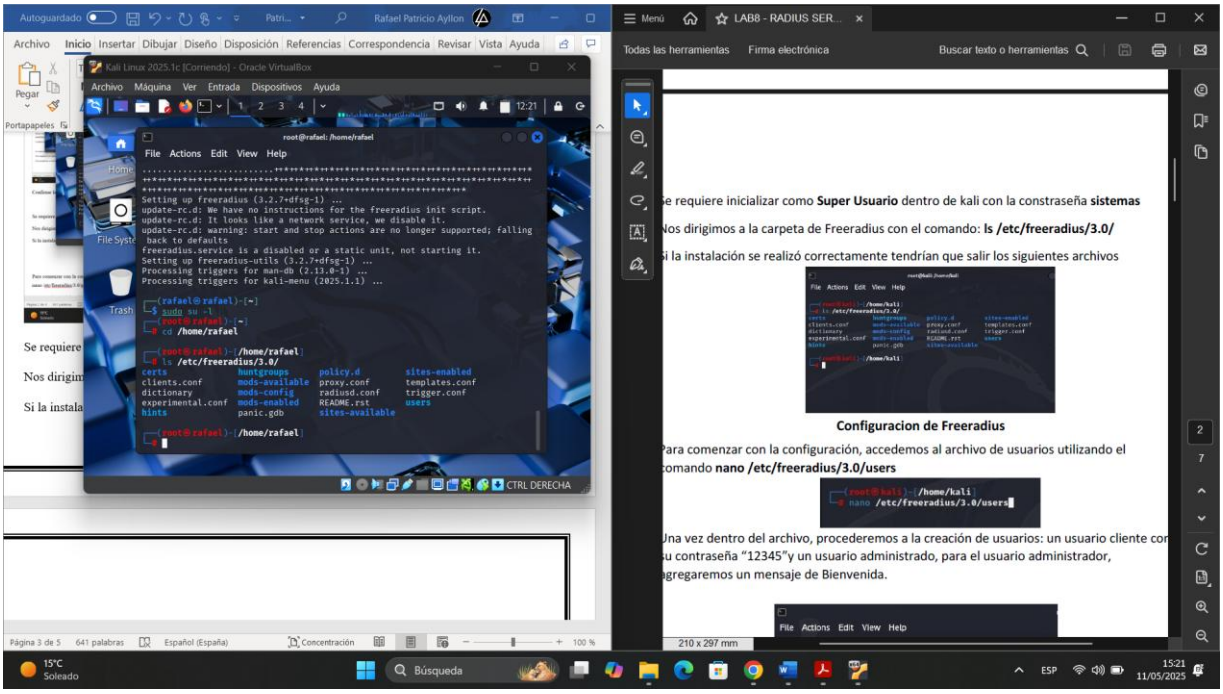
Confirme la instalación presionando la tecla Y



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

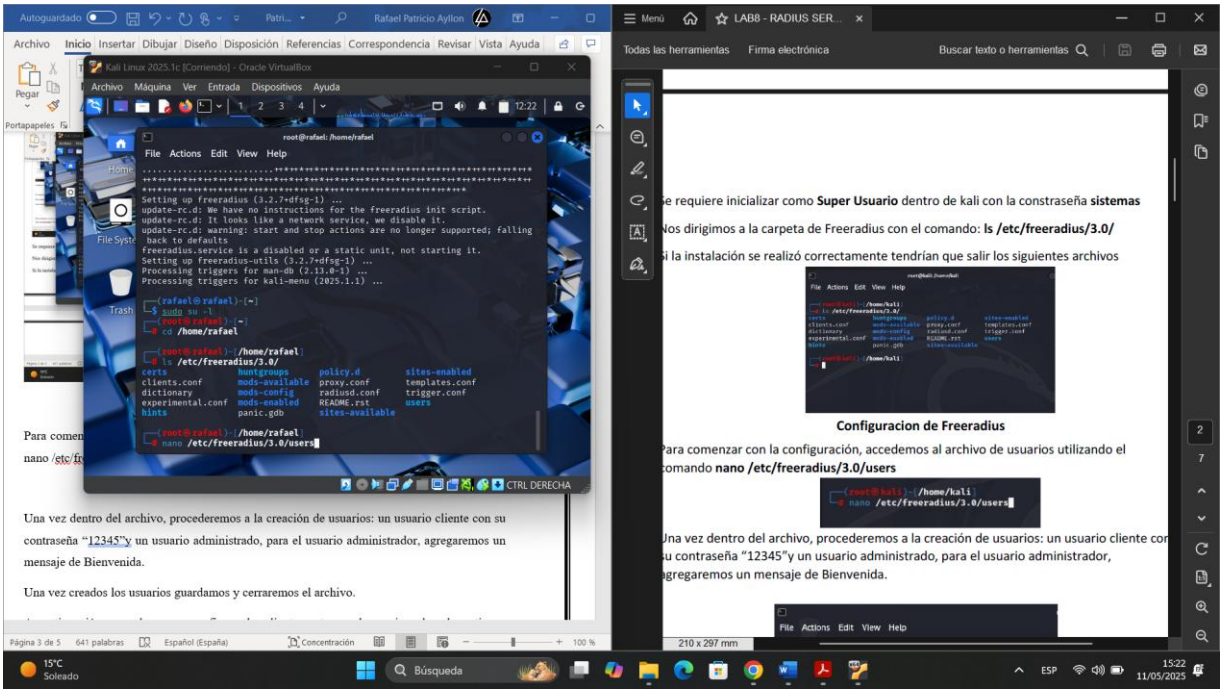
Nos dirigimos a la carpeta de Freeradius con el comando: ls /etc/freeradius/3.0/

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

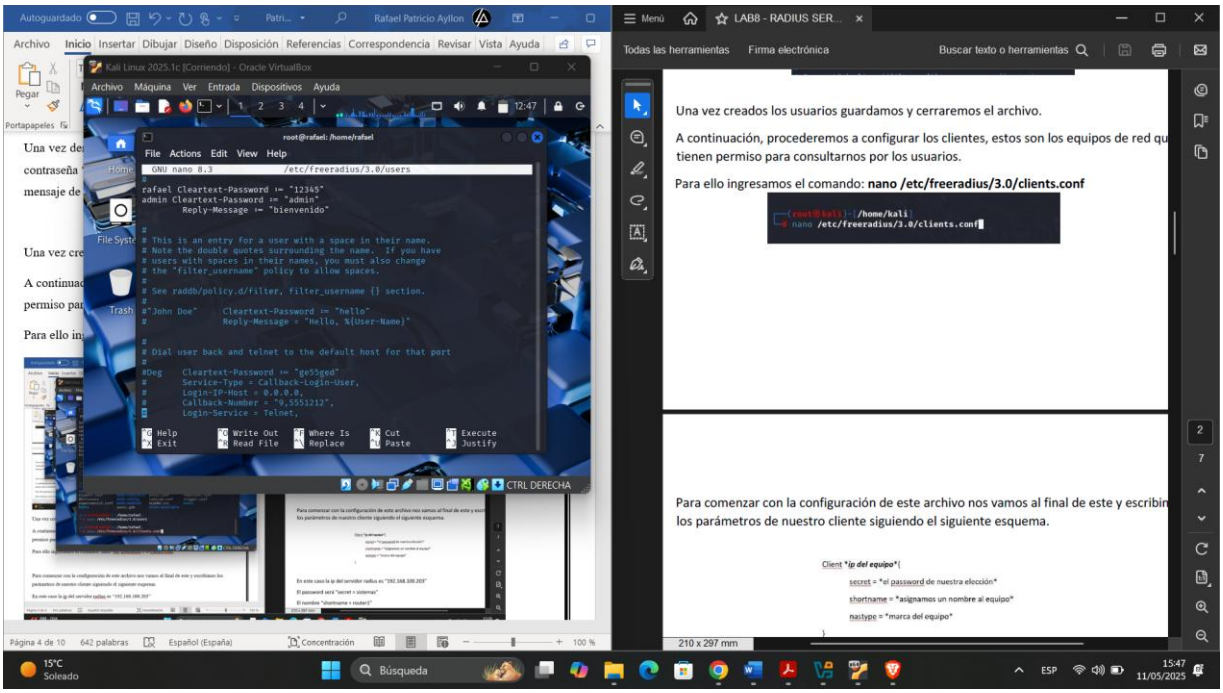


Configuración de Freeradius

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



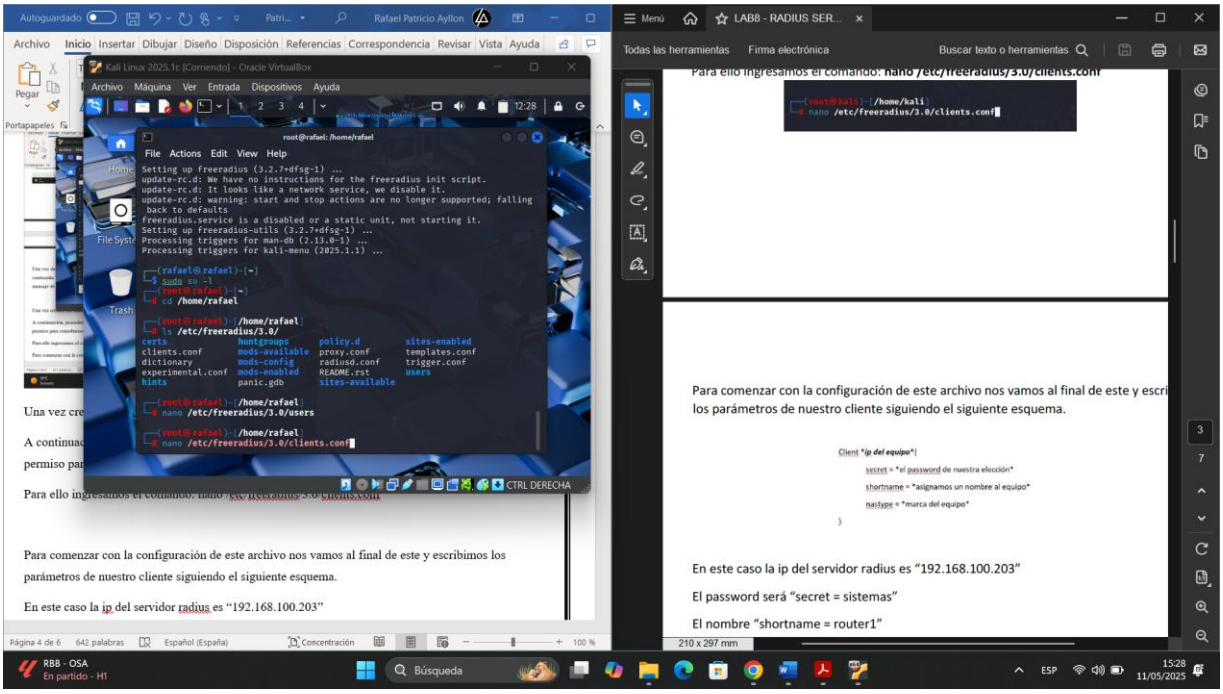
Una vez dentro del archivo, procederemos a la creación de usuarios: un usuario cliente con su contraseña “12345” y un usuario administrado, para el usuario administrador, agregaremos un mensaje de Bienvenida.



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



Para comenzar con la configuración de este archivo nos vamos al final de este y escribimos los parámetros de nuestro cliente siguiendo el siguiente esquema.

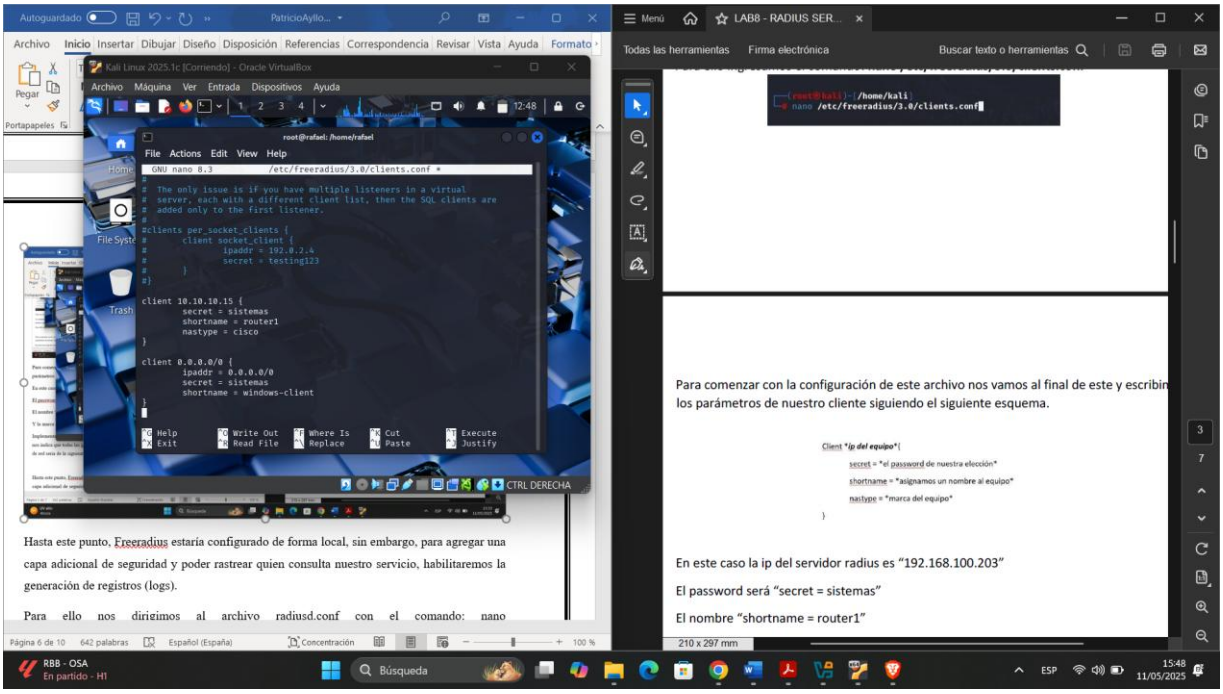
En este caso la ip del servidor radius es "192.168.100.203"

El password será "secret = sistemas"

El nombre "shortname = router1"

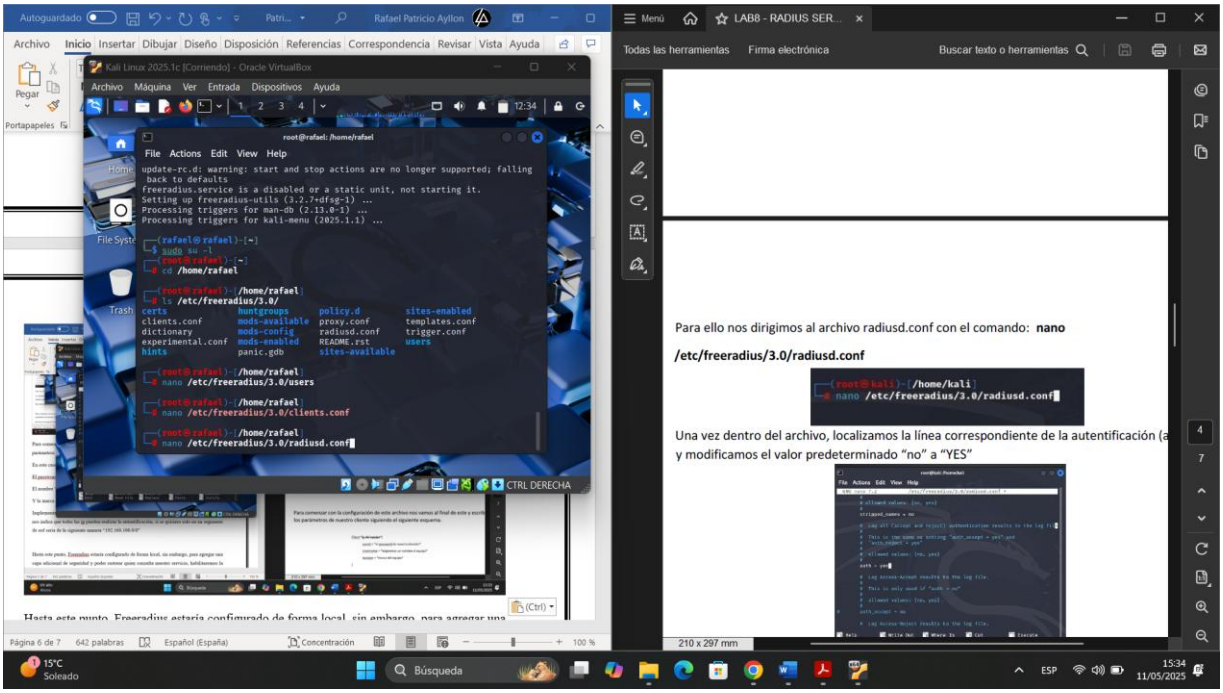
Y la marca del equipo "nastype = cisco"

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"

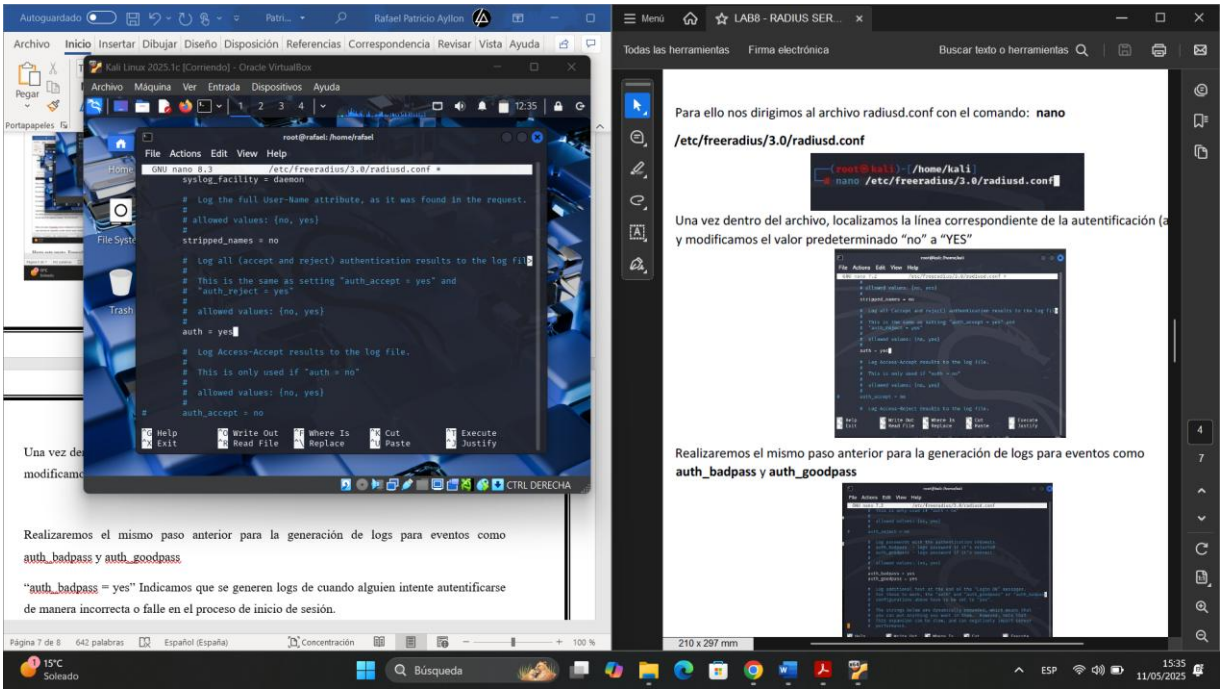


Hasta este punto, Freeradius estaría configurado de forma local, sin embargo, para agregar una capa adicional de seguridad y poder rastrear quien consulta nuestro servicio, habilitaremos la generación de registros (logs).

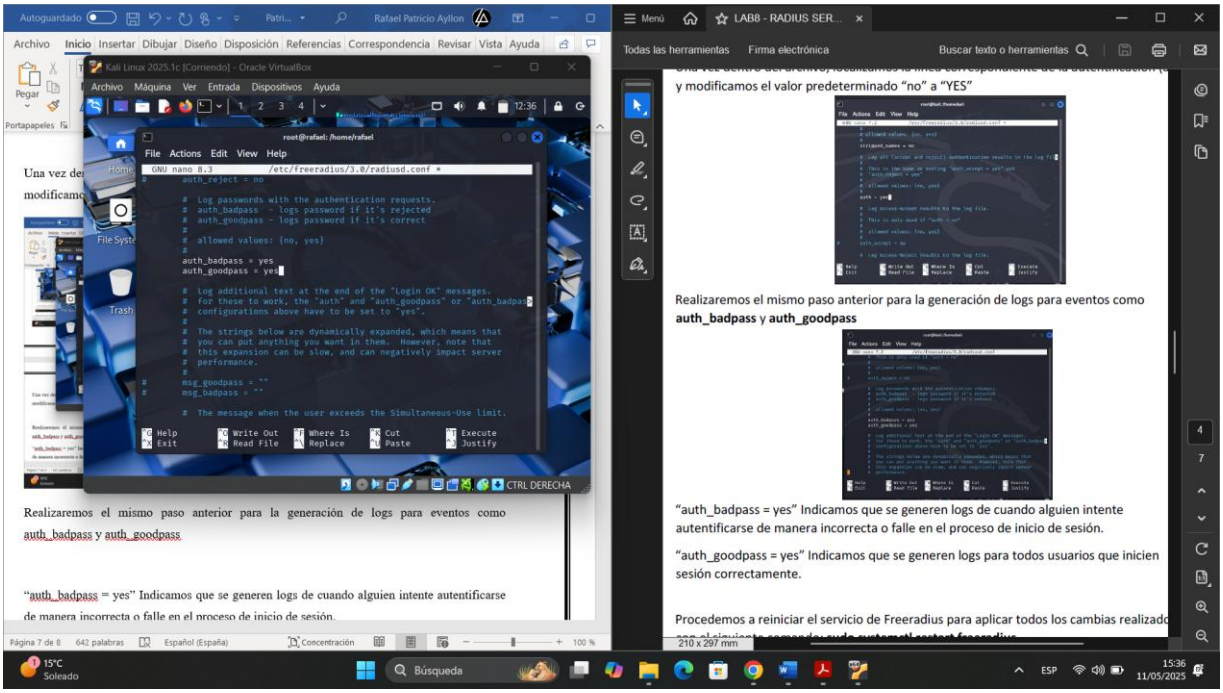
Para ello nos dirigimos al archivo radiusd.conf con el comando: nano /etc/freeradius/3.0/radiusd.conf



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



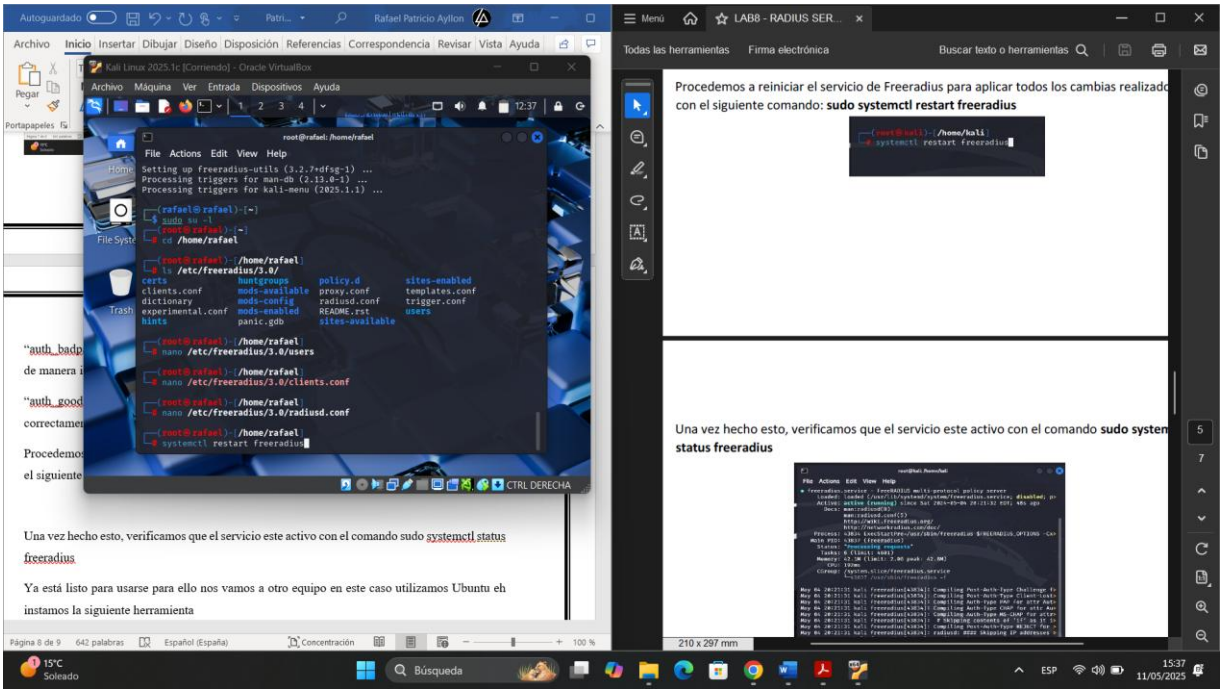
Realizaremos el mismo paso anterior para la generación de logs para eventos como auth_badpass y auth_goodpass



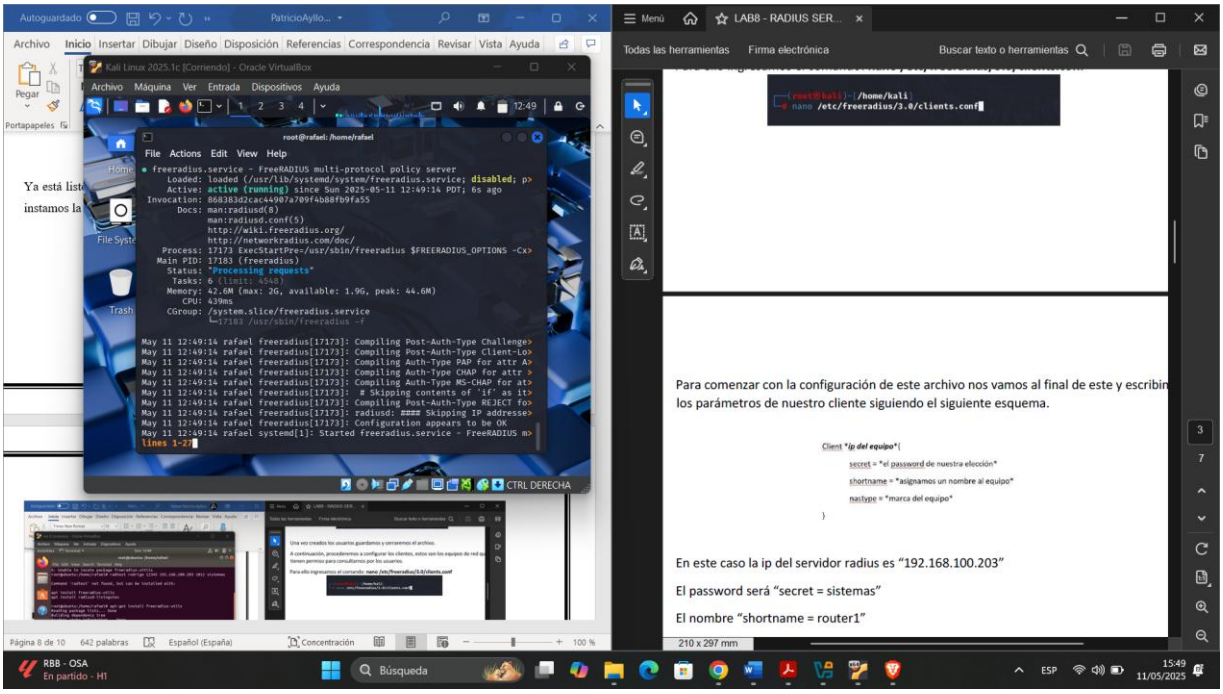
“auth_badpass = yes” Indicamos que se generen logs de cuando alguien intente autentificarse de manera incorrecta o falle en el proceso de inicio de sesión.

“auth_goodpass = yes” Indicamos que se generen logs para todos usuarios que inicien sesión correctamente.

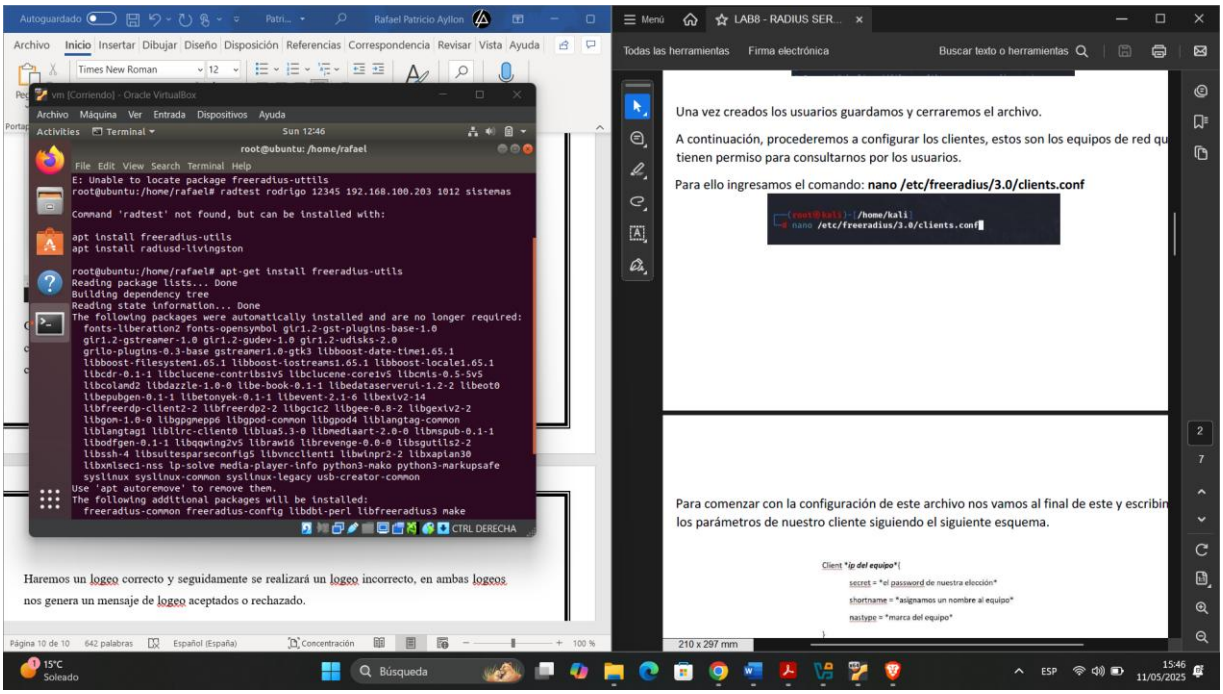
Procedemos a reiniciar el servicio de Freeradius para aplicar todos los cambias realizados con el siguiente comando: sudo systemctl restart freeradius

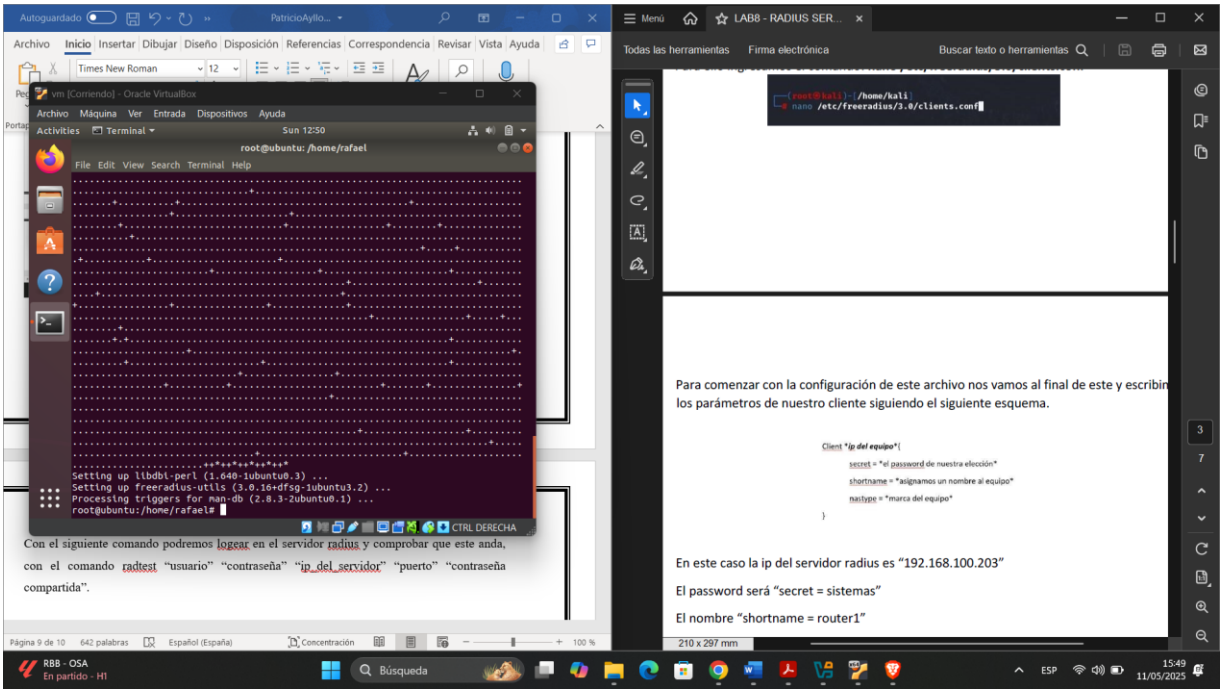


Una vez hecho esto, verificamos que el servicio este activo con el comando sudo systemctl status freeradius

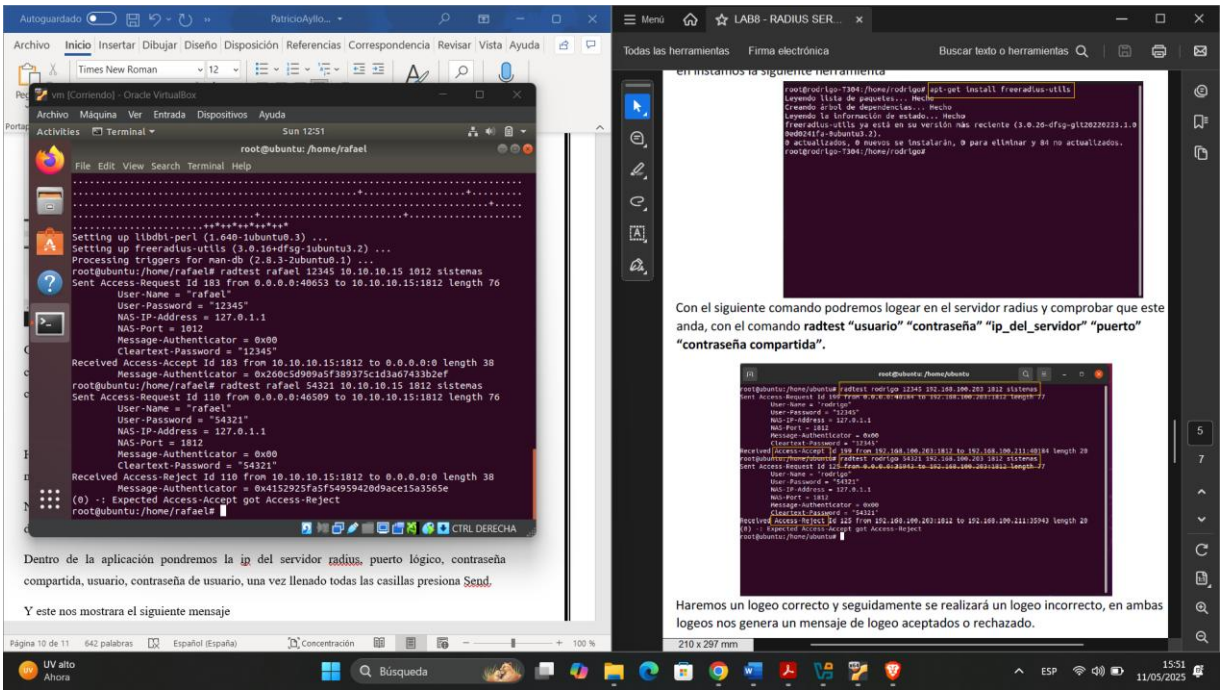


Ya está listo para usarse para ello nos vamos a otro equipo en este caso utilizamos Ubuntu eh instamos la siguiente herramienta



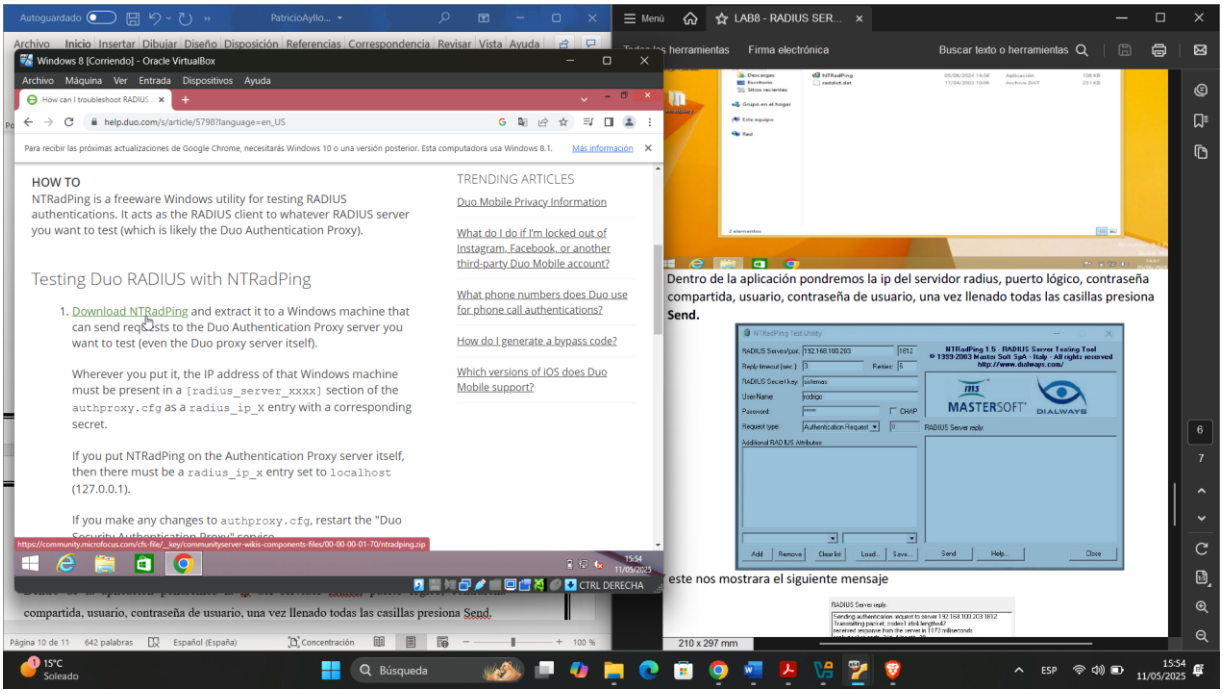


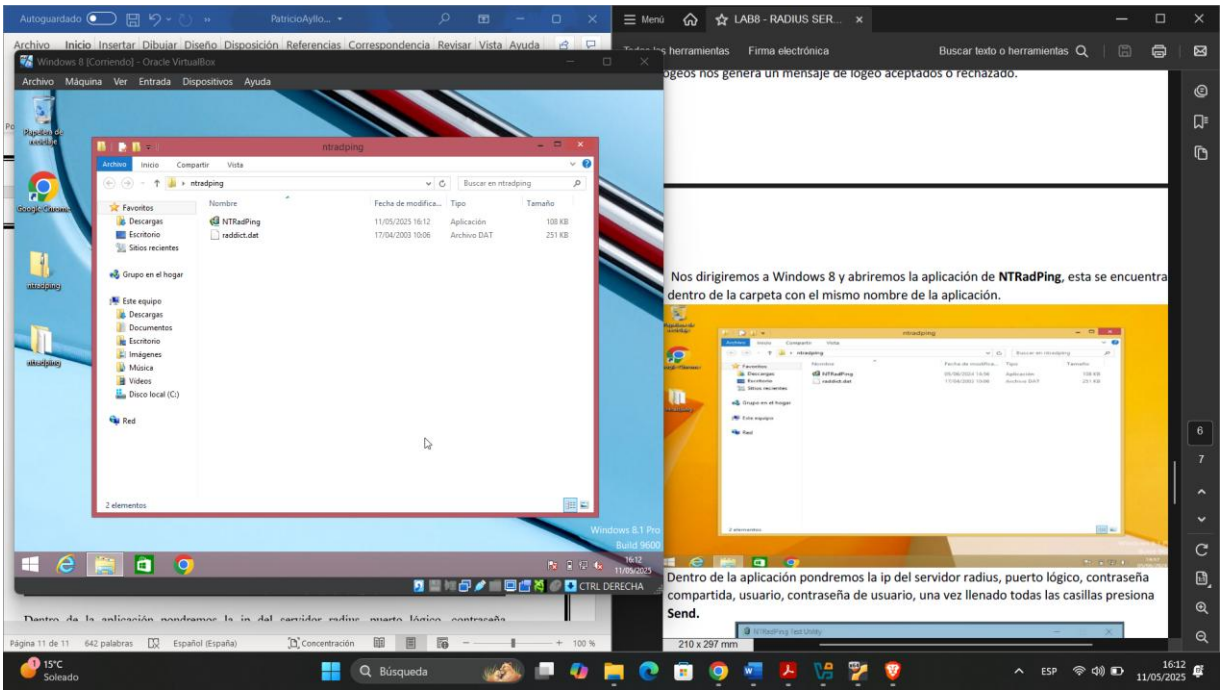
Con el siguiente comando podremos logear en el servidor radius y comprobar que este anda, con el comando radtest "usuario" "contraseña" "ip_del_servidor" "puerto" "contraseña compartida".



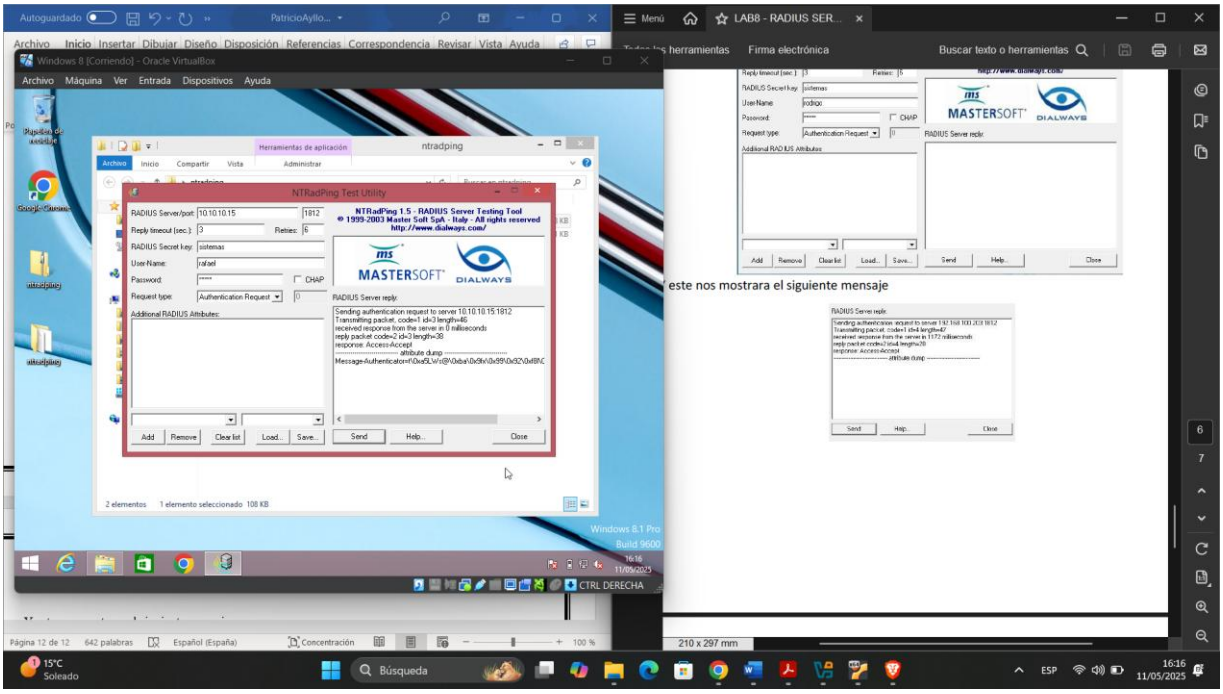
Haremos un logeo correcto y seguidamente se realizará un logeo incorrecto, en ambas logeos nos genera un mensaje de logeo aceptados o rechazado.

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.

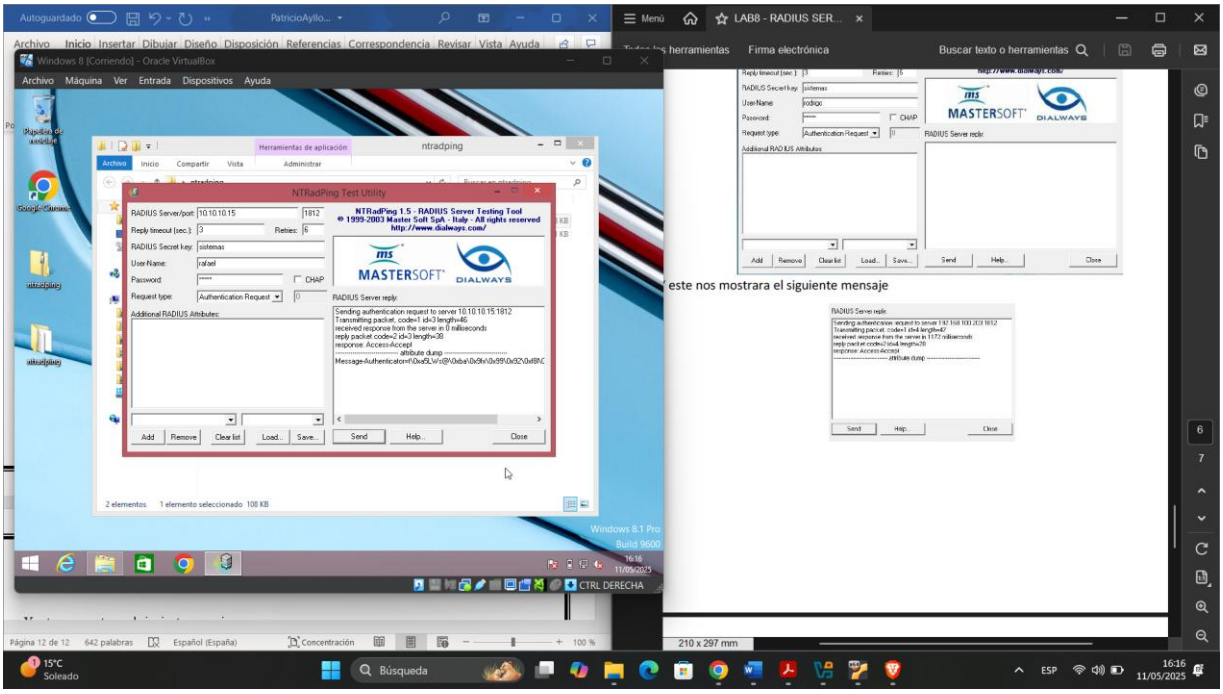




Dentro de la aplicación pondremos la ip del servidor radius, puerto lógico, contraseña compartida, usuario, contraseña de usuario, una vez llenado todas las casillas presiona Send.



Y este nos mostrara el siguiente mensaje



Evaluación

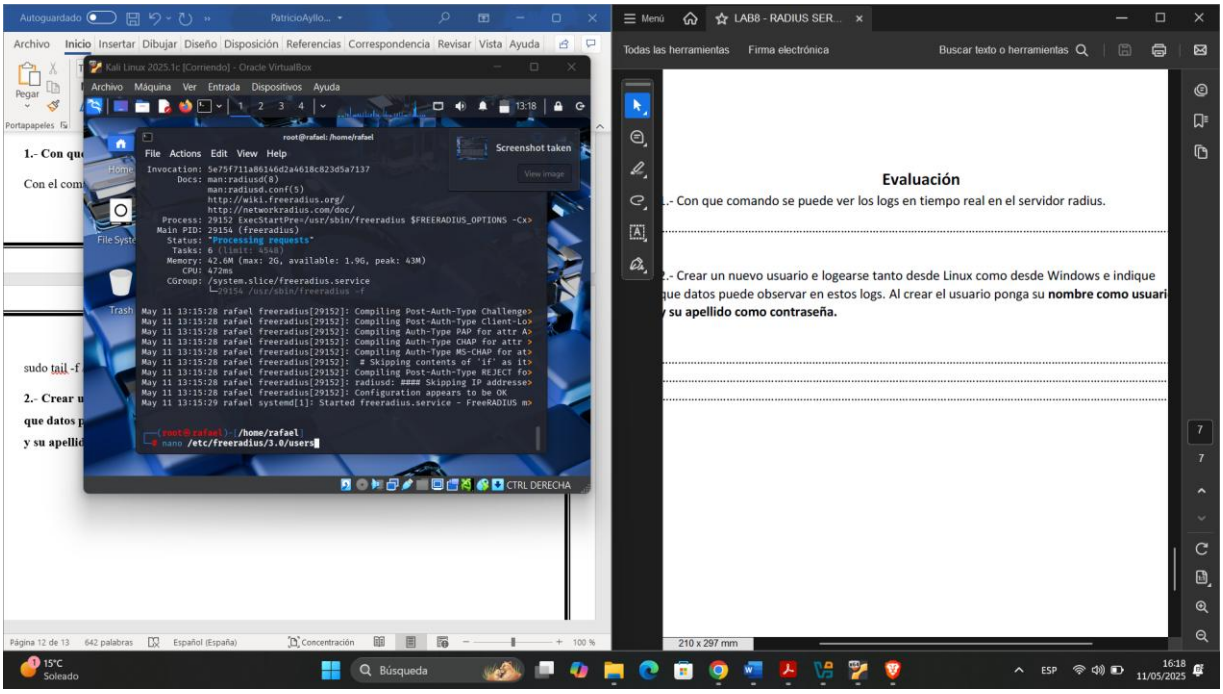
1.- Con que comando se puede ver los logs en tiempo real en el servidor radius.

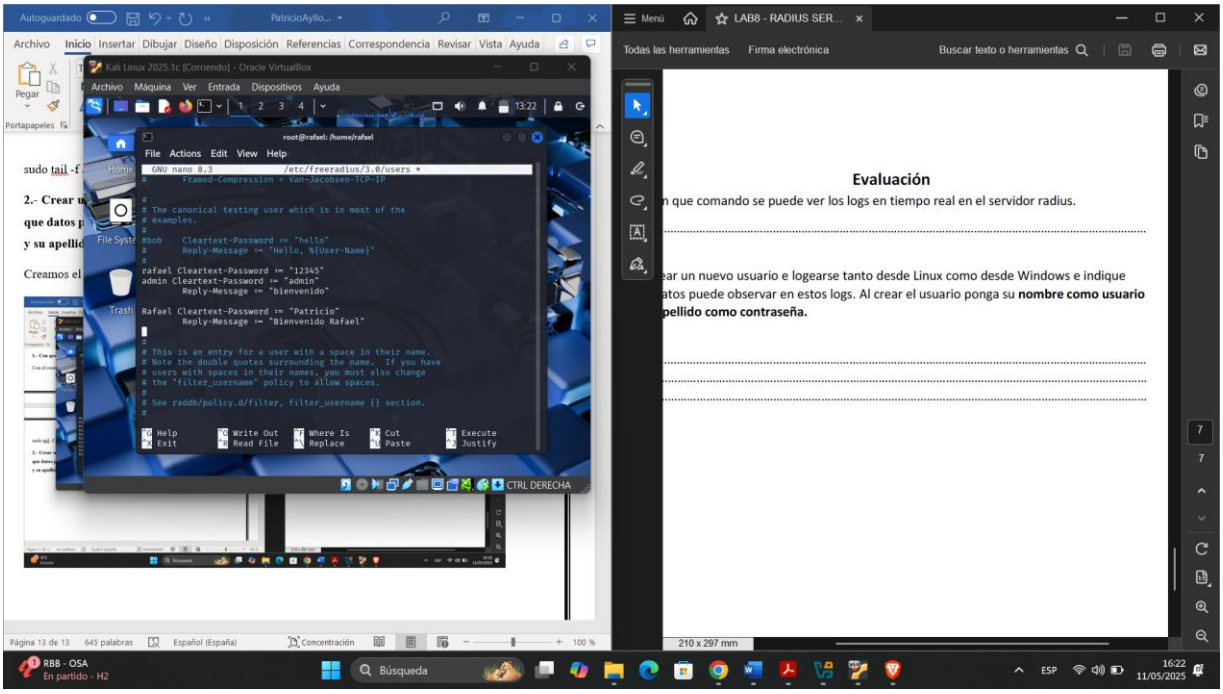
Con el comando:

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

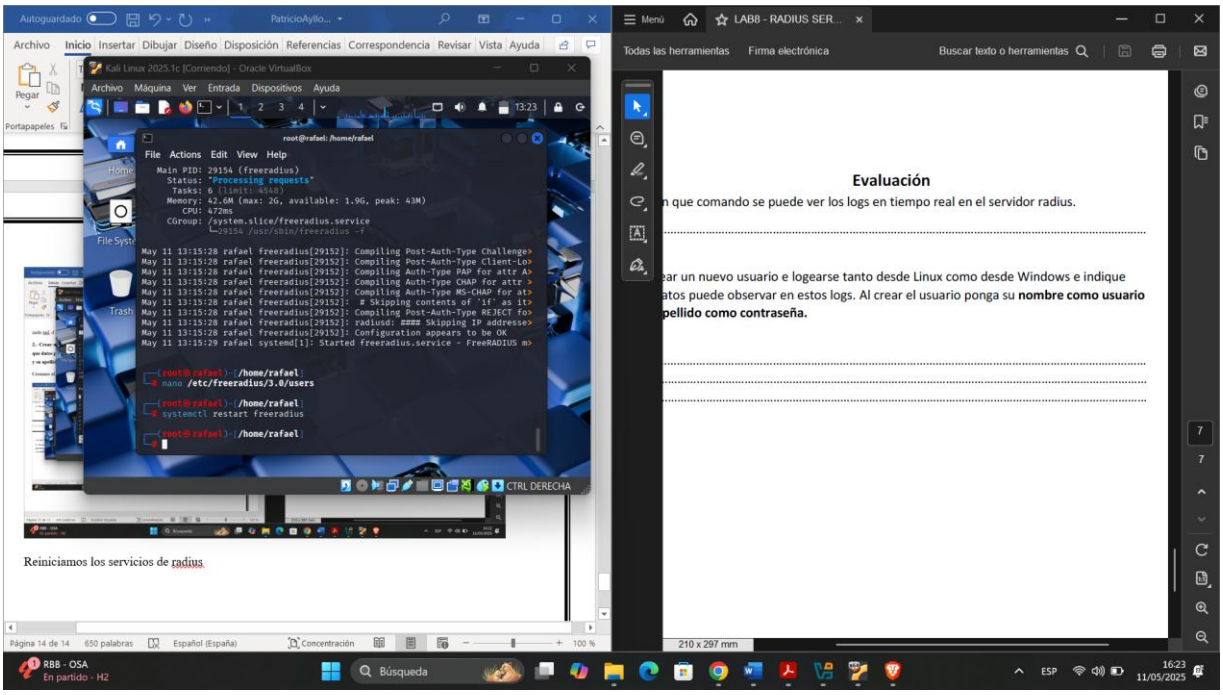
2.- Crear un nuevo usuario e logearse tanto desde Linux como desde Windows e indique que datos puede observar en estos logs. Al crear el usuario ponga su nombre como usuario y su apellido como contraseña.

Creamos el usuario

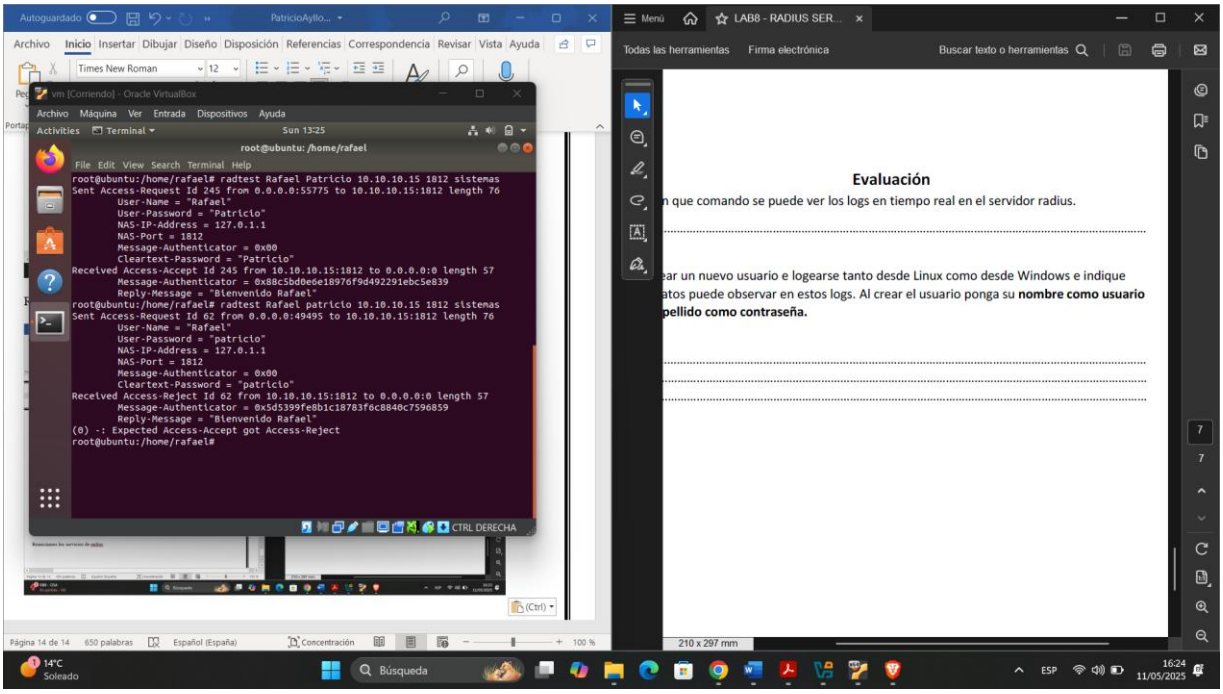




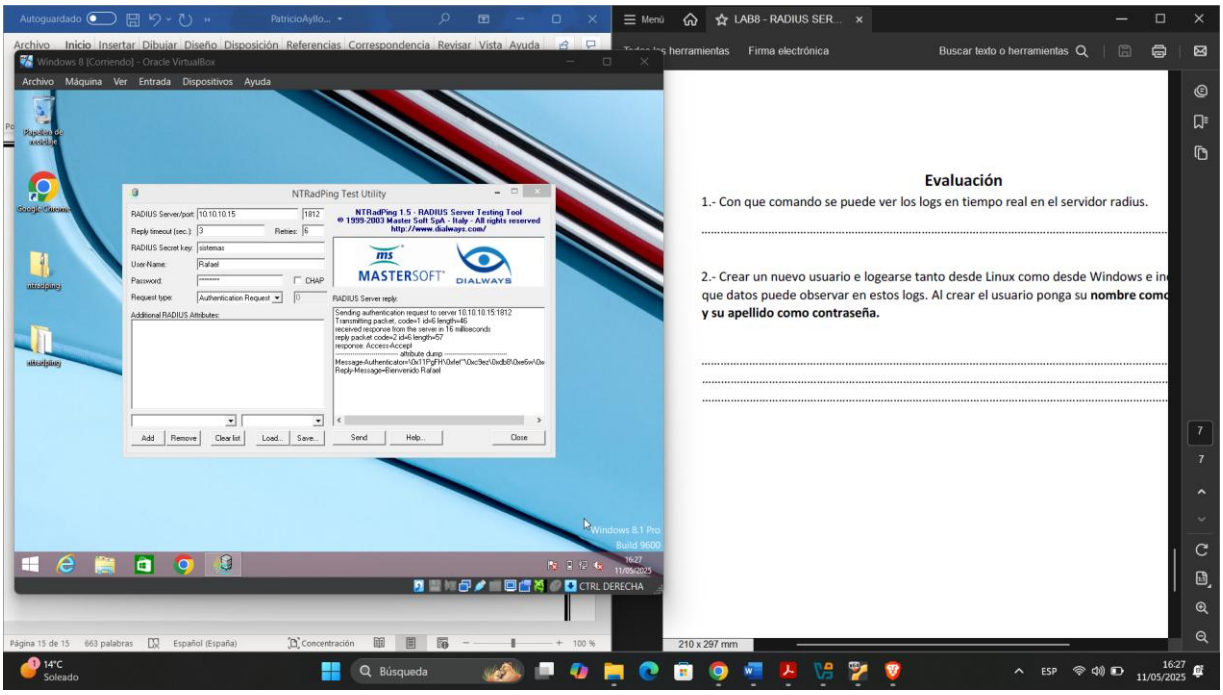
Reiniciamos los servicios de freeradius



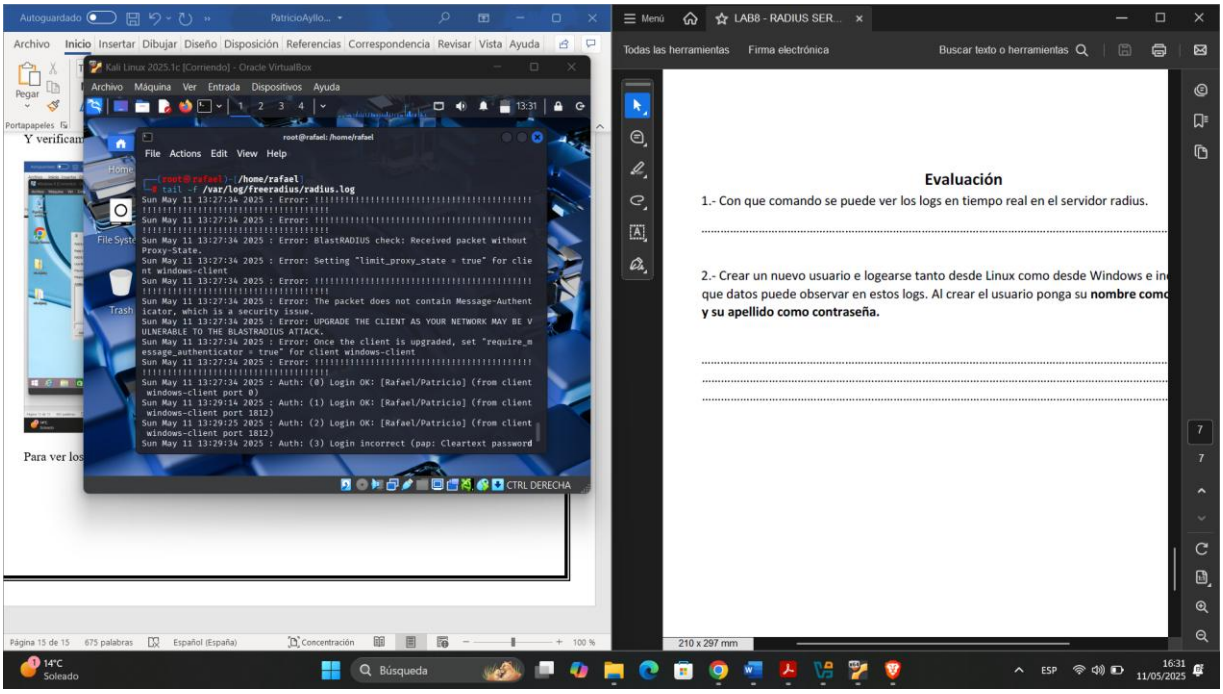
Verificamos en Ubuntu con la contraseña correcta e incorrecta

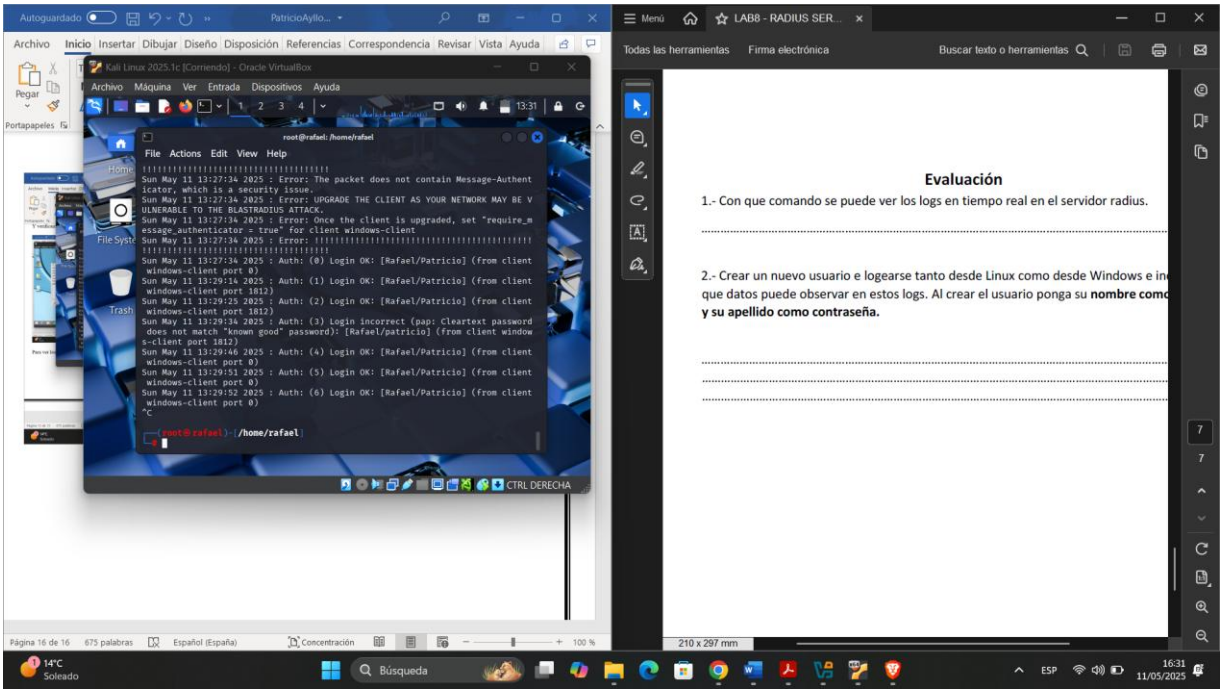


Y verificamos en Windows



Para ver los logs de freeradius utilizamos el comando tail -f /var/log/freeradius/radius.log





Se observa que para las pruebas aparecerá:

Autenticación exitosa: Mensaje "Login OK" con detalles del usuario

Autenticación fallida: Mensaje "Login incorrect " con razón "Invalid password"

Marca de tiempo exacta

Tiempo de procesamiento