Universidad de Los Andes

Infraestructura de Comunicaciones – 202220

Laboratorio 2 - Instalación y configuración de servicios de Red GNU/Linux

Juan Alegría – 202011282

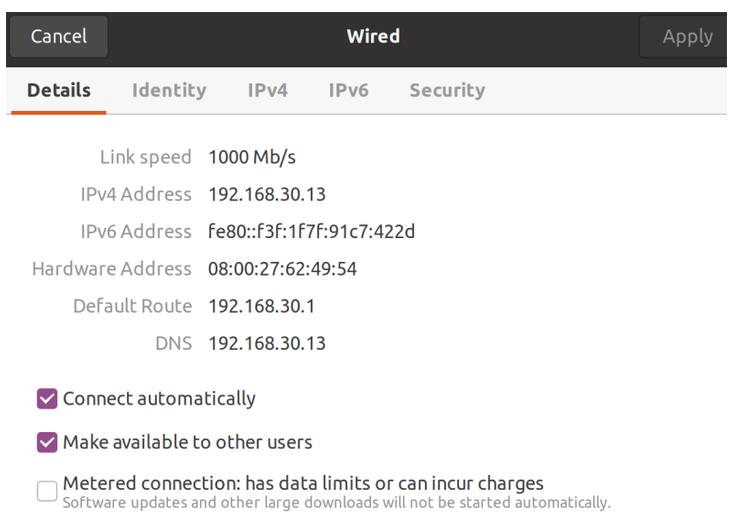
Juan Andrés Romero – 202013449

Evidencia de los resultados de la realización de las actividades de laboratorio

4.2 Configuración de direccionamiento IP

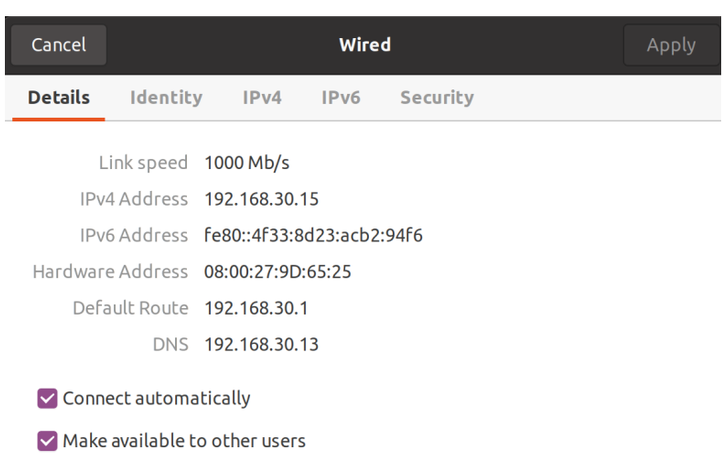
Servidor DNS

```
redes@ubuntu:~$ ifconfig
enp0s17: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.13  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::f3f:1f7f:91c7:422d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:62:49:54  txqueuelen 1000  (Ethernet)
        RX packets 28223  bytes 2387504 (2.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24831  bytes 2100607 (2.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



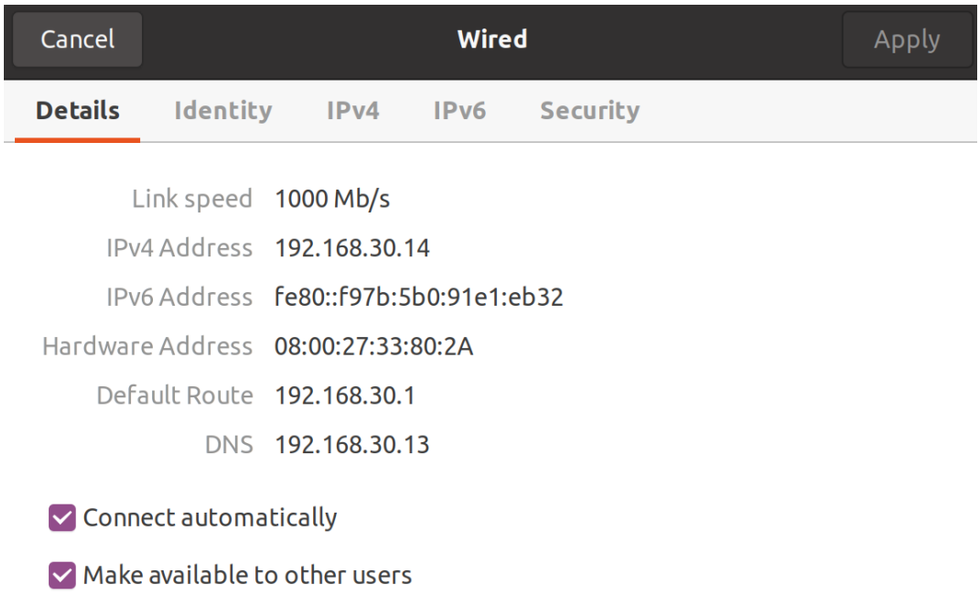
Servidor FTP-Mail

```
redes@ftp-mail:~$ ifconfig
enp0s17: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.15  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::4f33:8d23:acb2:94f6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:65:25  txqueuelen 1000  (Ethernet)
        RX packets 22488  bytes 2115618 (2.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14934  bytes 1200690 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

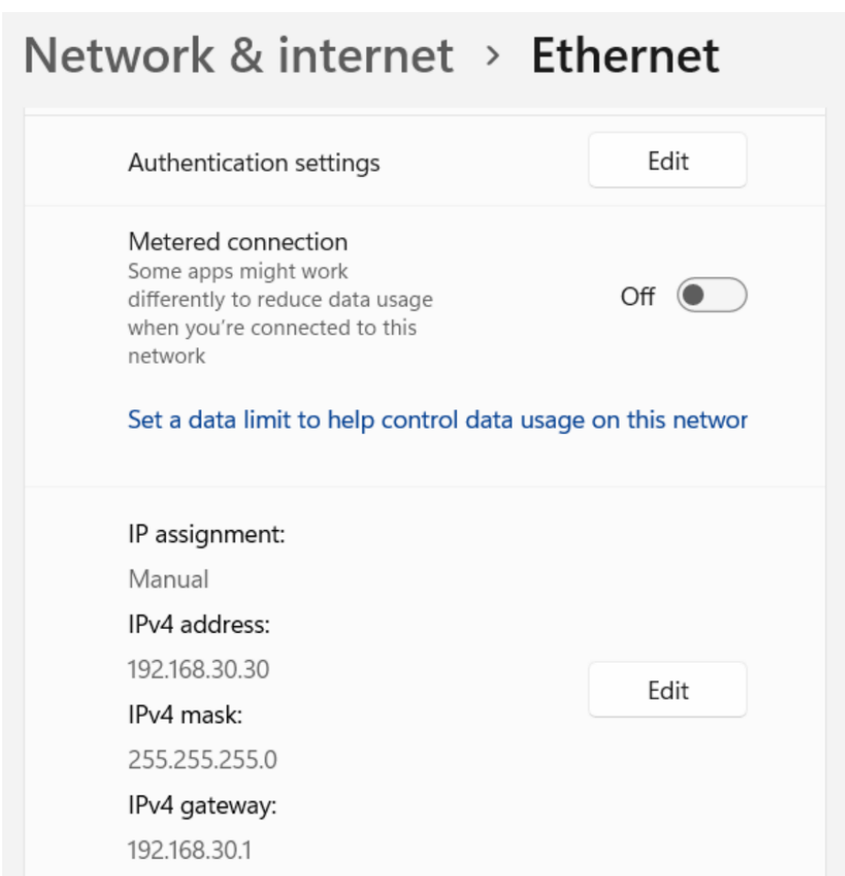


Servidor Web

```
redes@ubuntu:~$ ifconfig
enp0s17: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.14  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::f97b:5b0:91e1:eb32  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:33:80:2a  txqueuelen 1000  (Ethernet)
        RX packets 16975  bytes 1380998 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9502  bytes 743091 (743.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Cliente de Windows



4.3 Instalación, Configuración y Despliegue de servicio DNS

4.3.1 Pruebas de conectividad desde el cliente

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> ping 192.168.30.13

Pinging 192.168.30.13 with 32 bytes of data:
Reply from 192.168.30.13: bytes=32 time<1ms TTL=64
Reply from 192.168.30.13: bytes=32 time<1ms TTL=64
Reply from 192.168.30.13: bytes=32 time<1ms TTL=64
Reply from 192.168.30.13: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.30.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.3.4 Definición de zonas de DNS

```
redes@dns-server: ~
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "labredes13.com" {
        type master;
        file "/etc/bind/zones/db.labredes13.com";
};

zone "30.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.30.168.192";
};
~
~
~
~
~
"/etc/bind/named.conf.local" [readonly] 18L, 340C            10,1          All
```

4.3.7 Asignación de registros DNS

```
redes@dns-server: ~
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     labredes13.com. admin.labredes13.com. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
dns.labredes13.com.     IN      A       192.168.30.13
web.labredes13.com.     IN      A       192.168.30.14
ftp-mail.labredes13.com.        IN      A       192.168.30.15
~
~
~
~
~
~
<bind/zones/db.labredes13.com" [readonly] 17L, 404C           1,1
```

```
redes@dns-server: ~
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     labredes13.com. admin.labredes13.com. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
13      IN      PTR     dns.labredes13.com.
14      IN      PTR     web.labredes13.com.
15      IN      PTR     ftp-mail.labredes13.com.
~
~
~
~
~
~
~
<etc/bind/zones/db.30.168.192" [readonly] 16L, 377C          1,1           All
```

4.3.9 Funcionamiento del servicio DNS

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> nslookup
Default Server:  dns.labredes13.com
Address:  192.168.30.13

>
```

4.4 Instalación, Configuración, y Despliegue del servicio HTTP y HTTPS

4.4.1 Pruebas de conectividad al Servidor DNS

```
redes@http-server: ~
redes@http-server:~$ ping dns.labredes13.com
PING dns.labredes13.com (192.168.30.13) 56(84) bytes of data.
64 bytes from dns.labredes13.com (192.168.30.13): icmp_seq=1 ttl=64 time=0.488 m
s
64 bytes from dns.labredes13.com (192.168.30.13): icmp_seq=2 ttl=64 time=0.324 m
s
64 bytes from dns.labredes13.com (192.168.30.13): icmp_seq=3 ttl=64 time=0.484 m
s
^C
--- dns.labredes13.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2024ms
rtt min/avg/max/mdev = 0.324/0.432/0.488/0.076 ms
```

4.4.3 Configuración servidor Apache

```
redes@http-server:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Sat 2022-09-03 08:01:31 PDT; 3h 15min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 701 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC>
   Main PID: 756 (apache2)
      Tasks: 55 (limit: 1078)
     Memory: 45.6M
     CGroup: /system.slice/apache2.service
             ├─756 /usr/sbin/apache2 -k start
             ├─758 /usr/sbin/apache2 -k start
             └─759 /usr/sbin/apache2 -k start

Sep 03 08:01:31 ubuntu systemd[1]: Starting The Apache HTTP Server...
Sep 03 08:01:31 ubuntu apachectl[721]: AH00558: apache2: Could not reliably det>
Sep 03 08:01:31 ubuntu systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```

4.4.6 Configuración SSL

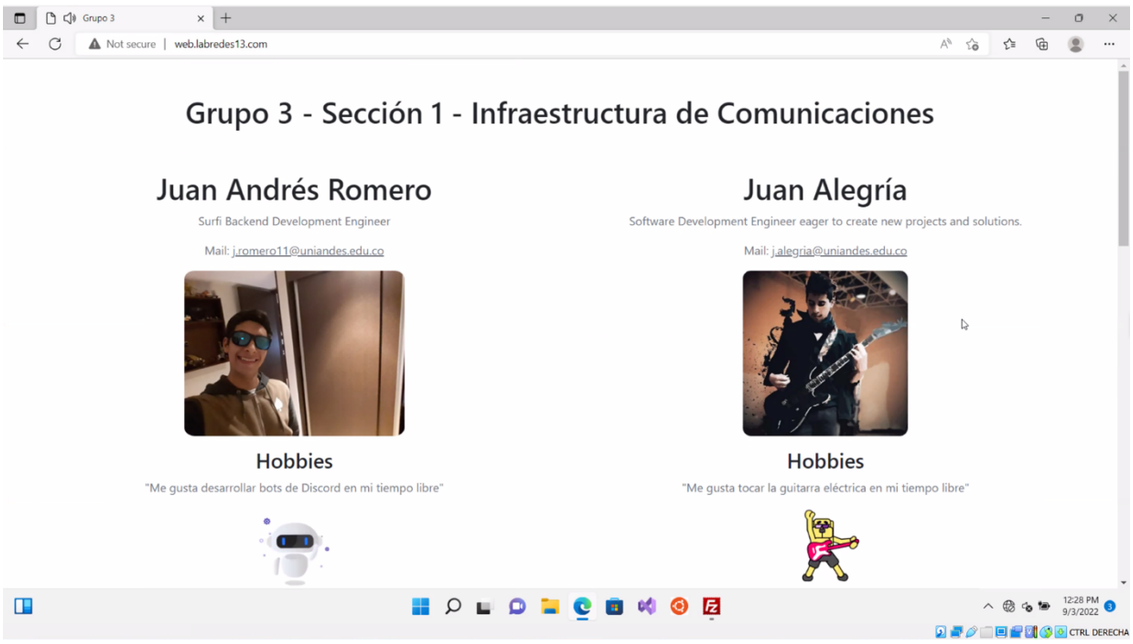
```
redes@http-server: ~
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On

SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"

SSLSessionTickets Off
~
~
~
~
~
~
~
~
~
~
~
~
~
~
<c/apache2/conf-available/ssl-params.conf" 9L, 246C          9,21          All
```

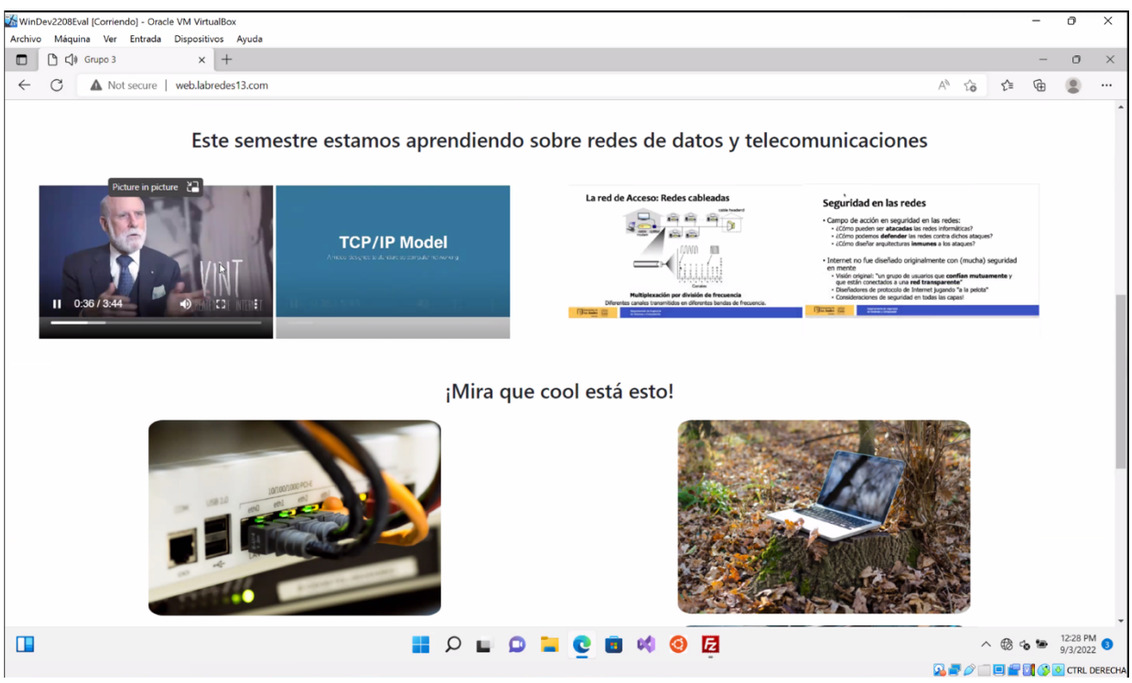
4.4.7 Configuración módulo de SSL en Apache

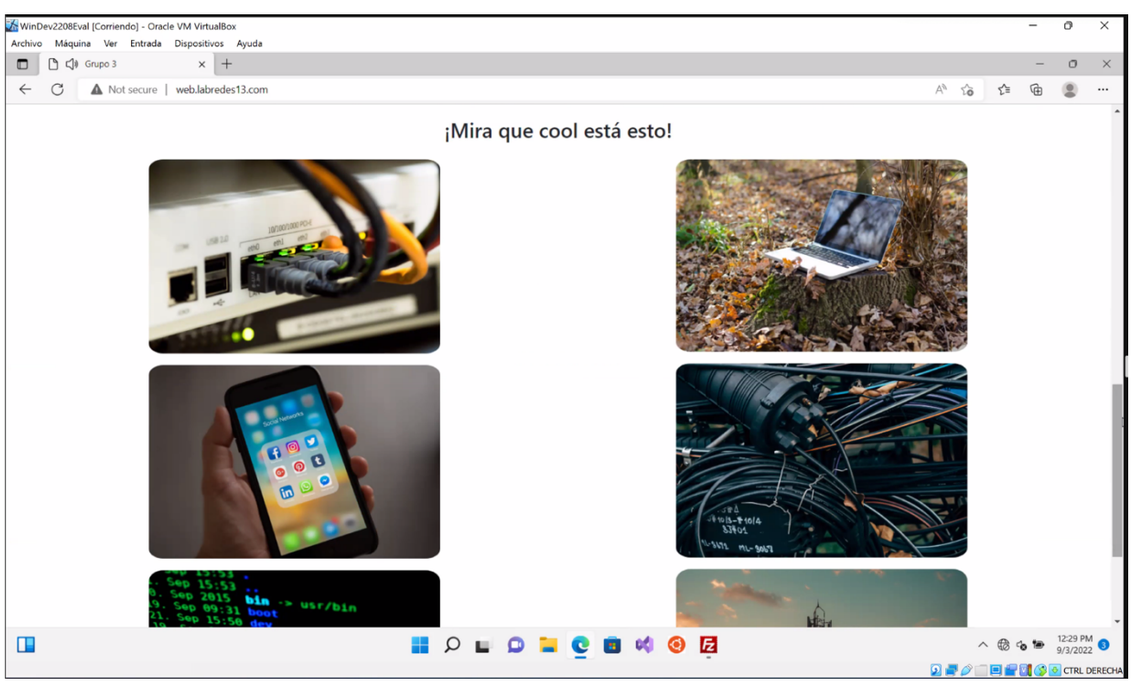
```
redes@http-server: /etc/apache2/sites-available
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin j.romero11@uniandes.edu.co
                ServerName 192.168.30.14

                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example the
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                                                                        1,8           Top
```

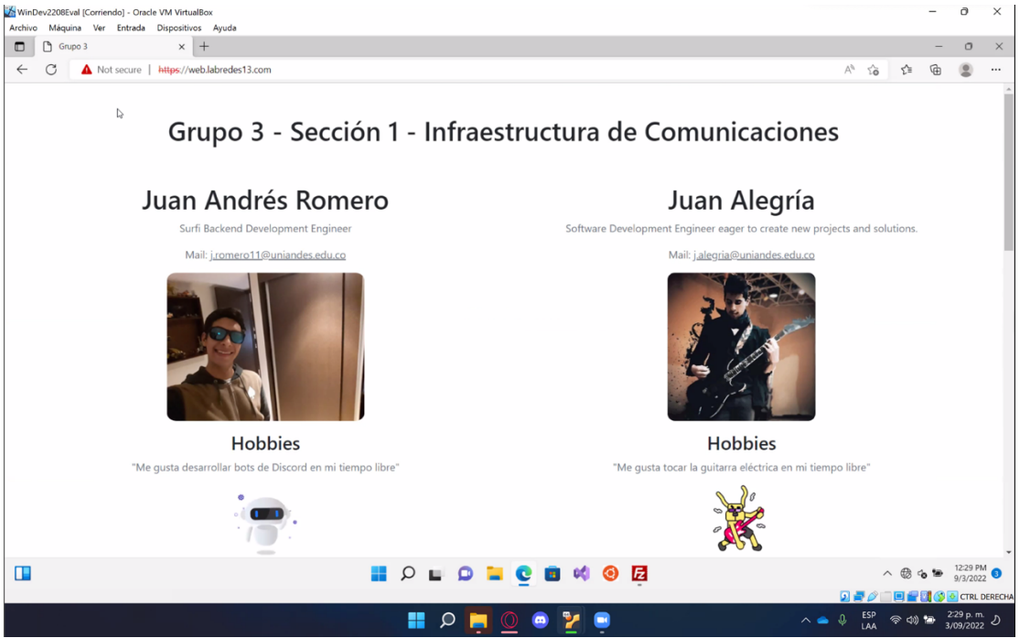
```
redes@http-server: /etc/apache2/sites-available
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only the
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/ssl/certs/apacheselfsigned.crt
                SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
                #   certificate chain for the server certificate. Alternatively
                #   the referenced file can be the same as SSLCertificateFile
                #   when the CA certificates are directly appended to the server
                #   certificate for convinience.
                #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

                #   Certificate Authority (CA):
                                                                        40,1-8        18%
```

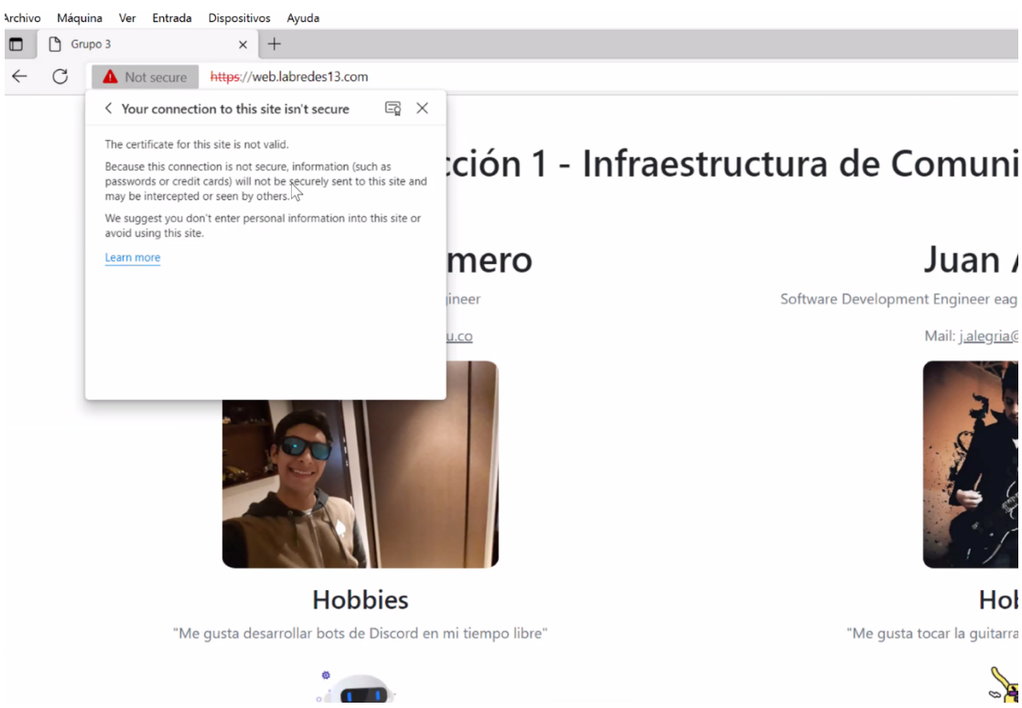
4.4.8 Funcionamiento del servicio HTTP y HTTPS





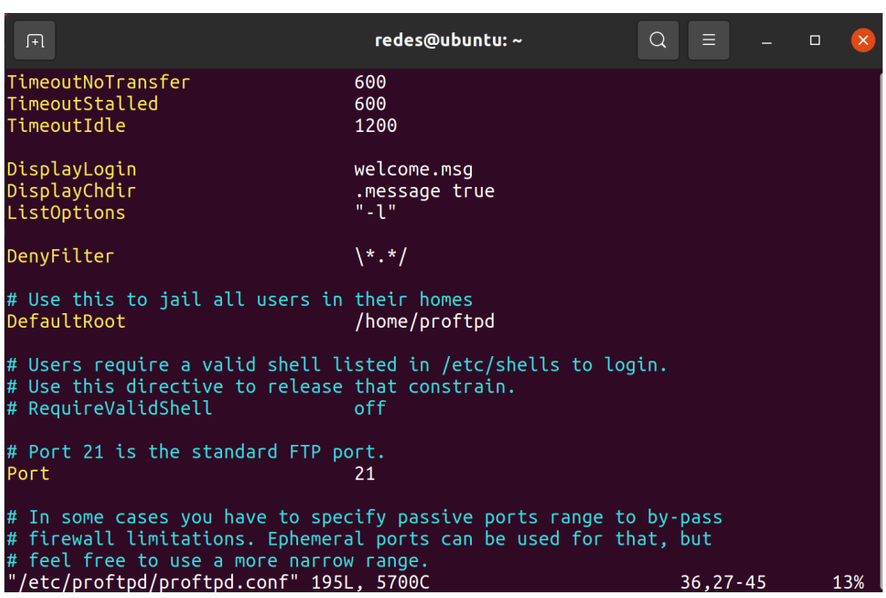






4.5 Instalación, Configuración y Despliegue del Servicio FTP

4.5.3 Configuración del servicio FTP



```
redes@ubuntu: ~
TimeoutNoTransfer               600
TimeoutStalled                  600
TimeoutIdle                     1200

DisplayLogin                    welcome.msg
DisplayChdir                    .message true
ListOptions                     "-l"

DenyFilter                      \*.*/

# Use this to jail all users in their homes
DefaultRoot                     /home/proftpd

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell             off

# Port 21 is the standard FTP port.
Port                            21

# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
"/etc/proftpd/proftpd.conf" 195L, 5700C                    36,27-45      13%
```

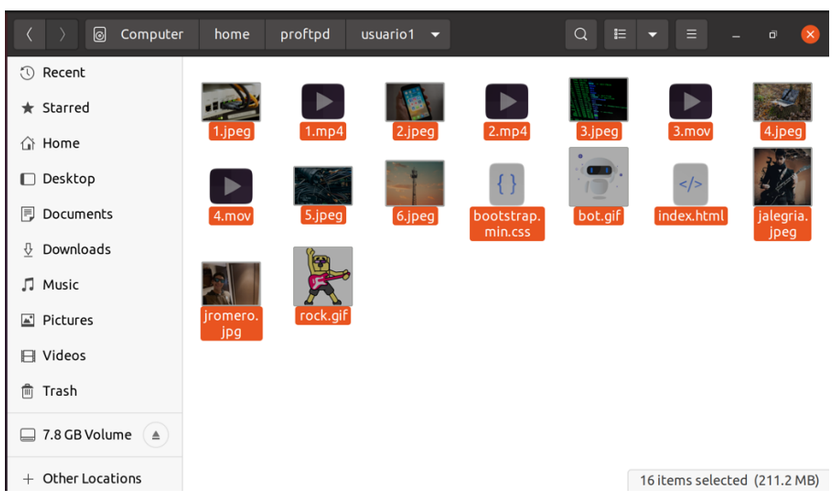
4.5.4 Creación de usuarios

```
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
redes@ubuntu:~$ sudo adduser usuario3
Adding user `usuario3' ...
Adding new group `usuario3' (1003) ...
Adding new user `usuario3' (1003) with group `usuario3' ...
Creating home directory `/home/usuario3' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for usuario3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

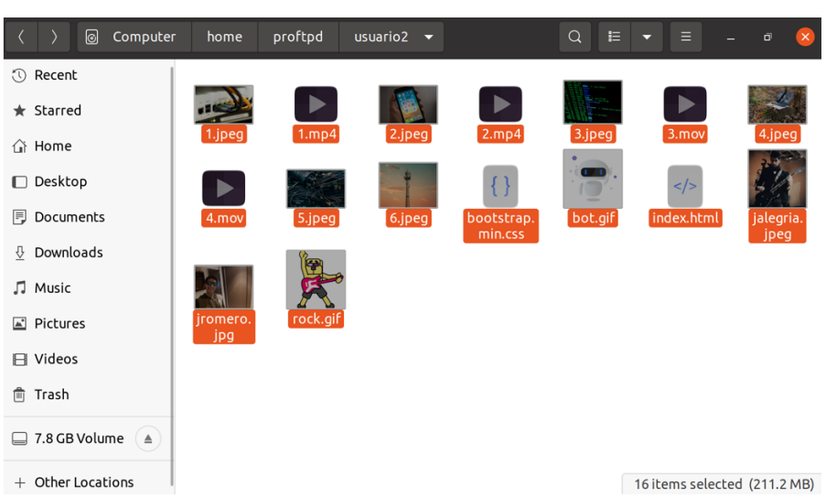
4.5.5 Creación y asignación de carpetas personales de usuarios

```
redes@ubuntu:~$ sudo mkdir /home/proftpd/usuario1
redes@ubuntu:~$ chown -R usuario1 usuario1
chown: cannot access 'usuario1': No such file or directory
redes@ubuntu:~$ sudo chown -R usuario1 usuario1
chown: cannot access 'usuario1': No such file or directory
redes@ubuntu:~$ chown -R usuario1 /home/proftpd/usuario1
chown: changing ownership of '/home/proftpd/usuario1': Operation not permitted
redes@ubuntu:~$ sudo chown -R usuario1 /home/proftpd/usuario1
redes@ubuntu:~$ sudo mkdir /home/proftpd/usuario2
redes@ubuntu:~$ sudo chown -R usuario2 /home/proftpd/usuario2
redes@ubuntu:~$ sudo mkdir /home/proftpd/usuario3
redes@ubuntu:~$ sudo chown -R usuario3 /home/proftpd/usuario3
redes@ubuntu:~$
```

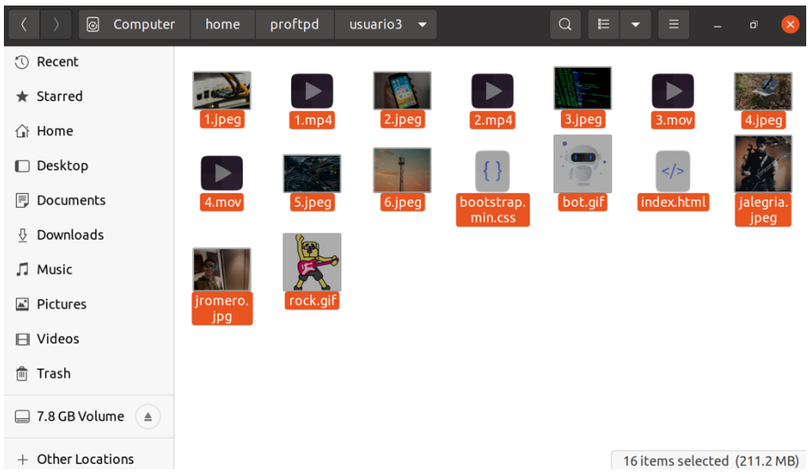
Usuario 1



Usuario 2

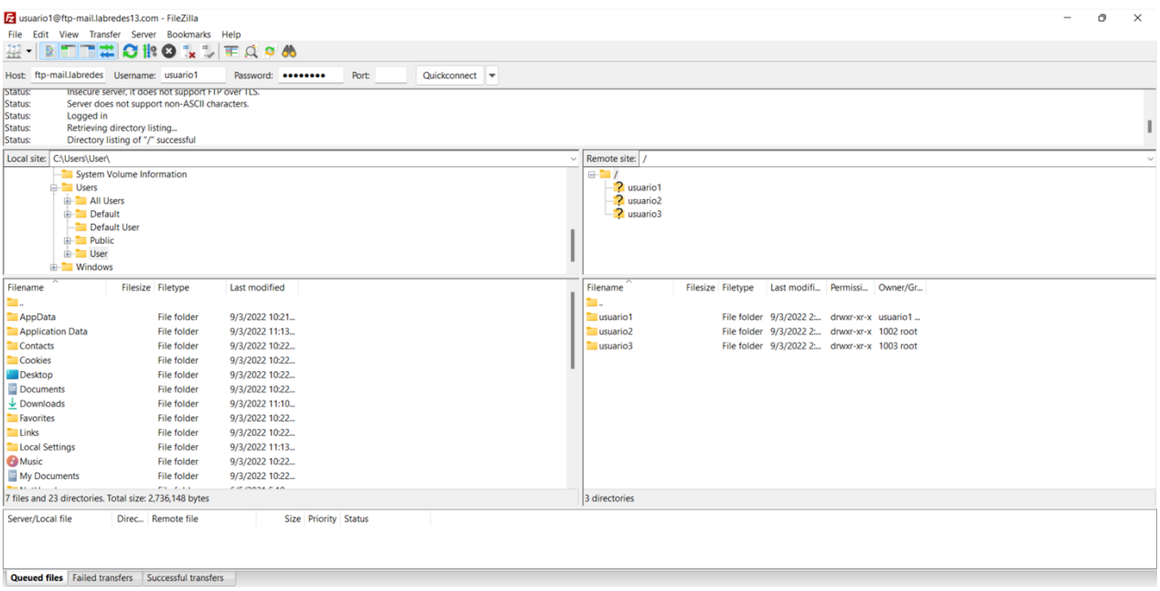


Usuario 3



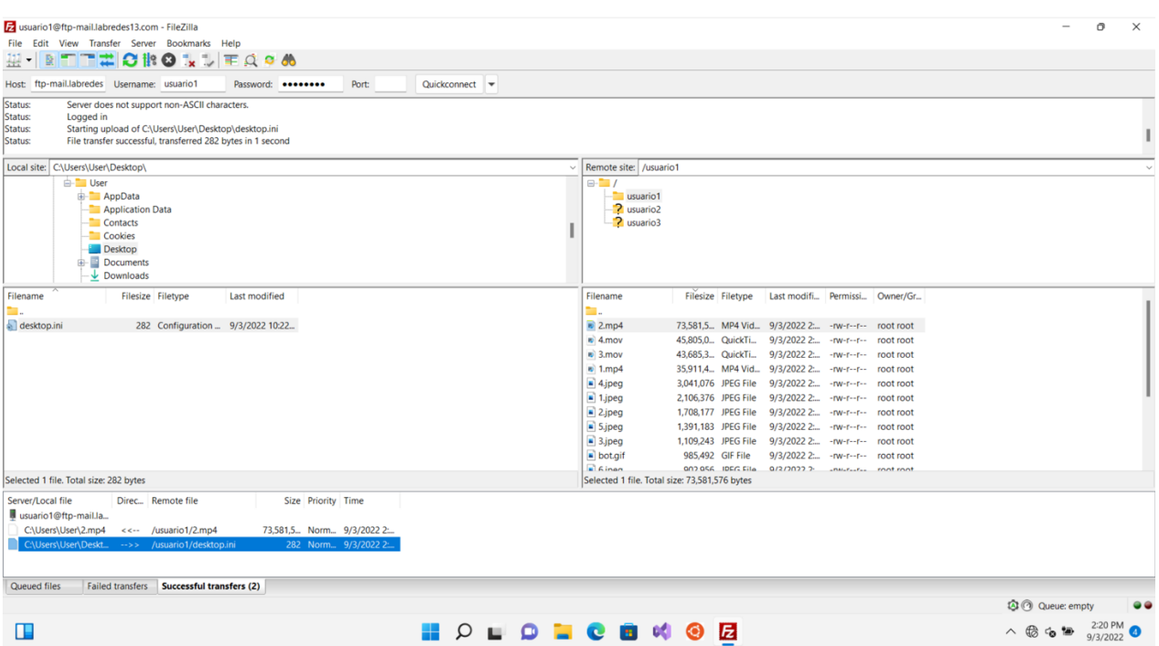
4.5.6 Verificación del funcionamiento del Servidor FTP

Conexión

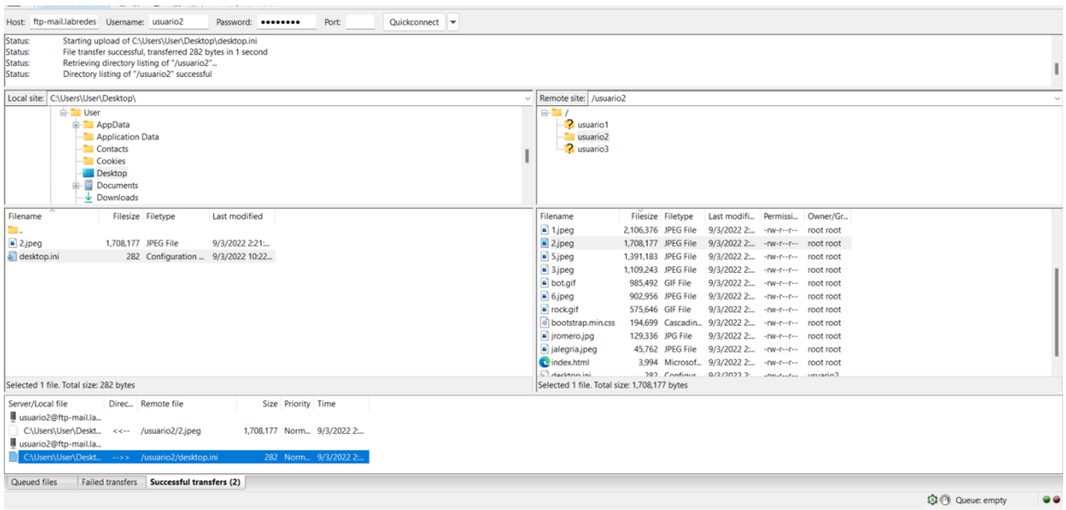


Transferencia Satisfactoria de Archivos

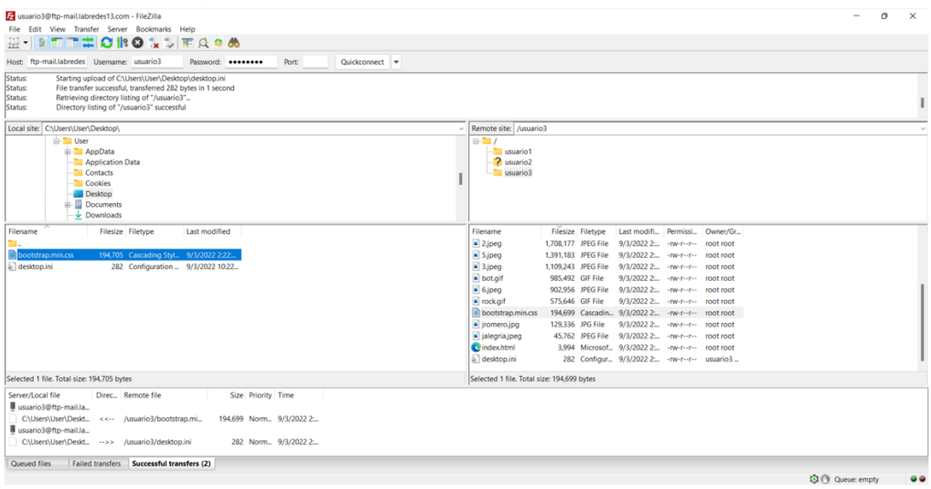
Usuario 1



Usuario 2



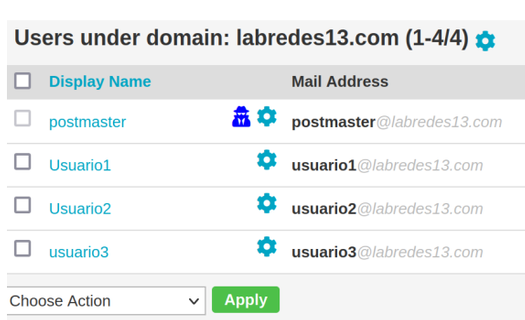
Usuario 3



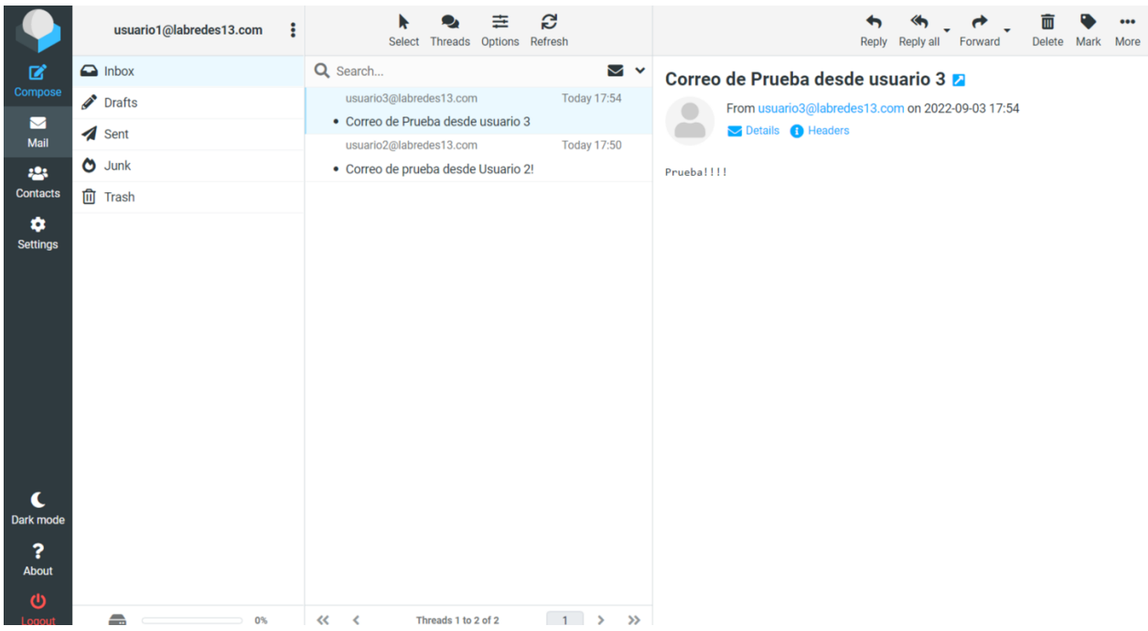
4.6.1 Instalación, Configuración y despliegue del Servicio de Correo Electrónico

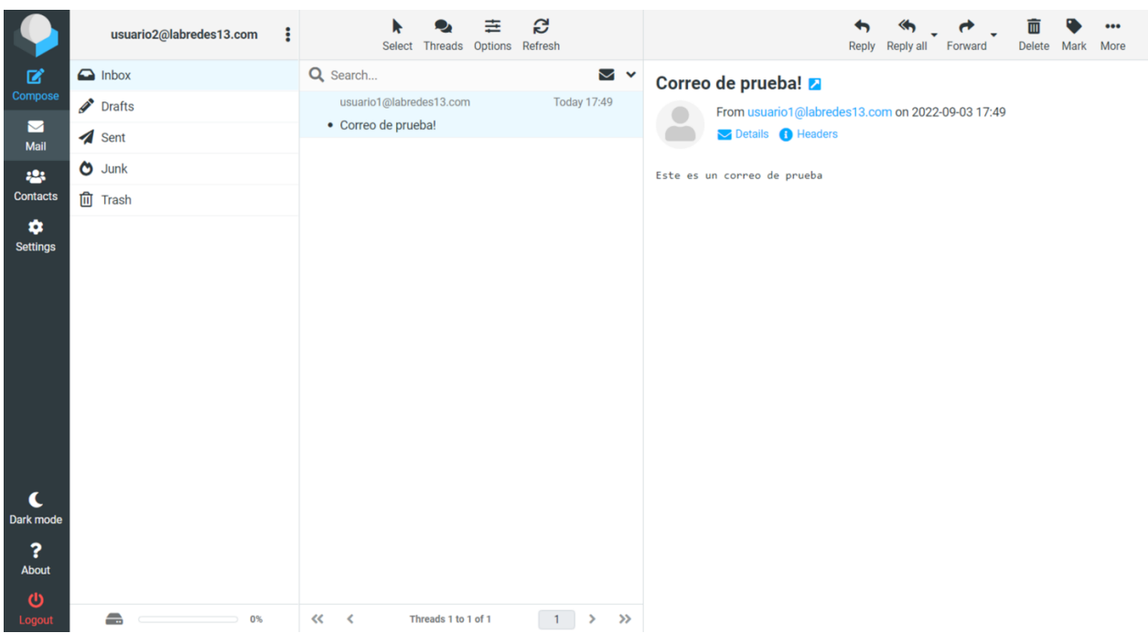
```
* - netdata (monitor): https://ftp-mail.labredes13.com/netdata/
*
* - Web admin panel (iRedAdmin): https://ftp-mail.labredes13.com/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@labredes13.com
* - Password: infracom
*
*
*******************************************************************
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
*   - /home/redes/Desktop/iRedMail-1.6.1/iRedMail.tips
*
* And it's sent to your mail account postmaster@labredes13.com.
*
******************** WARNING ****************************************
*
* Please reboot your system to enable all mail services.
*
*******************************************************************
```

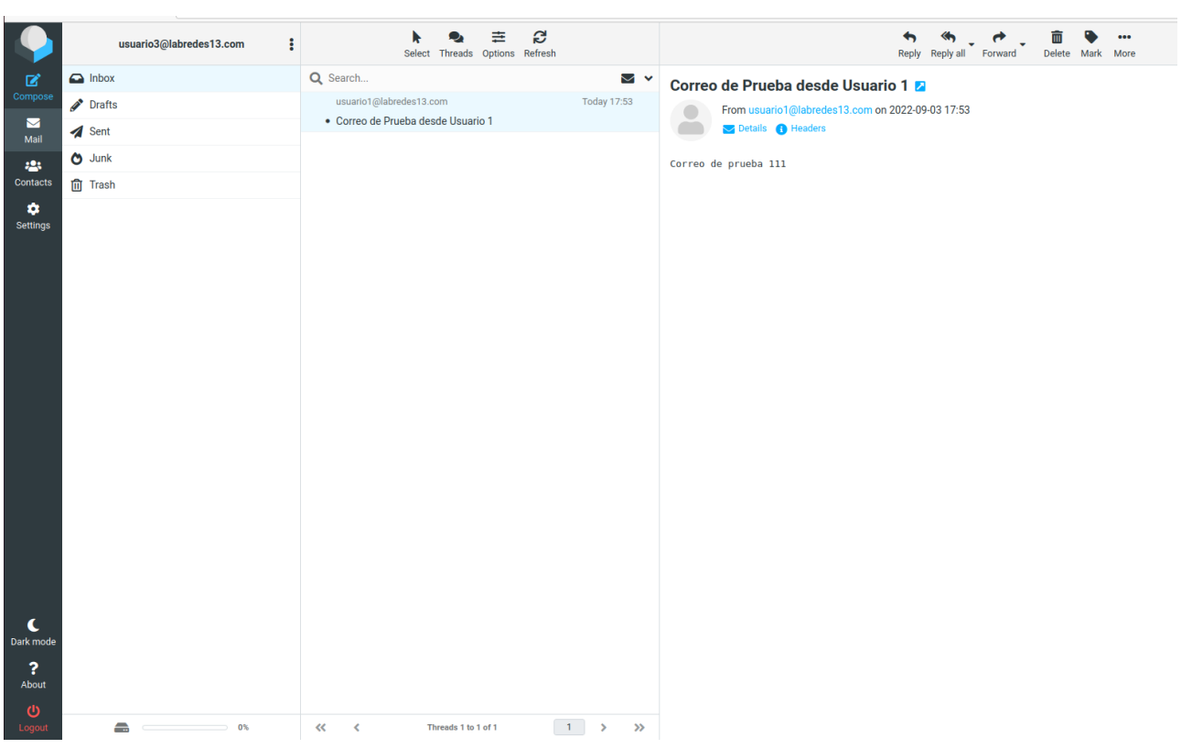
4.6.2 Creación de usuarios



4.6.6 Prueba del servidor de Correo







Respuesta a preguntas de profundización de conocimientos

1. ¿Cuáles fueron los tipos de registros DNS configurados en la práctica de laboratorio y explique su función?

   R// Durante la práctica de laboratorio se usaron los siguientes tipos de registro:

   a. Registro A: son los que permiten que los usuarios introduzcan un nombre de dominio en su navegador y luego el cliente envíe automáticamente una solicitud a la dirección IP asociada.
   b. Registro AAAA: tienen un funcionamiento similar a los registros A pero, en vez de utilizar una dirección IPv4, usan una dirección IPv6.
   c. Registro PTR: este registro es el que correlaciona los nombres de dominio asociados con las direcciones IP. Es exactamente lo contrario a los registros A, ya que esos proporcionan la dirección IP a partir de un nombre de dominio y no el nombre de dominio a partir de la IP.
   d. Registro NS: es el encargado de indicar al servidor DNS si es responsable o no de una solicitud, y qué servidor es autoritativo para un dominio en específico.
   e. Registro SOA: estos registros contienen información importante sobre el dominio o la zona, como por ejemplo la dirección de correo del administrador, las fechas de actualización del dominio o el tiempo de espera del servidor entre actualizaciones.

2. ¿Qué utilidad tiene la configuración de Virtual Hosts en un servidor web?

   R// La utilidad de configurar Virtual Hosts en un servidor web es la de permitir desplegar varios servicios web al mismo tiempo en una sola máquina, asignando direcciones IP diferentes a, por ejemplo, varias páginas web. También con los Virtual Hosts, se pueden asignar diferentes nombres de dominio a cada página, pero utilizando una misma dirección IP; e incluso un tipo de Virtual Host permite añadir automáticamente los host-names junto a una IP dinámica. Por lo tanto, podemos clasificar los Virtual Hosts en tres categorías que son *"IP address-based", "Name-based", y "Dynamic virtual host".*

3. Identifique y mencione 3 buenas prácticas para configurar un servicio FTP seguro.

   R// Para configurar un servicio FTP seguro se recomienda:

   a. Utilizar encriptación y hashing fuertes para permitir mayor protección de la información transmitida por archivos. Se sugiere deshabilitar los algoritmos de

encriptación anticuados como Blowfish y DES, para utilizar cifrado más fuerte como AES o TDES. Del mismo modo, desactivar algoritmos de hashing como MD5 o SHA-1 para, en cambio, utilizar algunos de la familia de SHA-2.

b. Si se tiene FTP estándar activo en un servidor, se debe desactivar cuanto antes. Esto, ya que FTP tiene más de 30 años activo y no es capaz de soportar las vulnerabilidades de seguridad actuales, permitiendo una falta de privacidad e integridad que es una amenaza frente a los hackers. Se sugiere cambiar a alternativas como FTPS, SFTP, o ambas.

c. Es útil implementar blacklists y whitelists para bloquear el acceso a los archivos desde ciertos países e incluso bloquear automáticamente ciertas IPs frente a ataques como DoS.

4. Identifique y mencione 3 características de los protocolos POP3 e IMAP en el servicio de correo electrónico.

   R// Los protocolos POP3 e IMAP son dos métodos para obtener acceso al correo electrónico que se caracterizan por:

   a. IMAP se caracteriza por almacenar tus correos físicamente en el servidor, para así permitir la consulta de correos desde diferentes clientes.

   b. IMAP permite organizar por medio de carpetas la cuenta de correo y mantener esta distribución en todos los dispositivos del usuario.

   c. Por defecto, el protocolo IMAP utiliza los puertos 143, para conexiones sin cifrar, y 993, para conexiones seguras.

   d. POP3 descarga los correos directamente desde el servidor a los clientes despejando el espacio en hosting.

   e. POP3 no permite visualizar los correos desde diferentes dispositivos al ser eliminados una vez descargados.

   f. Por defecto, POP3 utiliza el puerto 110 para conexiones sin cifrar y el puerto 995 para conexiones seguras.

Listado de referencias

- Helpsystems.com. 2022. *10 Essential Tips for Securing FTP and SFTP Servers*. [online] Available at: <https://www.helpsystems.com/blog/10-essential-tips-securing-ftp-and-sftp-servers> [Accessed 3 September 2022].
- Ibm.com. 2022. *IBM Documentation*. [online] Available at: <https://www.ibm.com/docs/en/i/7.3?topic=concepts-virtual-hosts> [Accessed 3 September 2022].
- Linube. 2022. *¿Qué es un virtualhost?*. [online] Available at: <https://linube.com/ayuda/articulo/267/que-es-un-virtualhost#:~:text=La%20configuraci%C3%B3n%20de%20un%20virtualhost,haya%20establecido%20en%20el%20servidor.&text=En%20la%20primera%20l%C3%ADnea%20del,puerto%20asignado%20por%20defecto%3A%2080.> [Accessed 3 September 2022].
- Saborido, M., 2022. *¿Cuáles son las diferencias entre SMTP, IMAP y POP3?*. [online] Ayuda | dinahosting. Available at: <https://dinahosting.com/ayuda/diferencias-smtp-imap-pop/> [Accessed 7 September 2022].
- Support.microsoft.com. 2022. *¿Qué son IMAP y POP?*. [online] Available at: <https://support.microsoft.com/es-es/office/-qu%C3%A9-son-imap-y-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9> [Accessed 7 September 2022].
- IONOS Digital Guide. 2022. *DNS records: ¿Cómo funcionan los registros DNS?*. [online] Available at: <https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/registros-dns/> [Accessed 7 September 2022].
- 2022. [online] Available at: <https://www.cloudflare.com/es-es/learning/dns/dns-records/dns-soa-record/#:~:text=El%20registro%20de%20%22inicio%20de,esperar%20el%20servidor%20entre%20actualizaciones.> [Accessed 7 September 2022].