PROYECTO FINAL

Administración de Sistemas Operativos

Maria Fernanda Campero Lara

Boleta: 2022640059

Protocolo de SSH:

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

El cifrado simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por el cliente como por el host. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere.

El cifrado simétrico a menudo se llama clave compartida (shared key) o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.

Las claves simétricas se utilizan para cifrar toda la comunicación durante una sesión SSH. Tanto el cliente como el servidor derivan la clave secreta utilizando un método acordado, y la clave resultante nunca se revela a terceros. El proceso de creación de una clave simétrica se lleva a cabo mediante un algoritmo de intercambio de claves.

A diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key). Juntas, estas claves forman el par de claves pública-privada (public-private key pair).

La clave pública, como sugiere el nombre, se distribuye abiertamente y se comparte con todas las partes. Si bien está estrechamente vinculado con la clave privada en términos de funcionalidad, la clave privada no se puede calcular matemáticamente desde la clave pública. La relación entre las dos claves es altamente compleja: un mensaje cifrado por la clave pública de una máquina, sólo puede ser descifrado por la misma clave privada de la máquina. Esta relación unidireccional significa que la clave pública no puede descifrar sus propios mensajes ni descifrar nada cifrado por la clave privada.
La clave privada debe permanecer privada, es decir, para que la conexión sea asegura, ningún tercero debe conocerla. La fuerza de toda la conexión reside en el hecho de que la clave privada nunca se revela, ya que es el único componente capaz de descifrar mensajes que fueron cifrados usando su propia clave pública. Por lo tanto, cualquier parte con la capacidad de descifrar mensajes firmados públicamente debe poseer la clave privada correspondiente.

A diferencia de la percepción general, el cifrado asimétrico no se utiliza para cifrar toda la sesión SSH. En lugar de eso, sólo se utiliza durante el algoritmo de intercambio de claves de cifrado simétrico. Antes de iniciar una conexión segura, ambas partes generan pares de claves públicas-

privadas temporales y comparten sus respectivas claves privadas para producir la clave secreta compartida.

Una vez que se ha establecido una comunicación simétrica segura, el servidor utiliza la clave pública de los clientes para generar y desafiar y transmitirla al cliente para su autenticación. Si el cliente puede descifrar correctamente el mensaje, significa que contiene la clave privada necesaria para la conexión. Y entonces comienza la sesión SSH.

Configuración en Linux

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/y 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"

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 Reporte Maria Fernanda Legorreta Rodriguez Proyecto final 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

Diferencia del comando adduser y useradd.

Según Castro (2019): El comando useradd ejecuta un binario del sistema. El usuario adduser es un script en perl que utiliza el binario useradd. El comando adduser crea el directorio home del usuario de manera automática, a diferencia del comando useradd..

Variantes de sintaxis del comando adduser:

• -c: Permite añadir un comentario al usuario.

• -d: Permite cambiar el directorio por defecto del usuario.

• -e: Permite seleccionar la fecha en la que la cuenta de deshabilitará. El formato es AñoMesDía: AAAAMMDD. 15

• -f: Permite seleccionar el tiempo en días a partir de la fecha de expiración de la contraseña en la cual al cuenta de deshabilitará.

• -g: Permite añadir al usuario a un grupo. Debe existir con anterioridad para poder añadirlo. El grupo puede introducirse mediante su nombre o ID.

• -G: Similar a la variante anterior, pero permite introducir varios grupos separados por comas.

• m: Crea el directorio del usuario, si no existe.

• M: No crea eldirectorio del usuario.

• -n: No crea un grupo privado para el usuario.

• -r: La cuenta se convierte en una cuenta del sistema, con ID de usuario menor a 500 y sin directorio.

• -p: Establece una contraseña para el usuario.

• -s: Permite modificar la Shell de inicio de sesión del usuario.

• -u: Permite especificar el ID del usuario (debe ser mayor a 499 y única

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

La respuesta es no, aunque la mayoría de las distribuciones si ejecutan este comado, 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 65 635 bytes.

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

Servidor Apache:

Es un servidor HTTP de código abierto. Desde 1996 es el servidor WEB más usado en el mundo debido a su seguridad y estabilidad. Da a los usuarios todos los ficheros necesarios para visualizar los sitios WEB. Generalmente, las solicitudes de los usuarios se hacen a través de un navegador. La estructura de apache está basada en módulos, que permite activar y desactivar funciones adicionales. Cuenta con módulos de seguridad, caché, personalización de cabeceras, etc. Ventajas:
• De código abierto y gratuito.

• Parches de seguridad regulares y actualizados frecuentemente.

• Estructura basada en módulos.

• Multiplataforma (Windows y Linux).

• Personalización.

• Compatible con los principales sistemas de gestión de contenido, tiendas online y plataformas e-learning.

Desventajas:

• Problemas de estabilidad por encima de las 10 000 conexiones.

• El uso abusivo de los módulos puede generar brechas de seguridad. Servidor WEB en Windows (IIS): Según De León (2019): Las iniciales son de: Internet Information Services. Es un conjunto de servicios que transforma un sistema Microsoft Windows en servidor capaz de ofrecer servicios: WEB, FTP, SMPT, etc. SMTP está pensado en este tipo de software como una herramienta a disposición de las aplicaciones web alojadas para poder enviar correos electrónicos a diferentes destinatarios, pero no recibir correos de otros proveedores porque no incorpora los protocolos necesarios. Su mayor cuota se encuentra en servidores privados, pues es usado por empresas para aplicaciones internas. 17 IIS usa el modelo de proceso único (que maneja todas las peticiones), a diferencia de Apache y Nginx que dividen la carga de trabajo en subprocesos. En algunas ocasiones, IIS reparte algunas operaciones especiales en subprocesos, aunque es solo una parte; el proceso principal es siempre el que recibe y responde la petición. Incorpora el manejo de peticiones, estas pueden ser atendidas de manera concurrente. Esta es una gran ventaja, debido a la alta necesidad que tienen las aplicaciones de realizar peticiones al servidor para enviar y recibir datos. Otra ventaja es la mejor en la entrada y salida de datos asíncrona, que permite aumentar el desempeño de la aplicación. Brinda soporte para los protocolos: HTTP/HTTPS, FTP/FTPS, SMTP Y NNTP, etc. Su arquitectura es modular, permitiendo una gestión ordenada y la posibilidad de agregar funciones adicionales. Los módulos son de : lenguajes de programación, scripting, seguridad, contenido, compresión, almacenamiento cache, registro y diagnóstico. Configuración en Linux del servidor Apache:

Instalar el servicio de Apache
2: sudo apt install apache2 Indicar que sí se desea continuar cuando el sistema lo pregunte. 2. Verificar que el servicio esté instalado. También debe estar activo. sudo systemctl status apache2
3. Consultar la dirección IP de la máquina que será host, la misma en la que se instaló el servicio de Apache. ip a NOTA: Si se trabaja con una máquina virtual, esta debe estar configurada como una interfaz puente.
4. Validar que el servidor WEB está funcionando. Para esto, hay que ingresar desde cualquier navegador en la Intranet del equipo que está corriendo el servidor, la dirección IP del mismo equipo.
5. Dentro del equipo que está ejecutando el servicio de Apache, dirigirse a la carpeta ubicada en /var/www/html. cd /var/www/html
6. Visualizar lo que hay dentro de la carpeta html. ll
7. Si se desea, el usuario puede visualizar lo que contiene el archivo HTML que viene por defecto. 18 sudo cat index.html 4
8. Como recomendación, el archivo default se moverá y no se eliminará. sudo mv index.html index.html.bk
9. Crear un nuevo archivo HTML. sudo touch index.html
10. Editar el nuevo archivo HTML. sudo gedit index.html
11. Escribir el código HTML deseado en el archivo.
12. Guardar el archivo HTML. Configurar el servidor para que otros usuarios del host puedan tener su propia página WEB. 1. Cargar el módulo correspondiente a Apache. sudo a2enmod userdir 2. Reiniciar el servidor Apache. sudo systemctl restart apache2 3. Iniciar sesión con el usuario que se desee. Se creará la página WEB del mismo. su – "usuario" El guion medio te envía a la carpeta home del usuario con el cual iniciaste sesión. 4. Crear una carpeta llamada public_html . mkdir public_html 5. Cambiar el permiso a la carpeta creada. chmod 755 public_html/ Así solo el usuario puede editar, los demás entran con permisos de lectura. 6. Entrar a la carpeta public_html cd public_html/ 7. Crear archivo HTML. touch index.html 8. Editar el archivo HTML creado. gedit index.html 9. Escribir el código HTML deseado en el archivo. 10. Guardar el archivo HTML. 19 Configuración mínima para garantizar la seguridad de la conexión WEB: Para garantizar la seguridad de la conexión WEB hay que asignar los permisos correctos a las carpetas public_html, donde se encuentran los documentos HTML que serán visualizados en el sitio WEB. Este permiso es el 755, para que solo el dueño de la carpeta pueda escribir sobre la misma. Los demás, tanto grupo de la carpeta como terceros solo podrán leer lo que contiene. ¿Por qué se utiliza el puerto 8009? Según MuleSoft (s.f.): Se utiliza porque incluye los conectores AJP. Los conectores AJP trabajan de forma similar a los conectores HTTP, pero usan el protocolo AJP en vez del protocolo HTTP El protocolo Apache JServ es una versión binaria optimizada de HTTP que se suele usar para permitir a Tomcat (contenedor de servlets que se puede usar para compilar y ejecutar aplicaciones WEB realizadas en Java) comunicarse con un servidor WEB Apache. Los conectores AJP se implementan comúnmente en Tomcat mediante plug-in's. Esta funcionalidad es requerida en situaciones de alto tráfico, donde las agrupaciones de Tomcat son ejecutadas detrás de un servidor WEB Apache. Esto permite al servidor Apache entregar contenido estático y solicitudes proxy para balancear la carga de

solicitudes a través de la red y dejar a al servidor Tomcat enfocarse en entregar el contenido dinámico. Según (Anónimo, s.f.):

El protocolo 8009 TCP está orientado a la conexión.

Garantiza la entrega de paquetes de datos en el mismo orden en que fueron mandados. EL puerto UDP no garantiza la comunicación como el TCP.

Porque utilizamos el puerto 8009 y para qué sirve el puerto 80 y 8080
El 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.1

Variantes del servidor apache

- sudo systemctl status apache2: Sirve para ver el estado del servidor.
- sudo systemctl start apache2: Sirve para encender el servidor. 20
- sudo systemctl stop apache2: Sirve para detener el servidor.
- sudo systemctl restart apache2: Sirve para reiniciar el servidor.

Porque 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.

Creación de 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.

Modificación de los permisos de la carpeta public_html a 755

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.

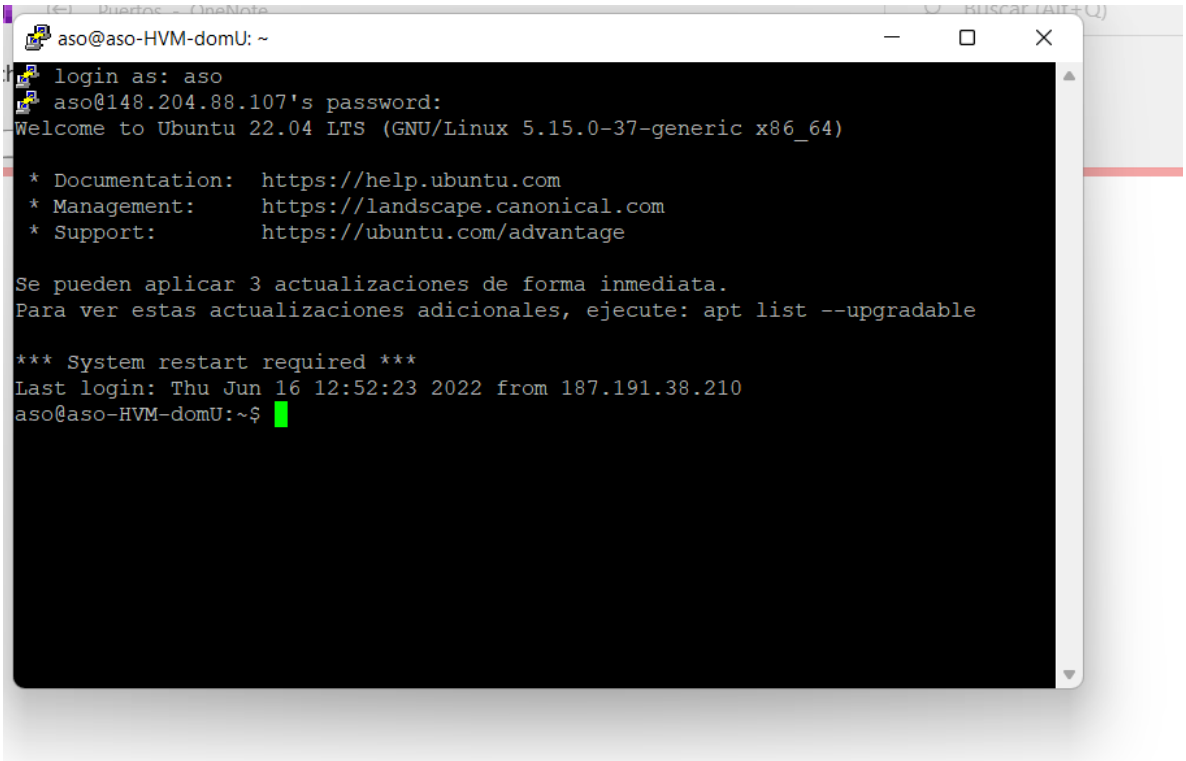
• Todos los usuarios: Los permisos de "Todos los usuarios" se aplican a todos los demás usuarios del sistema, este es el grupo que más tenemos que vigilar.

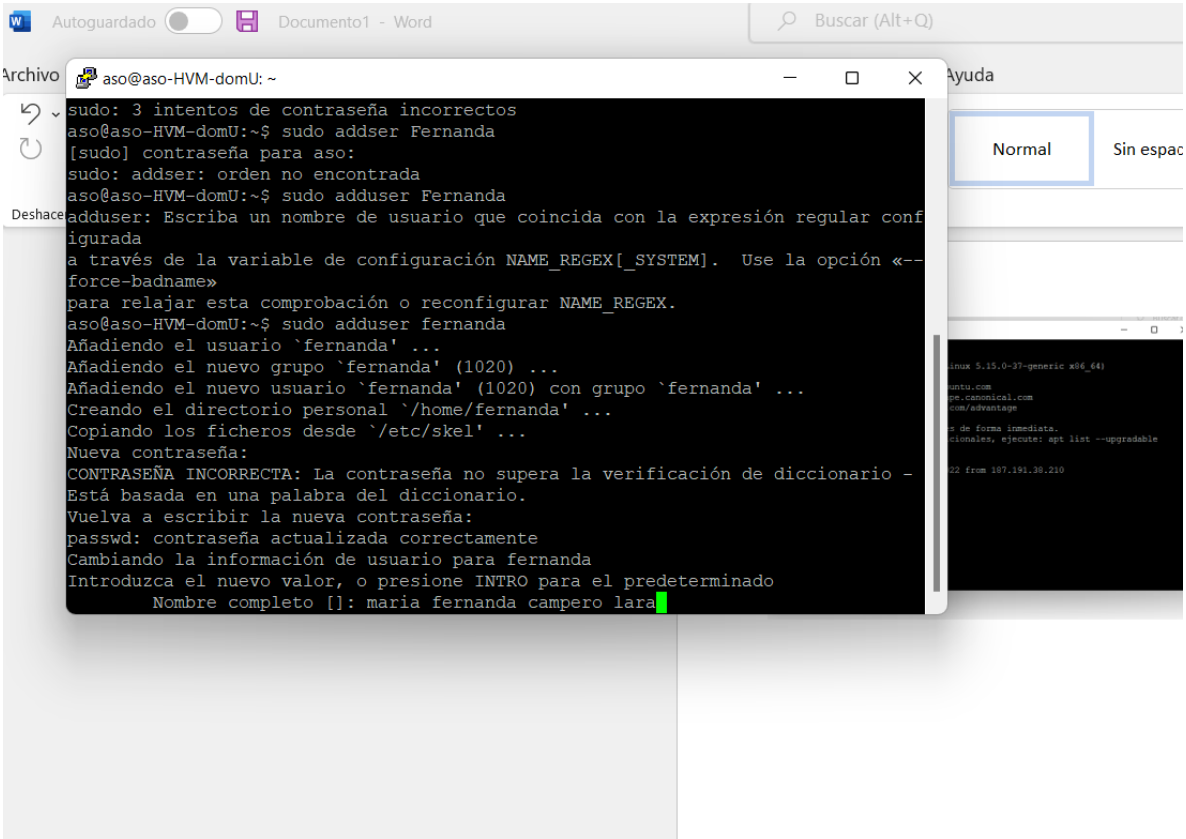
Tipos de permisos Cada archivo o directorio tiene tres tipos de permisos básicos:

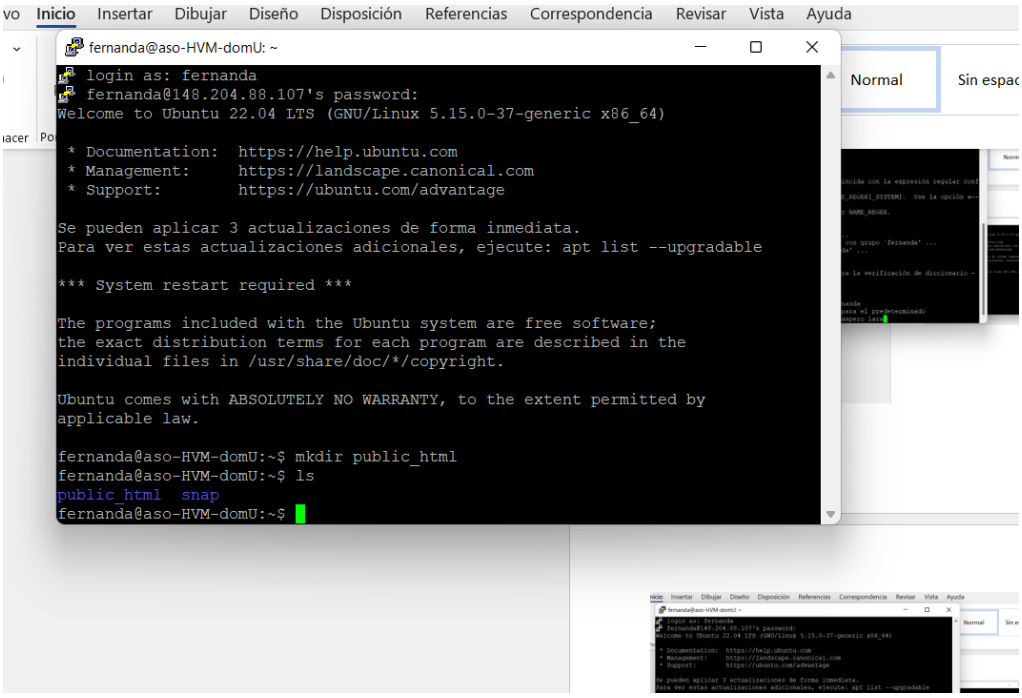
• Lectura: El permiso de lectura se refiere a la capacidad del usuario para leer el contenido del fichero.

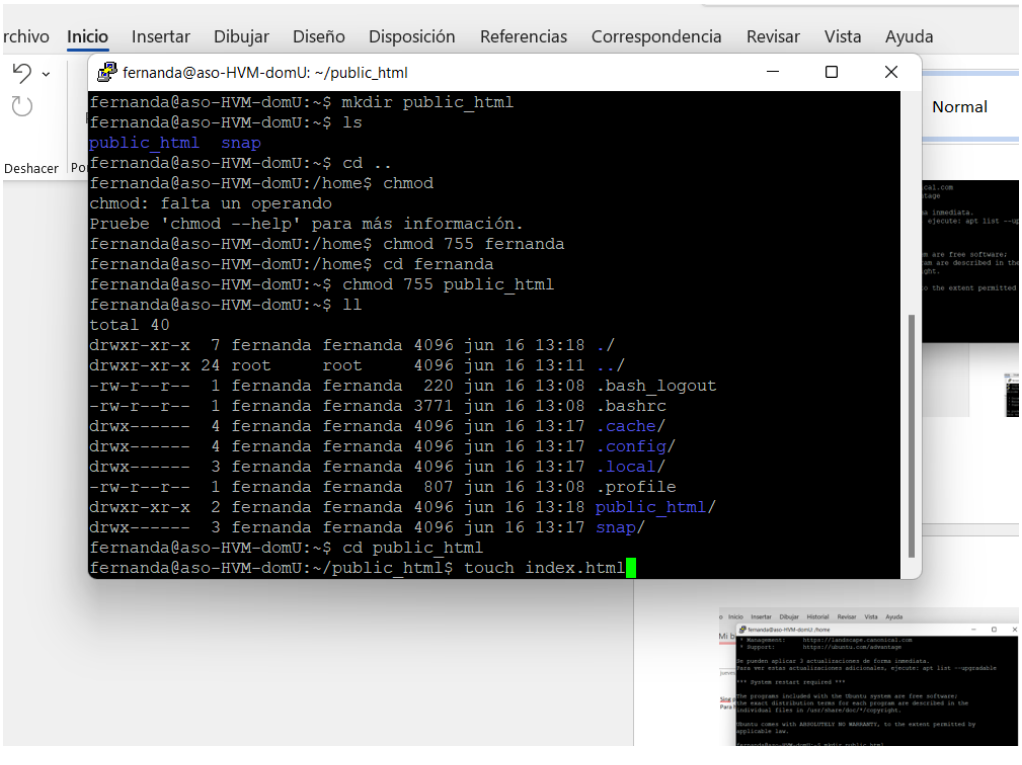
• Escritura: Los permisos de escritura hacen referencia a la capacidad de un usuario para escribir o modificar un archivo o directorio.

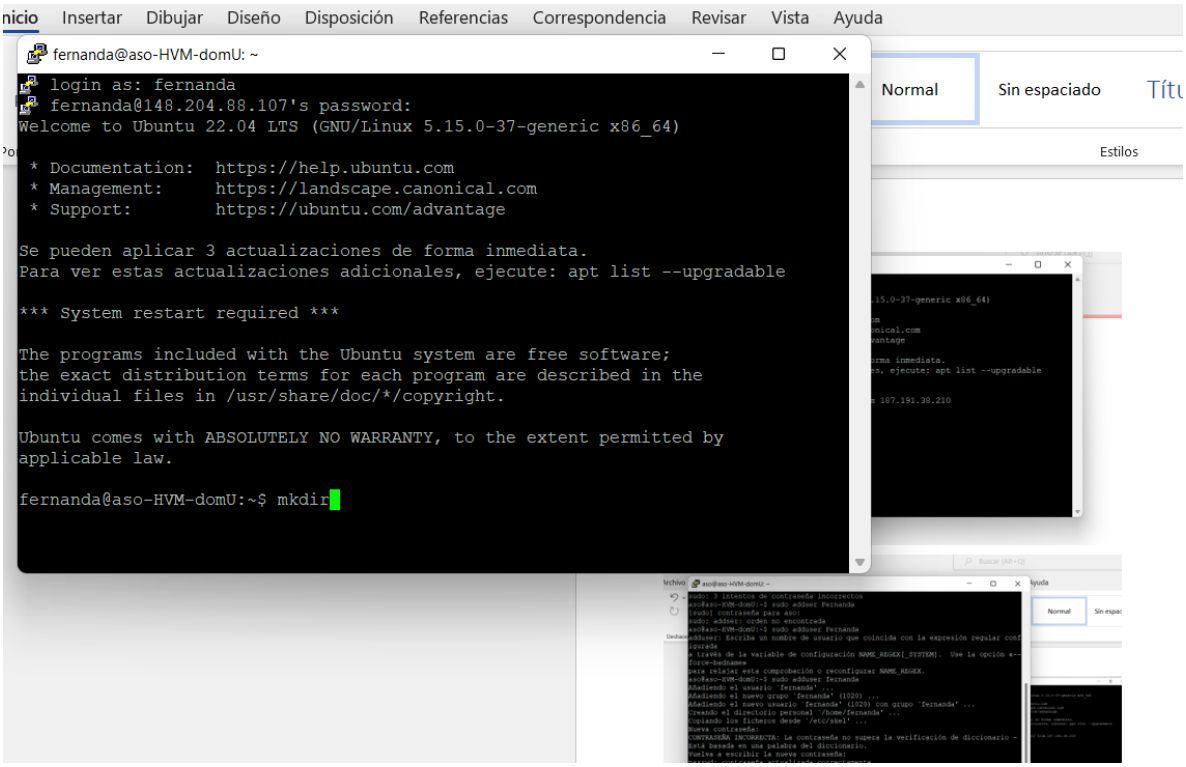
• Ejecución: El permiso de ejecución afecta a la capacidad del usuario para ejecutar un archivo o ver el contenido de un directorio.

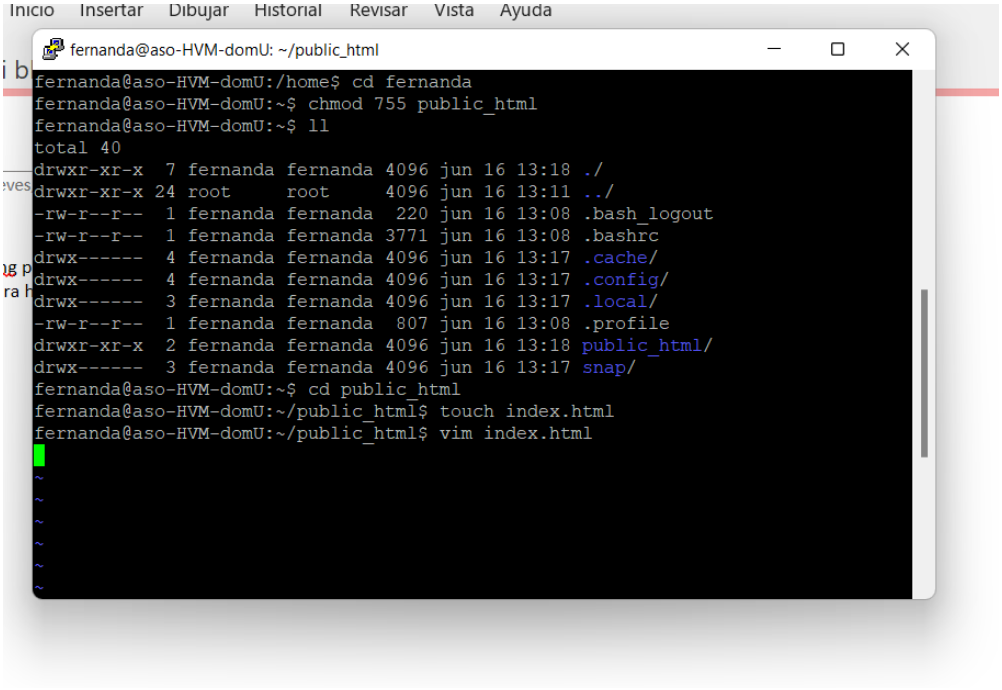

aso@aso-HVM-domU: ~
login as: aso
aso@148.204.88.107's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-37-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Se pueden aplicar 3 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
*** System restart required ***
Last login: Thu Jun 16 12:52:23 2022 from 187.191.38.210
aso@aso-HVM-domU:~$

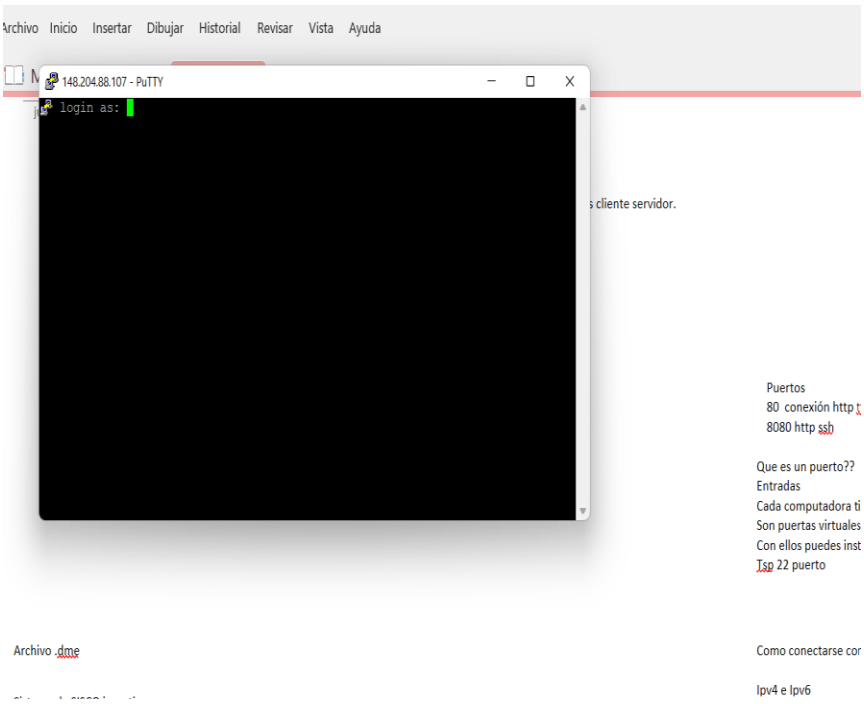

Autoguardado
Documento1 - Word
Buscar (Alt+Q)
Archivo
Ayuda
Deshace
Normal
Sin espac
aso@aso-HVM-domU: ~
sudo: 3 intentos de contraseña incorrectos
aso@aso-HVM-domU:~$ sudo addser Fernanda
[sudo] contraseña para aso:
sudo: addser: orden no encontrada
aso@aso-HVM-domU:~$ sudo adduser Fernanda
adduser: Escriba un nombre de usuario que coincida con la expresión regular conf
igurada
a través de la variable de configuración NAME_REGEX[_SYSTEM]. Use la opción «--
force-badname»
para relajar esta comprobación o reconfigurar NAME_REGEX.
aso@aso-HVM-domU:~$ sudo adduser fernanda
Añadiendo el usuario `fernanda' ...
Añadiendo el nuevo grupo `fernanda' (1020) ...
Añadiendo el nuevo usuario `fernanda' (1020) con grupo `fernanda' ...
Creando el directorio personal `/home/fernanda' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña no supera la verificación de diccionario -
Está basada en una palabra del diccionario.
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para fernanda
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []: maria fernanda campero lara

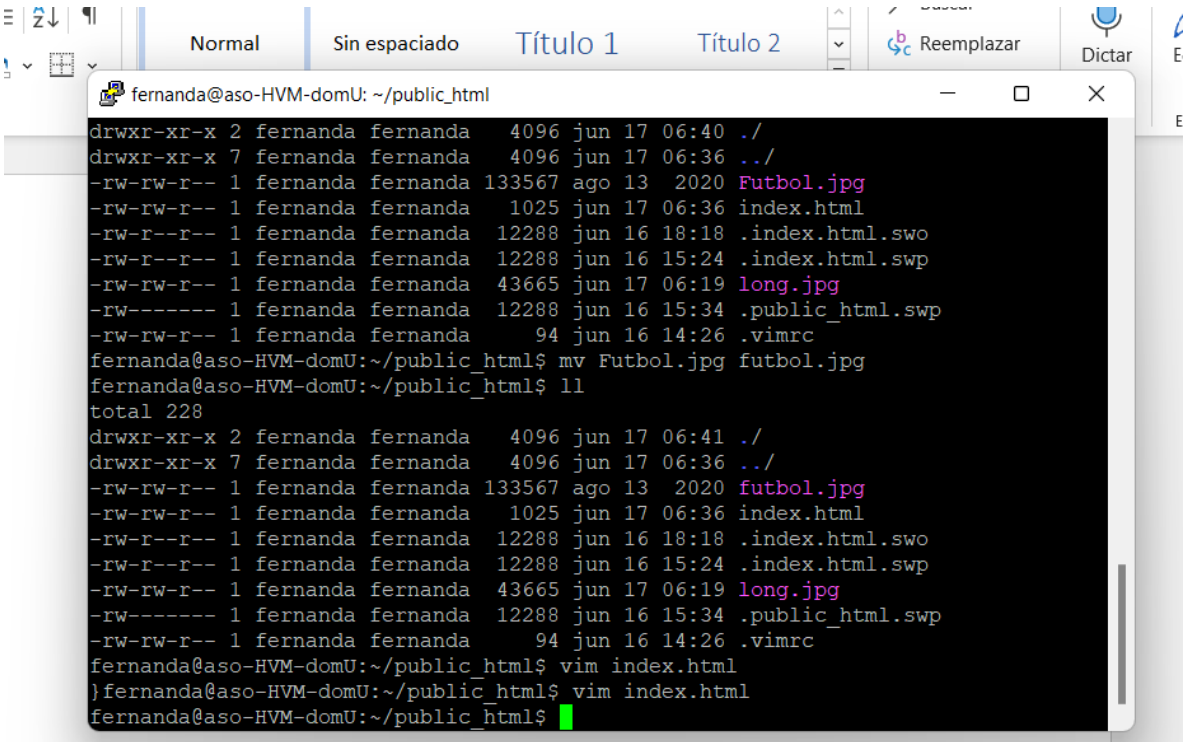

Inicio Insertar Dibujar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda
fernanda@aso-HVM-domU: ~
login as: fernanda
fernanda@148.204.88.107's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-37-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* 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.
fernanda@aso-HVM-domU:~$ mkdir public_html
fernanda@aso-HVM-domU:~$ ls
public_html snap
fernanda@aso-HVM-domU:~$
Normal
Sin espac

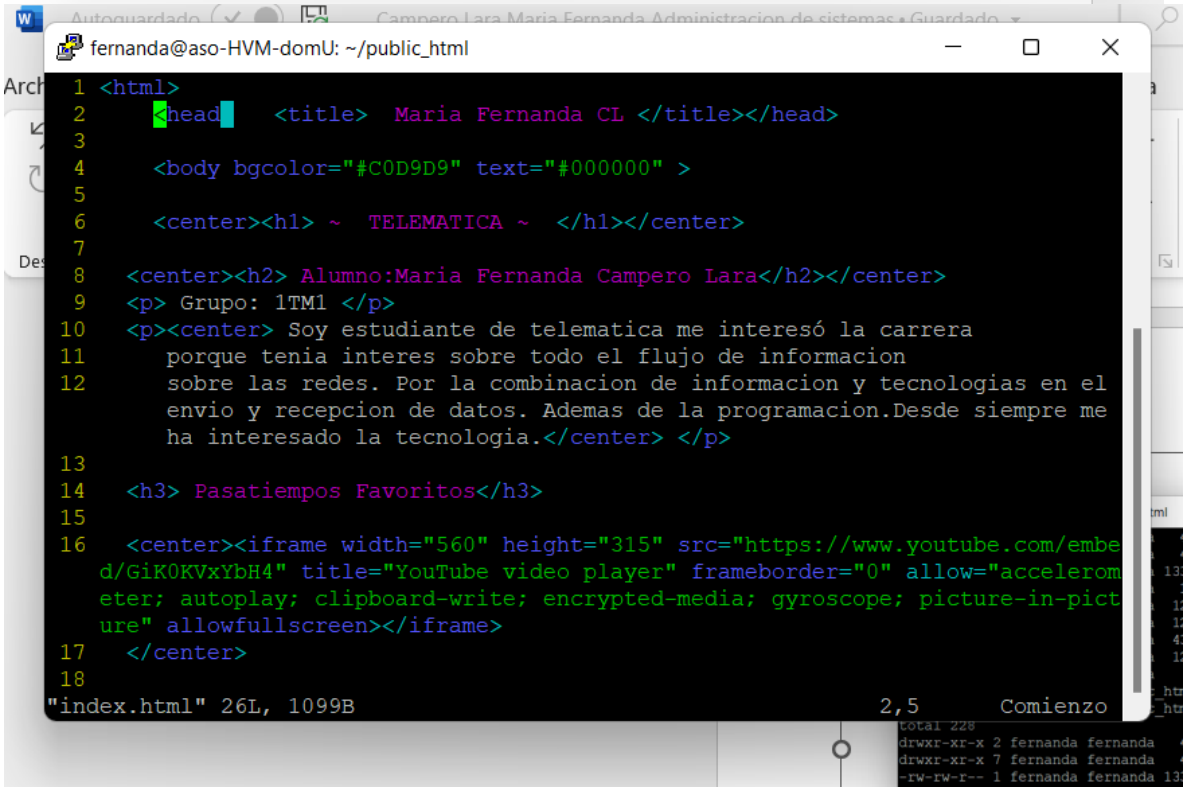

rchivo Inicio Insertar Dibujar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda
fernanda@aso-HVM-domU: ~/public_html
fernanda@aso-HVM-domU:~$ mkdir public_html
fernanda@aso-HVM-domU:~$ ls
public_html snap
fernanda@aso-HVM-domU:~$ cd ..
fernanda@aso-HVM-domU:/home$ chmod
chmod: falta un operando
Pruebe 'chmod --help' para más información.
fernanda@aso-HVM-domU:/home$ chmod 755 fernanda
fernanda@aso-HVM-domU:/home$ cd fernanda
fernanda@aso-HVM-domU:~$ chmod 755 public_html
fernanda@aso-HVM-domU:~$ ll
total 40
drwxr-xr-x 7 fernanda fernanda 4096 jun 16 13:18 ./
drwxr-xr-x 24 root root 4096 jun 16 13:11 ../
-rw-r--r-- 1 fernanda fernanda 220 jun 16 13:08 .bash_logout
-rw-r--r-- 1 fernanda fernanda 3771 jun 16 13:08 .bashrc
drwx------ 4 fernanda fernanda 4096 jun 16 13:17 .cache/
drwx------ 4 fernanda fernanda 4096 jun 16 13:17 .config/
drwx------ 3 fernanda fernanda 4096 jun 16 13:17 .local/
-rw-r--r-- 1 fernanda fernanda 807 jun 16 13:08 .profile
drwxr-xr-x 2 fernanda fernanda 4096 jun 16 13:18 public_html/
drwx------ 3 fernanda fernanda 4096 jun 16 13:17 snap/
fernanda@aso-HVM-domU:~$ cd public_html
fernanda@aso-HVM-domU:~/public_html$ touch index.html
Deshacer
Normal


nicio Insertar Dibujar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda
fernanda@aso-HVM-domU: ~
login as: fernanda
fernanda@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.
fernanda@aso-HVM-domU:~$ mkdir
Normal
Sin espaciado
Estilos


Inicio Insertar Dibujar Historial Revisar Vista Ayuda
fernanda@aso-HVM-domU: ~/public_html
fernanda@aso-HVM-domU:/home$ cd fernanda
fernanda@aso-HVM-domU:~$ chmod 755 public_html
fernanda@aso-HVM-domU:~$ ll
total 40
drwxr-xr-x 7 fernanda fernanda 4096 jun 16 13:18 ./
drwxr-xr-x 24 root   root   4096 jun 16 13:11 ../
-rw-r--r-- 1 fernanda fernanda 220 jun 16 13:08 .bash_logout
-rw-r--r-- 1 fernanda fernanda 3771 jun 16 13:08 .bashrc
drwx------ 4 fernanda fernanda 4096 jun 16 13:17 .cache/
drwx------ 4 fernanda fernanda 4096 jun 16 13:17 .config/
drwx------ 3 fernanda fernanda 4096 jun 16 13:17 .local/
-rw-r--r-- 1 fernanda fernanda 807 jun 16 13:08 .profile
drwxr-xr-x 2 fernanda fernanda 4096 jun 16 13:18 public_html/
drwx------ 3 fernanda fernanda 4096 jun 16 13:17 snap/
fernanda@aso-HVM-domU:~$ cd public_html
fernanda@aso-HVM-domU:~/public_html$ touch index.html
fernanda@aso-HVM-domU:~/public_html$ vim index.html


Archivo Inicio Insertar Dibujar Historial Revisar Vista Ayuda
148.204.88.107 - PuTTY
login as:
cliente servidor.
Puertos
80 conexión http
8080 http ssh
Que es un puerto??
Entradas
Cada computadora ti
Son puertas virtuales
Con ellos puedes inst
Tsp 22 puerto
Archivo .dme
Como conectarse cor
Ipv4 e Ipv6


Normal
Sin espaciado
Título 1
Título 2
Reemplazar
Dictar
fernanda@aso-HVM-domU: ~/public_html
drwxr-xr-x 2 fernanda fernanda   4096 jun 17 06:40 ./
drwxr-xr-x 7 fernanda fernanda   4096 jun 17 06:36 ../
-rw-rw-r-- 1 fernanda fernanda 133567 ago 13 2020 Futbol.jpg
-rw-rw-r-- 1 fernanda fernanda   1025 jun 17 06:36 index.html
-rw-r--r-- 1 fernanda fernanda 12288 jun 16 18:18 .index.html.swo
-rw-r--r-- 1 fernanda fernanda 12288 jun 16 15:24 .index.html.swp
-rw-rw-r-- 1 fernanda fernanda 43665 jun 17 06:19 long.jpg
-rw------- 1 fernanda fernanda 12288 jun 16 15:34 .public_html.swp
-rw-rw-r-- 1 fernanda fernanda   94 jun 16 14:26 .vimrc
fernanda@aso-HVM-domU:~/public_html$ mv Futbol.jpg futbol.jpg
fernanda@aso-HVM-domU:~/public_html$ ll
total 228
drwxr-xr-x 2 fernanda fernanda   4096 jun 17 06:41 ./
drwxr-xr-x 7 fernanda fernanda   4096 jun 17 06:36 ../
-rw-rw-r-- 1 fernanda fernanda 133567 ago 13 2020 futbol.jpg
-rw-rw-r-- 1 fernanda fernanda   1025 jun 17 06:36 index.html
-rw-r--r-- 1 fernanda fernanda 12288 jun 16 18:18 .index.html.swo
-rw-r--r-- 1 fernanda fernanda 12288 jun 16 15:24 .index.html.swp
-rw-rw-r-- 1 fernanda fernanda 43665 jun 17 06:19 long.jpg
-rw------- 1 fernanda fernanda 12288 jun 16 15:34 .public_html.swp
-rw-rw-r-- 1 fernanda fernanda   94 jun 16 14:26 .vimrc
fernanda@aso-HVM-domU:~/public_html$ vim index.html
}fernanda@aso-HVM-domU:~/public_html$ vim index.html
fernanda@aso-HVM-domU:~/public_html$


fernanda@aso-HVM-domU: ~/public_html
1 <html>
2 <head> <title> Maria Fernanda CL </title></head>
3
4 <body bgcolor="#C0D9D9" text="#000000" >
5
6 <h1> ~ TELEMATICA ~ </h1>
7
8 <h2> Alumno:Maria Fernanda Campero Lara</h2>
9 Grupo: 1TM1
10 Soy estudiante de telematica me interesó la carrera
11 porque tenia interes sobre todo el flujo de informacion
12 sobre las redes. Por la combinacion de informacion y tecnologias en el
envio y recepcion de datos. Ademas de la programacion.Desde siempre me
ha interesado la tecnologia.
13
14 <h3> Pasatiempos Favoritos</h3>
15
16 <iframe width="560" height="315" src="https://www.youtube.com/embe
d/GiK0KVxYbH4" title="YouTube video player" frameborder="0" allow="accelerom
eter; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-pict
ure" allowfullscreen></iframe>
17
18
"index.html" 26L, 1099B 2,5 Comienzo

Conclusiones:

La practica se me hizo muy interesante el hacer una pagina web y subirla a internet. Por medio de los comandos de creación de carpetas y permisos. Me doy cuenta de la importancia de trabajar de manera remota por medio de la conexión entre servidor y cliente.

Ya que así pude realizar todo este trabajó ya que nunca se estuvo trabajando dentro de la computadora de la escuela. Y veo como es que en las empresas alrededor del mundo se le es muy útil trabajar de esta forma.

La verdad este ultimo proyecto de me hizo más complicado que todos los demás tuve que pedir ayuda a algunos compañeros, pero creo que el resultado fue gratificante y me llevo mucho de esta última práctica. Además de que sé que estos conocimientos me ayudaran bastante en la carrera y en mi vida laboral.