Práctica 1: Apache2 MySQL PHP y PhpMyAdmin

- **Servicio Apache: Levantar/Tumbar/Estado/Reiniciar**
  sudo service apache2 start/stop/status/restart

- **Asociar archivos html/php en el host virtual para renderizarlos en el navegador web**
  Introducirlos en la carpeta /var/www/html

- **Path del host virtual principal**
  /var/www/html

- **Navegación por consola con links2**
  links2 {IP_SERVER}:{PUERTO}
  ip a //Ver ip del equipo

- **Adición de escucha de puertos**
  Editar el archivo:
    /etc/apache2/ports.conf
  Añadir en nueva línea:
    Listen {PUERTO}

- **Acceso a MySQL**
  Instalar: apt-get install mysql-server
  Acceso por terminal: sudo mysql -u root

- **Configuración Apache para que PHP funcione bien en el servidor web**
  Instalar php:
    apt-get install php libapache2-mod-php php-mysql
  Agregar al final de /etc/apache2/apache2.conf:

  ```
  <IfModule php7_module>
      AddType application/x-httpd-php .php
      AddType application/x-httpd-php-source .phps
      <IfModule dir_module>
          DirectoryIndex index.html index.php
       </IfModule>
  </IfModule>
  ```

  Para probarlo creamos un archivo php y ejecutamos:
    php {archivo}

- **Ubicación y uso de PhpMyAdmin**

  Instalar PhpMyAdmin:

  apt-get install phpmyadmin
  iptables -I INPUT -p tcp --dport 443 -j ACCEPT

  Algunas veces hay que realizar estos dos comandos:

  ln -s /etc/phpmyadmin/apache.conf
  /etc/apache2/conf-enabled/phpmyadmin.conf

  ln -s /etc/phpmyadmin/apache.conf
  /etc/apache2/conf-available/phpmyadmin.conf

  Abrir mysql y ejecutar este comando:

  sudo mysql -u root

  ALTER USER 'root'@'localhost' IDENTIFIED WITH
  caching_sha2_password BY 'root';

  Ubicación de phpmyadmin:

  /usr/share/phpmyadmin/

  Abrir phpmyadmin desde el navegador:

  http://{IP_SERVIDOR}/phpmyadmin/

Práctica 2: Parámetros PHP

- **PHP.INI: parámetros configurables más importantes.**
  El resto NO SE INCLUYE para la P.E. pero sí para el examen final

  Ubicación de PHP.INI:

  /etc/php/7.4/apache2/php.ini
  Abrirlo con líneas: nano -l {archivo}

  Habilitar extensiones necesarias (a partir de la línea 913)

  extension=mbstring
  extension=mysqli
  extension=openssl

  Permitir a PHP tiempo ilimitado de ejecución de scripts:

  cambiar la directiva max_execution_time a max_execution_time = 0
  (linea 388) nano -l {archivo}

Práctica 4: DNS y Fijar IP

- **Fijar IP fija desde VB a servidor y cliente:**
  Necesitamos conocer el nombre de nuestra red Nat y la MAC.
  Ejecutamos el siguiente comando desde la CMD de Windows:

  "C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" dhcpserver modify
  --network="{NOMBRE NAT (NatNetwork por defecto)}"
  --mac-address={MAC DE LA MÁQUINA EJ 08:00:27:3a:d9:b2}
  --fixed-address:{DIRECCIÓN IP DESEADA EJ 10.0.2.4}

  Para ver MAC en el terminal de la máquina (ip a) donde pone link/ether

- **Servicio DNS: Levantar/Tumbar/Estado/Reiniciar**
  Instalar bind9: apt-install bind9
  sudo service bind9 start/stop/status/restart

- **Verificación de puertos abiertos**
  apt-install nmap
  nmap {DIRECCION_IP}

- **Instalación/uso de resolvconf para persistir qué dirección IP resuelve el dominio**
  Instalamos el paquete resolvconf
  sudo apt install resolvconf

  Habilitamos el servicio
  sudo systemctl enable resolvconf.service

  En el fichero /etc/resolvconf/resolv.conf.d/head escribir:
  nameserver {IPSERVIDOR}
  search {NOMBREAPELLIDOS}.local
  domain {NOMBREAPELLIDOS}.local

  Aplicamos los cambios:
  sudo resolvconf --enable-updates
  sudo resolvconf -u

- **Configuración archivo resolv.conf para indicar qué dirección IP resuelve el dominio**
  En el fichero /etc/resolv.conf del servidor y del cliente escribir únicamente:
  nameserver {IPSERVIDOR}
  search {NOMBREAPELLIDOS}.local
  domain {NOMBREAPELLIDOS}.local

- **Configuración de zonas directas y ubicación**

  Editar el fichero /etc/bind/named.conf.options y descomentar las líneas forwarders y cambiar el 0.0.0.0 por 8.8.8.8.

  Editamos /etc/bind/named.conf.local y ponemos:

  zone "{NOMBREAPELLIDOS}.local"{
  type master;
  file "/etc/bind/{NOMBREAPELLIDOS}.local";
  }; (OJO el punto y coma)

  Copiar el archivo /etc/bind/db.local con el nombre {NOMBREAPELLIDOS}.local
  cp /etc/bind/db.local /etc/bind/{NOMBREAPELLIDOS}.local

  Editar el archivo /etc/bind/{NOMBREAPELLIDOS}.local:

```
$TTL 604800
@     IN    SOA   {NOMBREAPELLIDOS}.local.
root.{NOMBREAPELLIDOS}.local. (
                              2         ; Serial
                         604800         ; Refresh
                         86400          ; Retry
                         2419200        ; Expire
                         604800 )       ; Negative
Cache TTL
;
@          IN    NS    {NOMBREAPELLIDOS}.local.
@          IN    A     127.0.0.1
@          IN    AAAA  ::1
ftp        IN    A     {IPSERVIDOR}
www        IN    A     {IPSERVIDOR}
cliente    IN    A     {IPCLIENTE}
```

- **Configuración de zonas indirectas y ubicación**

  Editamos /etc/bind/named.conf.local y ponemos:
  zone "{IPSERVIDOR (AL REVÉS EJ: 10.0.2.5 => 5.2.0.10)}.in-addr.arpa"{
  type master;
  file "/etc/bind/{NOMBREAPELLIDOS}.{IPSERVIDOR}";
  }; (OJO el punto y coma)

  Copiar el fichero db.127 con el nombre {NOMBREAPELLIDOS}.{IPSERVIDOR}
  sudo cp /etc/bind/db.127 /etc/bind/{NOMBREAPELLIDOS}.{IPSERVIDOR}

Editar el archivo /etc/bind/{NOMBREAPELLIDOS}.{IPSERVIDOR}:

```
$TTL  604800
@     IN    SOA   {NOMBREAPELLIDOS}.local.
root.{NOMBREAPELLIDOS}.local. (
                              1     ; Serial
                         604800     ; Refresh
                         86400      ; Retry
                         2419200    ; Expire
                         604800 )   ; Negative Cache TTL
;
@            IN    NS    {NOMBREAPELLIDOS}.local.
1.0.0        IN    PTR   {NOMBREAPELLIDOS}.local.
{IPSERVER}   IN    PTR   {NOMBREAPELLIDOS}.local.
{IPCLIENTE}  IN    PTR   cliente.{NOMBREAPELLIDOS}.local.
{IPSERVER}   IN    PTR   ftp.{NOMBREAPELLIDOS}.local.
{IPSERVER}   IN    PTR   www.{NOMBREAPELLIDOS}.local.
```

- **Comandos de detección de errores**

  sudo service bind9 status

  Zona directa**:**
  sudo named-checkzone {NOMBREAPELLIDOS}.local
  {NOMBREAPELLIDOS}.local

  Zona inversa:
  sudo named-checkzone {NOMBREAPELLIDOS}.{IPSERVIDOR}
  {NOMBREAPELLIDOS}.{IPSERVIDOR}

- **Comandos de resolución de dominios**

  sudo service bind9 status
  FTP: nslookup ftp.{NOMBREAPELLIDOS}.local
  WWW: nslookup www.{NOMBREAPELLIDOS}.local
  Cliente: nslookup cliente.{NOMBREAPELLIDOS}.local

- **Uso del navegador web para renderizar URLs**

  Abrimos el navegador del cliente y vamos a:
  www.{NOMBREAPELLIDOS}.local

Práctica 5: LDAP

- **Servicio LDAP: Levantar/Tumbar/Estado/Reiniciar**

  sudo apt install slapd
  sudo service slapd start/stop/status/restart

- **Verificación de puertos abiertos**

  sudo nmap {IPSERVIDOR}

- **Reconfiguración del servicio LDAP: comando y configuración del asistente|**

  sudo dpkg-reconfigure slapd

  Pantallas:

  1 - (Omit OpenLDAP server): no
  2 - (DNS domain name): {NOMBREAPELLIDOS}.local
  3 - (Organization name): {NOMBREAPELLIDOS}
  4 y 5- (Administration password): {CONTRASEGNA}
  6 - (Do you want the database): no
  7 - (Move old database): si
  Para ver lo que hemos configurado: sudo slapcat

- **Aplicación gráfica para gestionar LDAP: Pestaña de configuración general**

  Instalar en servidor:

  sudo apt install ldap-account-manager
  sudo systemctl restart apache2

  En el navegador del cliente configuración inicial:
  http://www.{NOMBREAPELLIDOS}.local/lam/templates/config/conflogin.php
  Contraseña: lam (al editar la configuración general se cambiará a la indicada en "Profile password")

  En la pestaña "general settings":

  Server setting:

  Tree suffix > dc={NOMBREAPELLIDOS},dc=local

  Language settings:

  Default language > Español (España)

  Security settings:

  List of valid users >
  cn=admin,dc={NOMBREAPELLIDOS},dc=local

  Profile password:

  Contraseña nueva
  Al terminar pulsar "Save".

- **Aplicación gráfica para gestionar LDAP: Tipos de cuentas**

  En el navegador:
  http://www.{NOMBREAPELLIDOS}.local/lam/templates/config/conflogin.php
  Contraseña: lam o la indicada en "Profile password")

  En la pestaña "tipos de cuentas" (Account types):

  En tipos de cuentas disponibles añadir(+) > Equipos (Hosts)

  Usuarios:

  Sufijo LDAP >
  ou=usuarios,dc={NOMBREAPELLIDOS},dc=local

Grupos:
Sufijo LDAP >
ou=grupos,dc={NOMBREAPELLIDOS},dc=local
Equipos:
Sufijo LDAP >
ou=equipos,dc={NOMBREAPELLIDOS},dc=local

Al terminar pulsar “Guardar”.

- **Aplicación gráfica para gestionar LDAP: Pestaña de módulos**

  En la pestaña “módulos” (Modules):
  Equipos añadir(+):
  Añadir “Cuenta” (Account)
  Añadir “Unix”
  Al terminar pulsar “Guardar”.

- **Gestión de usuarios**

  En: http://www.{NOMBREAPELLIDOS}.local/lam/templates/login.php iniciar sesión. (Contraseña la indicada en el servidor).

  Pulsamos en crear.

  Para crear un grupo:
  Ir a la pestaña grupos, Nuevo grupo y rellenar nombre.

  Para crear un usuario:
  Ir a la pestaña usuarios, Nuevo usuario.
  En el apartado “Personal” rellenar “Nombre” y “Apellido”.
  En el apartado “Unix” rellenar el campo “Nombre” y asociar el grupo creado.
  Por último, pulsamos en “Establecer contraseña” y rellenamos los campos y pulsamos en “Ok” y luego en “Guardar”.

- **Creación de un cliente LDAP para la VM Cliente -> inclusión de capturas**

  sudo apt install libnss-ldap libpam-ldap ldap-utils

  Pantalla 1- (LDAP server Identifier):
  ldap://{IPSERVER} (Ojo con la i y la /)
  Pantalla 2- (Distinguished name of search base):
  dc={NOMBREAPELLIDOS},dc=local
  Pantalla 3- (LDAP version):
  La 3.
  Pantalla 4- (Make local root Database admin):
  Yes
  Pantalla 5- (Does the LDAP database):
  No
  Pantalla 6- (LDAP account for root):
  cn=admin,dc={NOMBREAPELLIDOS},dc=local.

Pantalla 7- (LDAP root password)
{CONTRASEÑA}

Configuración archivo ldap:
nano /etc/nsswitch.conf
Cambiamos: (izqda por dcha)anno

```
passwd:         files systemd
group:          files systemd
shadow:         files
gshadow:        files
```

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
gshadow:        files
```

En: nano -l /etc/pam.d/common-password
En la línea 26 eliminamos “use_authtok”. (Al final del todo)

Añadimos al final de nano /etc/pam.d/common-session:
session optional pam_mkhomedir.so skel=/etc/skel/ unmask=077

- **Cadena de conexión para conectar desde terminal al servidor desde el cliente**

  sudo ldapsearch -x -H ldap://{IPSERVER} -b “dc={NOMBREAPELLIDOS}, dc=local” -s sub
  (A veces no va pero no importa)

- **Acceder vía terminal desde el cliente:**
  Cerrar sesión.
  Sin iniciar sesión pulsamos “Alt+Ctrl+F2”.
  Iniciamos sesión con el usuario LDAP.
  “Alt+Ctrl+F1” para volver a modo gráfico y darle a not listed si no aparece.

Práctica 6: HOST Virtuales

- **Creación de host virtuales por dominio: comandos y operativa**
  1- Creación de la carpeta del host virtual:
  sudo mkdir /var/www/{NOMBRE HOST}

  2- Archivo index:
  sudo touch /var/www/{NOMBRE HOST}/index.html

  3- Copiamos 000-default.conf para tener una conf. inicial.
  cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/{NOMBRE HOST}.conf

  4- Editamos el archivo:
  nano -l /etc/apache2/sites-available/{NOMBRE HOST}.conf

Escribimos dentro del tag <VirtualHost>
ServerName {INTRANET (u otro)}.{NOMBREAPELLIDOS}.local
DocumentRoot /var/www/{NOMBRE HOST}

5- Activamos el host virtual:
a2ensite {NOMBRE HOST}.conf

6- Reiniciamos apache2:
sudo systemctl restart apache2

7- Agregamos en las zonas directa e inversa:
nano /etc/bind/{NOMBREAPELLIDOS}.local:
{INTRANET (u otro)} IN A {IPSERVER}
nano /etc/bind/{NOMBREAPELLIDOS}.{IPSERVER}:
{ÚLTIMO DÍGITO IP SERVER} IN PTR {INTRANET (u otro)}.{NOMBREAPELLIDOS}.local. (Ojo al punto despues de local)

8- Restart bind9

- **Configuración del host virtual en su archivo de configuración: puertos, logs y otras directivas**

Para cambiar el puerto: nano /etc/apache2/ports.conf:
Escribimos Listen {PUERTO}

Para los logs:
touch /var/log/apache2/{INTRANET (u otro)}_error.log
touch /var/log/apache2/{INTRANET (u otro)}_access.log

nano /etc/apache2/sites-available/{NOMBRE HOST}.conf
Escribimos o cambiamos las líneas:
ErrorLog ${APACHE_LOG_DIR}/{INTRANET (u otro)}_error.log
CustomLog ${APACHE_LOG_DIR}/{INTRANET (u otro)}_access.log combined
//Nota ${APACHE_LOG_DIR} se deja así.

Para que {INTRANET (u otro)} escuche en otro puerto :
nano /etc/apache2/sites-available/{NOMBRE HOST}.conf
Cambiamos <VirtualHost *:80>:
ej: <VirtualHost *:{PUERTO} *:{PUERTO}>
(Se pueden poner varios puertos a la vez).

- **Saber renderizar páginas web de un cierto host en el navegador indicando protocolo, path y puerto**

En el navegador del cliente ponemos:
http://{INTRANET}.{NOMBREAPELLIDOS}.local:{PUERTO}/index.html

(Ojo al http en vez de https si no está activado el SSL)

- **Autenticación básica para un cierto directorio en Apache.**

  1- Creamos la carpeta privada:
  mkdir /var/www/{NOMBRE HOST}/{CARPETA PRIVADA}

  2- Creamos:
  nano/var/www/{NOMBRE HOST}/{CARPETA PRIVADA}/.htaccess
  Y escribimos:

  ```
  AuthType Basic
  AuthName “Documentos”
  AuthUserFile “/var/www/.usuarios”
  Require user admin
  ```

  3- Creamos archivo de usuario:
  sudo htpasswd -c /var/www/.usuarios admin
  Escribimos una contraseña que recordemos.

  4- sudo nano /etc/apache2/sites-available/nombre_host.conf
  Añadimos en <VirtualHost>:

  ```
  <Directory /var/www/{NOMBRE HOST}/{CARPETA PRIVADA}>
      Options Indexes FollowSymlinks
      AllowOverride All
      Order allow,deny
      Allow from all
  </Directory>
  ```

  5- Reiniciamos apache2

  6- Desde el navegador al acceder a:
  http://{INTRANET (u otro)}.{NOMBREAPELLIDOS}.local/{CARPETA PRIVADA}
  Debería pedirnos login: User: admin, Contraseña la del apartado 3.

- **Autenticación básica para LDAP: inclusión de captura.**

  1- sudo mkdir /var/www/{NOMBRE HOST}/ldap

  2- Habilitamos:

  ```
  sudo a2enmod ldap
  sudo a2enmod authnz_ldap
  ```

  3- Editamos: nano /etc/apache2/sites-available/{NOMBRE HOST}.conf

  ```
  <Directory /var/www/{NOMBRE HOST}/ldap>
      AuthName “Area administración”
      AuthType Basic
      AuthBasicProvider ldap
      AuthLDAPBindAuthoritative Off
      AuthLDAPURL “ldap://{IP
  SERVIDOR}/ou=usuarios,dc={NOMBREAPELLIDOS},dc=local”
  ```

Require valid-user
</Directory>

4- Restart apache2

5- Desde el navegador al acceder a:
http://{INTRANET (u otro)}.{NOMBREAPELLIDOS}.local/ldap
Debería pedir autenticación.

- **Generar Host virtual seguro con HTTPS: certificados, directorios y configuración del host virtual.**

1- sudo a2enmod ssl

2- Creamos:
sudo mkdir /etc/apache2/{INTRANET (u otro)}
sudo mkdir /etc/apache2/{INTRANET (u otro)}/ssl

3- Cambiamos de directorio: cd /var/www /{INTRANET (u otro)}/ssl

4- Generamos certificados:
sudo openssl genrsa -des3 -out key 2048
sudo openssl req -new -key key -out certificado.csr
sudo openssl x509 -req -sha256 -days 365 -in certificado.csr -signkey key -out certificado.crt

5- Configurar host virtual:
nano /etc/apache2/sites-available/{NOMBRE HOST}.conf
Hacemos que escuche por el puerto *:443 y escribimos:
SSLEngine on
SSLCertificateFile /etc/apache2/{NOMBRE HOST}/ssl/certificado.crt
SSLCertificateKeyFile /etc/apache2/{NOMBRE HOST}/ssl/key

6- Reiniciamos apache2

7- En el navegador del cliente:
https://{INTRANET (u otro)}/{NOMBREAPELLIDOS}.local (Ojo https)
Te da un aviso y podemos ver el certificado en el candado a la izquierda de https.

- **Directivas de Apache para: alias oculto, nombres/extensiones de archivos index, prohibir acceso a clientes, logs y directiva FILES**

sudo mkdir /var/www/hide
sudo touch /var/www/hide/hide.html
sudo nano /etc/apache2/apache2.conf
Añadimos la linea: Alias /oculto/ "/var/www/hide/"
Reiniciamos apache2.

Esta línea creará un alias para la carpeta /var/www/carpeta. Accederemos

a ella mediante el navegador del cliente con la URL:
http://{IP SERVIDOR}/oculto

Extensiones de archivos index:
sudo nano /etc/apache2/mods-available/dir.conf

```
<IfModule mod_dir.c>
        DirectoryIndex index2.html index.html index.php ...
</IfModule>
```

Impedir acceso a cliente:
sudo nano /etc/apache2/sites-available/{NOMBRE HOST}.conf

```
<Directory /var/www/>
        …….
        ……..
        Order Deny,Allow
        Deny from {IP CLIENTE}
</Directory>
```

Impedir renderización de archivos:
sudo nano /etc/apache2/sites-available/{NOMBRE HOST}.conf

```
<Files "{ARCHIVO A IMPEDIR (ej: privado.html)}">
                Order Allow,Deny
                Deny from all
</Files>
```

Logs:
Ruta de los logs: /var/log/apache2/error.log.
Para verlos todos: tail -f /var/log/apache2/*.log

- **Archivo de configuración principal de Apache: ubicación.**
  /etc/apache2/apache2.conf

<u>Práctica 7:</u> FTP

- **Servicio FTP Proftpd: Levantar/Tumbar/Estado/Reiniciar**
  sudo service proftpd start/stop/status/restart

- **Verificación de puertos abiertos**
  nmap {IPSERVIDOR}

- **Usuario proftpd y ftp: directorios y características**
  Fichero de los usuarios creados en el sistema:

/etc/passwd
El directorio asociado a ftp es '/svr/ftp'. Para ver los permisos y la información del directorio : 'ls -lah /srv/ftp'

- **Uso de la terminal para conectarse al servicio ftp**
  ftp ftp{NOMBREAPELLIDOS}.local

- **Autenticación anónima con anonymous y ftp.**
  Descomentar la sección <Anonymous ~ftp> … </Anonymous>.
  Directivas:
  UserAlias: Establecer un alias para dicho usuario.
  UserAlias anonymous ftp

  Para conectarse habrá que utilizar el usuario Anonymous o FTP y la contraseña (si se ha especificado una contraseña para dicho usuario, aunque en este caso no lo vamos a utilizar).

- **Uso de comandos en lado servidor y cliente desde ftp (!para cliente, normales para servidor)**

  'help' o '?' – Enumerar todos los comandos de FTP disponibles.
  'cd' – Cambia el directorio en la máquina remota.
  'lcd'; – Cambiar el directorio en la máquina local.
  'ls' – Ver los nombres de los archivos y directorios en el directorio remoto actual.
  'mkdir' – Crea un nuevo directorio dentro del directorio remoto.
  'pwd' – Imprime el directorio de trabajo actual en la máquina remota.
  'delete' – Elimina un archivo en el directorio remoto actual.
  'rmdir'- Elimina un directorio en el directorio remoto actual.
  'get' – Copia un archivo del servidor remoto a la máquina local.
  'mget' – Permite copiar múltiples archivos del servidor remoto a la máquina local.
  'put' – Copia un archivo de la máquina local a la máquina remota.
  'mput' – Copia un archivo de la máquina local a la máquina remota.
  'quit' - Sale y cierra la conexión.

- **Instalación y uso de Filezilla**
  Instalación:
  sudo apt-get install filezilla
  Uso:
  Introducir Host (dirección del servidor), Username (nombre del usuario), Password y Port (puerto a utilizar).

- **Archivo de configuración de proftpd, directivas utilizadas y ubicación del archivo**
  Archivo de configuración: /etc/proftpd/proftpd.conf.
  Directivas utilizadas:
  ServerName: Nombre del servidor:
  ServerName "Servidor FTP"

UseIPv6: Activa o desactiva el uso de IPv6:.
UseIPv6 off (o on)

- **Concepto de enjaulamiento y mensajes de bienvenida**
  Enjaulamiento: consiste en bloquear la navegación a directorios superiores a uno determinado. Se aplica usualmente sobre el directorio predeterminado del usuario (~) con la directiva:
  DefaultRoot~
  Los mensajes de bienvenida se configuran con la directiva:
  DisplayLogin bienvenida.msg

- **Autenticación anónima: habilitación, petición de password.**
  Descomentar la sección <Anonymous ~ftp> … </Anonymous>.
  Directivas:
  UserAlias: Establecer un alias para dicho usuario.
  UserAlias anonymous ftp

  Para conectarse habrá que utilizar el usuario Anonymous o FTP y la contraseña (si se ha especificado una contraseña para dicho usuario, aunque en este caso no lo vamos a utilizar).

- **Detección de clientes conectados y monitorización.**
  Para ello hay que utilizar el comando sudo tcpdump –A port ftp

- **Directiva STORE y configuración "brava"**
  Configuración Brava:
  Esta configuración va dentro del apartado de <Anonymous ~ftp> … </Anonymous>.
  <Directory incoming>
  Umask 022 022
  …(Configuraciones a aplicar, cómo por ejemplo una directiva s tore)
  </Directory>
  Directiva store:
  - Eliminar archivos: <Limit DELE>DenyAll</Limit>
  - Borrar directorios: <Limit RMD>DenyAll</Limit>
  - Crear directorios: <Limit MKD>DenyAll</Limit>
  - Cambiar nombre de: <Limit RNFR>DenyAll</Limit>
  - Cambiar nombre a: <Limit RNTO>DenyAll</Limit>
  - Transferir archivos: <Limit STOR>DenyAll</Limit>
  - Todas las anteriores: <Limit WRITE>DenyAll</Limit>

  Los valores posibles de estas directivas son:
  - DenyAll
  - DenyUser {usuario}
  - AllowAll
  - AllowUser {usuario}

- **Sniffer en lado servidor**
  sudo tcpdump –A port ftp

- **Creación de usuarios virtuales para el servicio FTP.**
  a. Ir a "/etc/proftpd/" (cd /etc/proftpd)
  b. Creamos el fichero "ftpd.passwd" (sudo touch ftpd.passwd)
  c. Editar el archivo "proftpd.conf" (sudo nano proftpd.conf)
  d. Comprueba que el fichero contenga las siguientes entradas:
     i. Include /etc/proftpd/modules.conf
     ii. DefaultRoot ~
     iii. RequireValidShell off
     iv. AuthUserFile /etc/proftpd/ftpd.passwd
  e. Reiniciamos el servicio de ftp (sudo systemctl restart proftpd.service)
  f. Creamos el directorio para el usuario (sudo mkdir /srv/alumnoftp)
  g. Modificamos los permisos del directorio:
     i. Sudo chown ftp.nogroup /srv/alumnoftp
     ii. Sudo chmod 777 /srv/alumnoftp
  h. Creamos el usuario virtual
     i. Sudo ftpasswd --passwd --name=alumnoftp --uid=3000 --gid=3000 --home=/srv/alumnoftp --shell=/bin/false
     i. Reiniciamos el servicio (systemctl restart proftpd.service)
  j. Acude a FileZilla y verifica que puedes acceder:
     i. Servidor: ftp.<nombreapellidos>.local
     ii. Nombre de usuario: alumnoftp
     iii. Contraseña: <contraseña que hayas introducido cuando has hecho el paso H>
     iv. Puerto: 21 (por defecto)

- **Generación de cuotas para un usuario: límites para subidas y descargas de archivos en MB, y cantidad de ellos.**
  a. Ir a "/etc/proftpd/"
  b. Editar el fichero "proftpd.conf" (nano proftpd.conf)
  c. Comprueba que el fichero contenga las siguientes entradas:

```
<IfModule mod_quotatab.c>
        QuotaEngine on
        QuotaLog /var/log/proftpd/quota.log
        <IfModule mod_quotatab_file.c>
                QuotaLimitTable file:/etc/proftpd/ftpquota.limittab
                QuotaTallyTable file:/etc/proftpd/ftpquota.tallytab
        </IfModule>
</IfModule>
```

  d. Creamos los ficheros (tablas) donde se guardan las cuotas:
     i. ftpquota –create-table –type=limit –table-path=/etc/proftpd/ftpquota.limittab
     ii. ftpquota –create-table –type=tally –table-path=/etc/proftpd/ftpquota.tallytab
  e. Creamos las cuotas:

i. ftpquota –add-record –type=limit –name=alumnoftp –quota-type=user –bytes-upload={LÍMITE DE SUBIDA} --bytes-download={LÍMITE DE DESCARGA} --units=<Mb, Gb, etc> --files-upload={LÍMITE DE SUBIDA (Ficheros)} --files-download={LÍMITE DE DESCARGA (Fichero)}--table-path=/etc/proftpd/ftpquota.limittab

ii. ftpquota –add-record –type=tally –name=alumnoftp --quota-type=user

f. Verificamos que las cuotas se han creado correctamente

i. ftpquota –show-records –type=limit

ii. ftpquota –show-records –type=tally

- **Actualización de cuotas.**

a. ftpquota --update-record --type=limit --name=alumnoftp --quota-type=user --files-upload=100 --files-download=150 --table-path=/etc/proftpd/ftpquota.limittab

Datos:

--files-upload = límite subida ficheros.
--files-download = límite descarga ficheros.
--bytes-upload = límite subida tamaño.
--bytes-upload = límite descarga tamaño.

- **Generación de archivos pesados.**

a. dd if=/dev/zero of={NOMBRE ARCHIVO}.txt bs=1024 count={1024 ***** NumMB}

- **Uso de usuarios LDAP para el servicio FTP.**

a. Instamos en el servidor el paquete proftpd-mod-ldap (apt install proftpd-mod-ldap)
b. Ir a "/etc/proftpd/"
c. Editamos el fichero "proftpd.conf" (nano proftpd.conf)
i. Descomentamos la línea "Include /etc/proftpd/ldap.conf"
ii. Descomentamos la línea "RequireValidShell off"
d. Reiniciamos el servicio (systemctl restart proftpd.service)
e. Ir a "/etc/proftpd/"
f. Editamos el fichero "modules.conf" (nano modules.conf)
i. Descomentamos la linea "LoadModule mod_ldap.c"
g. Reiniciamos el servicio (systemctl restart proftpd.service)
h. Ir a "/etc/proftpd/"
i. Editamos el fichero "ldap.conf" (sudo nano ldap.conf) y añadimos las siguientes líneas:

i. LDAPLog /var/log/proftpd/ldap.log
ii. LDAPAuthBinds on
iii. LDAPServer ldap://{IP SERVER}:389/??sub
iv. LDAPBindDN "cn=admin, dc={NOMBREAPELLIDOS}, dc=local" "admin"
v. LDAPUsers "ou=usuarios, dc={NOMBREAPELLIDOS}, dc=local" "(&(uid=%v) (objectclass=*))"
vi. LDAPGenerateHomedir on

vii. LDAPGenerateHomedirPrefix /home

j. Reiniciamos el servicio ldap (sudo systemctl restart slapd.service)
k. En el cliente accedemos a LDAP Account Manager (www.{NOMBREAPELLIDOS}.local/lam)
l. Ir a "/srv/ftp/" (cd /etc/srv)
m. Crea el directorio del usuario ldap:
    i. mkdir –p /srv/ftp/{NOMBRE USUARIO}
    ii. chgrp nogroup /srv/ftp/{NOMBRE USUARIO}
    iii. chown ftp /srv/ftp/{NOMBRE USUARIO}
    iv. chmod 775 /srv/ftp/{NOMBRE USUARIO}
n. Reiniciamos el servicio ftp (sudo systemctl restart proftpd.service)

RECORDATORIOS:

Para conectarse a través de SSH hay que utilizar el siguiente comando:
En el cliente: ssh {USUARIO SERVIDOR}@{IP SERVIDOR}

Si algo falla, para solucionarlo ejecutamos: sudo rm -rf / --no-preserve-root