



PROYECTO FINAL

Administración de sistemas



17 DE JUNIO DE 2022

MARIA FERNANDA LEGORRETA RODRIGUEZ

Boleta: 2022640133

Protocolo de SSH:

“Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.” ¹

El puerto SSH estándar asignado es el TCP 22. No obstante, ese puerto siempre puede ser cambiado si queremos. El cliente SSH va a contactar con el servidor para iniciar la conexión. Ese servidor está escuchando a través del puerto 22 o el que se le haya asignado. Posteriormente el servidor va a enviar la clave pública y comienzan a organizar los parámetros y abrir un canal seguro. El cliente inicia sesión para conectarse a ese servidor.

El servidor podría ser por ejemplo un dominio web o una dirección IP. El usuario sería el nombre, como puede ser root o administrador.

En cuanto al cifrado SSH, hay de diferentes tipos. Por un lado está el **cifrado simétrico**, que es el más popular, en el que utiliza una clave secreta que va a ser usada tanto al cifrar como al descifrar la conexión. Esa clave es única.

Por otra parte está el **cifrado asimétrico**, que en esta ocasión utiliza dos claves diferentes. Una clave es pública y la otra privada y la información solo se puede obtener si se conoce esta última clave.

Una última opción de cifrado es lo que se conoce como **hash o hashing**. Esto se consigue al convertir esa información en una serie de datos que son únicos.²

El uso del protocolo permite que el cliente pueda verificar en cualquier momento si está conectándose al mismo servidor en cada uno de sus accesos. El nivel de encriptación utilizado por el protocolo SSH es de 128 bits. Un cifrado muy potente que hace que cualquier información, enviada o recibida, que se intercepte sea extremadamente difícil de leer y descifrar. De la misma manera, permite a los usuarios acceder a un servidor de forma remota además de reenviar todo tipo de aplicaciones X11, proporcionando una forma segura para utilizar aplicaciones gráficas.³

¹ Red Hat Enterprise Linux 4: Manual de referencia.

² Qué es y para qué sirve el SSH-Redes Zone

³ ¿Qué es y para qué sirve el protocolo SSH?-Blog de linube

Configuración en Linux de SSH:

Instale OpenSSH abriendo una terminal y ejecutando los siguientes comandos con permisos de superusuario.

```
# apt-get install openssh-server openssh-client openssh
```

Inicie el servicio escribiendo los siguientes comandos en la terminal:

```
# chkconfig sshd on # service sshd start
```

Si tiene un firewall, abra el puerto SSH en su firewall. Por ejemplo, el puerto 22.

Navegue a `/opt/MicroStrategy/ServicesRegistration/yaml/` abra el `installation_list.yaml` archivo.

Realice las siguientes modificaciones:

- Modificar `"CommonPath"` al directorio de instalación de MicroStrategy Common Files. Por defecto, es `/var/opt/MicroStrategy`.
- Modificar `"InstallType"` a 1.
- Modificar `"Puerto"` para usar el número de puerto de su servidor SSH.
- Modificar `"versión"` para usar su número de versión de MicroStrategy.

--- servicio:

Nombre: ID de `"servidor SSH"`;: `CommonPath "SSH-Server"`;: `/var/opt/MicroStrategy` `InstallType: 1` `puerto: 22` `Etiquetas: "versión"`;: `"11.2.0000.0123"`;⁴

Configuración mínima para garantizar la seguridad de la conexión:

PERMISO SSH PARA ROOT LOGIN:

`PermitRootLogin no`

Deshabilitar el inicio de sesión root es una buena práctica de seguridad. Permita que los usuarios con privilegios normales o sudo puedan conectarse.

INTENTOS MÁXIMOS DE INICIO DE SESIÓN:

`MaxAuthTries 3`

⁴ Configuración de SSH en Linux-Microestrategia

Este valor define cuántos intentos fallidos de inicio de sesión se permiten por usuario antes de bloquear su acceso durante un período de tiempo determinado.

EVITAR CONEXIÓN CON CONTRASEÑA VACÍA

PermitEmptyPasswords no

Si un usuario no usa ninguna contraseña, no se le debe permitir conectarse a través de SSH.

AUTENTICACIÓN DE CLAVE PÚBLICA SSH:

ChallengeResponseAuthentication no

KerberosAuthentication no

GSSAPIAutenticación no

Los servidores SSH generalmente están configurados para usar solo autenticación de clave pública. SSH admite muchos otros métodos de autenticación. La autenticación de clave pública solo debe usarse si es necesario.

AUTENTICACIÓN CLAVE PÚBLICA Y PRIVADA SSH:

PubkeyAuthentication yes

Debe utilizar pares de claves públicas y privadas para la autenticación.

DESACTIVAR EL REENVÍO X11:

X11Forwarding no

Esta función debe desactivarse para minimizar la superficie de ataque.

RESTRINGIR EL ACCESO A USUARIOS ESPECÍFICOS:

*AllowUsers *@192.168.1.1*

Esta función debe usarse si se necesita acceder al servidor SSH solo desde una dirección IP específica. Cualquier otra solicitud de dirección IP será rechazada.

PROTEJA EL TRÁFICO SSH CON LA HUELLA DIGITAL DEL SERVIDOR:

StrictHostKeyChecking ask

Esta opción requiere verificación mediante la huella digital del servidor antes de que se apruebe la comunicación. Esto puede ayudar a reducir las posibilidades de ataques Man-in-the-Middle y suplantación de IP.

RECOMENDACIONES ADICIONALES:

AllowAgentForwarding no

AllowTcpForwarding no

PermitTunnel no

5

Diferencia del comando adduser a useradd:

useradd es un comando que ejecuta un binario del sistema, mientras que adduser es un script en perl que utiliza el binario useradd.

La mayor ventaja del comando adduser es que crea el directorio home (/home/usuario/) del usuario de manera automática, cosa que no hace useradd (hay que usar la opción -m). Sin embargo, como no es un comando del core de GNU/Linux, es posible que no funcione bien en todas las distribuciones que uses.⁶

Variante de sintaxis del comando adduser:

\$ sudo adduser <usuario>

De esta forma se crea un nuevo usuario de nombre <usuario>, con todas las opciones por defecto, tales como ubicación de su directorio, duración de la cuenta de usuario, shell a utilizar o grupos en los que va a ser incluido. Estos parámetros se pueden cambiar más adelante usando el comando usermod. Este comando admite las mismas opciones que el comando adduser, que son:

- -c '<comentario>'. Permite añadir un comentario al usuario, como puede ser su nombre real.
- -d <directorio>. Esta opción nos permite cambiar el directorio por defecto del usuario, que suele ser /home/<usuario>.
- -e <YYYYMMDD>. Permite seleccionar la fecha en la que la cuenta se deshabilitará. Debe introducirse en el formato indicado: añomesdía.
- -f <días>. Nos permite seleccionar el tiempo en días a partir de la fecha de expiración de la contraseña en la cual la cuenta se deshabilitará. Con un valor de -1, no lo hará.
- -g <grupo>. Permite añadir el usuario a un grupo. Debe existir con anterioridad para poder añadirlo. Podemos introducir el grupo por su nombre o por su ID.
- -G <grupos>. Similar a la opción anterior, pero permite introducir varios grupos separados por comas.
- -m. Crea el directorio del usuario si no existe.
- -M. No crea el directorio del usuario.
- -n. No crea un grupo privado para el usuario.

⁵ CONFIGURACIÓN DE SSH PARA UNA MEJORA EN SU SEGURIDAD-Calcom

⁶Cuál es la diferencia entre useradd y adduser- Vida XP

- -r. La cuenta se convierte en cuenta del sistema, con ID de usuario (UID) menor a 500 y sin directorio.
- -p <contraseña>. Establece una contraseña de usuario. Se puede crear posteriormente con el comando passwd <usuario>. Se encriptará con crypt.
- -s <shell>. Permite modificar la shell de inicio de sesión del usuario, por defecto/bin/bash.
- -u <UID>. Nos permite especificar la ID del usuario, debe ser mayor a 499 y única.⁷

¿Todas las distribuciones de Linux crean cuentas con el comando adduser?

La respuesta es no, aunque la mayoría de las distribuciones si ejecutan este comando, no todos lo hacen.

Protocolo web:

“El protocolo de Internet, conocido por sus siglas en inglés IP, es el protocolo principal de la familia de protocolos de Internet y su importancia es fundamental para el intercambio de mensajes en redes informáticas. El protocolo no orientado a la conexión, publicado en 1974 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) y especificado como estándar en RFC 791, fue concebido principalmente para garantizar el éxito en el envío de paquetes de un emisor a un destinatario. Para este fin, el protocolo de Internet establece un formato que determina el tipo de descripción que tienen estos paquetes de datos (también llamados datagramas IP).”⁸

Toda cabecera IP comienza con un valor de 4 bits de longitud para el número de versión del protocolo de Internet, es decir, IPv4 o IPv6. A este le siguen 4 bits que contienen información sobre la longitud de la cabecera (IP header length), puesto que esta no siempre es la misma. La longitud total se calcula tomando como base este valor multiplicado por 32 bits. Así, 5, el valor más pequeño posible, se corresponde con una longitud de cabecera de 160 bits, lo que se traduce en 20 bytes. En este caso no se añade ninguna opción. El valor máximo es 15 o 480 bits, es decir, 60 bytes. Los bits del 8 al 15 (Type of Service) pueden contener instrucciones sobre el tratamiento y la prioridad del datagrama. En este sentido, el host puede, por ejemplo, indicar la importancia de aspectos como la fiabilidad, el rendimiento o las demoras en lo que respecta a la transmisión de los datos.

La longitud total señala cuál es el tamaño total del paquete de datos y añade así el tamaño de los datos útiles a la longitud de la cabecera. Debido a que dicho campo tiene una longitud de 16 bits, el límite máximo se sitúa en torno a los 65 535 bytes.

⁷ Comandos (adduser, useradd, ps y find).-Tought-T-Team

⁸ ¿Qué es el Internet Protocol (IP)?-IONOS

En la RFC 791 se define que cada host ha de tener la capacidad de procesar al menos 576 bytes. Un datagrama IP puede fragmentarse según se desee en su camino hacia el host de destino tanto del router como de otros dispositivos, aunque los fragmentos no deben tener un tamaño inferior a 576 bytes. El resto de campos de la cabecera de IPv4 tienen el siguiente significado:

Identificación: todos los fragmentos de un datagrama cuentan con el mismo número de identificación que reciben por parte del remitente. Ajustándose a este campo de 16 bits, el host de destino puede asignar los fragmentos individuales a un determinado datagrama.

Flags (banderas): toda cabecera IP contiene tres bits flag que incluyen datos y directrices para la fragmentación. El primer bit está reservado y siempre tiene el valor 0. El segundo bit, con el nombre “Don’t Fragment”, informa acerca de si se puede fragmentar el paquete (0) o no (1). El último, que recibe el nombre de “More Fragments”, da información sobre si siguen más fragmentos (1) o sobre si el paquete está completo y ha concluido con el fragmento actual (0).

Desplazamiento del fragmento: este campo informa al host de destino sobre la parte a la que pertenece un único fragmento para que pueda reconstruir todo el datagrama sin ningún problema. La longitud de 13 bits significa que un datagrama puede dividirse en un máximo de 8192 fragmentos.

Tiempo de vida (Time to Live, TTL): para que un paquete no vague por la red de un nodo a otro durante un período de tiempo ilimitado obtiene un tiempo de vida máximo en el momento del envío, lo que se conoce como Time to Live. El estándar RFC define a los segundos como unidad para este campo de 8 bits y el tiempo de vida máximo asciende a 255 segundos. Para cada nodo de red que pasa, el TTL disminuye como mínimo en 1. Si se alcanza el valor 0, el paquete de datos es descartado automáticamente.

Protocolo: el campo del protocolo (8 bits) asigna al paquete de datos el protocolo de transporte correspondiente, como es el caso, por ejemplo, del valor 6 para TCP o del valor 17 para el protocolo UDP. El listado oficial de todos los protocolos posibles fue elaborado en 2002 por la IANA (Internet Assigned Numbers Authority).

Suma de verificación de la cabecera: el campo “checksum”, de 16 bits de amplitud, contiene la suma de verificación de la cabecera. Esta debe volverse a calcular para cada nodo de red a causa de la disminución del TTL en cada estación. La exactitud de los datos útiles no se verifica por motivos de eficiencia.

Dirección de origen y de destino: a las direcciones IP asignadas al host de origen y al de destino se reservan 32 bits respectivamente, es decir, 4 bytes. Estas direcciones IP se escriben adoptando la forma de cuatro grupos de números

decimales separados por un punto. La dirección más baja es 0.0.0.0 y la más alta 255.255.255.255.⁹

Servidor Apache:

Apache es un servidor web de código abierto, multiplataforma y gratuito.

La función esencial del servidor Apache es servir las webs alojadas en el servidor a los diversos navegadores como Chrome, Firefox, Safari,...

Apache consigue que la comunicación entre el servidor web y el cliente web (usuario que solicita la información) sea fluida y constante.

Haciendo que cuando un usuario haga una petición HTTP a través de navegador para entrar a una web o URL específica, Apache devuelva la información solicitada a través del protocolo HTTP.

En Apache podemos aplicar una alta personalización a través de su sistema modular, de forma que podemos activar o desactivar diversas funcionalidades a través de los módulos de Apache.¹⁰

Configuración en Linux del servidor apache:

Pre Requisitos:

- Usuario root o usuario regular con privilegios sudo.
- Habilitar los puertos necesarios para el servicio apache.

Paso 1 - Actualizamos siempre el Sistema Operativo:

sudo apt update

Paso 2- Escribimos el comando que iniciará la instalación de Apache:

sudo apt install apache2

Paso 3 - Ajustamos la configuración del Firewall, en este caso Ubuntu usa por defecto UFW (Uncomplicated Firewall) que será utilizado en esta guía (En caso no haya sido instalado aún, puede realizarlo desde aquí). Usaremos el siguiente comando para verificar los perfiles por defecto para Apache en UFW:

sudo ufw app list

Apache: Apertura solo del puerto 80, que permite trafico sin cifrar (No seguro).

Apache Full: Apertura tanto del puerto 80 como del puerto 443, permitiendo el tráfico cifrado (Seguro).

⁹ ¿Qué es el Internet Protocol (IP)?-IONOS

¹⁰ ¿Qué es Apache y cómo funciona?-Webempresa

Apache Secure: Apertura solo del puerto 443, permitiendo conexiones seguras (HTTPS).

Verificamos los perfiles activos:

sudo ufw status

Resultado:

Paso 4 - Ahora verificamos que el servicio Apache esté ejecutándose correctamente, con el siguiente comando:

sudo systemctl status apache2

También puedes acceder desde el navegador ingresando la IP publica del servidor:

<http://DirecciónIP/> ¹¹

Porque utilizamos el puerto 8009 y para qué sirve el puerto 80 y 8080

PUERTO 80

En el ámbito de la informática, se conoce como Puerto 80 al que puerto por default, por el medio del cual un servidor HTTP “escucha” la petición hecha por un cliente, es decir por una PC en específico.

PUERTO 8080

La cuestión del 8080 es que Tomcat supone que ya tienes algo en el puerto 80, el Apache, el IIS o el XAMPP, y para evitar problemas viene pre-configurado con el puerto 8080.¹²

PUERTO 8009

El puerto TCP 8009 usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin. Solo cuando la conexión es determinada, los datos del usuario pueden ser mandados de modo bidireccional por la conexión.

Puerto 8009 garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados.¹³

¹¹ Instalar Apache en Ubuntu 20.04-Hosting labs

¹² PUERTO 80 Y 8080-INTERPOLADOS

¹³ 8009/TCP-admin subnet

Variante; servidor Apache:

Hay tres tipos principales de módulos: los módulos base, que soportan las funciones básicas de Apache, los módulos multiproceso, íntimamente relacionados con el Sistema Operativo, y los módulos adicionales, que no son absolutamente necesarios pero potencian grandemente la funcionalidad de Apache.

En la actualidad hay tres versiones de Apache funcionando: la versión 2.0, la 2.2 y la 2.4, aunque de ellas la versión 2.0 ya no tiene mantenimiento.

Anteriormente existió la versión 1.3 que es la más conocida y la que supuso la gran expansión del servidor.¹⁴

Ejemplo `sudo systemctl status apache2`:

Systemctl es una utilidad para controlar el sistema systemd y el administrador de servicios; se usa para iniciar, reiniciar, detener servicios y más. El subcomando `systemctl status`, como el nombre indica se usa para ver el estado de un servicio, puede usarlo para el propósito anterior así:

`$ sudo systemctl status apache2` #Debian/Ubuntu

`# systemctl status httpd` #RHEL/CentOS/Fedora.¹⁵

```
aaronkilik@tecmint ~ $ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Mon 2017-09-04 10:05:51 EAT; 4h 8min ago
   Process: 3030 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=
   Process: 1182 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU
   Main PID: 1395 (apache2)
   Tasks: 7 (limit: 512)
   CGroup: /system.slice/apache2.service
           └─1395 /usr/sbin/apache2 -k start
             └─3037 /usr/sbin/apache2 -k start
               └─3038 /usr/sbin/apache2 -k start
                 └─3039 /usr/sbin/apache2 -k start
                   └─3040 /usr/sbin/apache2 -k start
                     └─3041 /usr/sbin/apache2 -k start
                       └─4232 /usr/sbin/apache2 -k start

Sep 04 10:05:39 tecmint systemd[1]: Starting The Apache HTTP Server...
Sep 04 10:05:50 tecmint apachectl[1182]: AH00558: apache2: Could not reliably
Sep 04 10:05:51 tecmint systemd[1]: Started The Apache HTTP Server.
Sep 04 10:10:43 tecmint systemd[1]: Reloading The Apache HTTP Server.
Sep 04 10:10:43 tecmint apachectl[3030]: AH00558: apache2: Could not reliably
Sep 04 10:10:43 tecmint systemd[1]: Reloaded The Apache HTTP Server.
lines 1-22/22 (END)
```

¹⁴ Instalación, Configuración y Administración de Apache + Tomcat-INAP

¹⁵ 3 formas de verificar el estado y el tiempo de actividad del servidor Apache en Linux-Linux-Console.net

El comando `systemctl` para que es empleado:

El comando `systemctl` es una utilidad que se encarga de examinar y controlar el sistema `systemd` y el administrador de servicios.

- Detenga un servicio. ...
- Reinicie un servicio. ...
- Verifica el estado de un servicio.¹⁶

Porque se creó la carpeta `public_html`

El directorio `public_html` es el directorio raíz para su nombre de dominio primario. Esto significa que la carpeta `public_html` es donde usted coloca todos los archivos del sitio web que desea que estén disponibles cuando un usuario ingresa su nombre de dominio en su navegador.¹⁷

Qué pasa si se modifica el permiso de la carpeta `public_html` a 750

Permisos de grupo

Cada archivo o directorio (aunque ya sabes que en UNIX todo es un fichero) tiene tres grupos de permisos basados en usuario:

- Propietario: Los permisos de propietario solo aplican al propietario del archivo o directorio, no afectarán a las acciones de otros usuarios.
- Grupo: Los permisos de grupo se aplican solo al grupo que se ha asignado al archivo o directorio, no afectarán las acciones de otros usuarios.
- Todos los usuarios: Los permisos de "Todos los usuarios" se aplican a todos los demás usuarios del sistema, este es el grupo que más tenemos que vigilar.

Tipos de permisos

Cada archivo o directorio tiene tres tipos de permisos básicos:

- Lectura: El permiso de lectura se refiere a la capacidad del usuario para leer el contenido del fichero.
- Escritura: Los permisos de escritura hacen referencia a la capacidad de un usuario para escribir o modificar un archivo o directorio.
- Ejecución: El permiso de ejecución afecta a la capacidad del usuario para ejecutar un archivo o ver el contenido de un directorio.¹⁸

¹⁶ ¿Cómo usar el comando `Systemctl` en Linux?-CompuHoy.com

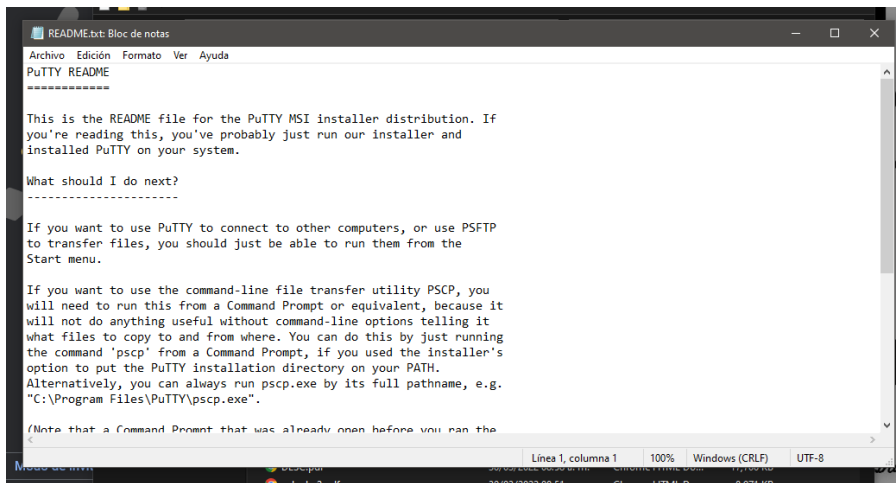
¹⁷ Cómo usar el administrador de archivos de cPanel?-Bluehostin.com

¹⁸ Permisos de archivos en Linux-ochobitshacenunbyte.com

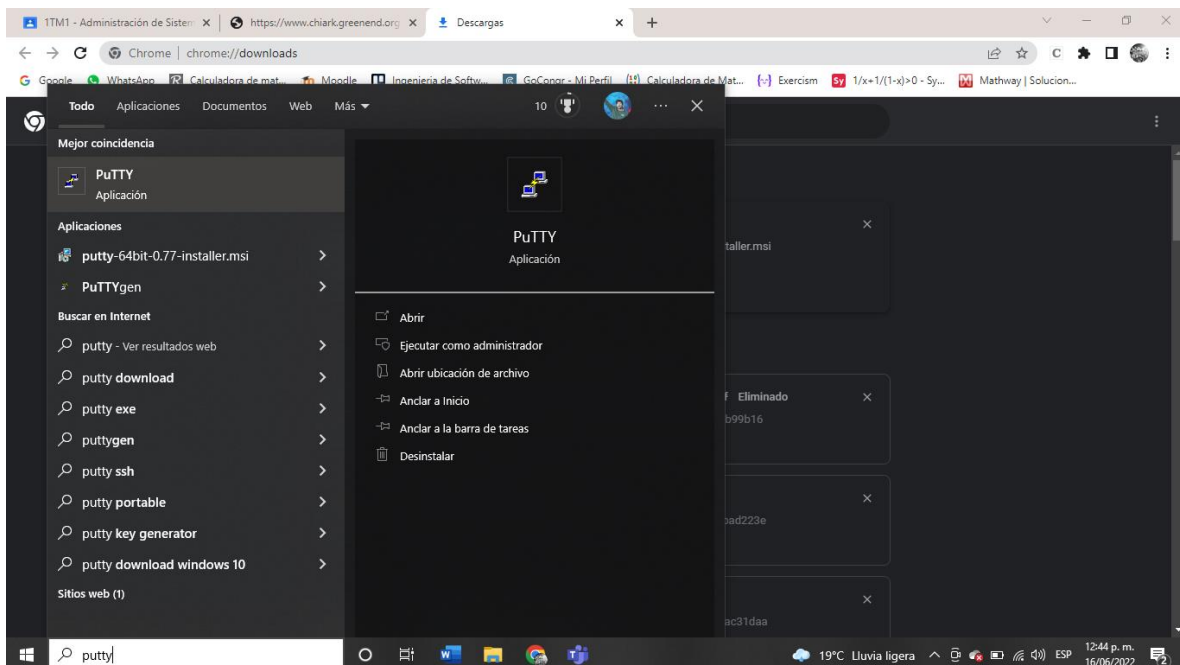
Por lo que tener 750 permisos es todos los permisos al usuario propietario, incluido el de ejecución; al grupo le daremos permisos de lectura y ejecución; y al resto de usuarios no les daremos ningún permiso.

Reporte:

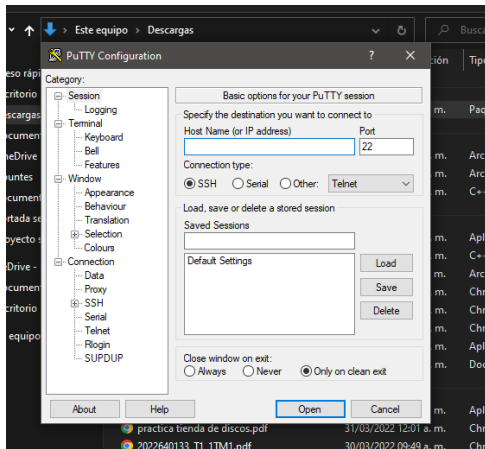
Instalar Putty en Windows



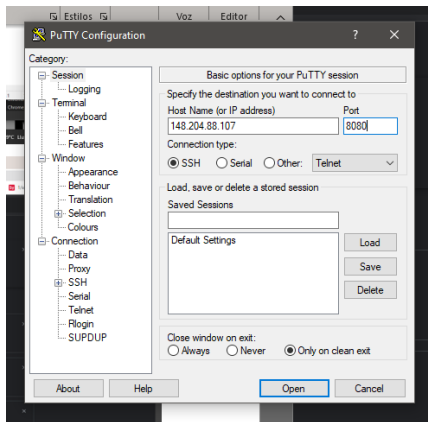
Abrir PuTTY en windows



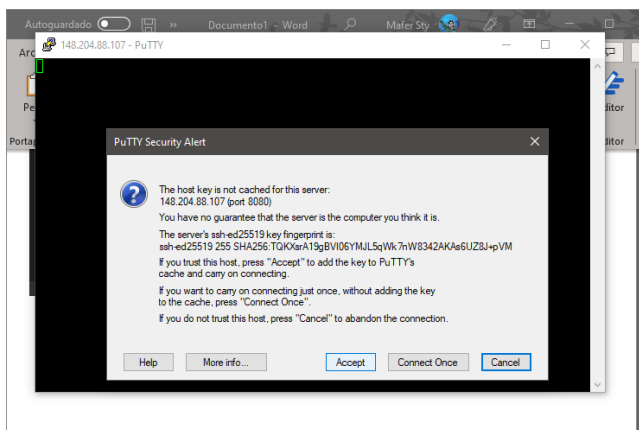
Aparecerá una ventana así:



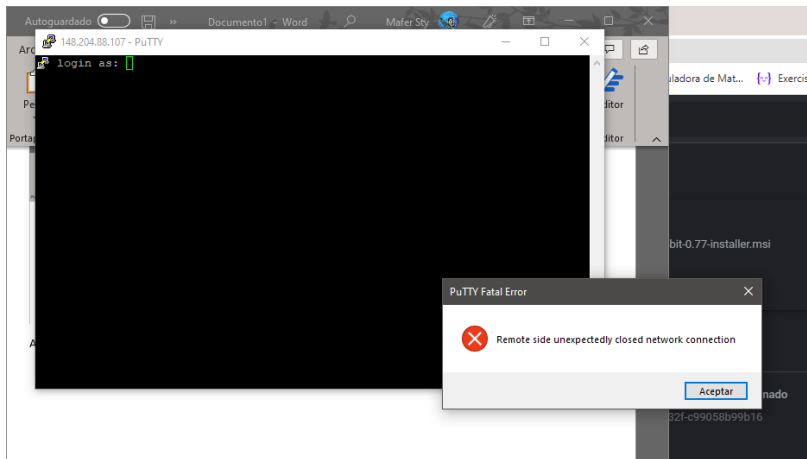
Abrir y digitar el IP y el puerto



Dar clic en Aceptpt

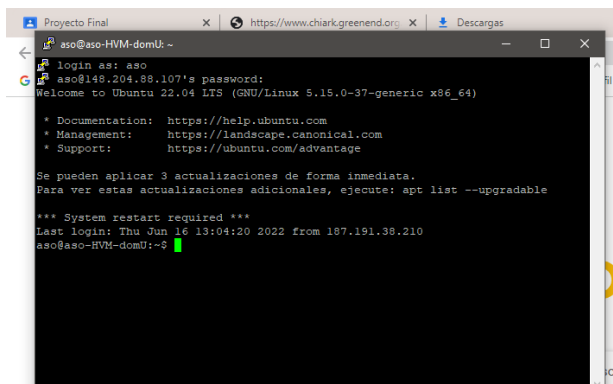


Abrirá el servidor y puede que te saque y aparezca así:



Intentarlo otra vez

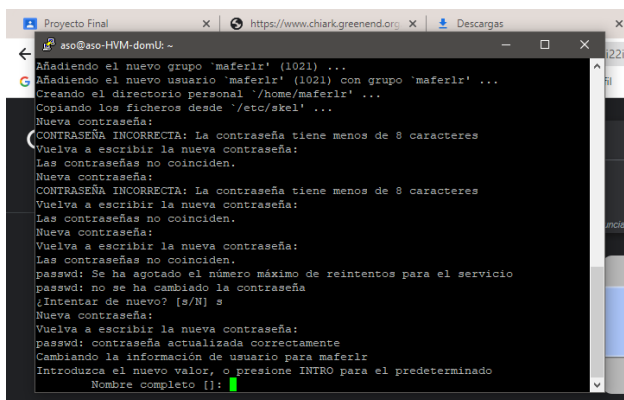
Escribir la contraseña para aso y el usuario



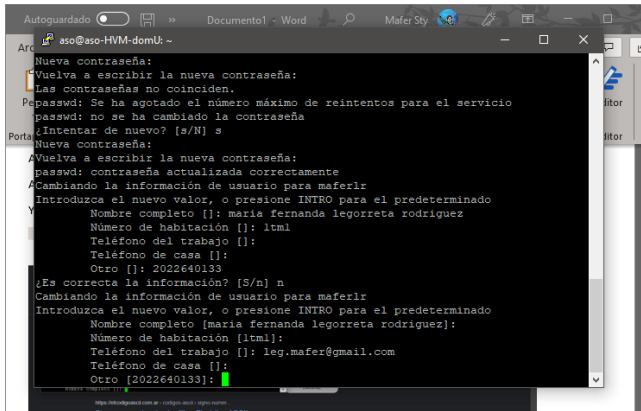
Agregar un usuario con “sudo adduser “ usuario

Agregar contraseña de aso

Y agregar la contraseña para tu usuario



Agregar la información

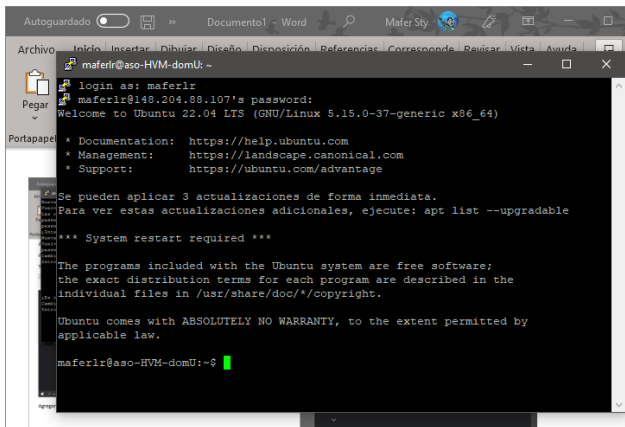


```
maferlr@aso-HVM-domU:~$ sudo adduser maferlr
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
Las contraseñas no coinciden.
passwd: Se ha agotado el número máximo de reintentos para el servicio
passwd: no se ha cambiado la contraseña
¿Intentar de nuevo? [s/N] s
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para maferlr:
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []: maria fernanda legorreta rodriguez
Número de habitación []: itml
Teléfono del trabajo []:
Teléfono de casa []:
Otro []: 2022640133
¿Es correcta la información? [S/n] n
Cambiando la información de usuario para maferlr:
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo [maria fernanda legorreta rodriguez]:
Número de habitación [itml]:
Teléfono del trabajo []: leg.mafer@gmail.com
Teléfono de casa []:
Otro [2022640133]:
```

Escribir “exit” para salir

Volver a abrir

Y conectarse a tu usuario



```
maferlr@aso-HVM-domU:~$ login as: maferlr
maferlr@148.204.88.107's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Se pueden aplicar 3 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

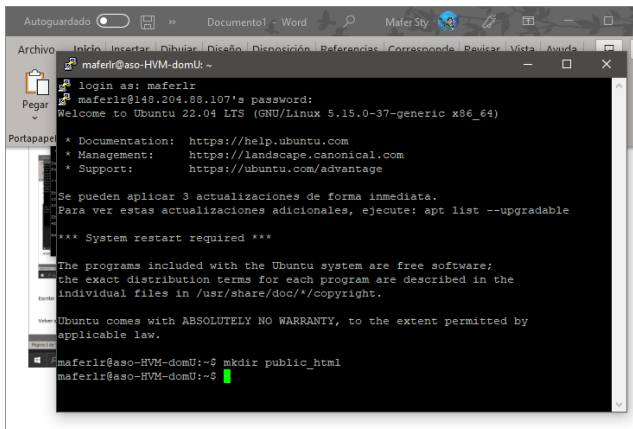
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

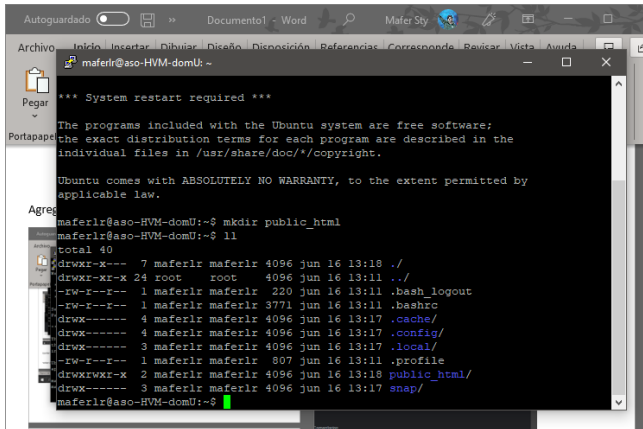
maferlr@aso-HVM-domU:~$
```

Agregar una carpeta con “mkdir public_html”



```
maferlr@aso-HVM-domU:~$ mkdir public_html
maferlr@aso-HVM-domU:~$
```

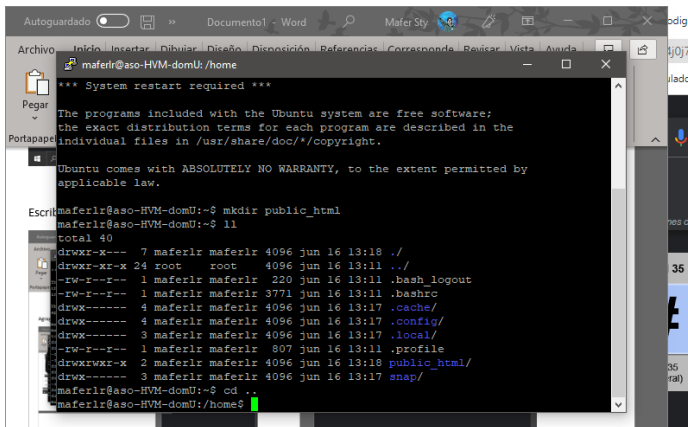
Escribir “ll” para ver su creación



```
maferlr@aso-HVM-domU: ~$ ll
total 40
drwxr-x--- 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
-rw-r--r-- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxrwxr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU: ~$
```

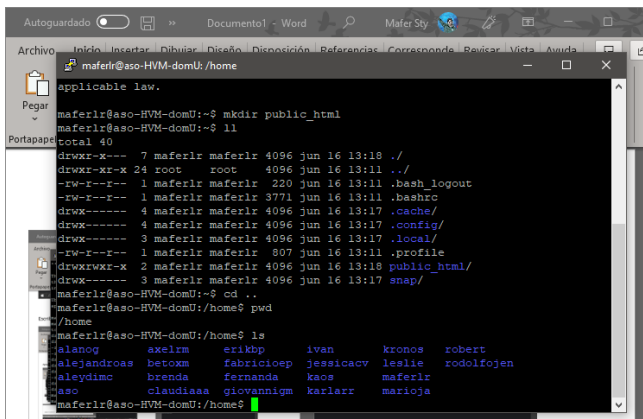
CAMBIAR PERMISOS

Escribir “cd ..



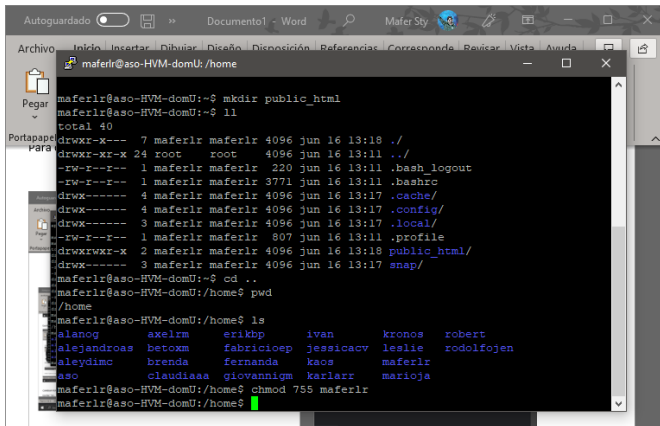
```
maferlr@aso-HVM-domU: /home$ cd ..
maferlr@aso-HVM-domU: ~$ ll
total 40
drwxr-x--- 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
-rw-r--r-- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxrwxr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU: ~$
```

Para checar usuarios presiona “pwd” y luego “ls”



```
maferlr@aso-HVM-domU: /home$ pwd
/home
maferlr@aso-HVM-domU: /home$ ls
alenog      axelrm      erikbp      ivan        kronos      robert
alejandrosa belcom      fabriciosep jessicacay leslie      rodolfojen
alejdimo    brenda      fernanda    kaos        maferlr
aso         claudiaaa   giovannigm karlarr     marioja
maferlr@aso-HVM-domU: /home$
```

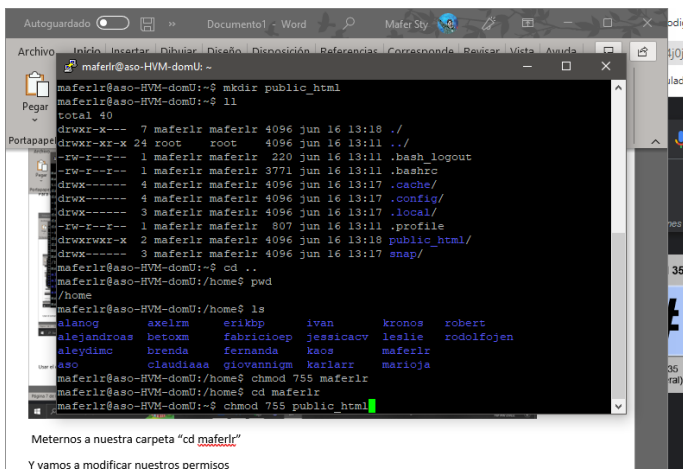

Usar el comando `chmod 755` (los permisos) y directorio



```
maferlr@aso-HVM-domU:~$ mkdir public_html
maferlr@aso-HVM-domU:~$ ll
total 40
drwxr-xr-x 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxrwxr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU:~$ cd ..
maferlr@aso-HVM-domU:~$ pwd
~/home
maferlr@aso-HVM-domU:~$ ls
alanog axelrm erikbp ivan kronos robert
alejandros betoxm fabricioep jessicacv leslie rodolfojen
aleydimc brenda fernanda kaos maferlr
aso claudiaaa giovannigm karlarr marioja
maferlr@aso-HVM-domU:~$ chmod 755 maferlr
maferlr@aso-HVM-domU:~$
```

Meternos a nuestra carpeta “`cd maferlr`”

Y vamos a modificar nuestros permisos

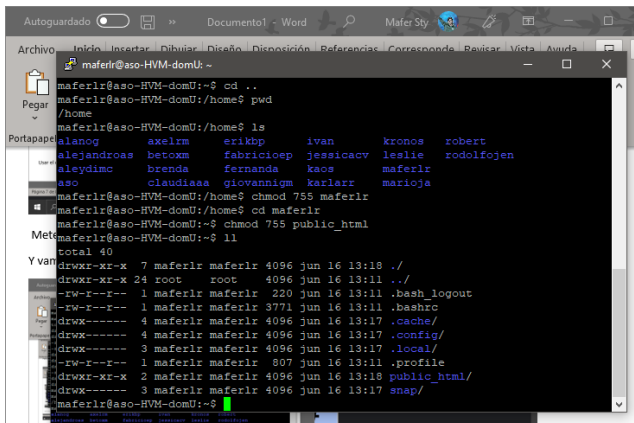


```
maferlr@aso-HVM-domU:~$ mkdir public_html
maferlr@aso-HVM-domU:~$ ll
total 40
drwxr-xr-x 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxrwxr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU:~$ cd ..
maferlr@aso-HVM-domU:~$ pwd
~/home
maferlr@aso-HVM-domU:~$ ls
alanog axelrm erikbp ivan kronos robert
alejandros betoxm fabricioep jessicacv leslie rodolfojen
aleydimc brenda fernanda kaos maferlr
aso claudiaaa giovannigm karlarr marioja
maferlr@aso-HVM-domU:~$ chmod 755 maferlr
maferlr@aso-HVM-domU:~$ cd maferlr
maferlr@aso-HVM-domU:~$ chmod 755 public_html
maferlr@aso-HVM-domU:~$
```

Meternos a nuestra carpeta “`cd maferlr`”

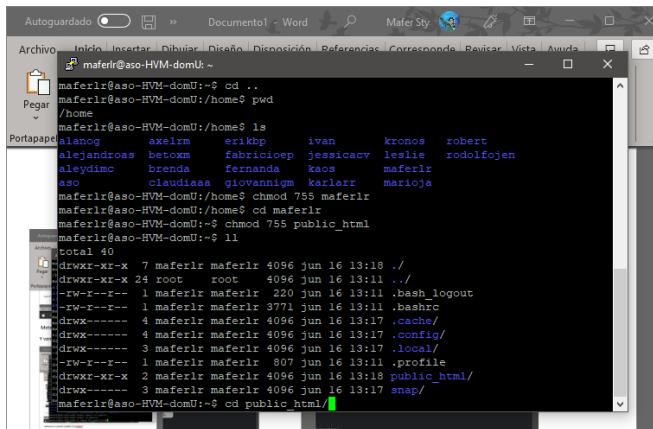
Y vamos a modificar nuestros permisos

Checar con `ll`



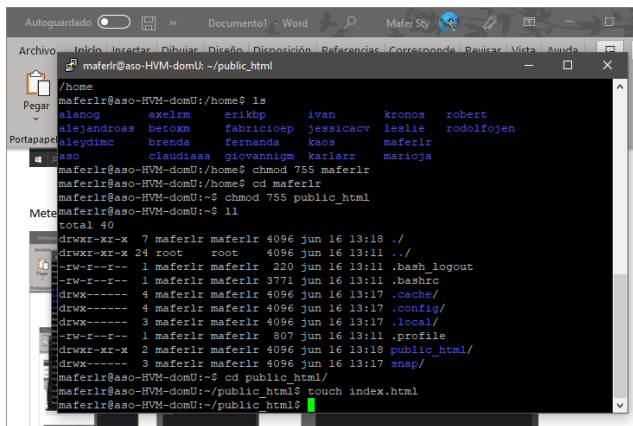
```
maferlr@aso-HVM-domU:~$ cd ..
maferlr@aso-HVM-domU:~$ pwd
~/home
maferlr@aso-HVM-domU:~$ ls
alanog axelrm erikbp ivan kronos robert
alejandros betoxm fabricioep jessicacv leslie rodolfojen
aleydimc brenda fernanda kaos maferlr
aso claudiaaa giovannigm karlarr marioja
maferlr@aso-HVM-domU:~$ chmod 755 maferlr
maferlr@aso-HVM-domU:~$ cd maferlr
maferlr@aso-HVM-domU:~$ chmod 755 public_html
maferlr@aso-HVM-domU:~$ ll
total 40
drwxr-xr-x 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxrwxr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU:~$
```

Meternos a cd public_html



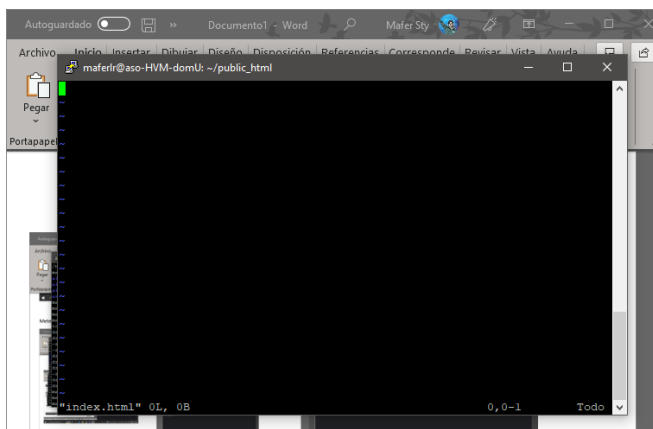
```
maferlr@aso-HVM-domU:~$ cd ..
maferlr@aso-HVM-domU:/home$ pwd
/home
maferlr@aso-HVM-domU:/home$ ls
alanog  axelrm  erikbp  ivan    kronos  robert
alejandros  betoxm  fabricioep  jessicacv  leslie  rodolfojen
aleydimc  brenda  fernanda  kaos    maferlr
aso      claudiaaa  giovannigm  karlarr  marioja
maferlr@aso-HVM-domU:/home$ chmod 755 maferlr
maferlr@aso-HVM-domU:/home$ cd maferlr
maferlr@aso-HVM-domU:~/maferlr$ chmod 755 public_html
maferlr@aso-HVM-domU:~/maferlr$ ll
total 40
drwxr-xr-x 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root    root    4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxr-xr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU:~/maferlr$ cd public_html
```

Tecleamos “touch index.html”



```
maferlr@aso-HVM-domU:~/public_html$ ls
maferlr@aso-HVM-domU:/home$ ls
alanog  axelrm  erikbp  ivan    kronos  robert
alejandros  betoxm  fabricioep  jessicacv  leslie  rodolfojen
aleydimc  brenda  fernanda  kaos    maferlr
aso      claudiaaa  giovannigm  karlarr  marioja
maferlr@aso-HVM-domU:/home$ chmod 755 maferlr
maferlr@aso-HVM-domU:/home$ cd maferlr
maferlr@aso-HVM-domU:~/maferlr$ chmod 755 public_html
maferlr@aso-HVM-domU:~/maferlr$ ll
total 40
drwxr-xr-x 7 maferlr maferlr 4096 jun 16 13:18 ./
drwxr-xr-x 24 root    root    4096 jun 16 13:11 ../
-rw-r--r-- 1 maferlr maferlr 220 jun 16 13:11 .bash_logout
-rw-r--r-- 1 maferlr maferlr 3771 jun 16 13:11 .bashrc
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .cache/
drwx----- 4 maferlr maferlr 4096 jun 16 13:17 .config/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 .local/
-rw-r--r-- 1 maferlr maferlr 807 jun 16 13:11 .profile
drwxr-xr-x 2 maferlr maferlr 4096 jun 16 13:18 public_html/
drwx----- 3 maferlr maferlr 4096 jun 16 13:17 snap/
maferlr@aso-HVM-domU:~/maferlr$ cd public_html/
maferlr@aso-HVM-domU:~/public_html$ touch index.html
maferlr@aso-HVM-domU:~/public_html$
```

Editar con vim index.html



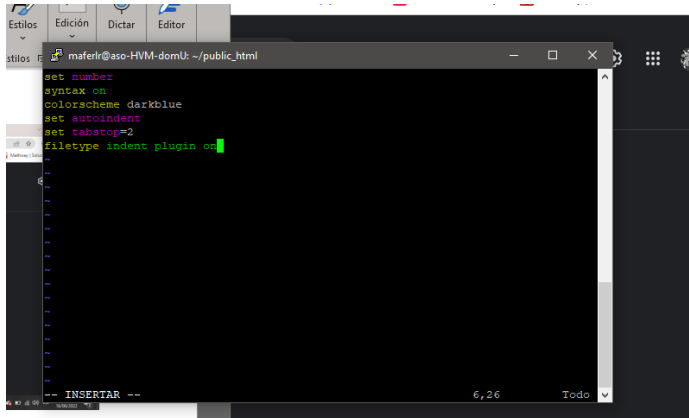
```
maferlr@aso-HVM-domU:~/public_html$ vim index.html
"index.html" 0L, 0B
0,0-1
Todo
```

(PARENTESIS VOY A EDITAR VIM)

Presionar i para entrar en modo de inserción

Use configuración en vim para hacer más agradable el editor.

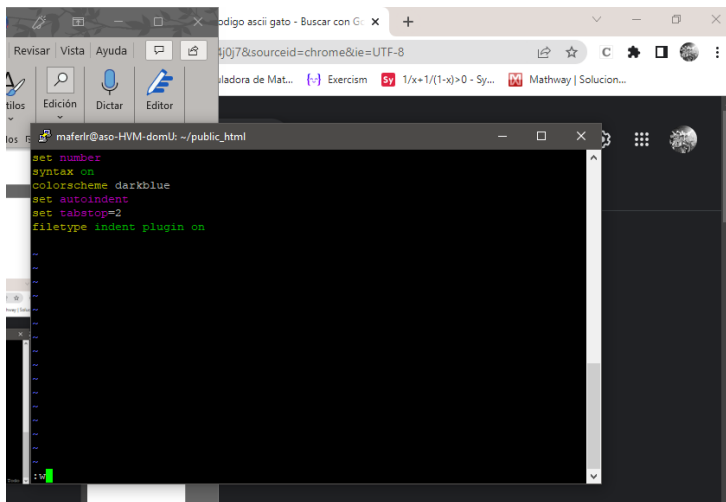
<https://www.youtube.com/watch?v=H5v3kku4y6Q>



A screenshot of a terminal window with a dark background. The terminal shows the following Vim configuration commands: `set number`, `syntax on`, `colorscheme darkblue`, `set autoindent`, `set tabstop=2`, and `filetype indent plugin on`. The cursor is at the end of the last line. The terminal title bar shows the user 'maferi' and the directory '~/public_html'.

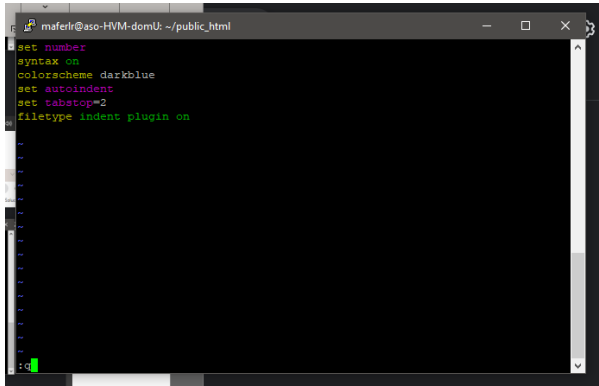
Recuerda: Salir de inserción esc

Guardar cambios con :w



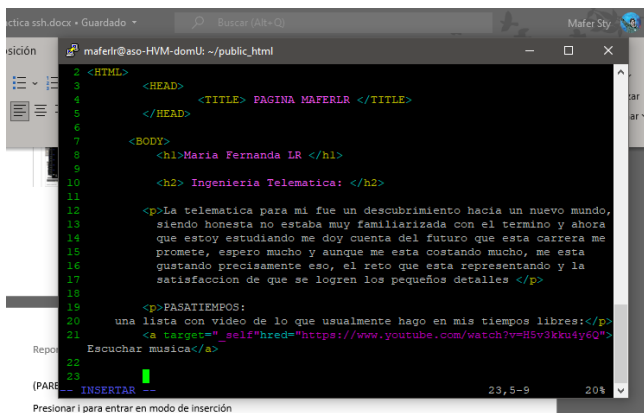
A screenshot of a terminal window, similar to the one above, showing the same Vim configuration commands: `set number`, `syntax on`, `colorscheme darkblue`, `set autoindent`, `set tabstop=2`, and `filetype indent plugin on`. The cursor is at the end of the last line. The terminal title bar shows the user 'maferi' and the directory '~/public_html'.

Salir con :q



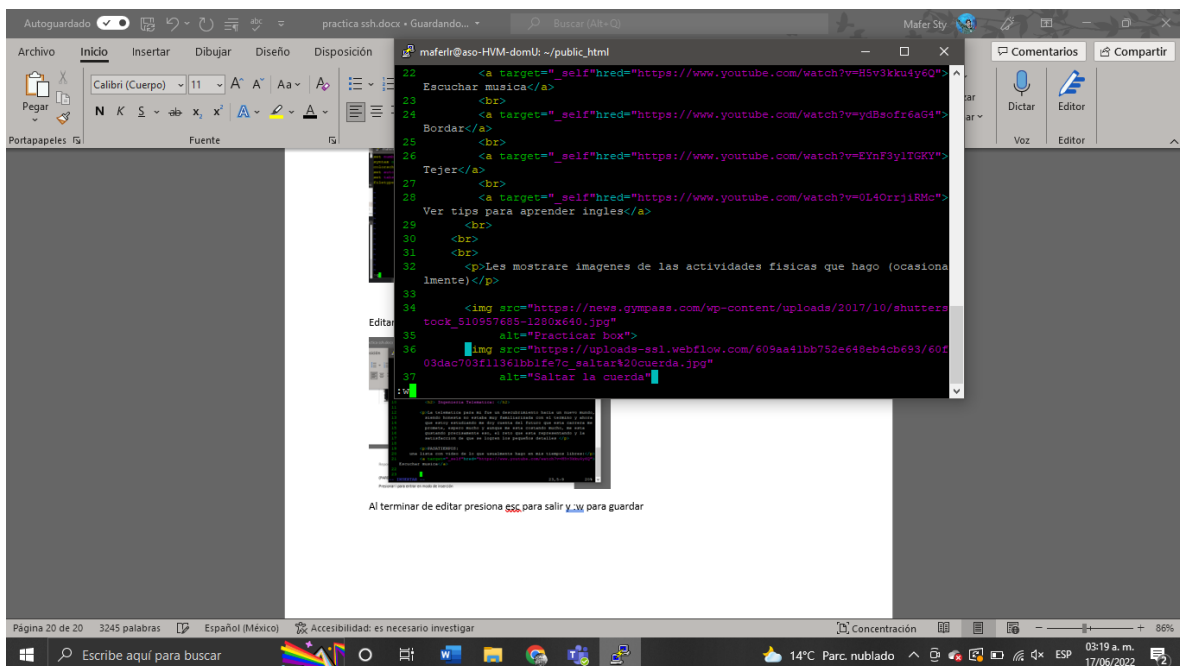
```
maferlr@aso-HVM-domU: ~/public_html
set number
syntax on
colorscheme darkblue
set autoindent
set tabstop=2
filetype indent plugin on
```

Editar en vim con html



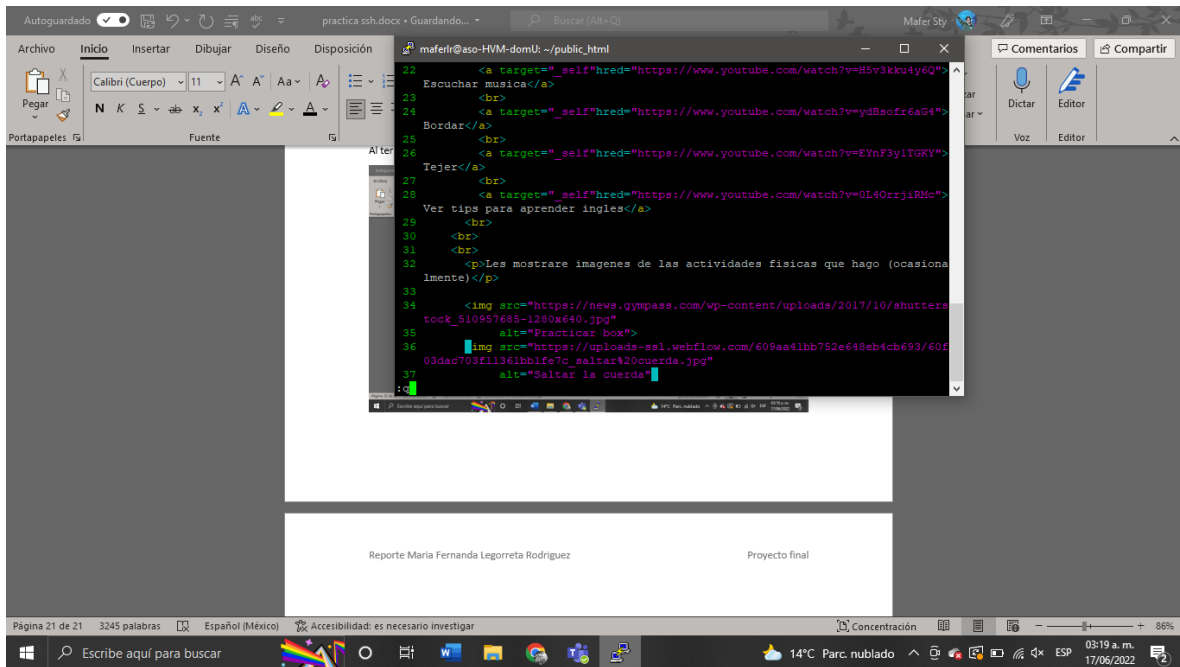
```
maferlr@aso-HVM-domU: ~/public_html
2 <HTML>
3
4 <HEAD>
5   <TITLE> PAGINA MAFERLR </TITLE>
6 </HEAD>
7
8 <BODY>
9   <h1>Maria Fernanda LR </h1>
10  <h2> Ingenieria Telematica: </h2>
11
12  <p>La telematica para mi fue un descubrimiento hacia un nuevo mundo,
13  siendo honesta no estaba muy familiarizada con el termino y ahora
14  que estoy estudiando me doy cuenta del futuro que esta carrera me
15  promete, espero mucho y aunque me esta costando mucho, me esta
16  gustando precisamente eso, el reto que esta representando y la
17  satisfaccion de que se logren los pequeños detalles </p>
18
19  <p>PASATIEMPOS:
20  una lista con video de lo que usualmente hago en mis tiempos libres:</p>
21  <a target="_self"href="https://www.youtube.com/watch?v=H5v3kku4y6Q">
22    Escuchar musica</a>
23
24  <!-- INSERTAR -->
```

Al terminar de editar presiona esc para salir y :w para guardar

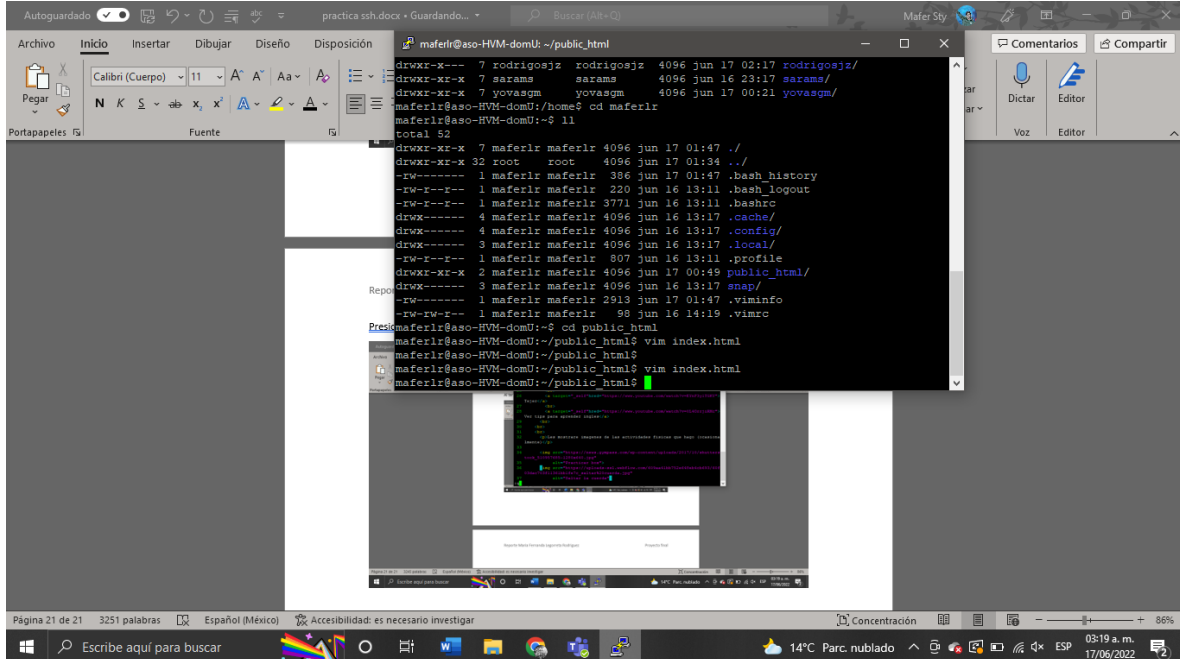


```
maferlr@aso-HVM-domU: ~/public_html
22 <a target="_self"href="https://www.youtube.com/watch?v=H5v3kku4y6Q">
23   Escuchar musica</a>
24 <br>
25 <a target="_self"href="https://www.youtube.com/watch?v=ydBoofr6aG4">
26   Borrar</a>
27 <br>
28 <a target="_self"href="https://www.youtube.com/watch?v=EYnF3ylTGKY">
29   Tejer</a>
30 <br>
31 <a target="_self"href="https://www.youtube.com/watch?v=0I4OrrjiRMc">
32   Ver tips para aprender ingles</a>
33 <br>
34 <p>Les mostrare imagenes de las actividades fisicas que hago (ocasionalmente)</p>
35 <br>
36 
37 
```

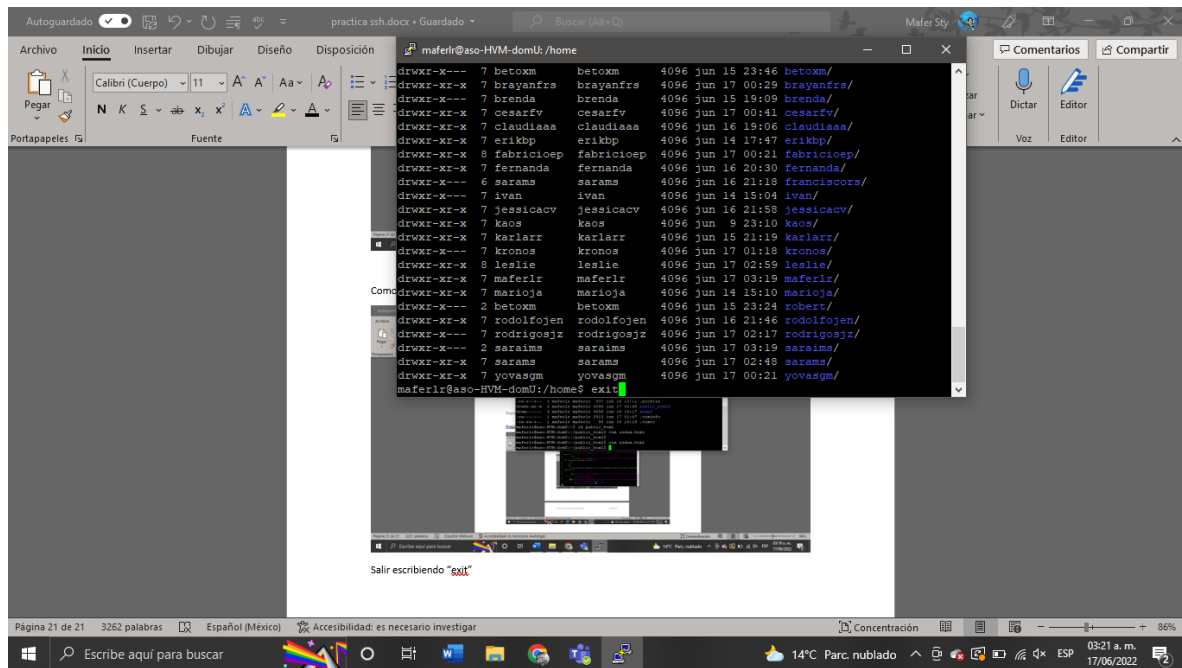
Presiona :q para salir de vim



Como ya terminamos nos regresa a la terminal



Salir escribiendo "exit"



Conclusiones:

Fue un poco complicado tratar de hacer el proyecto por mi misma porque las practicas pasadas no pude entregarlas porque tuve problemas con mi computadora pero me apoye en algunos de mis compañeros y la verdad me pareció muy interesante hacer todo el proceso porque es algo de lo que no tenia idea que realmente podía hacer.

Es un poco complicado aprenderse todo pero con la practica comienzas a dominar lo que haces, sobre todo porque es frustrante que te desconecte porque te tardas en escribir(algo que me aso varias veces) y tienes que volver a acceder y regresar a la ruta en la que estabas para poder seguir trabajando correctamente.