



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Fons Social Europeu

L'FSE inverteix en el teu futur

# EJERCICIOS UNIDAD TRABAJO 2

## GENERACIÓN DE UN *HIDDEN SERVICE*

---

### INVESTIGACIÓN EN FUEBTES ABIERTAS (OSINT)

Esta unidad didáctica se ha desarrollado para el Curso de Especialización de Ciberseguridad en entornos de las Tecnologías de la Información. En concreto para el módulo de Puesta en Producción Segura, cuyos aspectos básicos del currículo vienen recogidos en el Real Decreto 479/2020.

**Licencia:** Creative Commons Atribución - No Comercial -Compartir Igual (CC BY-NC-SA 4.0)

**José Gaspar Sánchez García.**

|                             |  |
|-----------------------------|--|
| <b>NOMBRE Y APELLIDOS :</b> | <i>ALUMNO/A [Jose Francisco Murcia Fuentes]</i>  |
| <b>FECHA DE COMIENZO</b>    | <i>[1/05/2025]</i>   |
| <b>ENLACE GITHUB</b>        | <i><a href="https://github.com/murcieta-gva/Tareas/blob/564261f4e37268e2e98d87c9d9e35afa96b8158f/Murcia-Jose-Francisco-Tarea%202.docx">https://github.com/murcieta-gva/Tareas/blob/564261f4e37268e2e98d87c9d9e35afa96b8158f/Murcia-Jose-Francisco-Tarea%202.docx</a></i> |

## Normas de entrega:

### Corrección:

- 📈 Por cada día de retraso sin justificación en la entrega, se restará 1 punto a la nota.
- ✌️ Es muy importante cuidar la presentación y limpieza de las respuestas entregadas al profesor.

### Forma de Entrega:

- A través de la plataforma Moodle GVA AULAS: <https://aulas.edu.gva.es/> **Documentos a entregar:**
- Este mismo fichero con las preguntas llenadas (usar fuente Verdana de tamaño 12 color azul en cursiva – **Estilo Respuesta**): **[Respuesta]**
- Cambia el nombre al documento, y añade tu primer apellido y tu nombre al final.
- Documento con la respuesta a las cuestiones y explicación al desarrollo de la práctica, En formato del documento **PDF**.

### Normas:

- Realizar los ejercicios sobre una máquina virtual **Debian Linux PePS-JFMF** como máquina atacante para realizar la penetración.
- - Preparamos una máquina **OSINTLinux PePS-<codId>**, que utilizaremos para instalar las distintas plataformas de entrenamiento.
- Cambiar **<codId>** por las iniciales de tu nombre y apellidos, más el año actual. Ejemplo: José Gaspar Sánchez García → **JGSG25**.
- Las respuestas deben ir entre los corchetes **[ ]**
- **Capturar pantallas completas**, donde se observe el nombre de la máquina virtual creada.
- Los enunciados de los ejercicios deben aparecer claramente con las respuestas a los ejercicios.

En caso de que se detecte copia o plagio con los ejercicios de otros compañeros, se invalidará la nota del ejercicio.

## Índice:

|  |    |
|--|----|
| 1. Enunciado .....   | 6  |
| 2. Conceptos previos .....   | 6  |
| 2.1. TOR .....   | 6  |
| 2.2. Hidden Services .....   | 6  |
| 3. Instalación Debian con servidores Web, FTP, SSH e IRC .....                 | 8  |
| 3.1. Instalación de un servidor Debian en Virtual Box .....                    | 8  |
| 3.2. Instalamos Apache 2, PHP y phpMyAdmin .....                               | 24 |
| 3.3. Generamos la página HTML que contiene el servicio oculto .....            | 28 |
| 3.4. Instalamos Servidor FTP ( <i>File Transfer Protocol</i> ) .....           | 29 |
| 3.5. Instalamos servidor Open SSH.....   | 30 |
| 3.6. Instalamos y configuramos IRC .....                                       | 32 |
| 4. Generación de <i>Hidden Services</i> en la red TOR .....                    | 35 |
| 4.1. Instalamos TOR y paquetes adicionales .....                               | 35 |
| 4.2. Configuración de los Hidden Services .....                                | 36 |
| 5. Lanzamiento de TOR .....  | 37 |
| 6. Verificación local de los <i>Hidden Services</i> .....                      | 38 |
| 6.1. Verificación del servicio web oculto en TOR .....                         | 38 |
| 6.2. Verificación local Hidden Service FTP .....                               | 39 |
| 6.3. Verificación de funcionamiento local Hidden Service SSH .....             | 40 |
| 6.4. Verificación de funcionamiento local <i>Hidden Service</i> chat IRC ..... | 41 |
| 7. Verificación remota de los <i>Hidden Services</i> .....                     | 42 |
| 7.1. Verificación del servicio web oculto en TOR .....                         | 42 |
| 7.2. Verificación del servicio FTP oculto en TOR .....                         | 42 |
| 7.3. Verificación del servicio SSH oculto en TOR .....                         | 43 |
| 7.4. Verificación del servicio IRC oculto en TOR .....                         | 45 |
| 8. Conclusión .....  | 45 |
| 9. Referencias .....   | 46 |

# 1. Enunciado

---

El objetivo de esta tarea es generar un **Hidden Service** en una máquina virtual y acceder al mismo desde otra máquina a través de la **red Tor**:

Para el cumplimiento de los objetivos básicos, el alumno tendrá que generar un *hidden service* a partir de un *servidor Web* como *Apache* exponiéndolo en la red *Tor*.

Para conseguir puntuación adicional, se pueden configurar más de un *hidden service* en la máquina, por ejemplo, *hidden services* de acceso remoto por SSH o FTP así como servidores IRC entre otros.

Se debe también responder a la siguiente pregunta teniendo en mente la privacidad del usuario:  
¿Es mejor utilizar un mismo dominio **.onion** mapeando diferentes puertos al mismo **.onion** o es mejor generar **hidden services** diferentes?

# 2. Conceptos previos

---

## 2.1. TOR

La red conocida como TOR debe su nombre a las siglas en inglés “**The Onion Router**” o también conocido como el encaminador cebolla. Su origen se debe al trabajo realizado en 2003 por Roger Dingledine, Nick Mathewson y Paul Syverson a partir del proyecto desarrollado por el Laboratorio Naval de EE.UU. conocido como Onion Router. Desde 2005 hasta la actualidad es propiedad de la fundación sin ánimo de lucro Tor Project. [1]

Tor es un software multiplataforma gratuito que implementa una red de comunicaciones distribuida, cifrada, de baja latencia y superpuesta a Internet. En ella, el enrutamiento de paquetes se realiza ocultando la dirección IP de los usuarios, con lo que se consigue el anonimato en la capa IP o de red.

Para que esto sea posible es imprescindible que el camino o ruta sea impredecible, y en la medida de lo posible oculto, de forma que cada nodo sólo conozca el nodo anterior, del cual recibe el mensaje y el nodo siguiente, al cual enviará el mismo, sin que pueda saber si tanto uno como el otro son o no los nodos iniciales o finales respectivamente. Este nodo final, si la comunicación es realizada con una entidad fuera de la red “*onion*”, enviará su mensaje o petición en abierto, es decir no estará cifrado. La red TOR crea, por defecto, rutas de tres nodos. Los circuitos tienen una vida de diez minutos para seleccionar posteriormente, una nueva ruta. [2]

## 2.2. Hidden Services

Los **Hidden services** o servicios ocultos [3] son la principal característica de Tor y la gran ventaja que tiene sobre otros medios de comunicación anónima ya que permite desarrollar y ofrecer un servicio sobre internet (como puede ser una página Web, un chat, un servidor de correo, etc.) sin que ninguno de los usuarios conozca realmente su ubicación. Así tanto usuario como proveedor de servicios establecen una conexión a través de la red TOR sin que estos se conozcan.

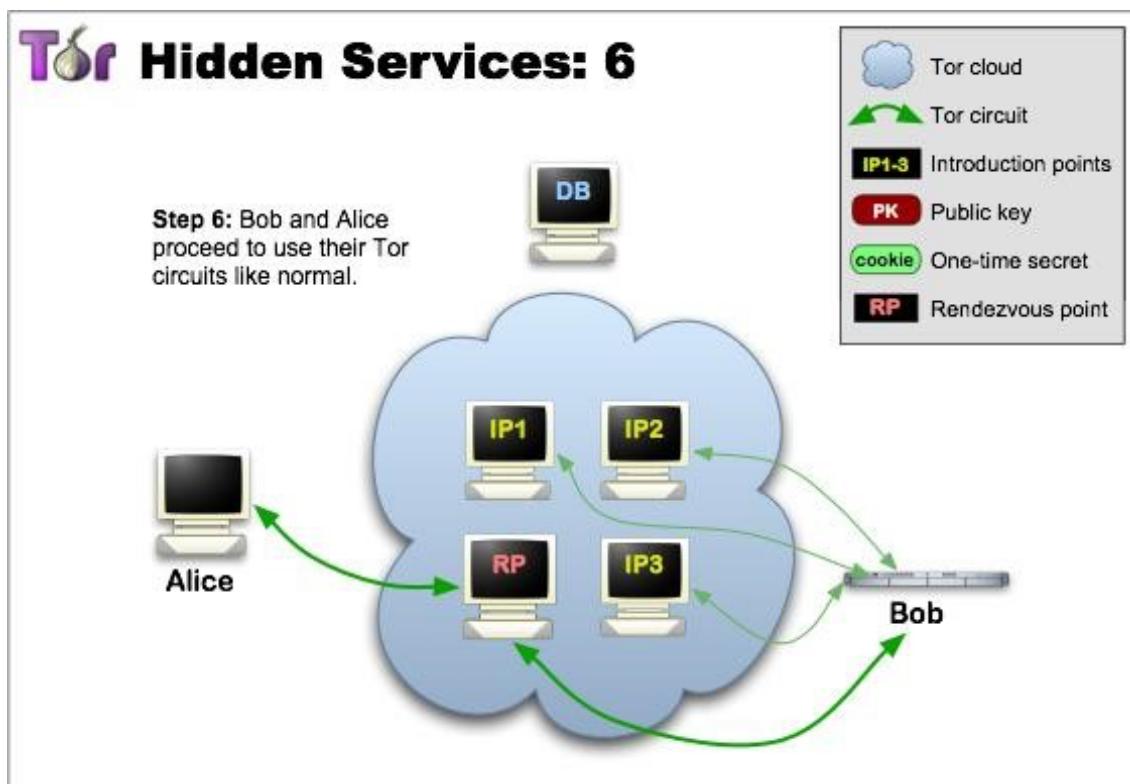


Figura 1. Conexión entre un cliente de Tor y un servicio oculto.

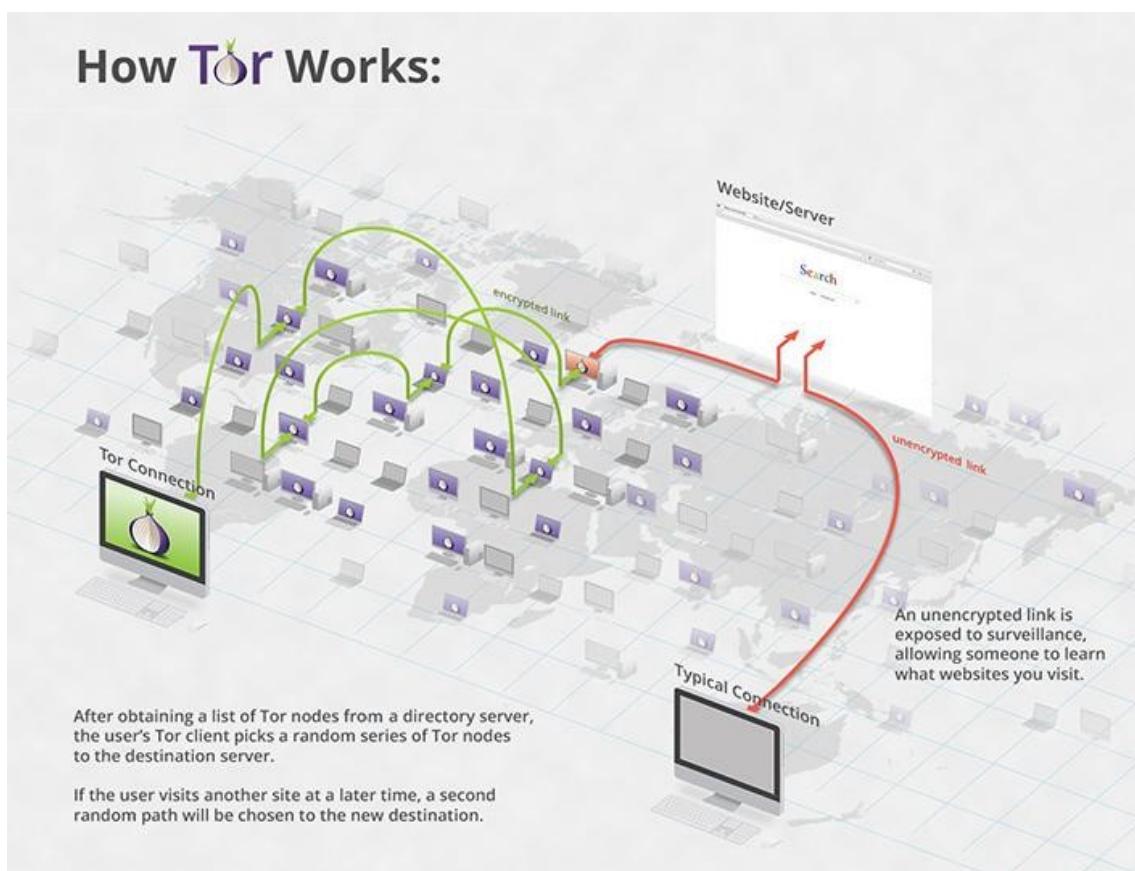


Figura 2. How Tor Works. [4]

### 3. Instalación Debian con servidores Web, FTP, SSH e IRC

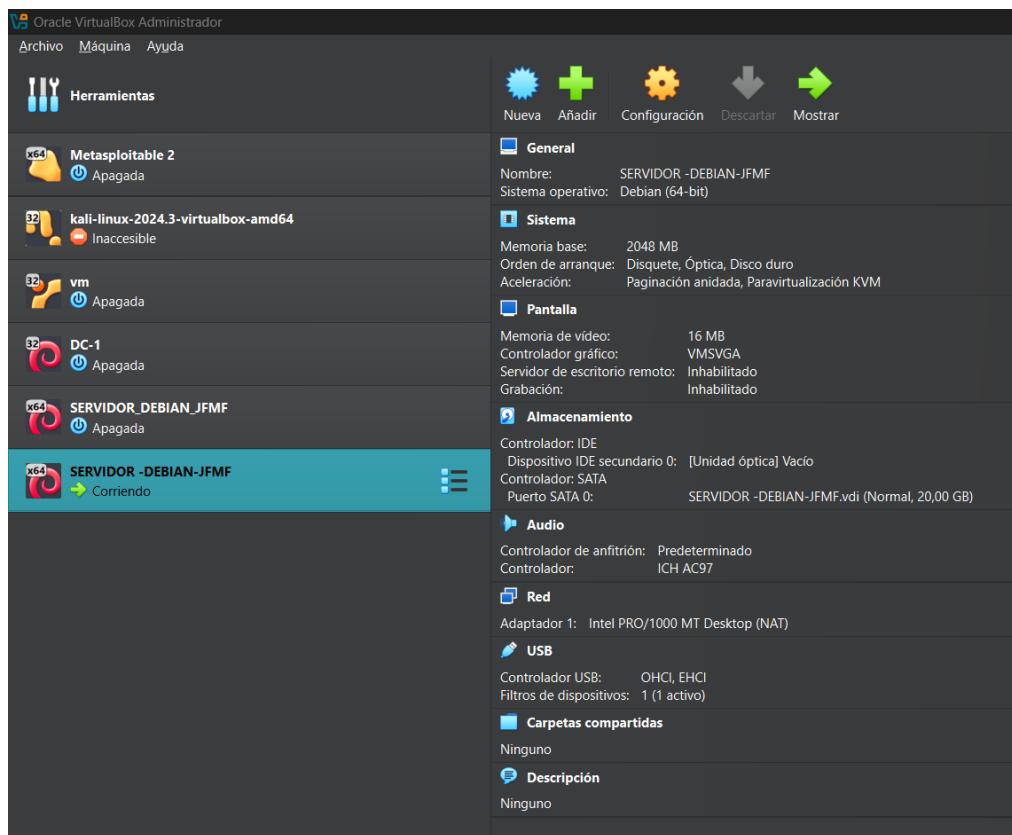
A continuación, se describen los principales pasos que se seguirán para el desarrollo de la tarea práctica propuesta.

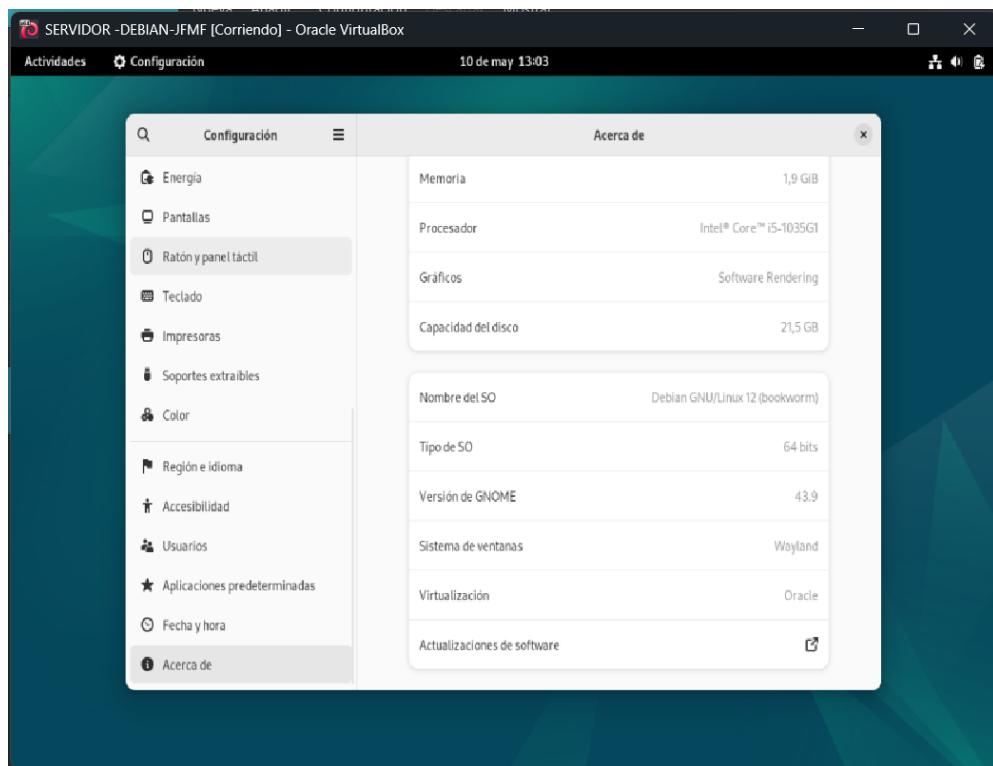
#### 3.1. Instalación de un servidor Debian en Virtual Box

En primer lugar, debemos realizar la instalación de un servidor Linux sobre una máquina virtual. En este caso hemos escogido la distribución Debian y el entorno de virtualización Virtual Box.

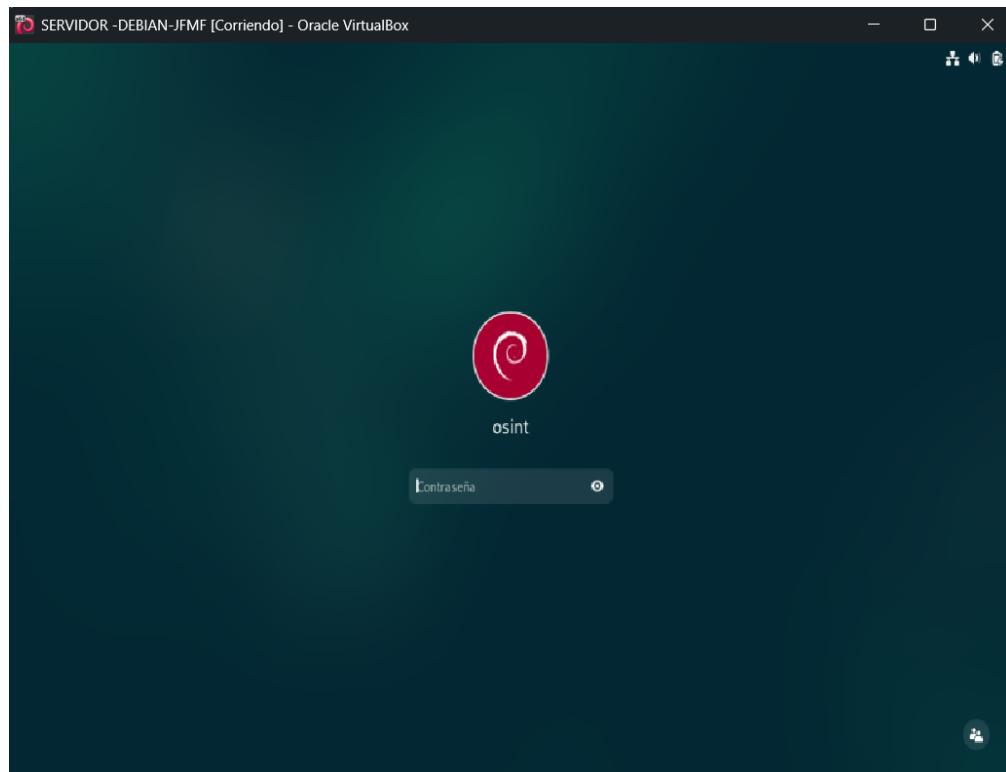
1. Descargamos una imagen ISO de la última versión disponible de Debian en la web
2. Creamos una máquina virtual para Debian 12 en VirtualBox version 7.1.4.

*[ Captura 1. Máquina Virtual Box Debian 12]*



*[ Captura 2. Debian 12]*

20. Una vez reiniciada la máquina podemos ingresar sesión con el usuario **osint / 12345678Bb**. Y comenzar a realizar las instalaciones y configuraciones para realizar la tarea propuesta.

*[ Captura 3. Autenticación de usuario osint]*

## 3.2. Instalamos Apache 2, PHP y phpMyAdmin

Antes de empezar, es una buena idea actualizar los paquetes de tu sistema a la última versión. Puedes actualizar todos los paquetes con el siguiente comando:

Una vez que tu sistema esté actualizado, puedes pasar al siguiente paso.

Instalamos el servidor web Apache 2 con los módulos que aseguran su compatibilidad con PHP.

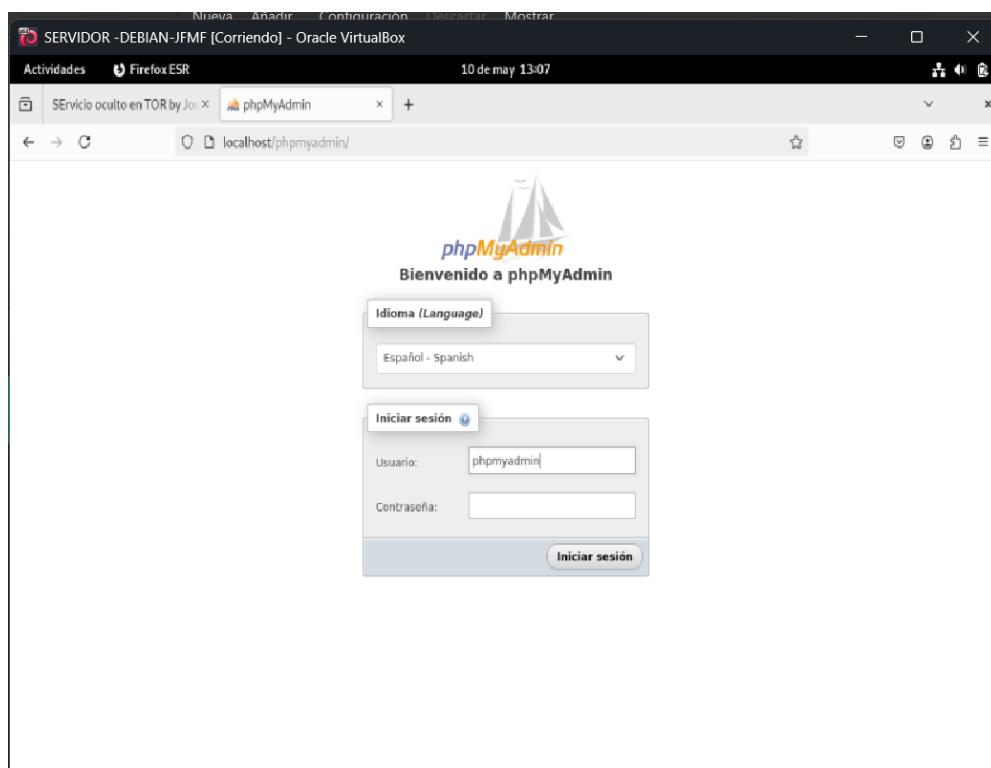
Ahora podemos instalar phpMyAdmin.

Una vez lanzada la instalación esta nos solicitará la configuración de diversos aspectos para asegurar la compatibilidad con el servidor Apache2.

Podemos comprobar que ahora tanto la web de inicio de Apache2 y de phpMyAdmin son accesibles a través del navegador web.

### [Capturas web inicio Apache2 y phpmyadmin]





Sin embargo, para poder autenticarnos correctamente con *phpMyAdmin* es necesario acceder a la base de datos My SQL y realizar algunas modificaciones para dar de alta el usuario y contraseña que tendrá acceso a *phpMyAdmin* (Usuario: **username** / Contraseña: **userpassword**).

### [Captura acceso base de datos phpmyadmin Usuario:username]

The screenshot displays the phpMyAdmin control panel with several tabs visible at the top: Bases de datos, SQL, Estado actual, Exportar, Importar, Configuración, Variables, Juegos de caracteres, Motores, and Complementos. The main content area is divided into several panels:

- Configuraciones generales:** Includes options for Cambio de contraseña, Cotejamiento de la conexión al servidor (set to utf8mb4\_unicode\_ci), and Más configuraciones.
- Configuraciones de apariencia:** Shows Idioma (Language) set to Español - Spanish, and Tema set to pmahomme.
- Servidor de base de datos:** Lists the server as Localhost via UNIX socket, MariaDB type, and MySQL 10.11.11-MariaDB-0+deb12u1 - Debian 12 version.
- Servidor web:** Lists Apache 2.4.62 (Debian), libmysql - mysqlnd 8.2.28 client version, PHP 8.2.28, and MySQL 8.0.28 extension.
- phpMyAdmin:** Lists version information (5.2.1deb1), documentation, official page, contribute, support, change log, and license.

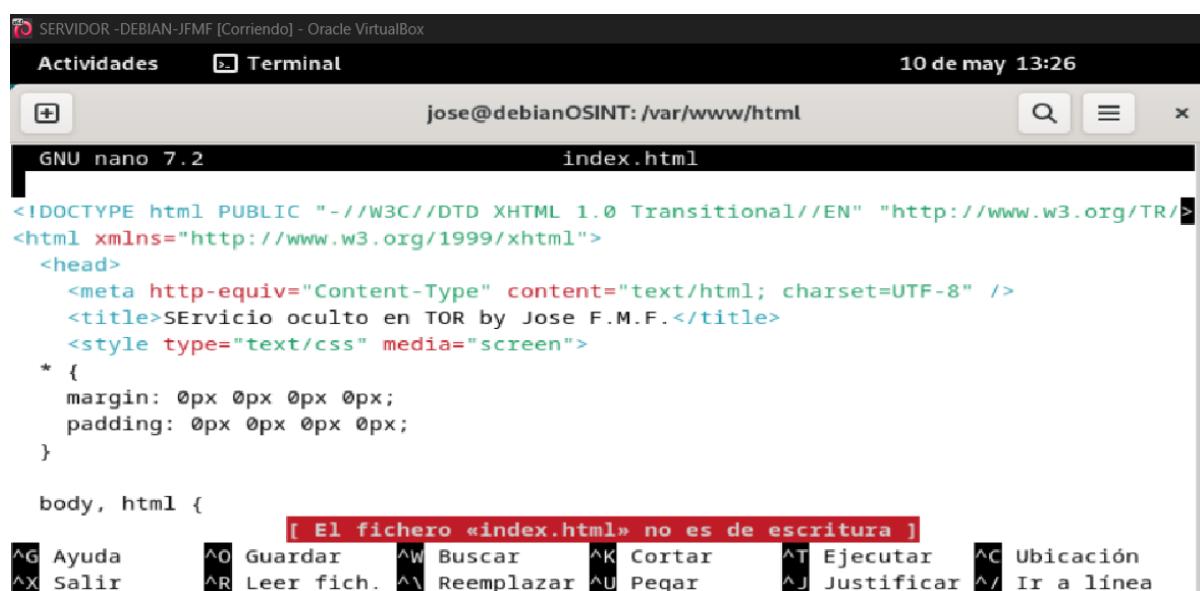
### 3.3. Generamos la página HTML que contiene el servicio oculto

Generamos o modificamos el fichero HTML que vamos a mostrar en Tor. En este caso editaremos el que viene por defecto en la configuración de inicio del Apache, lo podemos encontrar en el directorio `/var/www/html/`.

```
# nano index.html <html> <head><title>Servidor en TOR
de JoseGa</title></head> <body>Servicio oculto en TOR
by JoseGa</body> </html>
```

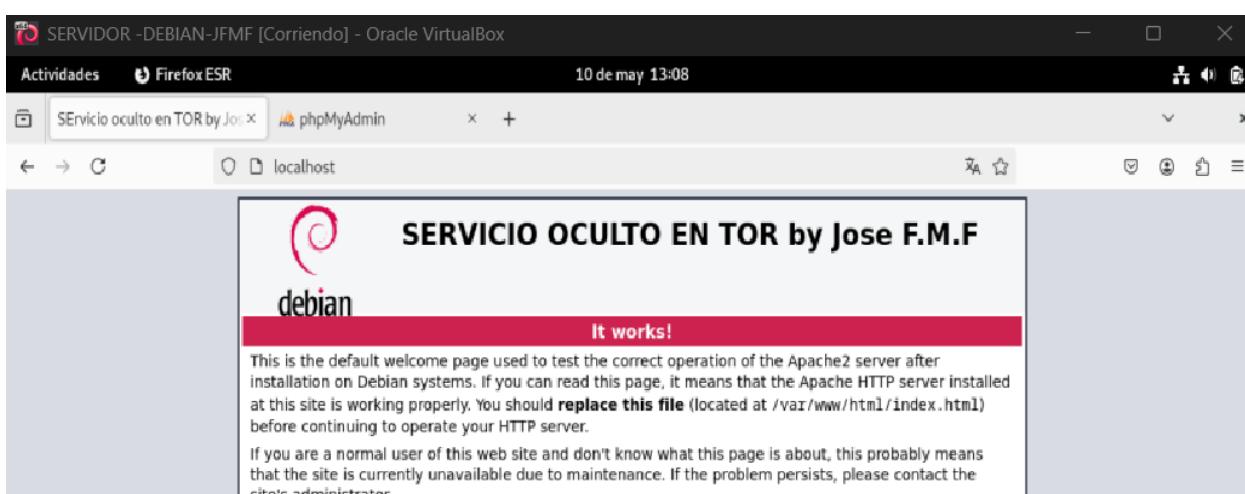
Salvamos el fichero.

*[Captura 8. Modificación archivo index.html.]*



The screenshot shows a terminal window titled "Terminal" with the command "jose@debianOSINT: /var/www/html". The file "index.html" is open in nano editor version 7.2. The content of the file is displayed, showing the HTML code for a page titled "Servicio oculto en TOR by Jose F.M.F.". A red box highlights the title text. At the bottom of the screen, there is a status bar with keyboard shortcuts for various functions like Ayuda (Help), Guardar (Save), Buscar (Search), Cortar (Cut), Ejecutar (Execute), Ubicación (Location), Salir (Exit), Leer fich. (Read file), Reemplazar (Replace), Pegar (Paste), Justificar (Justify), and Ir a línea (Go to line). A message "[ El fichero «index.html» no es de escritura ]" (The file "index.html" is not writable) is visible in the status bar.

*[Captura 9. Página HTML del servicio oculto]*



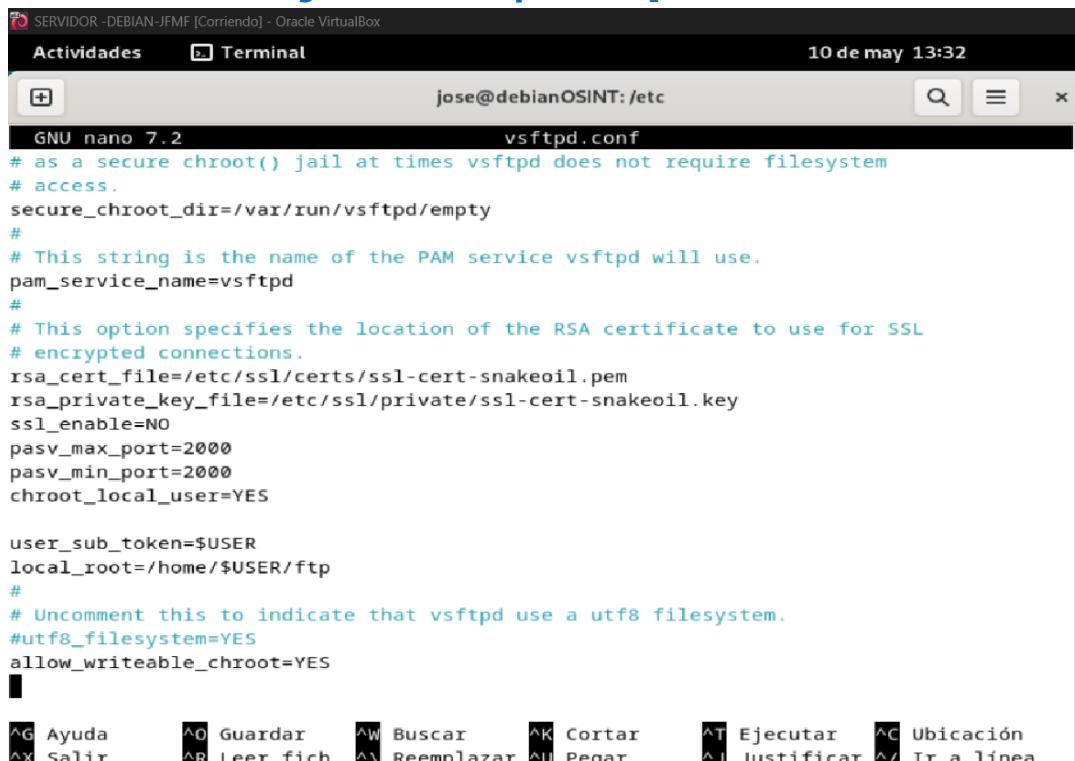
### 3.4. Instalamos Servidor FTP (*File Transfer Protocol*)

Vamos a instalar el servidor FTP (*vsftpd*), para lo que vamos a ejecutar el siguiente comando:

```
# apt install vsftpd -y
```

Una vez realizada la instalación es necesario ajustar su configuración a través del fichero **/etc/vsftpd/vsftpd.conf**. Descimentaremos algunas líneas del fichero e introduciremos algunas adicionales: [6]

*[Captura archivo de configuración vsftpd.conf]*



```

SERVIDOR-DEBIAN-JMF [Corriendo] - Oracle VirtualBox
Actividades Terminal 10 de may 13:32
jose@debianOSINT: /etc
GNU nano 7.2 vsftpd.conf
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=YES
pasv_max_port=2000
pasv_min_port=2000
chroot_local_user=YES

user_sub_token=$USER
local_root=/home/$USER/ftp
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
allow_writeable_chroot=YES

```

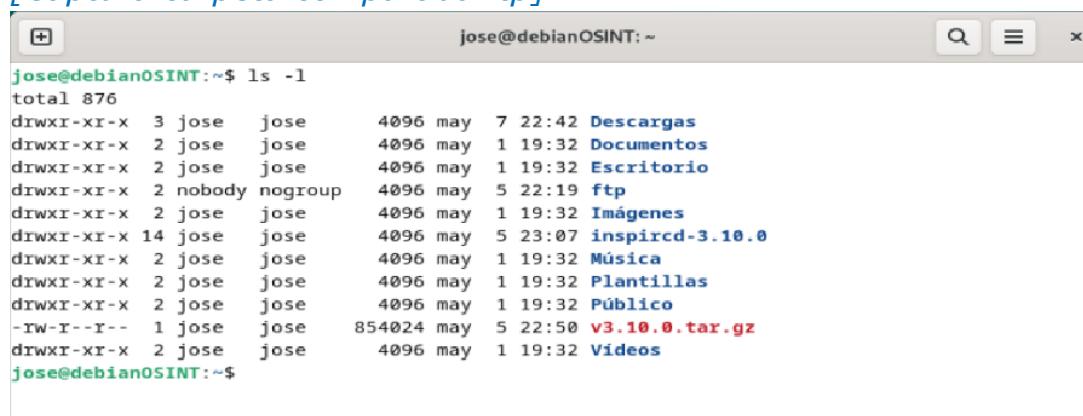
Ayuda Guardar Buscar Cortar Ejecutar Ubicación
 Salir Leer fich. Reemplazar Pegar Justificar Ir a línea

Para poder usar correctamente el servidor por cada usuario que vaya a utilizarlo debemos crear una carpeta *ftp*.

```
# mkdir /home/osint/ftp # chown nobody:nogroup /home/osint/ftp
```

```
# echo "Ejemplo de fichero compartido por FTP" >
/home/osint/ftp/sample.txt
```

*[Captura carpeta compartida ftp]*



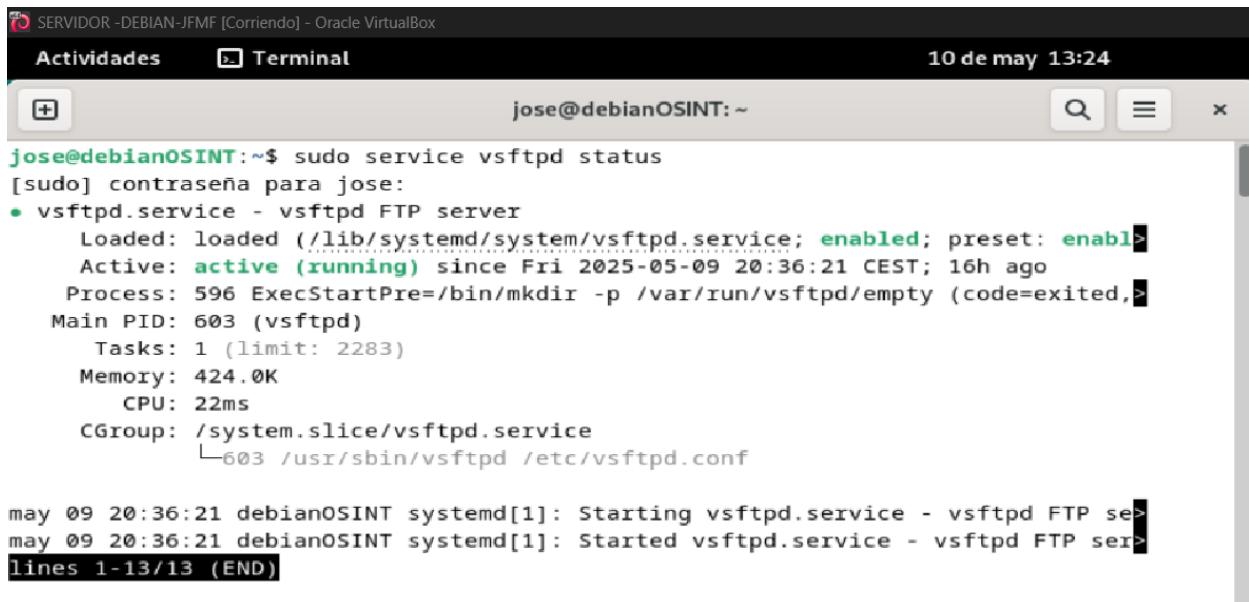
```

jose@debianOSINT:~$ ls -l
total 876
drwxr-xr-x 3 jose   jose      4096 may  7 22:42 Descargas
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Documentos
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Escritorio
drwxr-xr-x 2 nobody nogroup  4096 may  5 22:19 ftp
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Imágenes
drwxr-xr-x 14 jose   jose     4096 may  5 23:07 inspircd-3.10.0
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Música
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Plantillas
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 PÚBLICO
-rw-r--r-- 1 jose   jose    854024 may  5 22:50 V3.10.0.tar.gz
drwxr-xr-x 2 jose   jose      4096 may  1 19:32 Videos
jose@debianOSINT:~$
```

Paramos e iniciamos nuevamente el servidor FTP.

```
# service vsftpd stop # service vsftpd start
```

[Captura servicio ftp activo]



The screenshot shows a terminal window titled "SERVIDOR -DEBIAN-JFM [Corriendo] - Oracle VirtualBox". The window has tabs for "Actividades" and "Terminal". The terminal session is for user "jose@debianOSINT" at the prompt. The user runs the command "sudo service vsftpd status". The output shows the service is active and running. The user then runs "service vsftpd start", which starts the service. Log entries from "systemd[1]" show the service starting and being active. The terminal window has a dark theme with light-colored text. The status bar at the bottom right shows the date and time: "10 de may 13:24".

```
jose@debianOSINT:~$ sudo service vsftpd status
[sudo] contraseña para jose:
● vsftpd.service - vsftpd FTP server
  Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-05-09 20:36:21 CEST; 16h ago
    Process: 596 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, p...
  Main PID: 603 (vsftpd)
     Tasks: 1 (limit: 2283)
    Memory: 424.0K
      CPU: 22ms
     CGroup: /system.slice/vsftpd.service
             └─603 /usr/sbin/vsftpd /etc/vsftpd.conf

may 09 20:36:21 debianOSINT systemd[1]: Starting vsftpd.service - vsftpd FTP se...
may 09 20:36:21 debianOSINT systemd[1]: Started vsftpd.service - vsftpd FTP ser...
lines 1-13/13 (END)
```

### 3.5. Instalamos servidor Open SSH

Vamos a instalar el servidor SSH (`openssh-server`)

[Captura. Instalación servidor OpenSSH página estado del servicio]

```

SERVIDOR -DEBIAN-JFMF [Corriendo] - Oracle VirtualBox
Actividades Terminal 11 de may 12:36
jose@debianOSINT: /etc

● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-05-10 12:10:09 CEST; 24h ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 15710 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 15711 (sshd)
   Tasks: 1 (limit: 2283)
  Memory: 3.9M
    CPU: 132ms
   CGroup: /system.slice/ssh.service
           └─15711 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

may 10 12:10:09 debianOSINT systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
may 10 12:10:09 debianOSINT sshd[15711]: Server listening on 127.0.0.1 port 22.
may 10 12:10:09 debianOSINT systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
may 10 12:28:54 debianOSINT sshd[15773]: Accepted password for jose from 127.0.0.1 port 39224 ssh2
may 10 12:28:54 debianOSINT sshd[15773]: pam_unix(sshd:session): session opened for user jose(uid=1000) by >
may 10 12:28:54 debianOSINT sshd[15773]: pam_env(sshd:session): deprecated reading of user environment ena>
~
~
lines 1-19/19 (END)

```

Ajustamos la configuración mediante el archivo `/etc/ssh/sshd_config`.

Descomentaremos algunas líneas del fichero [7].

[Captura. Fichero de configuración de SSH]

```

GNU nano 7.2 sshd_config
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
ListenAddress 127.0.0.1
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes

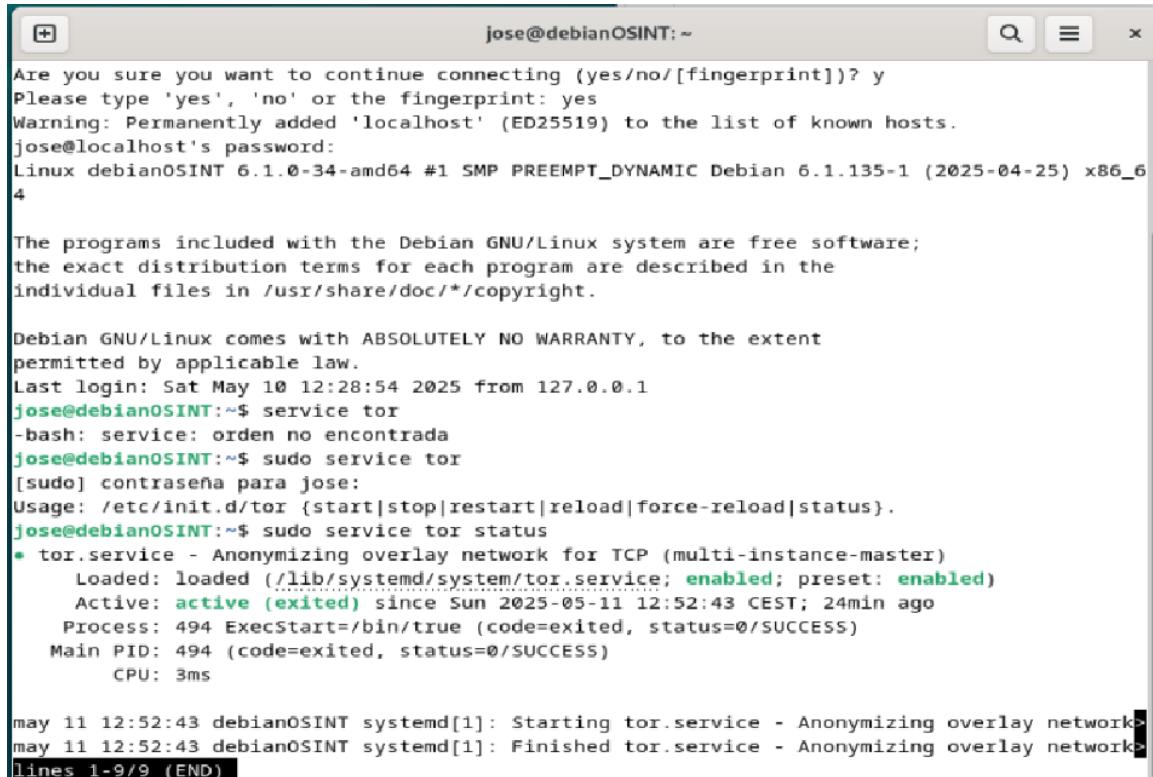
^G Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar  ^/ Ir a línea

```

Una vez hechos los cambios en la configuración, paramos e iniciamos el servidor SSH otra vez.

Probamos a realizar una conexión SSH con el servicio que acabamos de lanzar.

### [Captura. Conexión con el servidor SSH]



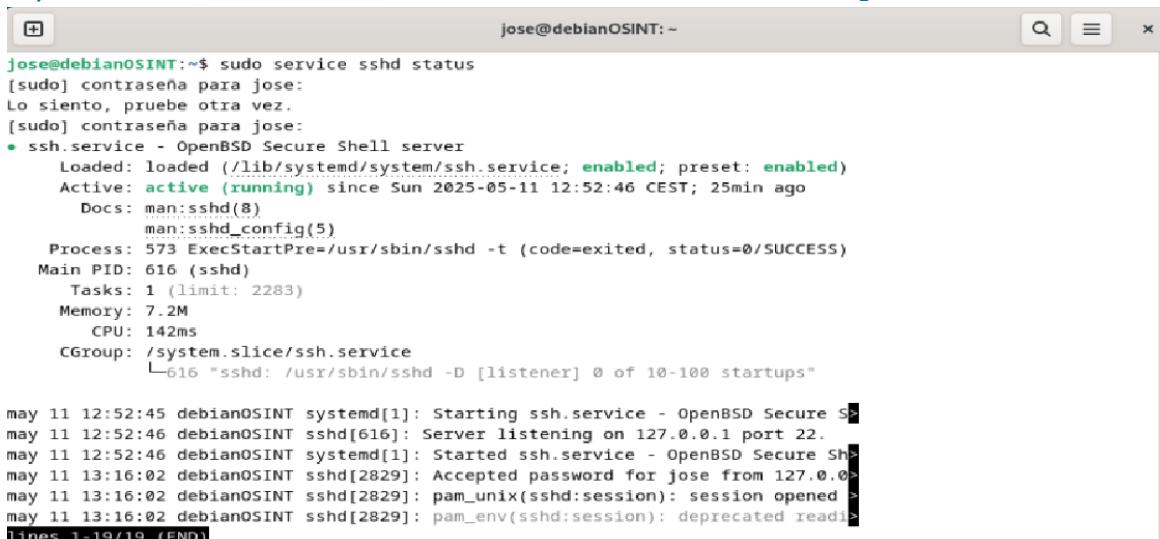
```
jose@debianOSINT:~$ ssh -v user@127.0.0.1
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
jose@localhost's password:
Linux debianOSINT 6.1.0-34- amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 10 12:28:54 2025 from 127.0.0.1
jose@debianOSINT:~$ service tor
-bash: service: orden no encontrada
jose@debianOSINT:~$ sudo service tor
[sudo] contraseña para jose:
Usage: /etc/init.d/tor {start|stop|restart|reload|force-reload|status}.
jose@debianOSINT:~$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; enabled; preset: enabled)
   Active: active (exited) since Sun 2025-05-11 12:52:43 CEST; 24min ago
     Process: 494 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 494 (code=exited, status=0/SUCCESS)
      CPU: 3ms

may 11 12:52:43 debianOSINT systemd[1]: Starting tor.service - Anonymizing overlay network>
may 11 12:52:43 debianOSINT systemd[1]: Finished tor.service - Anonymizing overlay network>
lines 1-9/9 (END)
```

### [Captura Información de estado del servicio ssh activo]



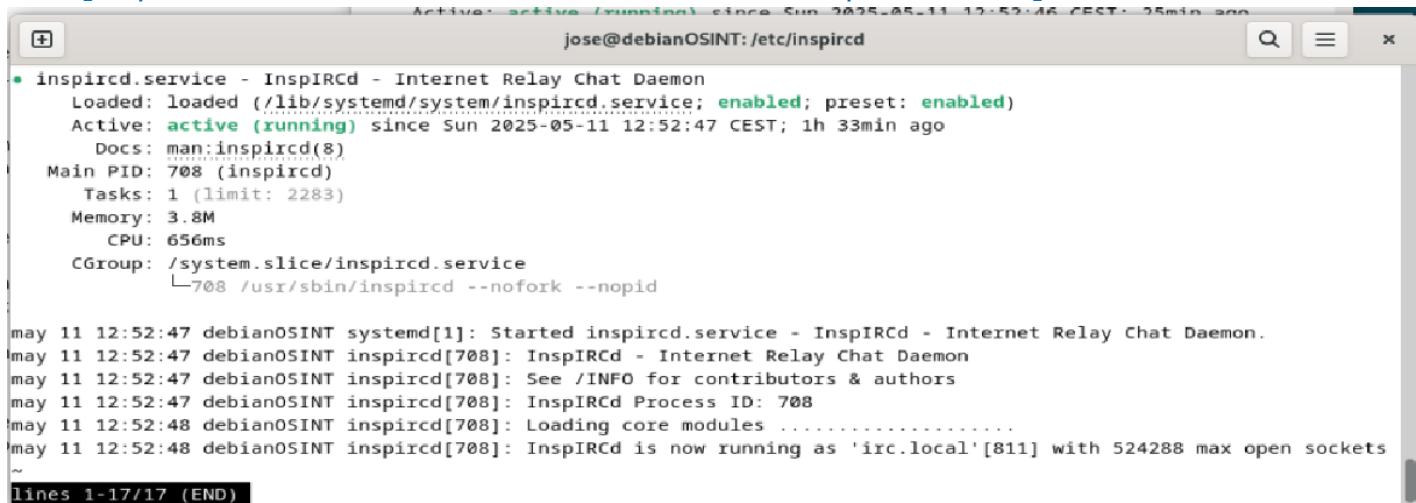
```
jose@debianOSINT:~$ sudo service sshd status
[sudo] contraseña para jose:
Lo siento, pruebe otra vez.
[sudo] contraseña para jose:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-05-11 12:52:46 CEST; 25min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 573 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 616 (sshd)
      Tasks: 1 (limit: 2283)
     Memory: 7.2M
        CPU: 142ms
       CGroup: /system.slice/sshd.service
               └─616 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

may 11 12:52:45 debianOSINT systemd[1]: Starting ssh.service - OpenBSD Secure S>
may 11 12:52:46 debianOSINT sshd[616]: Server listening on 127.0.0.1 port 22.
may 11 12:52:46 debianOSINT systemd[1]: Started ssh.service - OpenBSD Secure Sh>
may 11 13:16:02 debianOSINT sshd[2829]: Accepted password for jose from 127.0.0.>
may 11 13:16:02 debianOSINT sshd[2829]: pam_unix(sshd:session): session opened >
may 11 13:16:02 debianOSINT sshd[2829]: pam_env(sshd:session): deprecated readin>
lines 1-19/19 (END)
```

### 3.6. Instalamos y configuramos IRC

Por último instalaremos **InspIRCd**, un robusto servidor de IRC que funciona en entornos tipo UNIX, como las distribuciones de Linux y las variantes de BSD. [8]

[Captura Información de estado del servicio *inspircd* activo]



```
jose@debianOSINT:/etc/inspircd
● inspircd.service - InspIRCd - Internet Relay Chat Daemon
   Loaded: loaded (/lib/systemd/system/inspircd.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-05-11 12:52:47 CEST; 1h 33min ago
     Docs: man:inspircd(8)
 Main PID: 708 (inspircd)
    Tasks: 1 (limit: 2283)
   Memory: 3.8M
      CPU: 656ms
     CGroup: /system.slice/inspircd.service
             └─708 /usr/sbin/inspircd --nofork --nopid

may 11 12:52:47 debianOSINT systemd[1]: Started inspircd.service - InspIRCd - Internet Relay Chat Daemon.
may 11 12:52:47 debianOSINT inspircd[708]: InspIRCd - Internet Relay Chat Daemon
may 11 12:52:47 debianOSINT inspircd[708]: See /INFO for contributors & authors
may 11 12:52:47 debianOSINT inspircd[708]: InspIRCd Process ID: 708
may 11 12:52:48 debianOSINT inspircd[708]: Loading core modules .....
may 11 12:52:48 debianOSINT inspircd[708]: InspIRCd is now running as 'irc.local'[811] with 524288 max open sockets
~
lines 1-17/17 (END)
```

Realizamos una serie de configuraciones básicas sobre el servicio **inspircd**, para ello nos dirigimos al directorio de configuración **/etc/inspircd/** y actuamos sobre los ficheros **inspircd.conf** (Configuración propia del servidor) e **inspirc.motd** (Contiene el mensaje personalizado que se muestra al conectar con el servidor).

[Captura Archivo de configuración *inspircd.conf*]



```
jose@debianOSINT:/etc
GNU nano 7.2          inspircd.conf

<bind address="127.0.0.1" port="6667" type="clients">
<power diepass="3456" restartpass="7890">

<connect allow="*"
          timeout="120"
          threshold="10"
          pingfreq="120"
          hardsendq="262144"
          softsendq="8192"
          recvq="8192"
          localmax="3"
          globalmax="3">

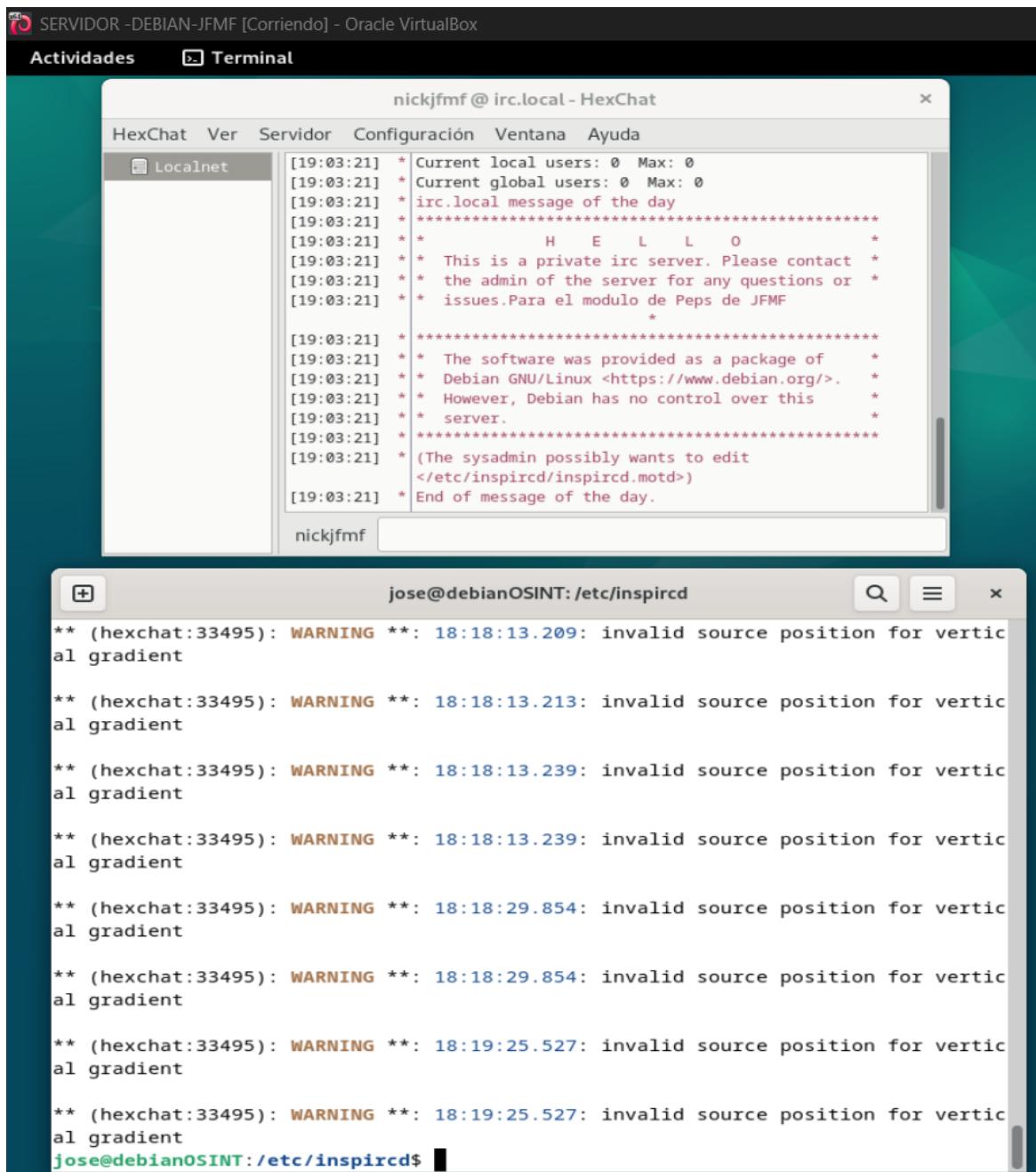
<class name="Shutdown"
      commands="DIE RESTART REHASH LOADMODULE UNLOADMODULE RELOADMODULE">
<class name="ServerLink"
      commands="CONNECT SQUIT RCONNECT RSQUIT MKPASSWD">
<class name="BanControl"
      commands="KILL GLINE KLINE ZLINE QLINE ELINE">
<class name="OperChat"
      commands="WALLOPS GLOBOPS SETIDLE SPYLIST SPYNAMES">
<class name="HostCloak"
      commands="SETHOST SETIDENT CHGNAME CHGHOST CHGIDENT">

<type name="NetAdmin"
      classes="OperChat BanControl HostCloak Shutdown ServerLink"
      host="netadmin.omega.org.za">
<type name="GlobalOp"
      classes="OperChat BanControl HostCloak ServerLink"
      host="ircop.omega.org.za">
<type name="Helper"
      classes="HostCloak"
      host="helper.omega.org.za">

<oper name="jfmf"
      password="12345"
      host="*@localhost"
      type="NetAdmin">
```

Una vez instalado, configurado y lanzado el servicio podemos comprobar que este funciona conectándonos localmente empleando para ello un cliente como **weechat**, **pidgin** o **hexchat**. Por comodidad y sencillez optaré por utilizar **hexchat**.

### [Captura Cliente de IRC HexChat configurado y lanzado]



## 4. Generación de *Hidden Services* en la red TOR

### 4.1. Instalamos TOR y paquetes adicionales

Una vez instalada la máquina Debian con los servicios que deseamos ofrecer, web, FTP, SSH e IRC, es el momento de instalar TOR y sus paquetes asociados para poder ocultar estos en la red cebolla.

```
# apt install screen build-essential libevent-dev openssl zlib1g-dev libssl-dev -y
# apt install tor-y
```

[Captura servicio tor instalado y habilitado]

```
jose@debianOSINT:~
```

```
root@debianOSINT:/var/lib/tor/hidden_service# tor
May 11 14:57:07.658 [notice] Tor 0.4.7.16 running on Linux with Libevent 2.1.12-stable, OpenSSL 3.0.15, Zlib 1.2.11
3, Liblzma 5.4.1, Libzstd 1.5.4 and Glibc 2.36 as libc.
May 11 14:57:07.658 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/staying-anonymous/
May 11 14:57:07.659 [notice] Read configuration file "/etc/tor/torrc".
May 11 14:57:07.685 [notice] Opening Socks listener on 127.0.0.1:9050
May 11 14:57:07.688 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 11 14:57:07.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
May 11 14:57:07.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
May 11 14:57:07.000 [warn] You are running Tor as root. You don't need to, and you probably shouldn't.
May 11 14:57:07.000 [notice] Bootstrapped 0% (starting): Starting
May 11 14:57:08.000 [notice] Starting with guard context "default"
May 11 14:57:08.000 [notice] Bootstrapped 5% (conn): Connecting to a relay
May 11 14:57:09.000 [notice] Bootstrapped 10% (conn_done): Connected to a relay
May 11 14:57:10.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay
May 11 14:57:10.000 [notice] Bootstrapped 15% (handshake_done): Handshake with a relay done
May 11 14:57:10.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits
May 11 14:57:10.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circuits
May 11 14:57:10.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
May 11 14:57:11.000 [notice] Bootstrapped 100% (done): Done
```

Una vez instalado TOR es necesario crear las carpetas donde se almacenará la información de cada uno de los servicios ocultos.

```
# cd /var/lib/tor/ # mkdir hidden_service # cd hidden_service #
mkdir web ftp ssh irc
```

[Captura. Directorios de configuración de los hidden services]

```
jose@debianOSINT:~
```

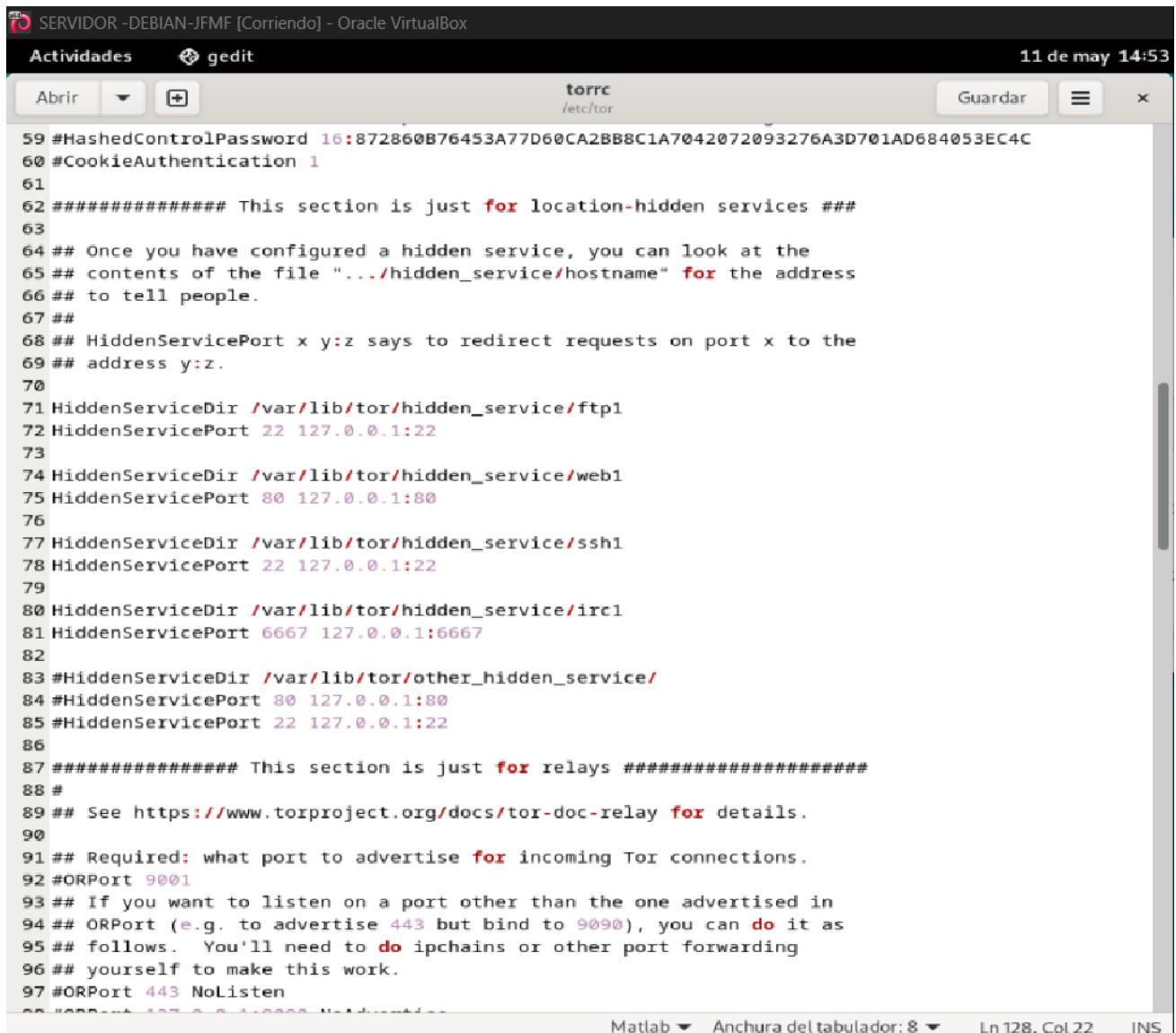
```
root@debianOSINT:/home/jose# cd /var/lib/tor/hidden_service
root@debianOSINT:/var/lib/tor/hidden_service# ls -l
total 16
drwx--S--- 3 root debian-tor 4096 may  9 20:41 ftpl
drwx--S--- 3 root debian-tor 4096 may  9 20:41 irc1
drwx--S--- 3 root debian-tor 4096 may  9 20:41 ssh1
drwx--S--- 3 root debian-tor 4096 may  9 20:41 web1
```

## 4.2. Configuración de los Hidden Services

Editamos el fichero de configuración de Tor (`/etc/tor/torrc`). Añadimos las líneas correspondientes por cada servicio oculto que deseamos ofrecer.

```
# gedit /etc/tor/torrc &
```

[Captura. Fichero configuración `torrc`]



```

SERVIDOR-DEBIAN-JFM [Corriendo] - Oracle VirtualBox
Actividades gedit
Abrir + torrc
/etc/tor
Guardar x
11 de may 14:53

59 #HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
60 #CookieAuthentication 1
61
62 ##### This section is just for location-hidden services #####
63
64 ## Once you have configured a hidden service, you can look at the
65 ## contents of the file ".../hidden_service/hostname" for the address
66 ## to tell people.
67 ##
68 ## HiddenServicePort x y:z says to redirect requests on port x to the
69 ## address y:z.
70
71 HiddenServiceDir /var/lib/tor/hidden_service/ftp1
72 HiddenServicePort 22 127.0.0.1:22
73
74 HiddenServiceDir /var/lib/tor/hidden_service/web1
75 HiddenServicePort 80 127.0.0.1:80
76
77 HiddenServiceDir /var/lib/tor/hidden_service/ssh1
78 HiddenServicePort 22 127.0.0.1:22
79
80 HiddenServiceDir /var/lib/tor/hidden_service/irc1
81 HiddenServicePort 6667 127.0.0.1:6667
82
83 #HiddenServiceDir /var/lib/tor/other_hidden_service/
84 #HiddenServicePort 80 127.0.0.1:80
85 #HiddenServicePort 22 127.0.0.1:22
86
87 ##### This section is just for relays #####
88 #
89 ## See https://www.torproject.org/docs/tor-doc-relay for details.
90
91 ## Required: what port to advertise for incoming Tor connections.
92 #ORPort 9001
93 ## If you want to listen on a port other than the one advertised in
94 ## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
95 ## follows. You'll need to do ipchains or other port forwarding
96 ## yourself to make this work.
97 #ORPort 443 NoListen

```

Matlab ▾ Anchura del tabulador: 8 ▾ Ln 128, Col 22 INS

Guardamos el fichero de configuración y cambiamos los permisos del directorio y subdirectorios que contendrán la información de los servicios ocultos (`/var/lib/tor/hidden_service`), este último paso es muy importante para realizar el correcto lanzamiento de TOR.

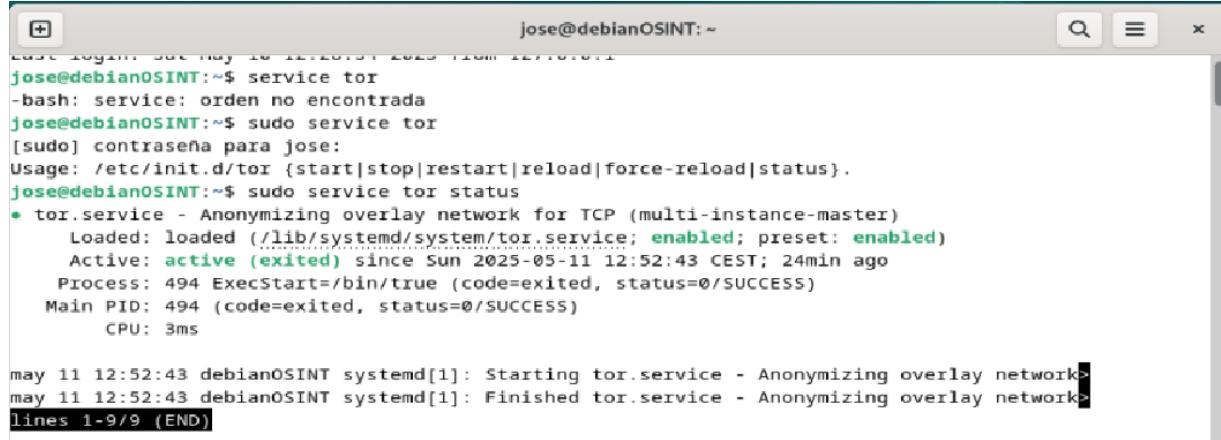
```
# chmod 700 /var/lib/tor/hidden_service/ -R
```

## 5. Lanzamiento de TOR

Reiniciamos el servicio TOR.

```
# service tor restart
```

[Captura. Fichero configuración torrc]



```
jose@debianOSINT:~$ service tor
-bash: service: orden no encontrada
jose@debianOSINT:~$ sudo service tor
[sudo] contraseña para jose:
Usage: /etc/init.d/tor {start|stop|restart|reload|force-reload|status}.
jose@debianOSINT:~$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; enabled; preset: enabled)
   Active: active (exited) since Sun 2025-05-11 12:52:43 CEST; 24min ago
     Process: 494 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 494 (code=exited, status=0/SUCCESS)
      CPU: 3ms

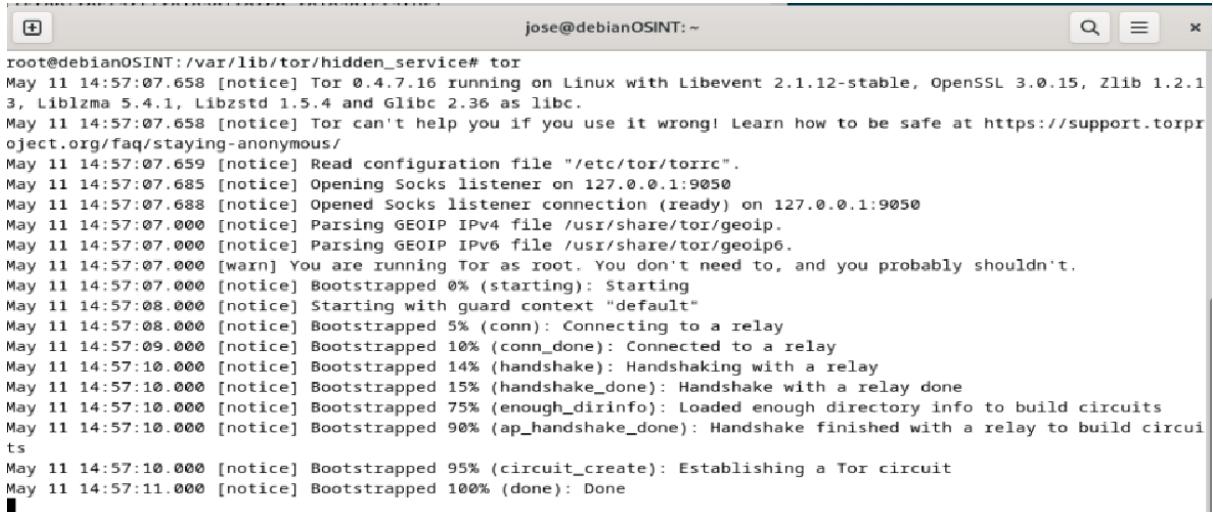
may 11 12:52:43 debianOSINT systemd[1]: Starting tor.service - Anonymizing overlay network...
may 11 12:52:43 debianOSINT systemd[1]: Finished tor.service - Anonymizing overlay network...
lines 1-9/9 (END)
```

Figura 54. Ejecutamos service tor restart.

Ahora podemos lanzar TOR.

```
# tor
```

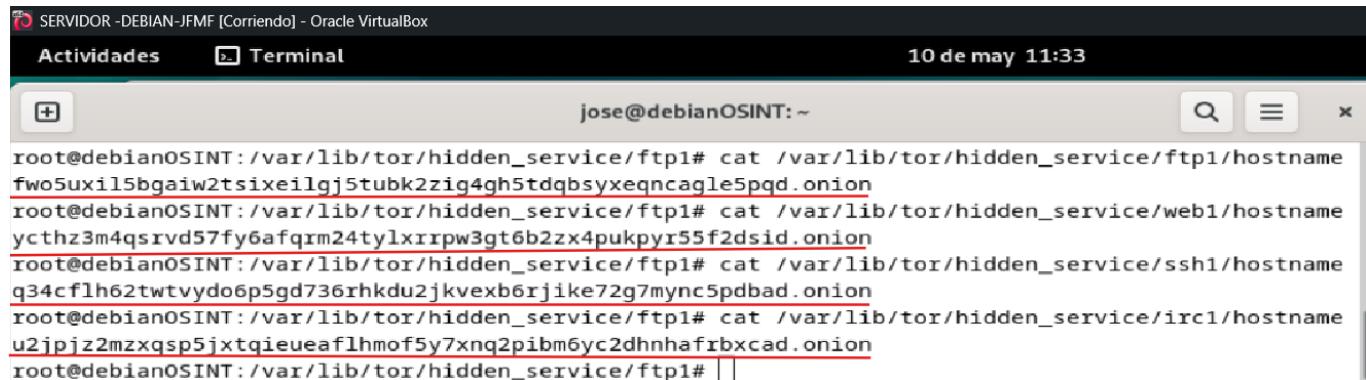
[Captura. Lanzado Tor]



```
jose@debianOSINT:/var/lib/tor/hidden_service# tor
May 11 14:57:07.658 [notice] Tor 0.4.7.16 running on Linux with Libevent 2.1.12-stable, OpenSSL 3.0.15, Zlib 1.2.1
3, Liblzma 5.4.1, Libzstd 1.5.4 and Glibc 2.36 as libc.
May 11 14:57:07.658 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torpr
oject.org/faq/staying-anonymous/
May 11 14:57:07.659 [notice] Read configuration file "/etc/tor/torrc".
May 11 14:57:07.685 [notice] Opening Socks listener on 127.0.0.1:9050
May 11 14:57:07.688 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
May 11 14:57:07.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
May 11 14:57:07.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
May 11 14:57:07.000 [warn] You are running Tor as root. You don't need to, and you probably shouldn't.
May 11 14:57:07.000 [notice] Bootstrapped 0% (starting): Starting
May 11 14:57:08.000 [notice] Starting with guard context "default"
May 11 14:57:08.000 [notice] Bootstrapped 5% (conn): Connecting to a relay
May 11 14:57:09.000 [notice] Bootstrapped 10% (conn_done): Connected to a relay
May 11 14:57:10.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay
May 11 14:57:10.000 [notice] Bootstrapped 15% (handshake_done): Handshake with a relay done
May 11 14:57:10.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits
May 11 14:57:10.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circui
ts
May 11 14:57:10.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
May 11 14:57:11.000 [notice] Bootstrapped 100% (done): Done
```

Se han generado dos ficheros por cada servicio oculto exportado en su correspondiente **HiddenServiceDir**. Los ficheros se denominan **private\_key** y **hostname**.

### [Captura. Ficheros servicios oculto generado]



```
jose@debianOSINT:~
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/ftp1/hostname
fwo5uxil5bgaiw2tsixeilgj5tubk2zig4gh5tdqbsyxeqncagle5pqd.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/web1/hostname
ycthz3m4qsrvd57fy6afqrm24tylxirrpw3gt6b2zx4pukpyr55f2dsid.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/ssh1/hostname
q34cflh62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdbad.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/irc1/hostname
u2jpjz2mzxqsp5jxtqieueaflhmo5y7xng2pibm6yc2dhnhafrbxcad.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# ||
```

## 6. Verificación local de los *Hidden Services*

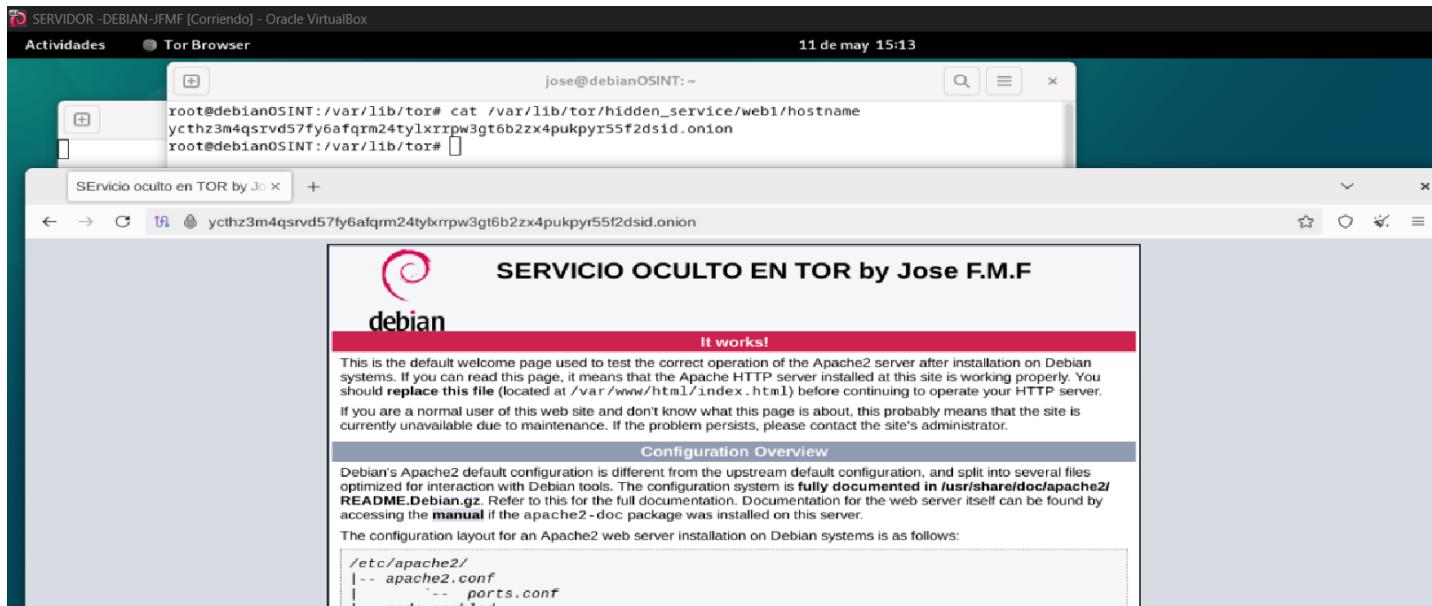
### 6.1. Verificación del servicio web oculto en TOR

La dirección *.onion* del servidor web oculto está disponible en el directorio establecido en el fichero de configuración */etc/tor/torrc*.

```
# cat /var/lib/tor/hidden_services/web/hostname
```

Ahora vamos al navegador Tor y comprobamos que accedemos.

### [Captura. Web Oculta Tor]



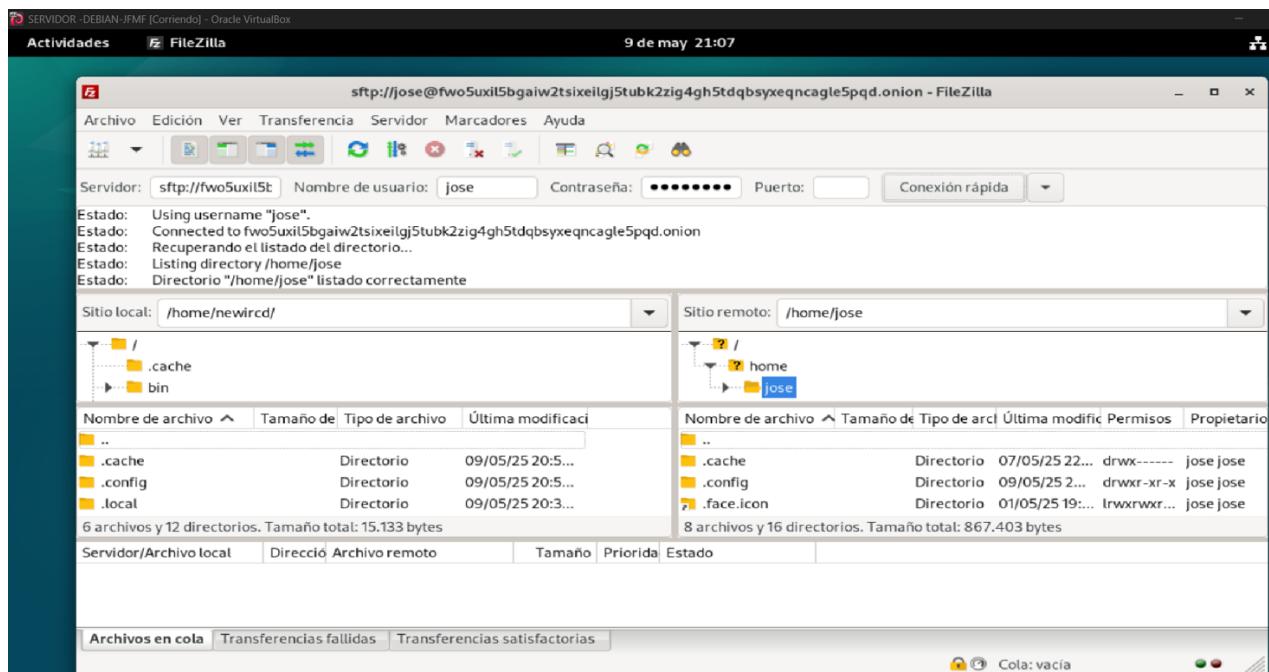
## 6.2. Verificación local Hidden Service FTP

Para comprobar el funcionamiento del servidor FTP es necesario instalar un cliente FTP, como por ejemplo FileZilla en el equipo remoto.

Una vez instalado el cliente FileZilla es necesario realizar su configuración para poder establecer conexión con el servidor a través de TOR.

Vaya a *Configuración del Proxy Genérico* y cambie el tipo a **SOCKS5**, el host a localhost y el puerto a **9050** (si ejecuta Tor como demonio) o **9150** (si ejecuta *Tor Browser*).

*[Captura. Servicio Hidden Service local FTP ]*



Una vez que hayas configurado todo correctamente, deberías poder conectarte con éxito y empezar a descargar archivos.

## 6.3. Verificación de funcionamiento local Hidden Service SSH

Después de que el servicio cliente Tor se ejecute de nuevo, ahora debería encontrar su nueva dirección de servicio oculto \*.onion de la siguiente manera:

```
# cat /var/lib/tor/hidden_services/ssh/hostname
q34cf1h62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdblbad.onion
```

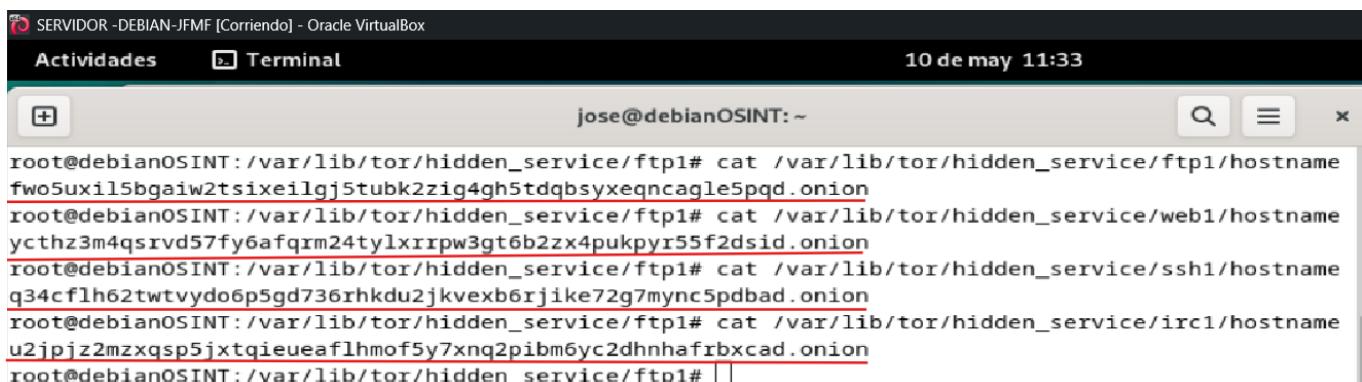
Para conectar con el cliente SSH desde una máquina remota que ejecute un cliente TOR podemos utilizar el siguiente comando:

```
$ torsocks q34cf1h62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdblbad.onion
```

*[Captura. Conexión local con el hidden service SSH conexión rechazada]*

```
root@debianOSINT:/etc/ssh# torsocks ssh q34cf1h62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdblbad.onion
1746871925 PERROR torsocks[15723]: socks5 libc connect: Connection refused (in socks5_connect() at socks5.c:202)
ssh: connect to host q34cf1h62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdblbad.onion port 22: Connection refused
root@debianOSINT:/etc/ssh# sudo service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-05-10 12:10:09 CEST; 2min 11s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 15710 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 15711 (sshd)
   Tasks: 1 (limit: 2283)
  Memory: 2.4M
    CPU: 32ms
   CGroup: /system.slice/sshd.service
           └─15711 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

may 10 12:10:09 debianOSINT systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
may 10 12:10:09 debianOSINT sshd[15711]: Server listening on 127.0.0.1 port 22.
may 10 12:10:09 debianOSINT systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@debianOSINT:/etc/ssh#
```

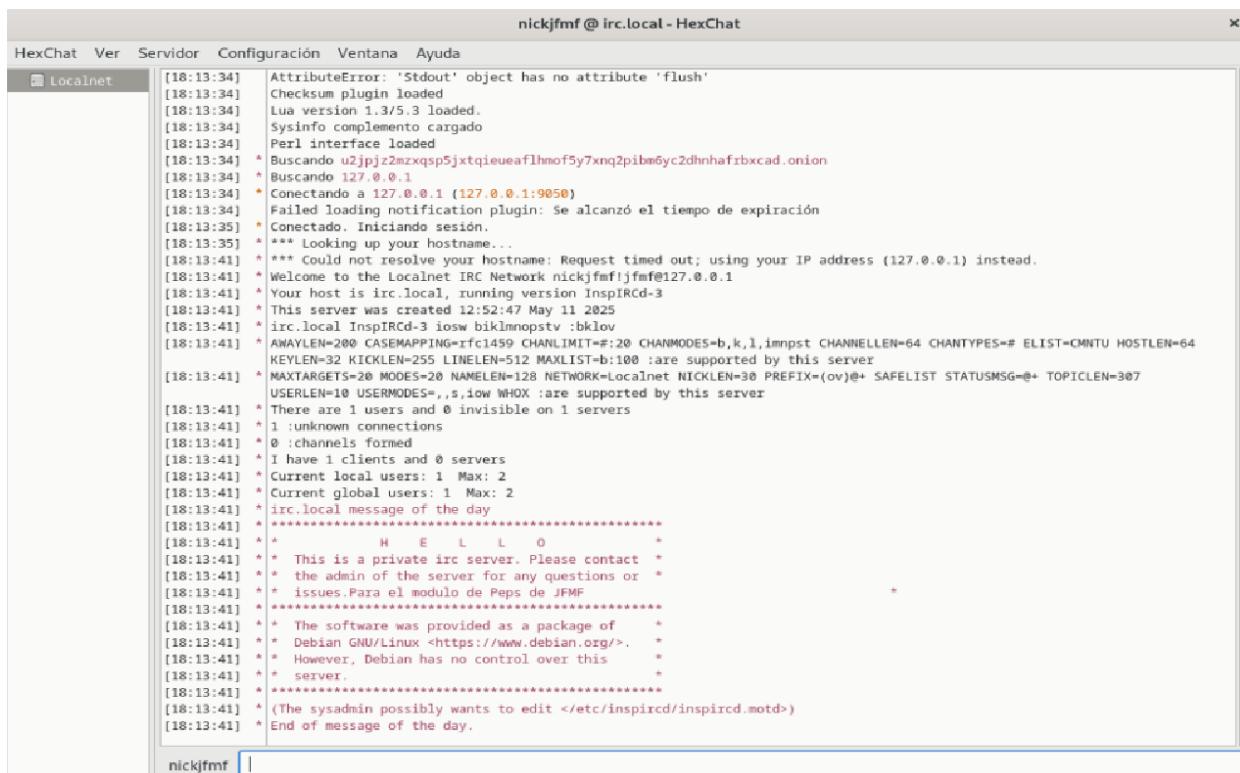


## 6.4. Verificación de funcionamiento local *Hidden Service chat IRC*

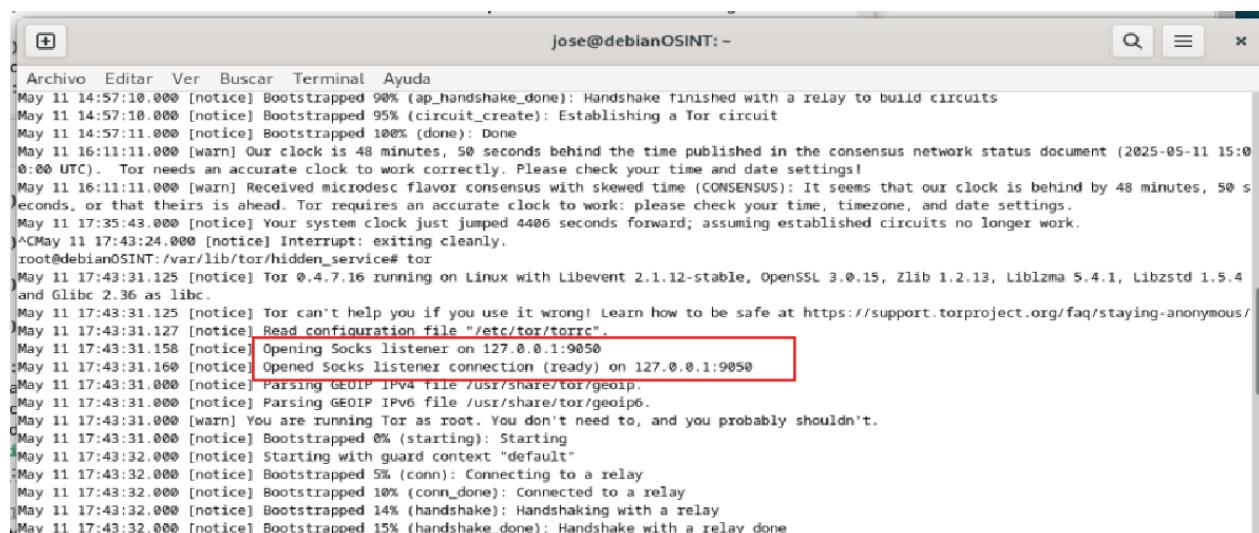
Averiguamos cual es el nombre del host que alberga el servicio oculto IRC en la red cebolla:

```
# cat /var/lib/tor/hidden_services/irc/hostname
u2jpjz2mzxqsp5jxtqieueaflhmo5y7xnq2pibm6yc2dhnhafrbxcad.onion
```

[Capturas. Conexión local con el hidden service IRC HexChat y del estado del servicio de tor y el servicio inspircd.]



Conectamos el cliente IRC con el servidor IRC oculto en la red TOR.



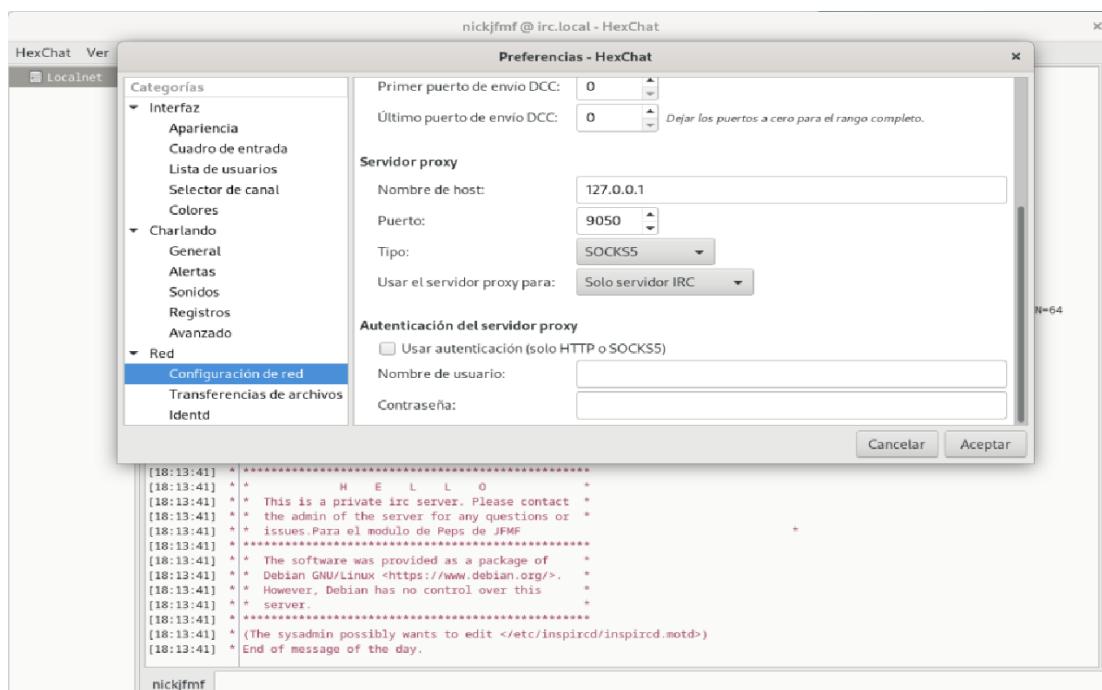
```
jose@debianOSINT: /var/lib/tor
** (hexchat:4803): WARNING **: 17:37:16.620: invalid source position for vertical gradient
jose@debianOSINT: /var/lib/tor$ hexchat
Gtk-Message: 17:41:07.975: Failed to load module "canberra-gtk-module"

** (hexchat:5219): WARNING **: 17:41:38.597: invalid source position for vertical gradient
** (hexchat:5219): WARNING **: 17:41:38.600: invalid source position for vertical gradient
** (hexchat:5219): WARNING **: 17:41:38.679: invalid source position for vertical gradient
** (hexchat:5219): WARNING **: 17:41:38.684: invalid source position for vertical gradient
[GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt
jose@debianOSINT: /var/lib/tor$ hexchat&
[1] 6374
jose@debianOSINT: /var/lib/tor$ Gtk-Message: 18:13:14.623: Failed to load module "canberra-gtk-module"

** (hexchat:6374): WARNING **: 18:13:19.724: invalid source position for vertical gradient
** (hexchat:6374): WARNING **: 18:13:19.724: invalid source position for vertical gradient
** (hexchat:6374): WARNING **: 18:13:19.797: invalid source position for vertical gradient
** (hexchat:6374): WARNING **: 18:13:19.806: invalid source position for vertical gradient
jose@debianOSINT: /var/lib/tor$ 
jose@debianOSINT: /var/lib/tor$ sudo service inspircd status
[sudo] contrasena para jose:
● inspircd.service - InspIRCd - Internet Relay Chat Daemon
  Loaded: loaded (/lib/systemd/system/inspircd.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-05-11 12:52:47 CEST; 5h 20min ago
    Docs: man:inspircd(8)
   Main PID: 708 (inspircd)
     Tasks: 1 (limit: 2283)
    Memory: 2.0M
      CPU: 1.939s
     CGroup: /system.slice/inspircd.service
             └─708 /usr/sbin/inspircd --nofork --novid

may 11 12:52:47 debianOSINT systemd[1]: Started inspircd.service - InspIRCd - Internet Relay Chat Daemon
may 11 12:52:47 debianOSINT inspircd[708]: InspIRCd - Internet Relay Chat Daemon
may 11 12:52:47 debianOSINT inspircd[708]: See /INFO for contributors & authors
may 11 12:52:47 debianOSINT inspircd[708]: InspIRCd Process ID: 708
may 11 12:52:48 debianOSINT inspircd[708]: Loading core modules .....
may 11 12:52:48 debianOSINT inspircd[708]: InspIRCd is now running as 'irc.local'[811] with 5 connections
[lines 1-17/17] [END]
```

## [Captura. Configuración HexChat ]



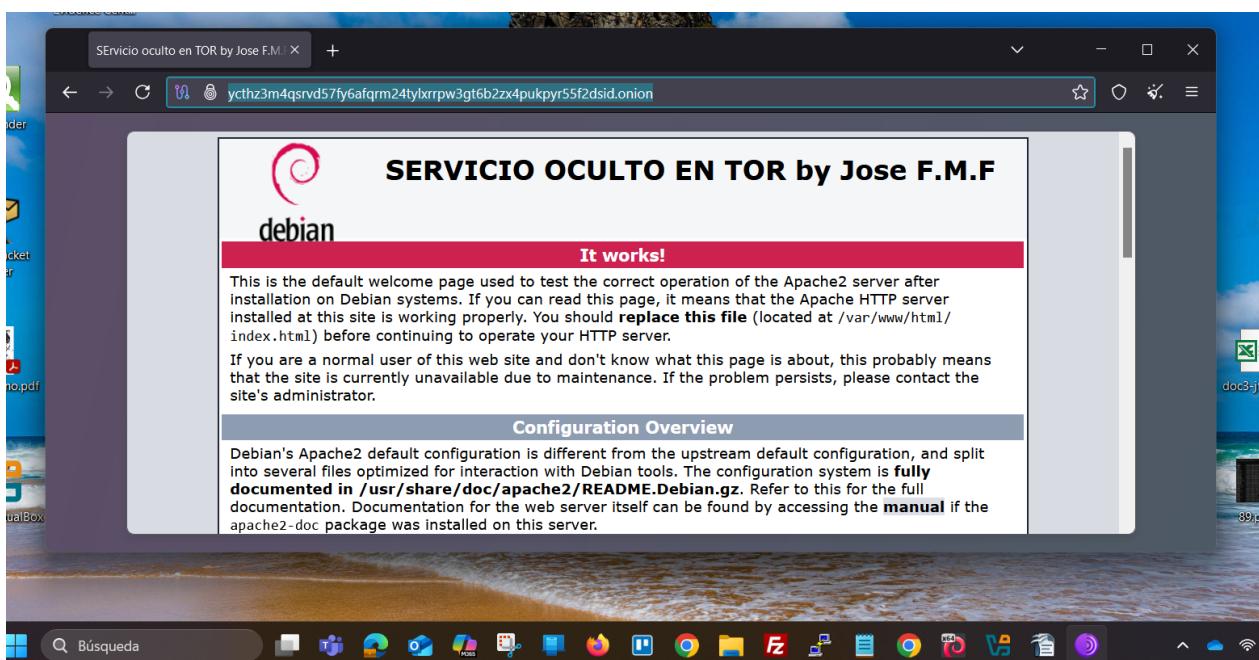
## 7. Verificación remota de los *Hidden Services*

Vamos a conectarnos desde otra máquina Windows remota a través de la red TOR a los servicios ocultos que hemos exportados en el servidor Debian 11.

### 7.1. Verificación del servicio web oculto en TOR

Podemos conectarnos tanto a través de la red superficial como de la red TOR con la página web alojada en el servidor Debian.

*[Captura. Conexión remota a la red TOR con la página web alojada en el servidor Debian]*



Una cuestión para considerar es si es conveniente que la web sea accesible tanto a través de la red y de TOR, o si por una cuestión de mayor privacidad es conveniente que únicamente esté disponible en la red cebolla y no sea accesible a través de la IP del servidor.

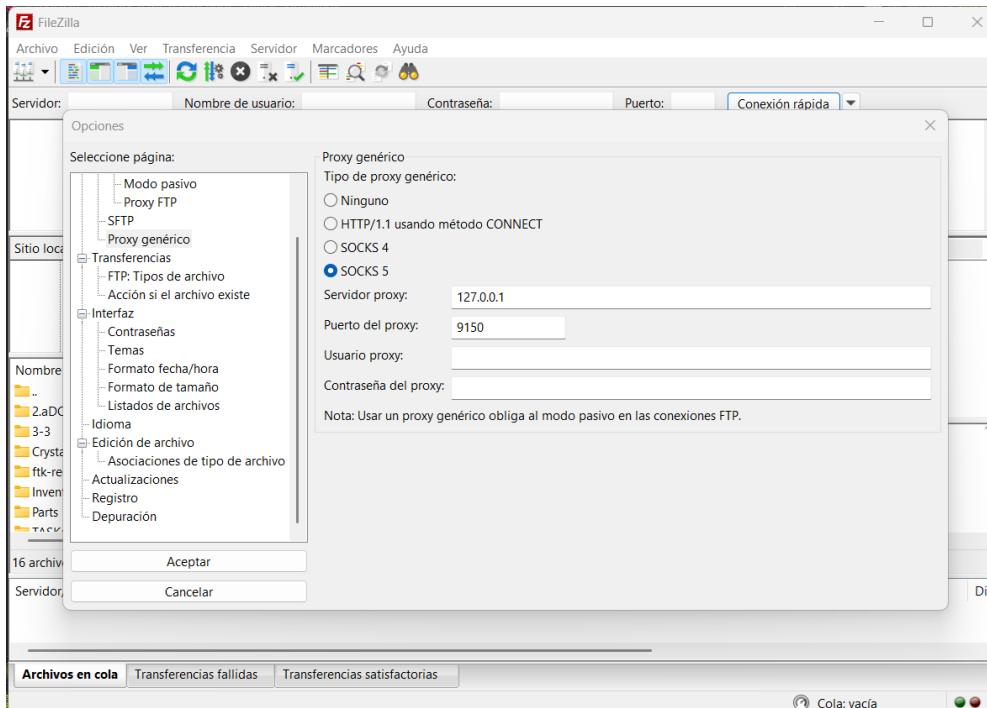
```

SERVIDOR -DEBIAN-JMF [Corriendo] - Oracle VirtualBox
Actividades Terminal 10 de may 11:33
jose@debianOSINT: ~
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/ftp1/hostname
fwoSuxil5bgaiw2tsixeilgj5tubk2zig4gh5tdqbsyxeqncagle5pqd.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/web1/hostname
ycthz3m4qsrqd57fy6afqrm24tylxrrpw3gt6b2zx4pukpyr55f2dsid.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/ssh1/hostname
q34cf1h62twtvydo6p5gd736rhkdu2jkvexb6rjike72g7mync5pdbad.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1# cat /var/lib/tor/hidden_service/irc1/hostname
u2jpjz2mzxqsp5jxtqieueaf1hmof5y7xnq2pibm6yc2dhnhafrbxcad.onion
root@debianOSINT:/var/lib/tor/hidden_service/ftp1#

```

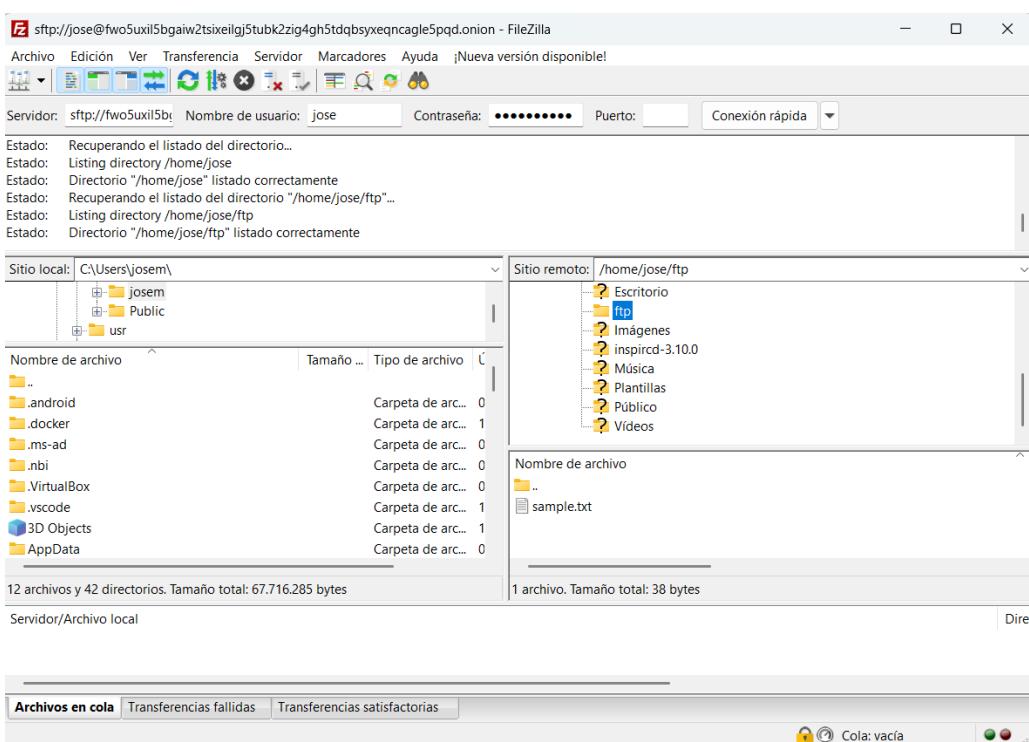
## 7.2. Verificación del servicio FTP oculto en TOR

[Captura. Opciones de configuración del cliente FileZilla]



Estableciendo conexión con el servidor TOR.

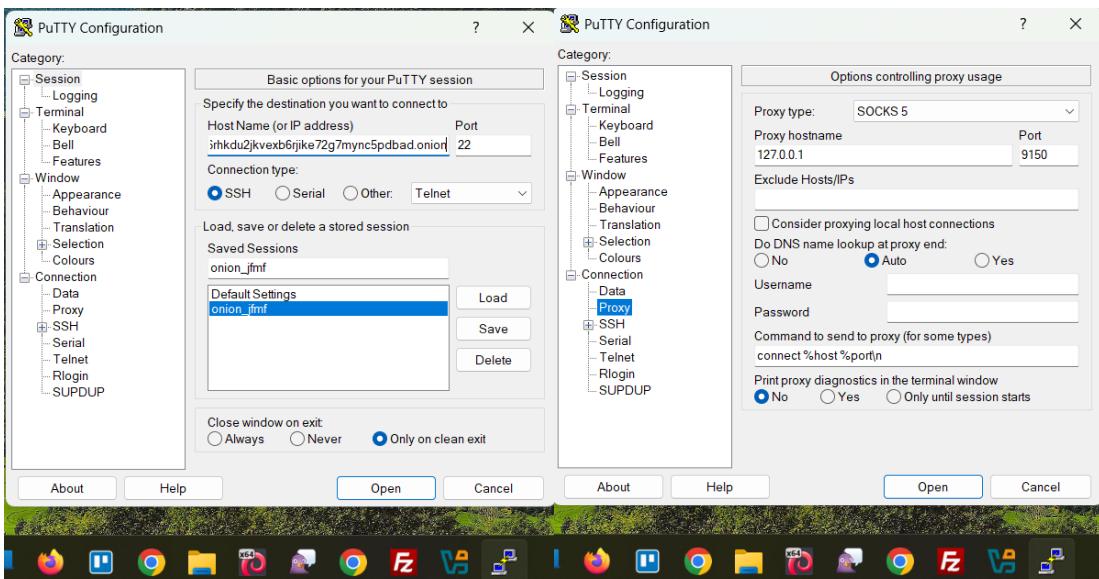
[Captura. Estableciendo conexión con servidor FTP]



## 7.3. Verificación del servicio SSH oculto en TOR

Tenemos que instalar y configurar PUTTY en Windows para poder conectar con el servidor SSH mediante la red TOR.

[Captura. Configuración conexión con servidor SSH]



[Captura. Estableciendo conexión con servidor FTP desde equipo remoto windows]

```
jose@debianOSINT: ~
  Making proxy SOCKS 5 connection to 127.0.0.1 port 9150
  Proxy username:
  Proxy password:
  Will use SOCKS 5 proxy at 127.0.0.1:9150 to connect to q34cfhlh62twtvydo6p5gd7
  36rhhkdu2jkvexb6rjike72g7mync5pbad.onion:22
  Looking up host "127.0.0.1" for proxy
  Connecting to SOCKS 5 proxy at 127.0.0.1 port 9150

  Making primary SSH connection to q34cfhlh62twtvydo6p5gd736rhhkdu2jkvexb6rjike72
  g7mync5pbad.onion
  login as: jose
  jose@q34cfhlh62twtvydo6p5gd736rhhkdu2jkvexb6rjike72g7mync5pbad.onion's password:
  d:
  Linux debianOSINT 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-0
  4-25) x86_64

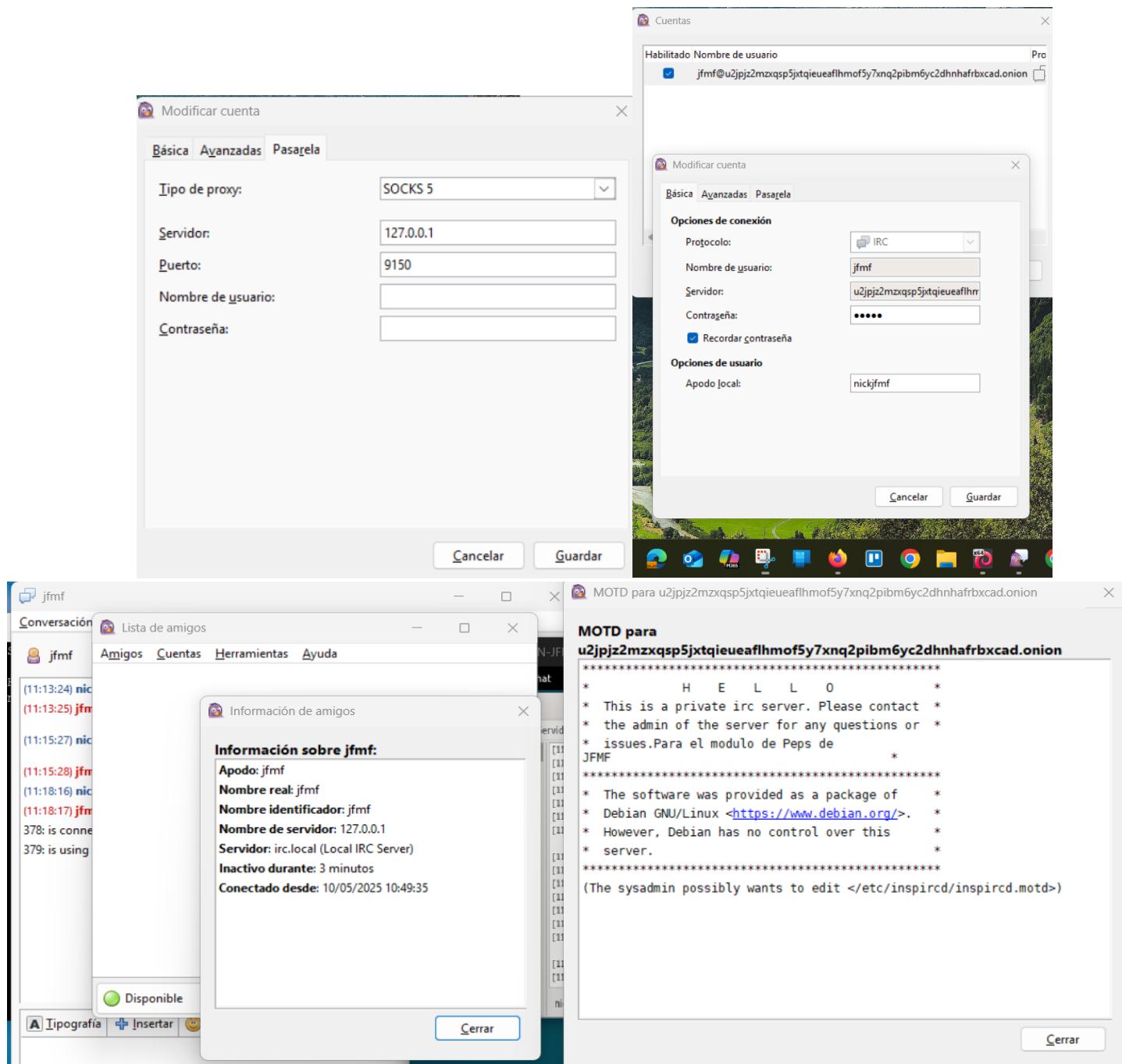
  The programs included with the Debian GNU/Linux system are free software;
  the exact distribution terms for each program are described in the
  individual files in /usr/share/doc/*copyright.

  Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
  permitted by applicable law.
  Last login: Sun May 11 13:16:02 2025 from 127.0.0.1
jose@debianOSINT:~$
```

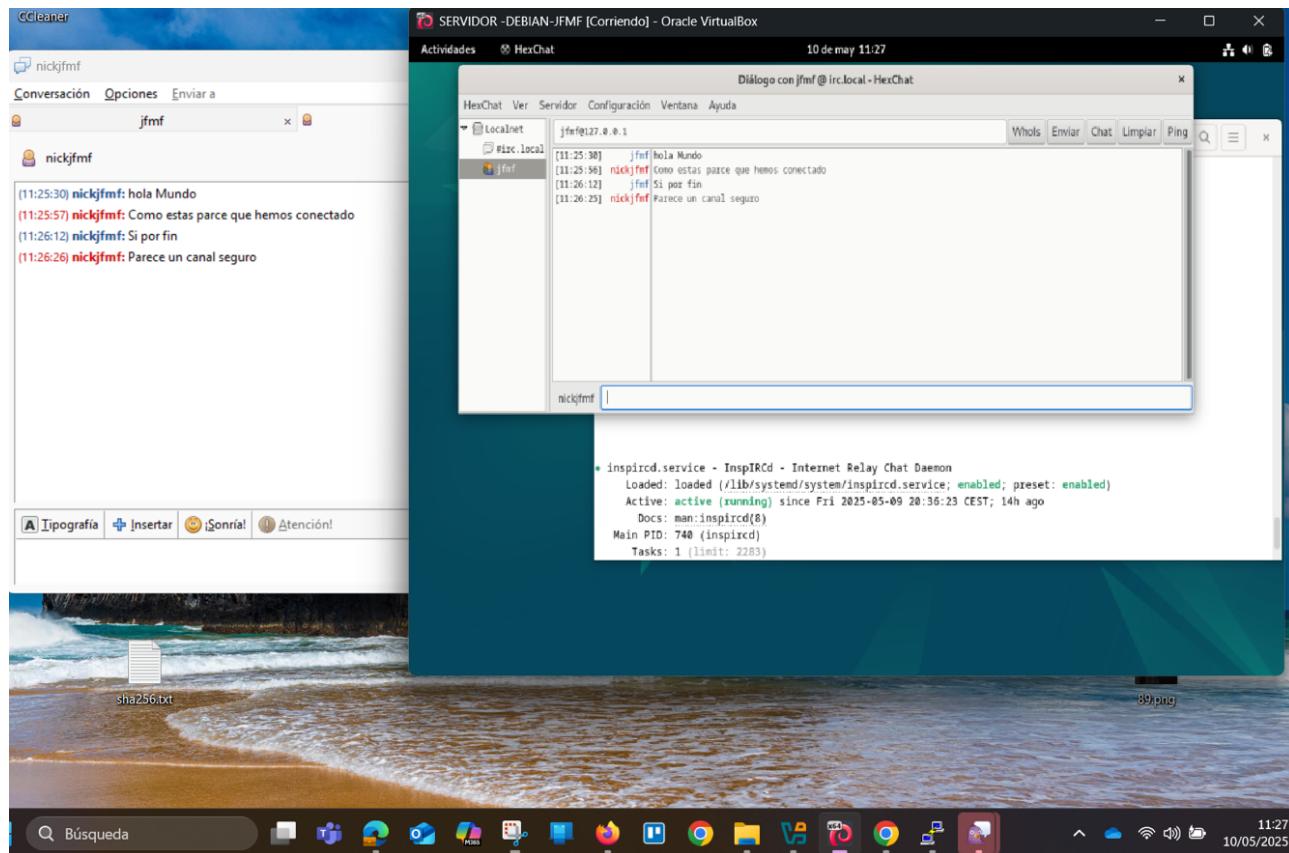
## 7.4. Verificación del servicio IRC oculto en TOR

Instalamos la aplicación [Pidgin](#) en Windows. Una vez instalada realizamos su configuración para poder conectar con la red TOR.

[Captura.Configuración de Pidgin en Windows para conexión con la red Tor equipo Debian Remoto.]



Una vez conectados al servidor IRC desde el cliente *Pigin*, es posible visualizar el mensaje MOTD personalizado, así como intercambiar mensajes con otros usuarios conectados.



## 8. Conclusión

Se debe también responder a la siguiente pregunta teniendo en mente la privacidad del usuario:  
 ¿Es mejor utilizar un mismo dominio **.onion** mapeando diferentes puertos al mismo **.onion** o es mejor generar **hidden services** diferentes?

[

Según la comunidad de expertos en ciberseguridad, es mejor generar **hidden services** diferentes en lugar de mapear diferentes puertos al mismo dominio **.onion**. Aunque se sugiere que es más seguro tener varios servicios en un mismo **.onion**, no se aclara completamente el motivo. Sin embargo, la recomendación general es crear **hidden services** separados para cada servicio que deseas ofrecer.

Esto puede proporcionar una mayor seguridad y aislamiento entre los servicios, reduciendo el riesgo de que el compromiso de uno afecte a los demás. Además, cada **hidden service** puede tener su propia configuración y medidas de seguridad específicas, lo que puede mejorar la protección general de tus servicios en la red Tor.

Otra cuestión para considerar es si es conveniente que la web sea accesible tanto a través de la red y de TOR, o si por una cuestión de mayor privacidad es conveniente que únicamente esté disponible en la red cebolla y no sea accesible a través de la IP del servidor. Yo considero que exponer acceso de un servicio privado en la web en cuanto a seguridad hace que el servidor sea vulnerable y está más expuesto a ataques y a la captura de la información es crucial mantener las comunicaciones a través de SSH.]

## 9. Referencias

- [1] TOR Project, «Proyecto TOR,» [En línea]. Available: <https://www.torproject.org/es/>. [Último acceso: 11 Febrero 2023].
- [2] Kaspersky daily, «¿Qué es TOR?,» [En línea]. Available: <https://www.kaspersky.es/blog/que-es-tor/716/>. [Último acceso: 11 Febrero 2023].
- [3] J. Díaz y (INCIBE), «Tor, servicios ocultos y desanonimización,» 7 Enero 2015. [En línea]. Available: <https://www.incibe-cert.es/blog/tor-servicios-ocultos-desanonimizacion>. [Último acceso: 11 Febrero 2023].
- [4] fwhibbit, «Creación de un Hidden Service de Tor,» 29 Febrero 2016. [En línea]. Available: <https://fwhibbit.es/creacion-de-un-hidden-service-de-tor>. [Último acceso: 11 Febrero 2023].
- [5] Debian, «Debian el Sistema Operativo completamente libre,» [En línea]. Available: <https://www.debian.org/>. [Último acceso: 11 Febrero 2023].
- [6] RedHat, Inc., «Manual de referencia - Opciones de configuración vsftpd,» 2005. [En línea]. Available: <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ftp-vsftpd-conf.html>. [Último acceso: 11 Febrero 2023].
- [7] <https://www.server-world.info/en/>, «Debian 11 - SSH Server,» 17 Agosto 2021. [En línea]. Available: [https://www.server-world.info/en/note?os=Debian\\_11&p=ssh&f=1](https://www.server-world.info/en/note?os=Debian_11&p=ssh&f=1). [Último acceso: 11 Febrero 2023].
- [8] OpErs LiNuX - La Red De Los Informáticos, «Como Crear Tu Propio IRC | Configurar Inspircd IRC En Linux,» 30 Diciembre 2020. [En línea]. Available: [https://youtu.be/1LzQWE4Ono?list=PLDywZyvGCR60KWgp2Dslvm4AkpeoG7gt\\_&t=478](https://youtu.be/1LzQWE4Ono?list=PLDywZyvGCR60KWgp2Dslvm4AkpeoG7gt_&t=478). [Último acceso: 11 Febrero 2023].
- [9] T. Isasia, «PoC: Instalación de un Hidden Service en TOR con una Máquina Virtual Debian 9,» 27 Octubre 2017. [En línea]. Available: <https://www.tiiizss.com/2017/10/27/pocinstalacion-hidden-service-tor-una-maquina-virtual-debian-9/>. [Último acceso: 11 Febrero 2023].
- [10] «Crear un hidden service (una pagina .onion) desde 0,» 24 Junio 2014. [En línea]. Available: <http://drvy.blogspot.com/2014/06/crear-pagina-onion-servidor.html>. [Último acceso: 11 Febrero 2023].
- [11] A. Wolf, «Tor Hidden Services,» 21 Abril 2019. [En línea]. Available: <https://roll.urown.net/server/tor/tor-hidden-service.html>. [Último acceso: 11 Febrero 2023].
- [12] My Sysadmin Cheatsheet, «Use ".onion" Address to Connect to SSH Server over Tor Hidden Service,» 10 Noviembre 2017. [En línea]. Available: <https://docs.j7k6.org/ssh-torionion-adress/>. [Último acceso: 11 Febrero 2023].

# Resultados de Aprendizaje y Criterios de Evaluación

| <b>Contenidos</b>  |  |
|--|--|
| <b>Resultados de aprendizaje</b>   | <b>Criterios de evaluación</b>   |
| <b>RA 2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.</b> | <p>a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).</p> <p>b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.</p> <p>c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.</p> <p>d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.</p> |