CHALLENGE 5 HOTH

1-Vpn

1.1-Introduction

During field missions, our Generals and Captains must have access to xxxx.local network from outside the network in a secure mode, in order to work in the local area network and be able to use shared resources such as the printers. For that purpose, we want to use a VPN (openVPN) with auto signed local digital certificates, both for server and each of the necessary clients. Generals' command booth is implemented on a Linux Debian 10 machine while Captains' command booth is a Windows 10 machine. Checking must be done from Coruscant network (coruscant.capital).

1.2-Configuration

Install openvpn in the router machine

Step 1 — Installing OpenVPN and EasyRSA

apt install openvpn

Download EasyRsa using wget and the url of the latest release

wget -P ~/ https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

Extract the file

tar xvf EasyRSA-unix-v3.0.6.tgz

Step 2 — Configuring the EasyRSA Variables and Building the CA

In order to sign certificates for all our clients, we must build a CA, this is a certificate authority, also sometimes referred to as a certification authority, is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates. A digital certificate provides:

Authentication, by serving as a credential to validate the identity of the entity that it is issued to.

Encryption, for secure communication over insecure networks such as the Internet.

Integrity of documents signed with the certificate so that they cannot be altered by a third party in transit.

In our case, we are going to use auto signed certificates. But this is not a problem because we don’t care about using these certificates in public, we just need them for our network and to validate them against us.

So, in order to create a CA the steps are:

Go to the created folder

```
cd ~/EasyRSA-v3.0.6/
```

Change the name of the vars.example file to only “vars”

```
cp vars.example vars
```

Open the file to edit it

```
nano vars
```

Find the settings that set field defaults for new certificates.

COUNTRY VALUE →	set_var EASYRSA_REQ_COUNTRY "HO"
PROVINCE VALUE →	set_var EASYRSA_REQ_PROVINCE "Hoth"
CITY VALUE →	set_var EASYRSA_REQ_CITY "Hoth"
ORGANIZATION VALUE →	set_var EASYRSA_REQ_ORG "Hoth"
EMAIL VALUE →	set_var EASYRSA_REQ_EMAIL "hoth@hoth.ally"
ORGANIZATIONAL UNIT VALUE →	set_var EASYRSA_REQ_OU "hoth"

Run the script that is in the easy rsa folder with the init-pki option to initiate the public key infrastructure on the CA server

```
./easyrsa init-pki
```

Run the script again but using the build-ca option, this will create the CA and 2 files ca.crt and ca.key

```
./easyrsa build-ca nopass
```

Step 3 — Creating the Server Certificate, Key, and Encryption Files

With this command below you will create a private key with name “server” (server.key) and a certificate request file called server.req

```
./easyrsa gen-req server nopass
```

Copy the server key to the /etc/openvpn/ directory

```
cp ~/EasyRSA-v3.0.6/pki/private/server.key /etc/openvpn/
```

Use this command to sign the request

```
./easyrsa sign-req server server
```

It will ask for confirmation, so just type “yes” and press enter

Then copy the server.crt and ca.crt files to the openvpn folder

```
cp pki/issued/server.crt /etc/openvpn
cp pki/ca.crt /etc/openvpn
```

Back to the easy rsa folder, we generate the dh.pem file with this command:

To use perfect forward secrecy cipher suites, you must set up Diffie-Hellman parameters (on the server side), or the PFS cipher suites will be silently ignored.

```
./easyrsa gen-dh
```

We generate an HMAC signature to strengthen the server’s TLS integrity verification capabilities:

```
openvpn --genkey --secret ta.key
```

We copy both ta.key and dh.pem to the openvpn:

```
cp ~/EasyRSA-v3.0.6/ta.key /etc/openvpn/
cp ~/EasyRSA-v3.0.6/pki/dh.pem /etc/openvpn/
```

Step 4 — Generating a Client Certificate and Key Pair

We create the folder to store the keys and client certificates

```
mkdir -p ~/client-configs/keys
```

We give the proper permissions to the folder:

chmod -R 700 ~/client-configs

We run the easyrsa script with the gen-req and nopass options, and with the common name for the client:

./easyrsa gen-req hothclient1 nopass

Then we type yes and this will create a client certificate named hothclient1.crt

And we copy the crt file to our client-config folder:

cp pki/issued/hothclient1.crt ~/client-configs/keys/

We also need to copy the key to our client-config folder:

cp pki/private/hothclient1.key /home/hoth/client-configs/keys/

We copy the ca.crt file and the ta.key to our client-config folder:

cp ~/EasyRSA-v3.0.6/ta.key ~/client-configs/keys/

cp /etc/openvpn/ca.crt ~/client-configs/keys/

Step 5 — Configuring the OpenVPN Service

Copy a sample openvpn conf file to our openvpn folder, then we extract it.

cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
gzip -d /etc/openvpn/server.conf.gz

The value of the parameter key-direction is different in both server and client configs.
The advantage of using different keys for each direction is that packets originating from one peer can never be replayed back to that peer by a man-in-the-middle attacker. Of course the underlying TLS and OpenVPN protocols *should* never accept such packets, but the goal of tls-auth is to offer (some) protection against bugs in the protocol or implementation that cause the underlying mechanisms to fail.

We edit it:

nano /etc/openvpn/server.conf

local 172.20.202.35 ----> the ip of our vpn server
port 1194 ----> the port in which our vpn server is listening
proto tcp ----> the protocol used

```
dev tun ---->
ca /etc/openvpn/ca.crt ----> we specify the route to our ca.crt file
cert /etc/openvpn/server.crt ----> we specify the route to our server.crt file
key /etc/openvpn/server.key ----> we specify the route to our server.key file
tls-auth ta.key 0
key-direction 0
dh /etc/openvpn/dh.pem ----> we specify the route to our dh.pem file
server 192.168.6.0 255.255.255.0 ----> we specify the network that the client will join when using vpn
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "route 192.168.50.0 255.255.255.0" --> we specify the network that the client will be pushed into
cipher AES-256-CBC ----> the cipher mode
auth SHA256
verb 3
user nobody
group nogroup
status /var/log/openvpn/openvpn-status.log
```

Step 6 — Adjusting the Server Networking Configuration (This step is not needed as we have activated the routing using our firewall rules)

Edit the sysctl.conf file

```
nano /etc/sysctl.conf
```

We edit this line and set a 1 instead of a 0 (

```
net.ipv4.ip_forward = 1
```

Start the the openvpn service

```
systemctl start openvpn@server
```

Step 7 — Creating the Client Configuration Infrastructure

Create a new directory where you will store client configuration files:

```
mkdir -p ~/client-configs/files
```

Copy an example client configuration file into the client-configs directory

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
~/client-configs/base.conf
```

Edit it using nano

```
nano ~/client-configs/base.conf
```

```
client
```

```
dev tun
proto tcp
remote 172.20.202.35 1194
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
key-direction 1
remote-cert-tls server
cipher AES-256-CBC
auth SHA256
verb 3
```

Create a simple script

nano ~/client-configs/make_config.sh

We add the following:

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=/home/sammy/client-configs/keys
OUTPUT_DIR=/home/sammy/client-configs/files
BASE_CONFIG=/home/sammy/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

Give permissions to the script

chmod 700 ~/client-configs/make_config.sh

Step 8 — Generating Client Configurations

Go to the root folder we created
cd ~/client-configs

Run the script with a name to create the ovpn file for your client:

```
./make_config.sh hothclient1
```

We will get a file called hothclient1.ovpn

Creating a brand new client configuration:
First we go do the easyrsa folder :

```
    cd ~/EasyRSA-v3.0.6
```

Then we generate a new req and key file for the client using this command:

```
    ./easyrsa gen-req prueba2 nopass
```

We sign the request and a new crt file will be created in the pki/issued folder

```
     ./easyrsa sign-req client prueba2
```

Then we copy both files into our client-config folder where we have the neccessary script to generate an ovpn file:

```
    cp pki/private/prueba2.key /home/hoth/client-configs/keys/
    cp pki/issued/prueba2.crt /home/hoth/client-configs/keys/
```

We go to the directory where we copied them and we execute the script:

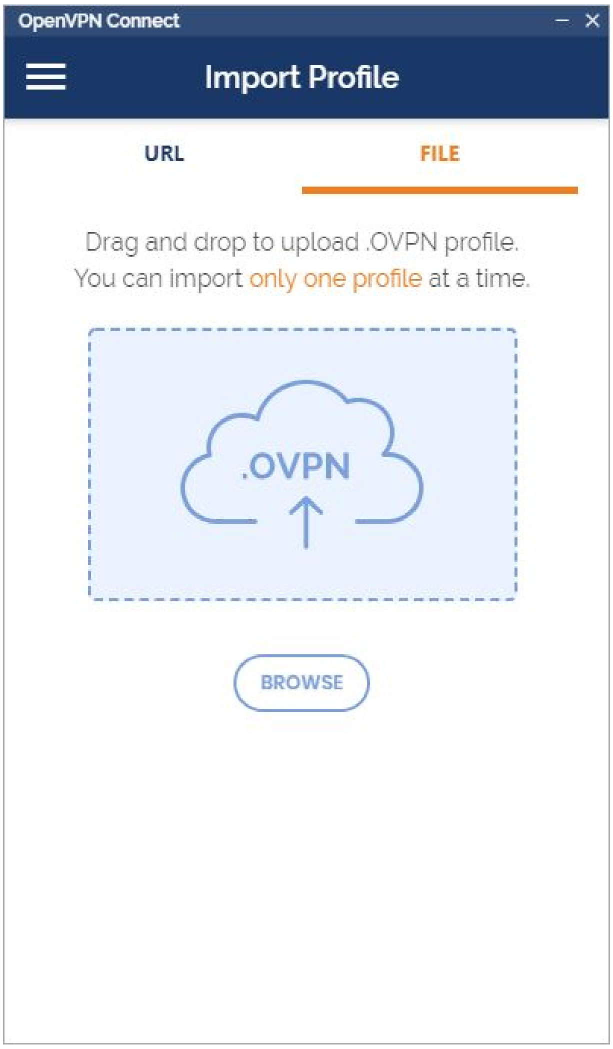
```
    cd /home/hoth/client-configs/
    ./make_config.sh prueba2
```

1.3-Checkings

In order to do the checking we are going to need a program, in this case “OpenVpn” to use these ovpn files. We will need to install it from the official web page of OpenVpn, it is very easy and quick.

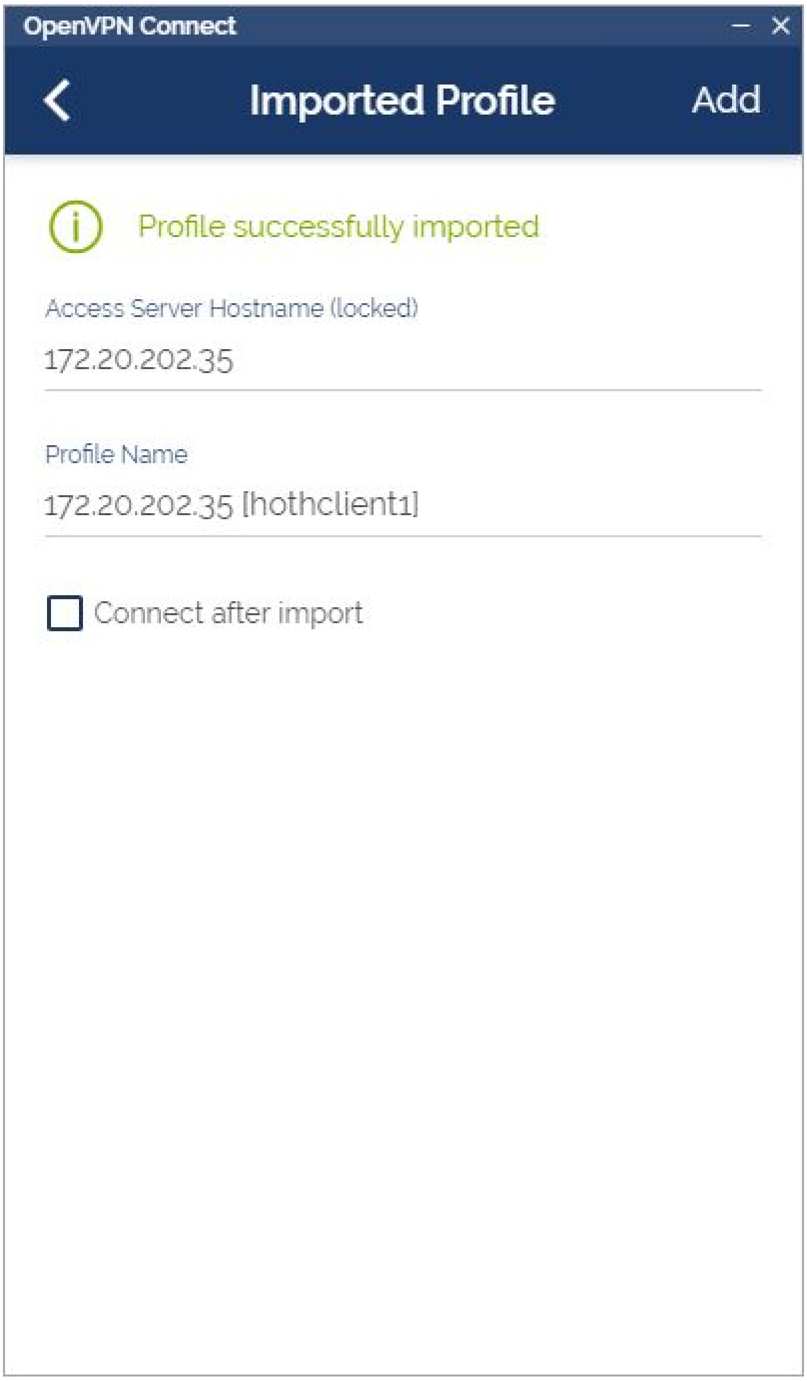
A new file with the ovpn extension has been created in the client-configs files folder, the only thing left to do is copying this file to the client and open it with the openvpn program:

1-Open the OpenVpn program
2-Click on File in order to upload the o.vpn file:



Drag and drop to upload .OVPN profile.
You can import only one profile at a time.

3-Import the .ovpn file



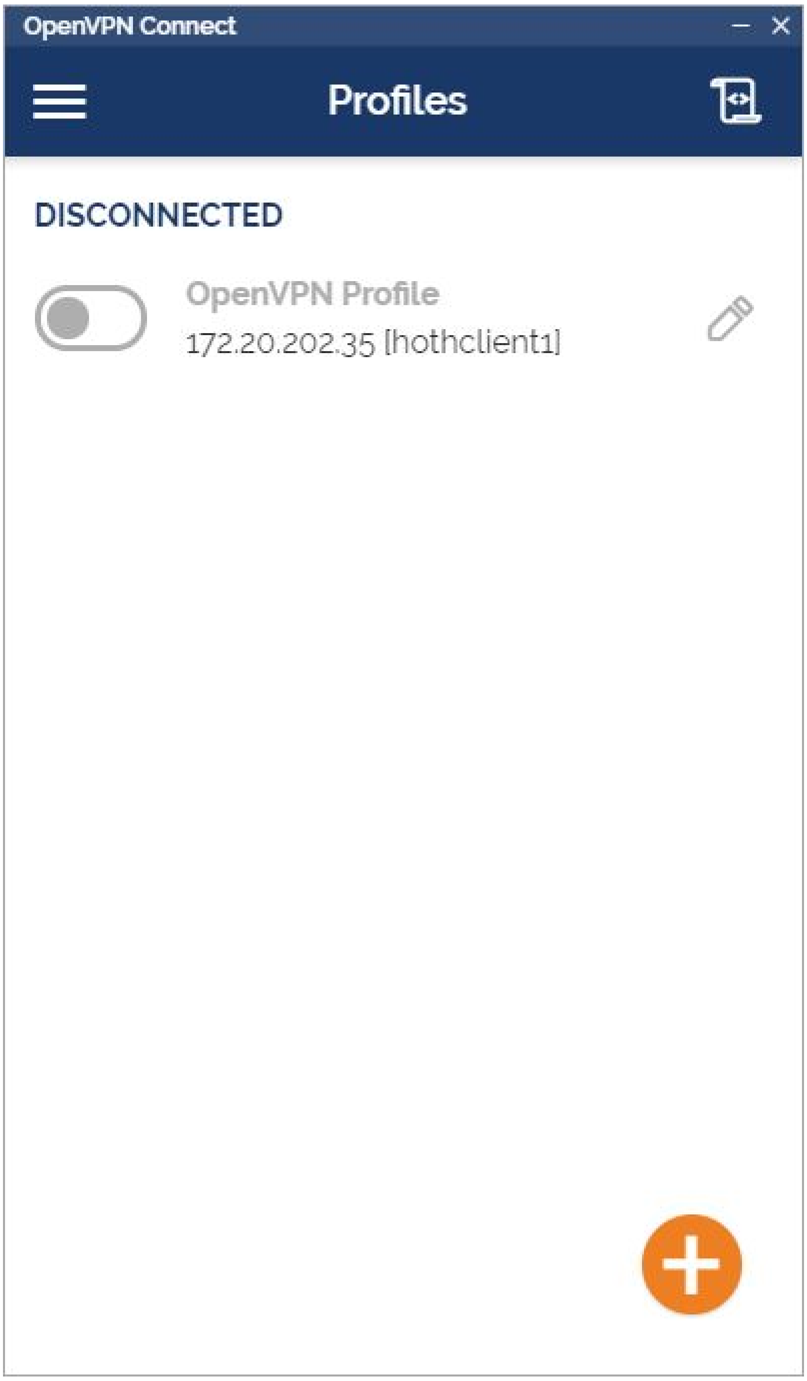
Profile successfully imported

Access Server Hostname (locked)
172.20.202.35

Profile Name
172.20.202.35 [hothclient1]

□ Connect after import

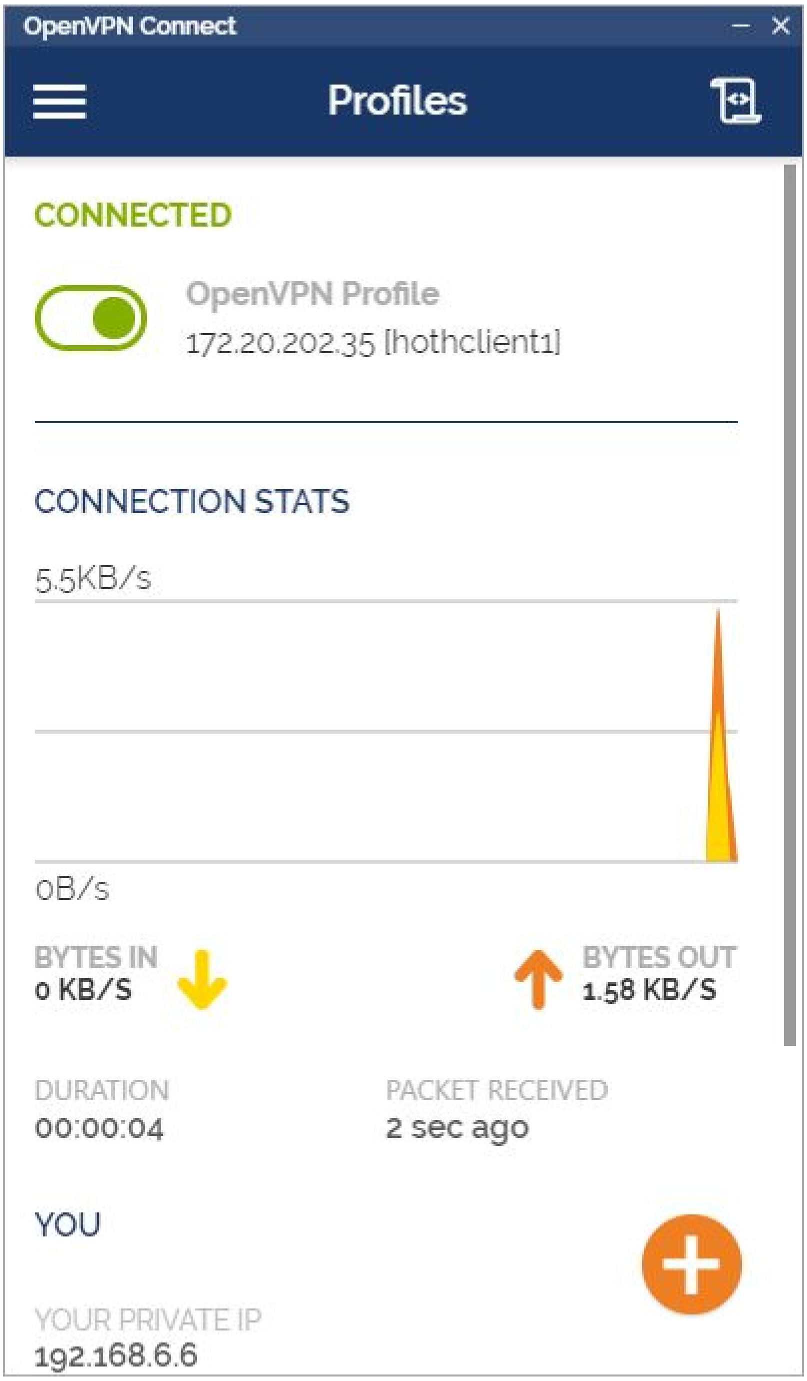
4-Click on “ADD”



DISCONNECTED

OpenVPN Profile
172.20.202.35 [hothclient1]

Now the file is correctly added to openvpn, just switch it on:



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile
172.20.202.35 [hothclient1]

CONNECTION STATS

BYTES IN
0 KB/S

BYTES OUT
1.58 KB/S

DURATION
00:00:04

PACKET RECEIVED
2 sec ago

YOU

YOUR PRIVATE IP
192.168.6.6

As you can see it has successfully connected using the .ovpn file and we now have a private ip: 192.168.6.6

1.4-Firewall rules for the vpn :

Define a variable for our vpn network
RED_VPN=192.168.6.0/24

Accept access from the tcp port 1194 (OpenVpn)
iptables -A INPUT -p tcp --dport 1194 -j ACCEPT

Forward packets from the network of our vpn (192.168.6.0/24)
iptables -A FORWARD -s $RED_VPN -p icmp -j ACCEPT

2-HTTP/HTTPS

2.1-Introduction

It is time to work in the access to remote information, giving our allies that are in the external networks access to the information inside and for this purpose we are going to use HTTPS protocol. We have decided to use this protocol because it is more secure for clients and server and our web pages are going to be authentified. We are going to have two main websites, www.hoth.ally, where the webpages of our Jedi Masters are going to be stored and intranet.hoth.ally. We are going to need the certificates and the LDAP server used in the last challenge so that we reach the highest security. We must ensure that this machine is an Ldap client.

2.2-Server configuration

First of all we have to install apache2 and create our webpage`s directories in /var/www directory with its correspondent permissions.

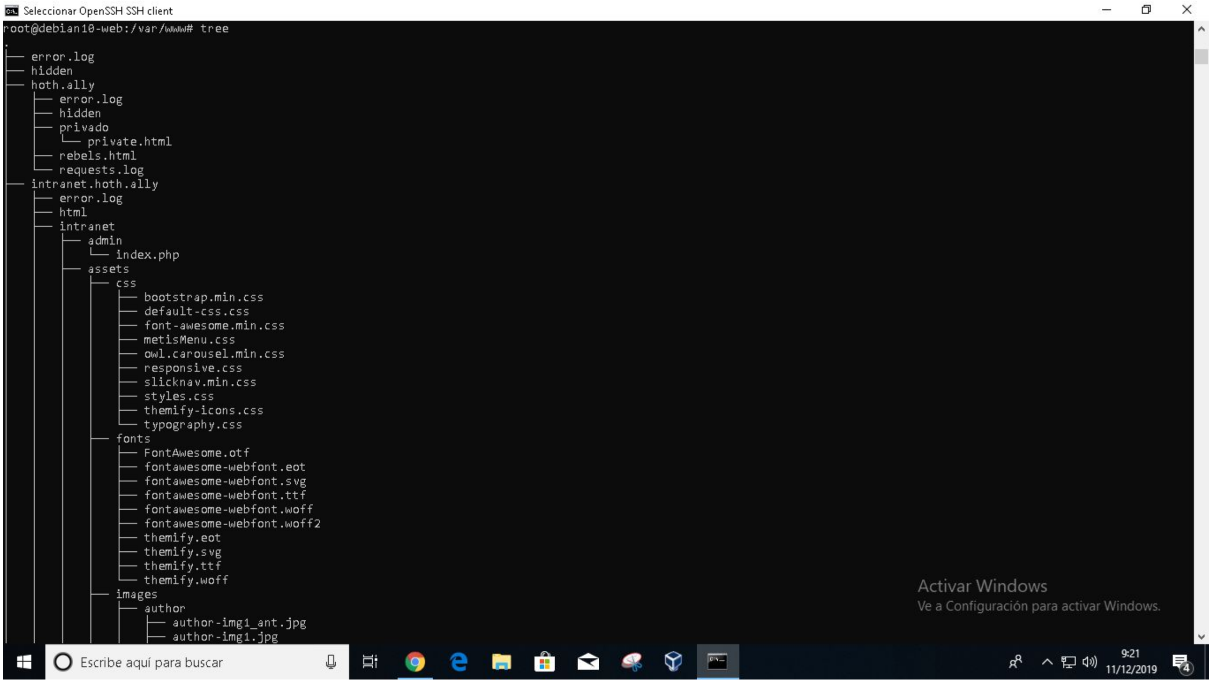
apt install apache2

mkdir -p /var/www/hoth.ally/html

chmod -R 755 /var/www/hoth.ally

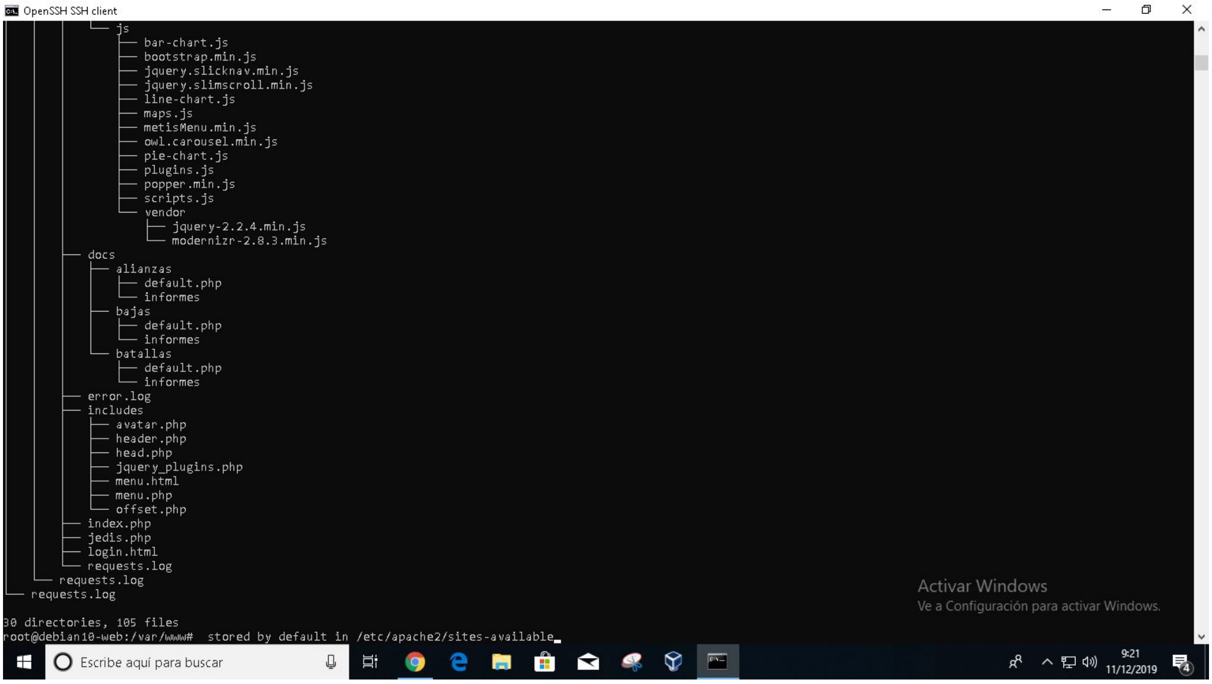
nano /var/www/hoth.ally/html/rebels.html

This it the tree structure our documents stored in /var/www are going to have



Seleccionar OpenSSH SSH client
Activar Windows
Ve a Configuración para activar Windows.
Escribe aquí para buscar
9:21
11/12/2019

```
root@debian10-web:/var/www# tree
.
├── error.log
├── hidden
├── hoth.ally
│   ├── error.log
│   ├── hidden
│   ├── privado
│   │   └── private.html
│   ├── rebels.html
│   └── requests.log
├── intranet.hoth.ally
│   ├── error.log
│   ├── html
│   ├── intranet
│   │   ├── admin
│   │   │   └── index.php
│   │   ├── assets
│   │   │   ├── css
│   │   │   │   ├── bootstrap.min.css
│   │   │   │   ├── default-css.css
│   │   │   │   ├── font-awesome.min.css
│   │   │   │   ├── metisMenu.css
│   │   │   │   ├── owl.carousel.min.css
│   │   │   │   ├── responsive.css
│   │   │   │   ├── slicknav.min.css
│   │   │   │   ├── styles.css
│   │   │   │   ├── themify-icons.css
│   │   │   │   └── typography.css
│   │   │   ├── fonts
│   │   │   │   ├── FontAwesome.otf
│   │   │   │   ├── fontawesome-webfont.eot
│   │   │   │   ├── fontawesome-webfont.svg
│   │   │   │   ├── fontawesome-webfont.ttf
│   │   │   │   ├── fontawesome-webfont.woff
│   │   │   │   ├── fontawesome-webfont.woff2
│   │   │   │   ├── themify.eot
│   │   │   │   ├── themify.svg
│   │   │   │   ├── themify.ttf
│   │   │   │   └── themify.woff
│   │   │   ├── images
│   │   │   │   ├── author
│   │   │   │   │   ├── author-img1_ant.jpg
│   │   │   │   │   ├── author-img1.jpg
```



```
│   │   │   └── js
│   │   │       ├── bar-chart.js
│   │   │       ├── bootstrap.min.js
│   │   │       ├── jquery.slicknav.min.js
│   │   │       ├── jquery.slimscroll.min.js
│   │   │       ├── line-chart.js
│   │   │       ├── maps.js
│   │   │       ├── metisMenu.min.js
│   │   │       ├── owl.carousel.min.js
│   │   │       ├── pie-chart.js
│   │   │       ├── plugins.js
│   │   │       ├── popper.min.js
│   │   │       ├── scripts.js
│   │   │       └── vendor
│   │   │           ├── jquery-2.2.4.min.js
│   │   │           └── modernizr-2.8.3.min.js
│   │   ├── docs
│   │   │   ├── alianzas
│   │   │   │   ├── default.php
│   │   │   │   └── informes
│   │   │   ├── bajas
│   │   │   │   ├── default.php
│   │   │   │   └── informes
│   │   │   └── batallas
│   │   │       ├── default.php
│   │   │       └── informes
│   │   ├── error.log
│   │   ├── includes
│   │   │   ├── avatar.php
│   │   │   ├── header.php
│   │   │   ├── head.php
│   │   │   ├── jquery_plugins.php
│   │   │   ├── menu.html
│   │   │   ├── menu.php
│   │   │   └── offset.php
│   │   ├── index.php
│   │   ├── jedis.php
│   │   ├── login.html
│   │   └── requests.log
│   └── requests.log
└── requests.log

30 directories, 105 files
root@debian10-web:/var/www#  stored by default in /etc/apache2/sites-available_
```

We are going to need some modules for the correct configuration.

cd /etc/apache2/mods-available

a2enmod userdir

Here we can check all the activated modules.

ls /etc/apache2/mods-enabled

After enabling the module, we have to create in our Jedi Masters webpage

This is going to be the main configuration file for our www.hoth.ally webpage:

nano /etc/apache2/sites-available/hoth.ally.conf

```
#Declaramos que va a escuchar peticiones HTTP por el puerto 80
<VirtualHost *:80>
        #Nombre y administrador de la web
        ServerName www.hoth.ally
        ServerAdmin yoda@hoth.ally
        # Redirect Requests to SSL
        Redirect permanent "/" "https://www.hoth.ally/"
        ErrorLog /var/www/hoth.ally/error.log
        CustomLog /var/www/hoth.ally/requests.log combined

</VirtualHost>
#Activamos el puerto 443 para escuchar peticiones HTTPS
<VirtualHost *:443>
```

```
   ServerName www.hoth.ally
   ServerAlias www.hoth.ally
   #Establecemos el directorio principal
   DocumentRoot /var/www/hoth.ally
   #Establecemos el archivo que saldrá por defecto
   DirectoryIndex rebels.html
   ErrorLog /var/www/hoth.ally/error.log
   CustomLog /var/www/hoth.ally/requests.log combined
   SSLEngine on
   #Debemos incluir los certificados y sus claves
   SSLCertificateFile /etc/ssl/hoth.pem
   SSLCertificateKeyFile /etc/ssl/key.pem
   SSLCertificateChainFile /etc/ssl/ca.pem
#Prohibir el acceso a cualquier fichero que contenga la palabra private excepto al #localhost
<FilesMatch (?:.*)private(?:.*)>
        #Antes de la version 2.4
        # order deny,allow
        # allow from 127.0.0.1
        # deny from all
        require ip 127.0.0.1
</FilesMatch>
#El directorio hidden sólo será accesible desde los servidores incluidos en el DNS #y desde
el AD local.
<Directory /var/www/hoth.ally/hidden>
        #Antes de la versión 2.4
        #   order deny,allow
        #   allow from ad.hoth.local
        #   allow from *.hoth.ally
        #   deny from all
        require host ad.hoth.local
        require host *.hoth.ally
</Directory>

</VirtualHost>
```

```
nano /etc/apache2/mods-enabled/userdir.conf
   #Solo los Jedi Masters tendrán su página personal
 UserDir home_html
     UserDir disabled
     UserDir enabled windu yoda
    <Directory /home/nfs/*/home_html>
          AllowOverride FileInfo AuthConfig Limit Indexes
          Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
          Require method GET POST OPTIONS
          DirectoryIndex index.html
    </Directory>
</IfModule>
```

We will also have to change the permissions of this directory as may be created with wrong permissions:

cd /home/nfs/

chown -R yoda yoda
chmod 755 yoda

chown -R windu windu

chmod 755 windu

ls /etc/apache2/sites-available

In this directory we can check which sites configurations are available to be uploaded on our webpages. There are two sites (0000-default.conf and default-ssl.conf) by default. They can be enabled by default and they could appear in /etc/apache2/sites-enabled.

To upload a configuration

a2ensite /etc/apache2/sites-available/hoth.ally.conf

After enabling the site it must appear in /etc/apache2/sites-enabled. You can also directly create here the configuration file and it's going to be already available.

To disable a enabled configuration

a2dissite 0000-default.conf

Configuration intranet.hoth.ally

chmod -R 755 /var/www/intranet.hoth.ally

The other webpage we have to create is intranet.hoth.ally and we need and authentication and authorization module. We must enable two modules for the correct LDAP authentication, modules are allocated in this directory:

cd /etc/apache2/mods-available

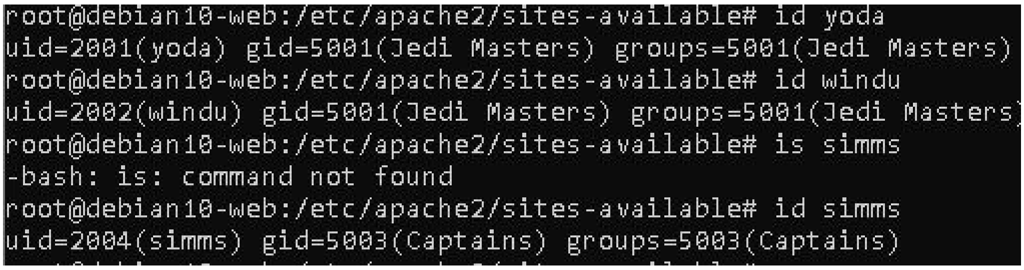
a2enmod auth_basic
a2enmod authnz_ldap

Here we can check all the activated modules.

ls /etc/apache2/mods-enabled

nano /etc/apache2/sites-available/intranet.hoth.ally.conf

```
#Declaramos que va a escuchar peticiones HTTP por el puerto 80
<VirtualHost *:80>
        #Nombre y administrador de la web
        ServerName intranet.hoth.ally
        ServerAdmin yoda@hoth.ally
        # Redirect Requests to SSL
        Redirect permanent "/" "https://intranet.hoth.ally/"
        ErrorLog ${APACHE_LOG_DIR}/example.com.error.log
        CustomLog ${APACHE_LOG_DIR}/example.com.access.log combined
</VirtualHost>
#Activamos el puerto 443 para escuchar peticiones HTTPS
<VirtualHost *:443>
    ServerName intranet.hoth.ally
    ServerAlias intranet.hoth.ally
    #Establecemos el directorio principal
    DocumentRoot /var/www/intranet.hoth.ally/intranet
    #Establecemos el archivo por defecto
    DirectoryIndex login.html
    ErrorLog /var/www/intranet.hoth.ally/intranet/error.log
    CustomLog /var/www/intranet.hoth.ally/intranet/requests.log combined
    #Debemos incluir los certificados y sus claves
    SSLEngine on
    SSLCertificateFile /etc/ssl/hoth.pem
    SSLCertificateKeyFile /etc/ssl/key.pem
    SSLCertificateChainFile /etc/ssl/ca.pem
#Al directorio admin solo podrán acceder los Jedi Masters y los Capitanes tras #previo login contra LDAP
<Directory /var/www/intranet.hoth.ally/intranet/admin>
        Require all denied
        Authname "Admin"
        AuthType Basic
        AuthBasicProvider ldap
        AuthLDAPURL ldap://ad.hoth.ally/dc=hoth,dc=ally?uid
        Require ldap-group cn=Jedi Masters,ou=groups,dc=hoth,dc=ally
        Require ldap-group cn=Captains,ou=groups,dc=hoth,dc=ally
        Require ldap-attribute gidNumber=5001
        Require ldap-attribute gidNumber=5003
```



```
root@debian10-web:/etc/apache2/sites-available# id yoda
uid=2001(yoda) gid=5001(Jedi Masters) groups=5001(Jedi Masters)
root@debian10-web:/etc/apache2/sites-available# id windu
uid=2002(windu) gid=5001(Jedi Masters) groups=5001(Jedi Masters)
root@debian10-web:/etc/apache2/sites-available# is simms
-bash: is: command not found
root@debian10-web:/etc/apache2/sites-available# id simms
uid=2004(simms) gid=5003(Captains) groups=5003(Captains)
```

```
#Index.php es el archivo por defecto
        DirectoryIndex index.php
</Directory>
#El archivo jedis.php sólo podrá verlo el equipo del Active Directory
<Files /var/www/intranet.hoth.ally/intranet/jedis.php>
        Require all denied
        Require host ad.hoth.local
</Files>
#Default.php es la página por defecto de estos documentos
<Directory /var/www/intranet.hoth.ally/intranet/docs/alianzas>
    DirectoryIndex default.php
</Directory>
<Directory /var/www/intranet.hoth.ally/intranet/docs/bajas>
    DirectoryIndex default.php
</Directory>
<Directory /var/www/intranet.hoth.ally/intranet/docs/batallas>
    DirectoryIndex default.php
</Directory>
</VirtualHost>
```

In case you want to check any syntax error in the configuration:

```
sudo apache2ctl configtest
```

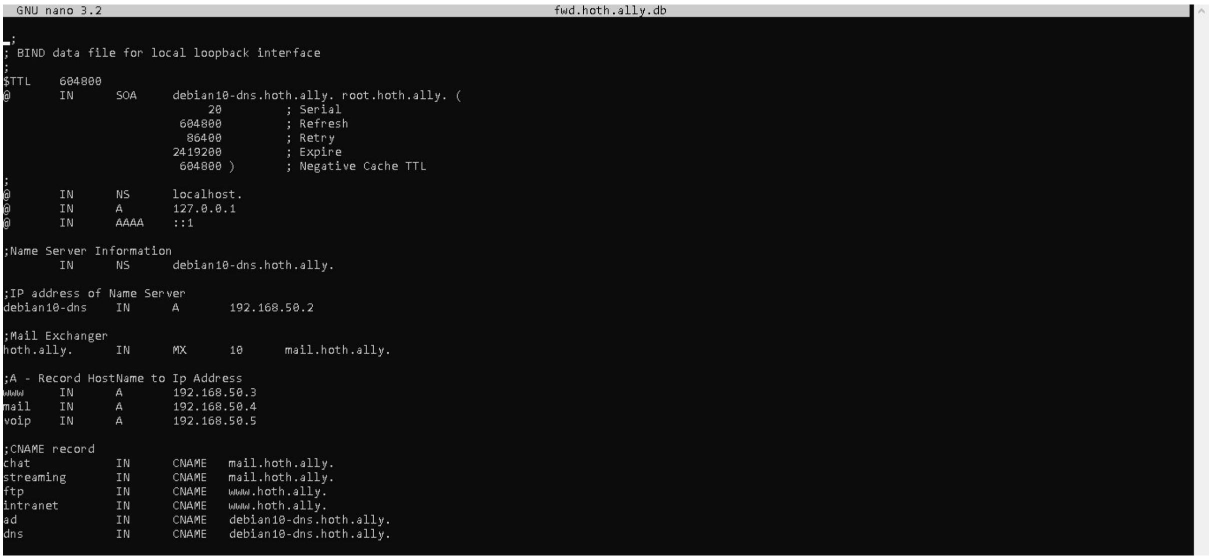
After all the configuration we must restart the service.

```
systemctl restart apache2
```

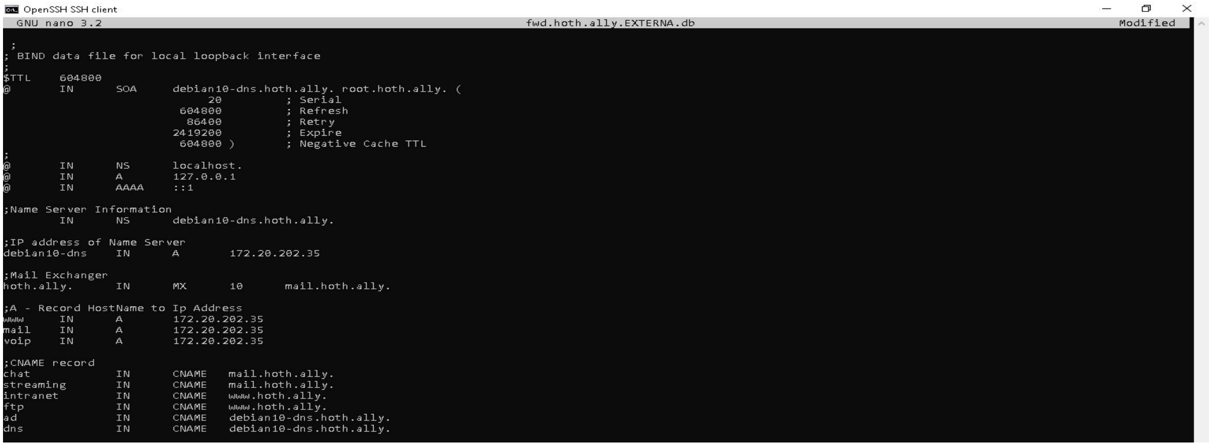
```
systemctl status apache2
```

2.3-Dns and Firewall configuration

We must configure our DNS server in order to be able to enter the websites typing its name. Internal configuration of the reverse and forward zones:

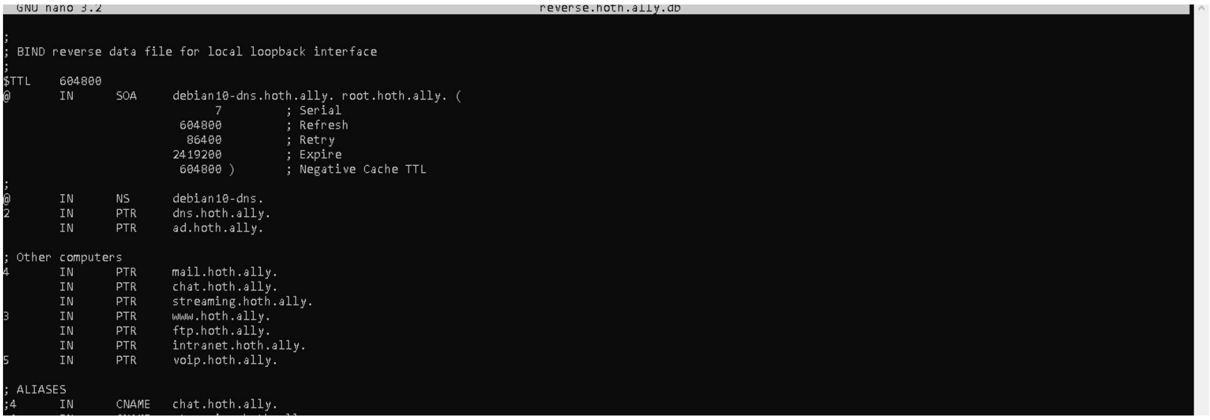


```
  GNU nano 3.2                                     fwd.hoth.ally.db

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian10-dns.hoth.ally. root.hoth.ally. (
                             20         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1

;Name Server Information
        IN      NS      debian10-dns.hoth.ally.

;IP address of Name Server
debian10-dns    IN      A       192.168.50.2

;Mail Exchanger
hoth.ally.      IN      MX      10      mail.hoth.ally.

;A - Record HostName to Ip Address
www     IN      A       192.168.50.3
mail    IN      A       192.168.50.4
voip    IN      A       192.168.50.5

;CNAME record
chat            IN      CNAME   mail.hoth.ally.
streaming       IN      CNAME   mail.hoth.ally.
ftp             IN      CNAME   www.hoth.ally.
intranet        IN      CNAME   www.hoth.ally.
ad              IN      CNAME   debian10-dns.hoth.ally.
dns             IN      CNAME   debian10-dns.hoth.ally.
```

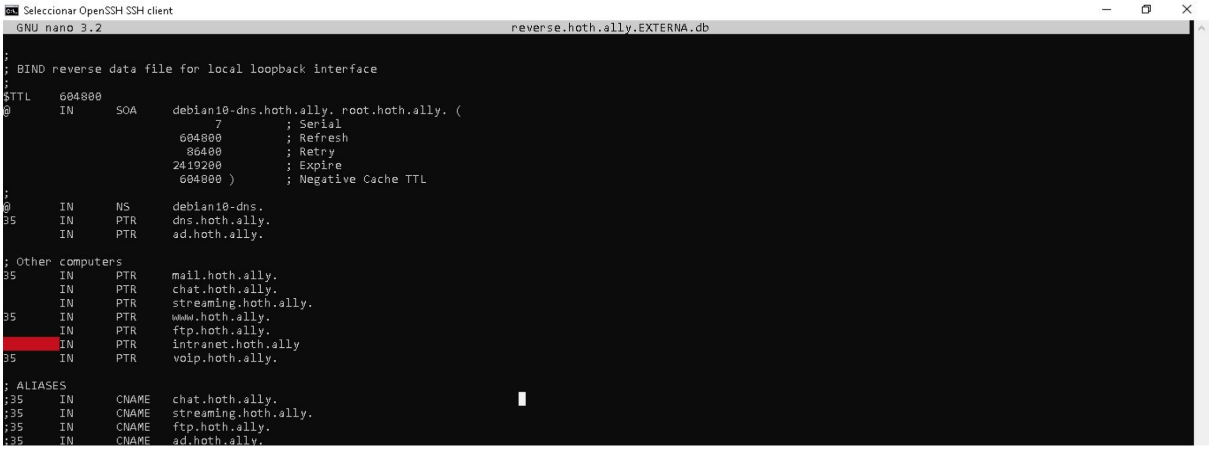


```
  GNU nano 3.2                              fwd.hoth.ally.EXTERNA.db                              Modified

 ;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian10-dns.hoth.ally. root.hoth.ally. (
                             20         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1

;Name Server Information
        IN      NS      debian10-dns.hoth.ally.

;IP address of Name Server
debian10-dns    IN      A       172.20.202.35

;Mail Exchanger
hoth.ally.      IN      MX      10      mail.hoth.ally.

;A - Record HostName to Ip Address
www     IN      A       172.20.202.35
mail    IN      A       172.20.202.35
voip    IN      A       172.20.202.35

;CNAME record
chat            IN      CNAME   mail.hoth.ally.
streaming       IN      CNAME   mail.hoth.ally.
intranet        IN      CNAME   www.hoth.ally.
ftp             IN      CNAME   www.hoth.ally.
ad              IN      CNAME   debian10-dns.hoth.ally.
dns             IN      CNAME   debian10-dns.hoth.ally.
```

External configuration of the reverse and forward zones:



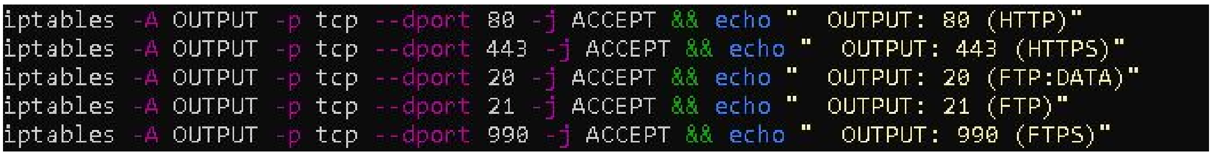
```
  GNU nano 3.2                                                                reverse.hoth.ally.db

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian10-dns.hoth.ally. root.hoth.ally. (
                              7         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian10-dns.
2       IN      PTR     dns.hoth.ally.
        IN      PTR     ad.hoth.ally.

; Other computers
4       IN      PTR     mail.hoth.ally.
        IN      PTR     chat.hoth.ally.
        IN      PTR     streaming.hoth.ally.
3       IN      PTR     www.hoth.ally.
        IN      PTR     ftp.hoth.ally.
        IN      PTR     intranet.hoth.ally.
5       IN      PTR     voip.hoth.ally.

; ALIASES
;4      IN      CNAME   chat.hoth.ally.
```



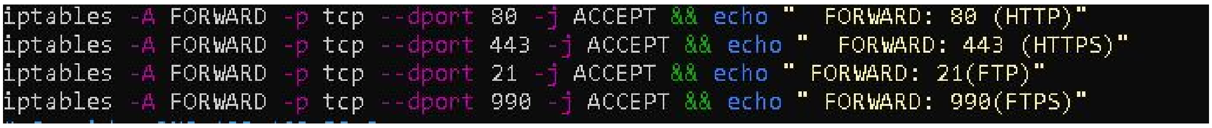
Seleccionar OpenSSH SSH client

```
  GNU nano 3.2                                                            reverse.hoth.ally.EXTERNA.db

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian10-dns.hoth.ally. root.hoth.ally. (
                              7         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian10-dns.
35      IN      PTR     dns.hoth.ally.
        IN      PTR     ad.hoth.ally.

; Other computers
35      IN      PTR     mail.hoth.ally.
        IN      PTR     chat.hoth.ally.
        IN      PTR     streaming.hoth.ally.
35      IN      PTR     www.hoth.ally.
        IN      PTR     ftp.hoth.ally.
        IN      PTR     intranet.hoth.ally
35      IN      PTR     voip.hoth.ally.

; ALIASES
;35     IN      CNAME   chat.hoth.ally.
;35     IN      CNAME   streaming.hoth.ally.
;35     IN      CNAME   ftp.hoth.ally.
;35     IN      CNAME   ad.hoth.ally.
```

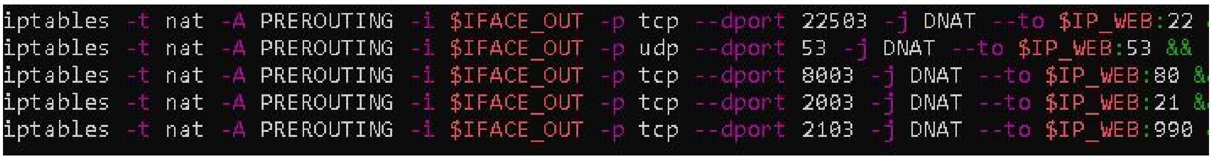
Firewall configuration



```
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT && echo "  OUTPUT: 80 (HTTP)"
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT && echo "  OUTPUT: 443 (HTTPS)"
iptables -A OUTPUT -p tcp --dport 20 -j ACCEPT && echo "  OUTPUT: 20 (FTP:DATA)"
iptables -A OUTPUT -p tcp --dport 21 -j ACCEPT && echo "  OUTPUT: 21 (FTP)"
iptables -A OUTPUT -p tcp --dport 990 -j ACCEPT && echo "  OUTPUT: 990 (FTPS)"
```



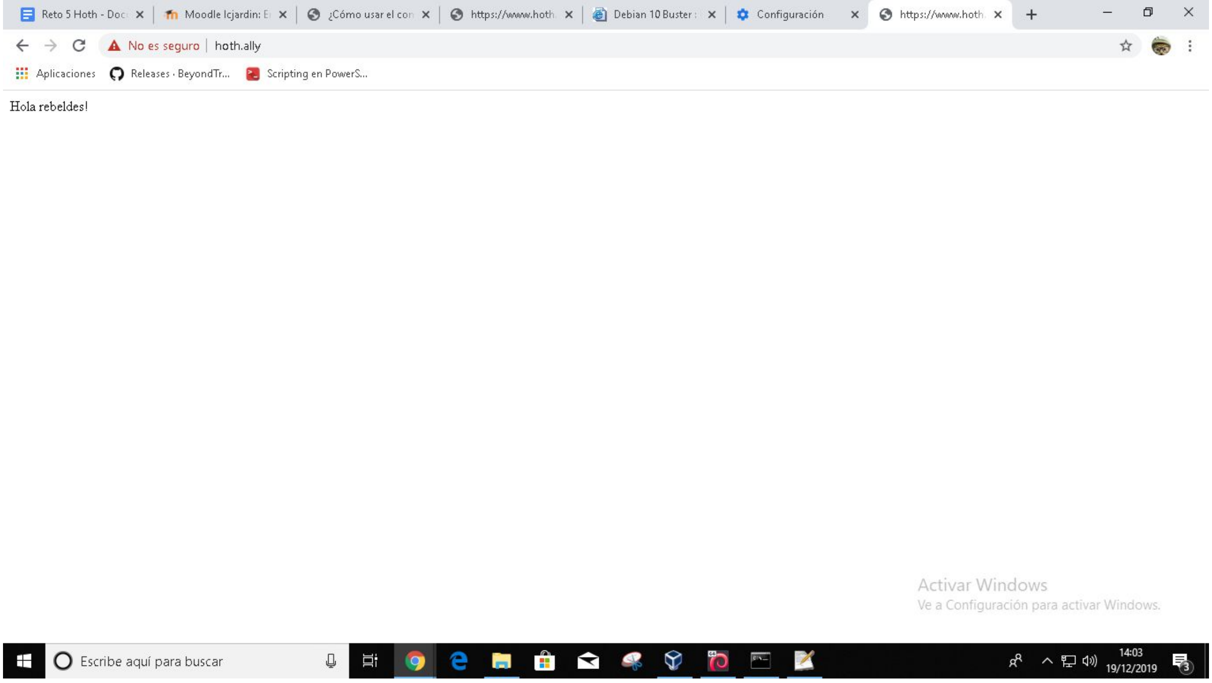
```
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT && echo "  FORWARD: 80 (HTTP)"
iptables -A FORWARD -p tcp --dport 443 -j ACCEPT && echo "  FORWARD: 443 (HTTPS)"
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT && echo " FORWARD: 21(FTP)"
iptables -A FORWARD -p tcp --dport 990 -j ACCEPT && echo " FORWARD: 990(FTPS)"
```



```
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 22503 -j DNAT --to $IP_WEB:22
iptables -t nat -A PREROUTING -i $IFACE_OUT -p udp --dport 53 -j DNAT --to $IP_WEB:53 &&
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 8003 -j DNAT --to $IP_WEB:80 &
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 2003 -j DNAT --to $IP_WEB:21 &
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 2103 -j DNAT --to $IP_WEB:990
```

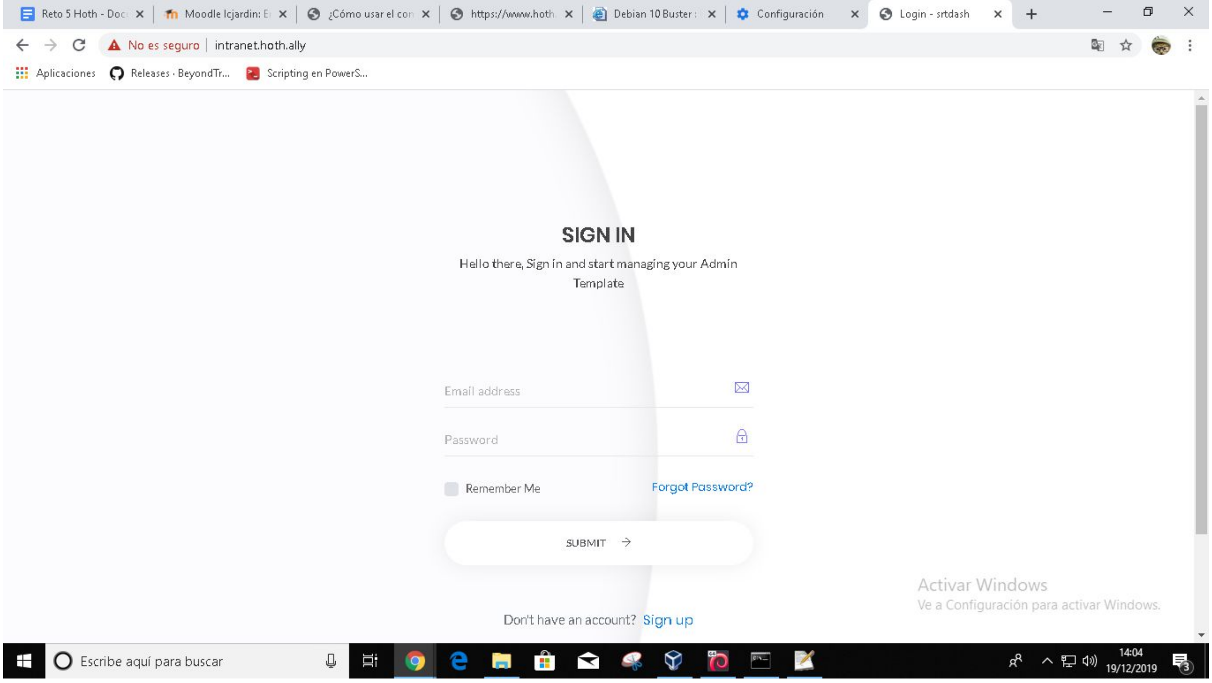
2.4-Checkings

The file that will appear by default is rebels.html and login.html.



hoth.ally

Hola rebeldes!



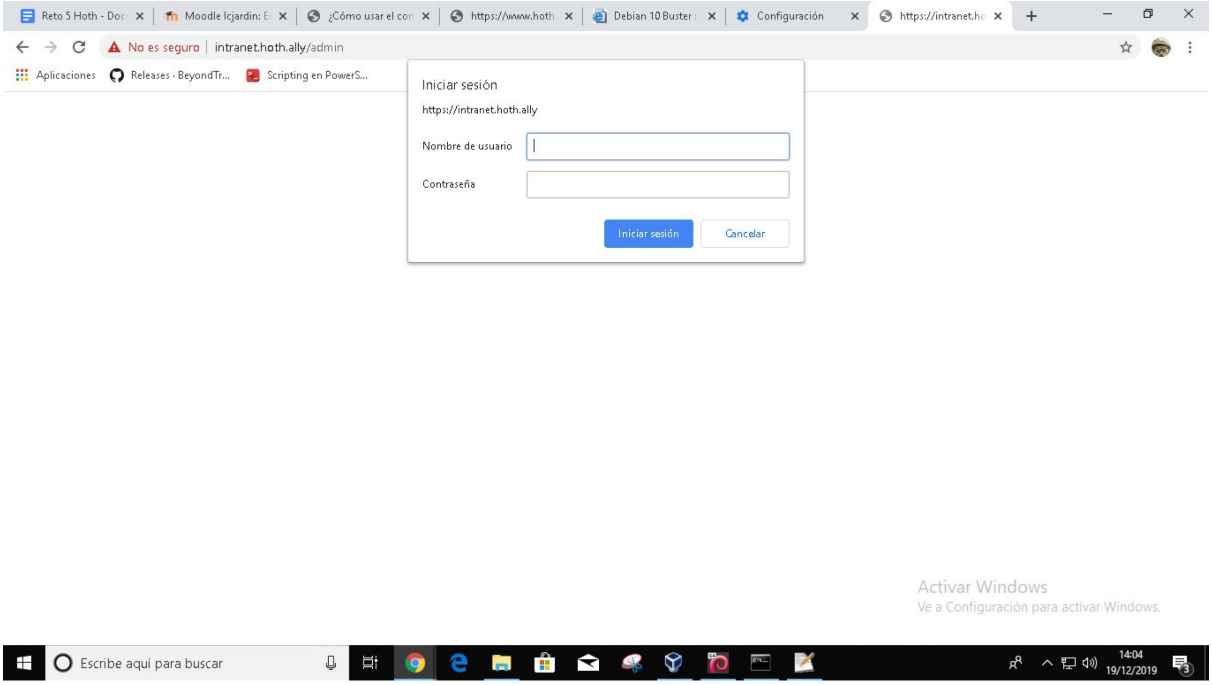
intranet.hoth.ally

SIGN IN

Hello there, Sign in and start managing your Admin Template

Don't have an account? Sign up

Asks for LDAP login and once you enter index.php appears.

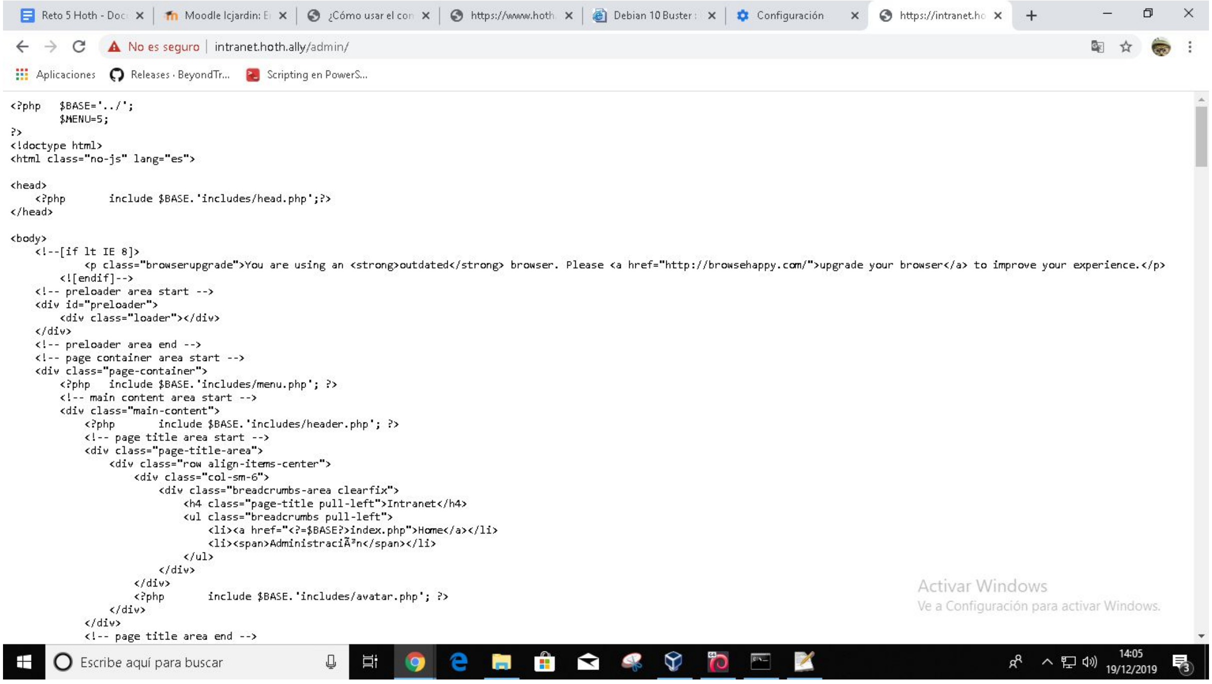


Iniciar sesión

https://intranet.hoth.ally

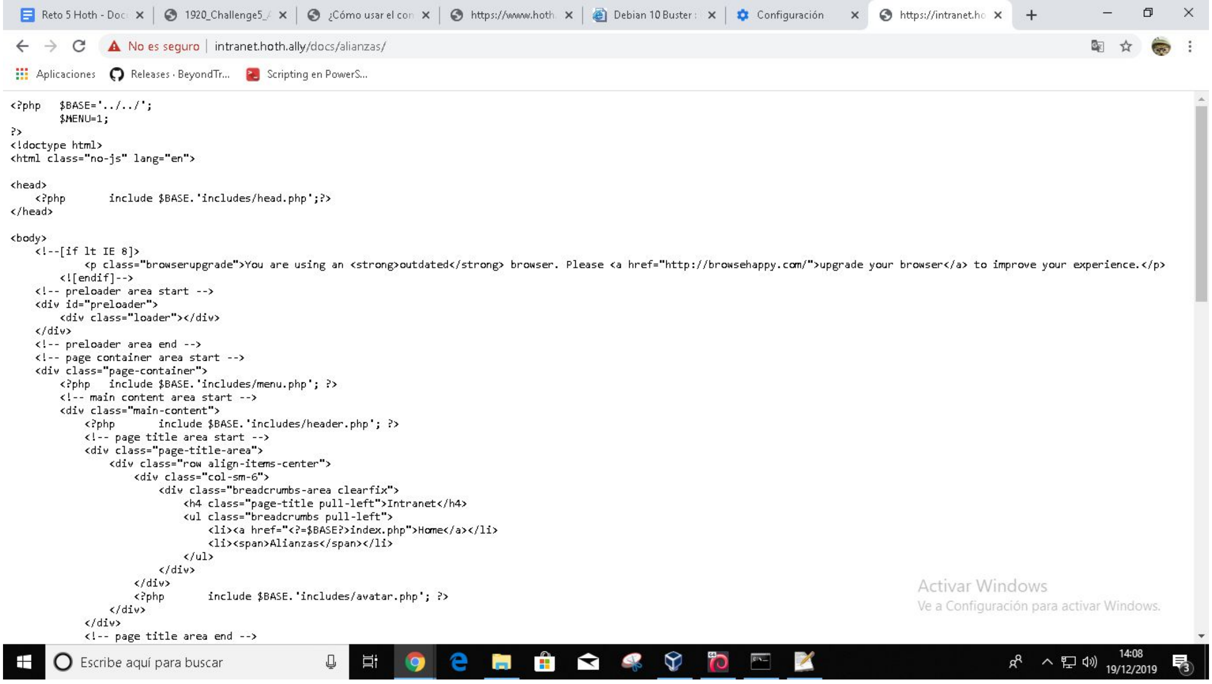
Nombre de usuario

Contraseña



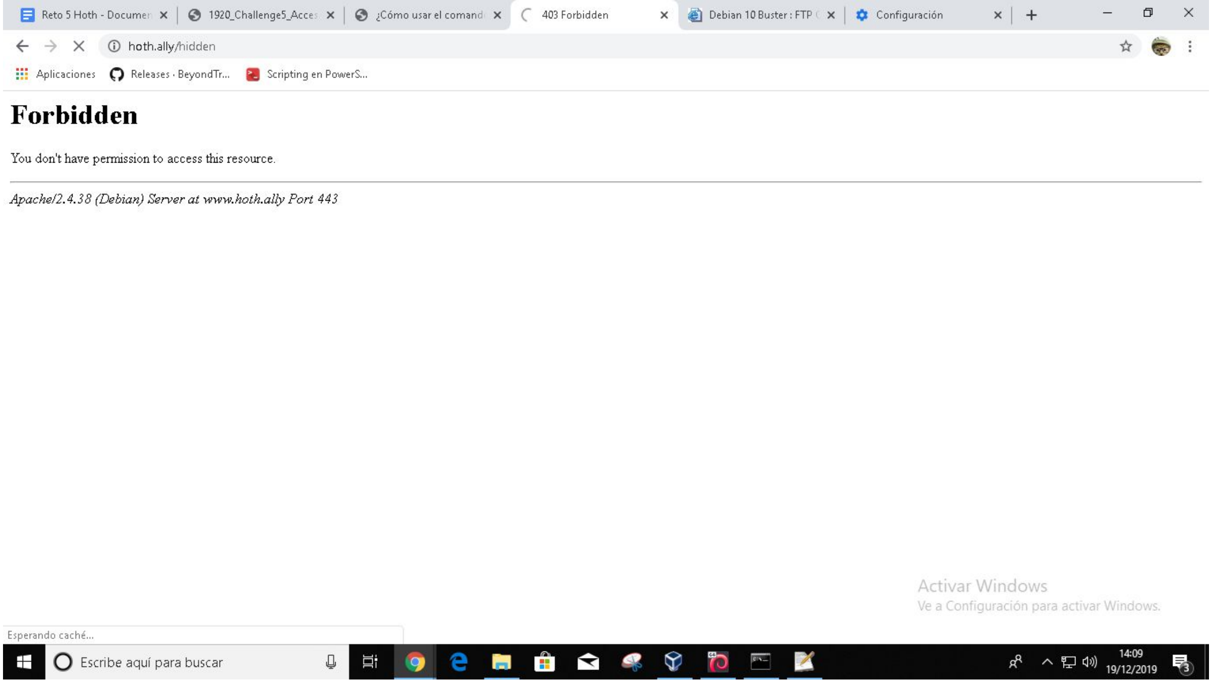
```
<?php   $BASE='../';
        $MENU=5;
?>
<!doctype html>
<html class="no-js" lang="es">

<head>
    <?php       include $BASE.'includes/head.php';?>
</head>

<body>
    <!--[if lt IE 8]>
            <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to improve your experience.</p>
        <![endif]-->
    <!-- preloader area start -->
    <div id="preloader">
        <div class="loader"></div>
    </div>
    <!-- preloader area end -->
    <!-- page container area start -->
    <div class="page-container">
        <?php   include $BASE.'includes/menu.php'; ?>
        <!-- main content area start -->
        <div class="main-content">
            <?php       include $BASE.'includes/header.php'; ?>
            <!-- page title area start -->
            <div class="page-title-area">
                <div class="row align-items-center">
                    <div class="col-sm-6">
                        <div class="breadcrumbs-area clearfix">
                            <h4 class="page-title pull-left">Intranet</h4>
                            <ul class="breadcrumbs pull-left">
                                <li><a href="<?=$BASE?>index.php">Home</a></li>
                                <li><span>AdministraciÃ³n</span></li>
                            </ul>
                        </div>
                    </div>
                    <?php       include $BASE.'includes/avatar.php'; ?>
                </div>
            </div>
            <!-- page title area end -->
```

index.php is the main webpage of the alianzas directory



```
<?php   $BASE='../../';
        $MENU=1;
?>
<!doctype html>
<html class="no-js" lang="en">

<head>
    <?php       include $BASE.'includes/head.php';?>
</head>

<body>
    <!--[if lt IE 8]>
            <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to improve your experience.</p>
        <![endif]-->
    <!-- preloader area start -->
    <div id="preloader">
        <div class="loader"></div>
    </div>
    <!-- preloader area end -->
    <!-- page container area start -->
    <div class="page-container">
        <?php   include $BASE.'includes/menu.php'; ?>
        <!-- main content area start -->
        <div class="main-content">
            <?php       include $BASE.'includes/header.php'; ?>
            <!-- page title area start -->
            <div class="page-title-area">
                <div class="row align-items-center">
                    <div class="col-sm-6">
                        <div class="breadcrumbs-area clearfix">
                            <h4 class="page-title pull-left">Intranet</h4>
                            <ul class="breadcrumbs pull-left">
                                <li><a href="<?=$BASE?>index.php">Home</a></li>
                                <li><span>Alianzas</span></li>
                            </ul>
                        </div>
                    </div>
                    <?php       include $BASE.'includes/avatar.php'; ?>
                </div>
            </div>
            <!-- page title area end -->
```

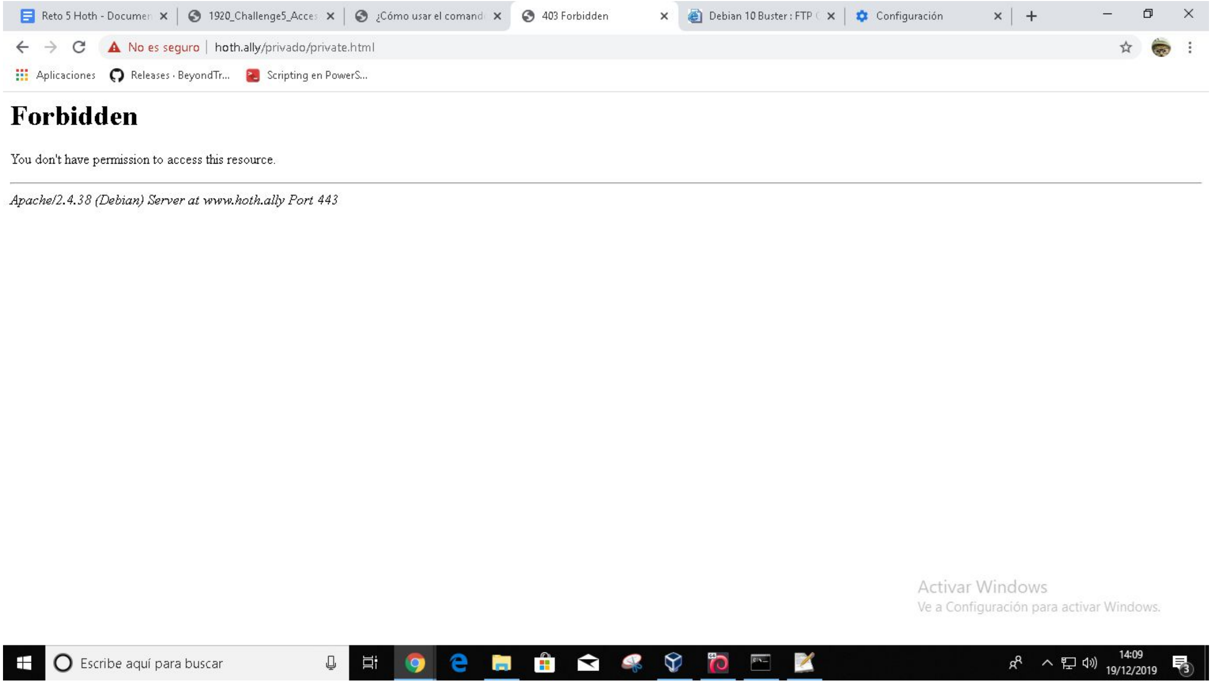
hidden directory and private chain like files are not available for all.



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at www.hoth.ally Port 443



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at www.hoth.ally Port 443

3-FTP

3.1-Introduction

It is time to work in the access to remote information, giving our allies that are in the external networks access to the information inside and for this purpose we are going to use FTPS protocol. We have decided to use this protocol because it is more secure for clients and server.
The content of the four websites in www.xxx.ally machine is going to be managed using an FTPS server. We are going to need the certificates and the LDAP server used in the last challenge so that we reach the highest security. We must ensure that this machine is an Ldap client.

3.2-Server Configuration

apt-get install vsftpd

By default most of the commands in /etc/vsftpd.conf are commented, to begin we are going to uncomment these lines:

```
# line 31: uncomment

write_enable=YES

# line 99,100: uncomment ( allow ascii mode transfer )

ascii_upload_enable=YES

ascii_download_enable=YES

# line 122: uncomment ( enable chroot )

chroot_local_user=YES

# line 123: uncomment ( enable chroot list )

chroot_list_enable=YES

# line 125: uncomment ( enable chroot list )

chroot_list_file=/etc/vsftpd.chroot_list

# line 131: uncomment

ls_recurse_enable=YES
```

Here is our configuration of the file, including only the uncommented commands.

nano -l /etc/vsftpd.conf

```
listen=NO
listen_ipv6=YES
# Allow anonymous FTP? (Disabled by default).
#anonymous_enable=YES
# Uncomment this to allow local users to log in.
local_enable=YES
# Uncomment this to enable any form of FTP write command.
write_enable=YES
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
dirmessage_enable=YES
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
# Activate logging of uploads/downloads.
xferlog_enable=YES
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
# ASCII mangling is a horrible feature of the protocol.
ascii_upload_enable=YES
ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
banner_file=/etc/ascii/ftp.msg
# You may restrict local users to their home directories.  See the FAQ for
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#We restrict local users to attach them to their home directories.
chroot_local_user=YES
#We enable the list the users that will move from their home directories.
chroot_list_enable=YES
# (default follows)
```

```
allow_writeable_chroot=YES
#With this command we define the file which will store the user that are able to move #from their respective home directories
chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# 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.ldap
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
implicit_ssl=YES
ssl_enable=YES
listen_port=990
ssl_ciphers=HIGH
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
#Using the certificates and keys generated in the last challenge
rsa_cert_file=/etc/ssl/hoth.pem
rsa_private_key_file=/etc/ssl/hoth.key
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
#local_root=/home/nfs/$user
seccomp_sandbox=NO
#Mantains sessions when login
session_support=YES
#only 3 users can be connected at the same time (2 of them from the same IP #address)
max_per_ip=2
max_clients=3
#In this list you can include which users won't be able to connect.
userlist_file=/etc/vsftpd.txt
#We enable that list
```

```
userlist_enable=YES
#file transmission speed will be 50 Kbyte/s
local_max_rate=50000
```

nano /etc/vsftpd.chroot_list

```
# add users you allow to move over their home directory
windu
yoda
```

nano /etc/vsftpd.txt

```
#This users won't be able to connect
naytaan
porkins
rue
narra
```

nano /etc/ascii/ftp.msg

```
  GNU nano 3.2
                                 /~\
                                |oo )
                                _\=/_
                ____             /  _  \
               /() \          //|/.\|\\
             _|______|_         \\ \_/  ||
            | | === | |         \|\ /| ||
            |_|  O  |_|          # _ _/ #
             ||  O  ||            | | |
             ||__*__||             | | |
            |~ \____/ ~|           []|[]
            /=\ /=\ /=\           | | |
\__________________[_]_[_]_[_]__________/_]_[_\___________________/
 WELCOME TO THE REBEL ALLIANCE! MAY THE FORCE BE WITH YOU!
```

nano /etc/pam.d/vsftpd.ldap

Add these lines:

```
#%PAM-1.0
auth required pam_ldap.so
account required pam_ldap.so
```

```
session required pam_ldap.so
password required pam_ldap.so
session required        pam_mkhomedir.so        skel=/etc/skel umask=0002

systemctl restart vsftpd
systemctl status vsftpd
```

We have also set the necessary permissions for yoda and windu in order they are the only ones which will manage their websites.

With this permission configuration windu and yoda are the only ones with read, write and execute permissions while the rest of the user will only be able to read.

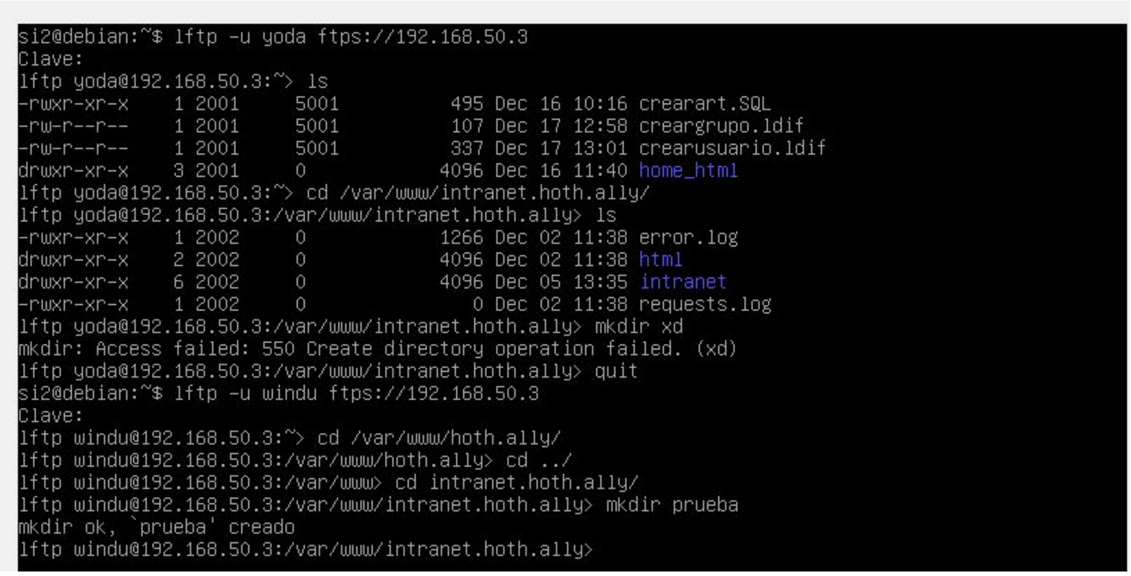
cd /var/www

chown -R yoda hoth.ally

chmod 755 hoth.allt

chown -R windu intranet.hoth.ally

chmod 755 intranet.hoth.ally



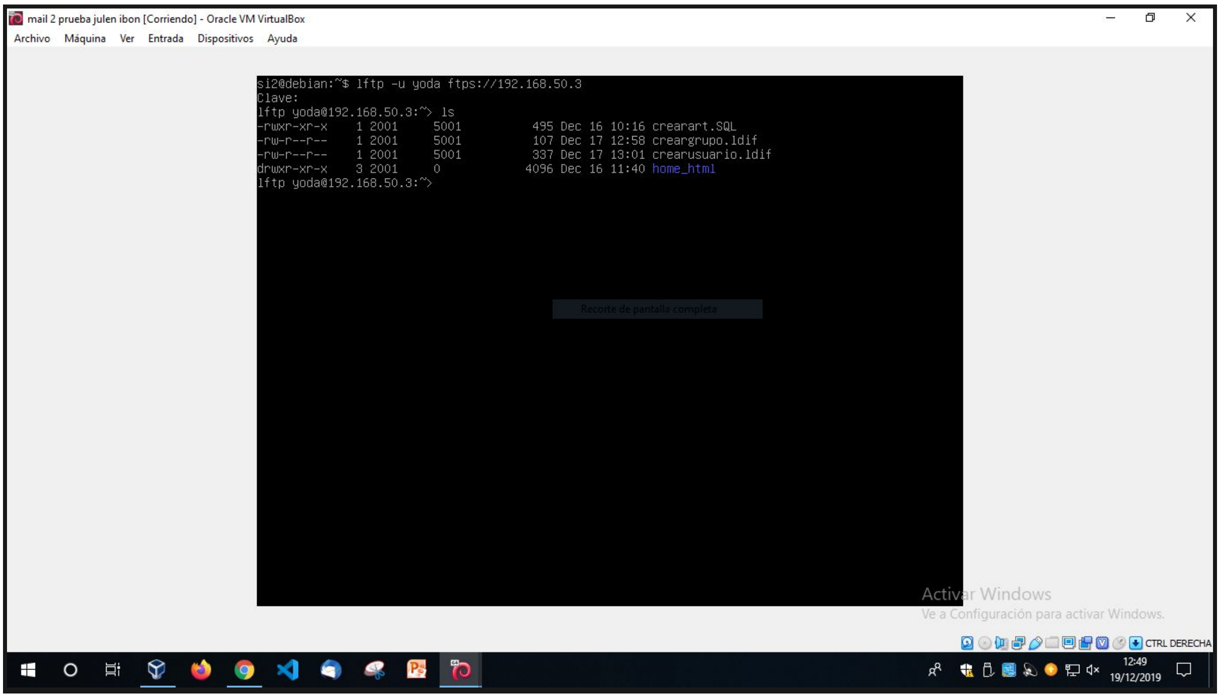
```
si2@debian:~$ lftp -u yoda ftps://192.168.50.3
Clave:
lftp yoda@192.168.50.3:~> ls
-rwxr-xr-x    1 2001     5001          495 Dec 16 10:16 crearart.SQL
-rw-r--r--    1 2001     5001          107 Dec 17 12:58 creargrupo.ldif
-rw-r--r--    1 2001     5001          337 Dec 17 13:01 crearusuario.ldif
drwxr-xr-x    3 2001     0            4096 Dec 16 11:40 home_html
lftp yoda@192.168.50.3:~> cd /var/www/intranet.hoth.ally/
lftp yoda@192.168.50.3:/var/www/intranet.hoth.ally> ls
-rwxr-xr-x    1 2002     0            1266 Dec 02 11:38 error.log
drwxr-xr-x    2 2002     0            4096 Dec 02 11:38 html
drwxr-xr-x    6 2002     0            4096 Dec 05 13:35 intranet
-rwxr-xr-x    1 2002     0               0 Dec 02 11:38 requests.log
lftp yoda@192.168.50.3:/var/www/intranet.hoth.ally> mkdir xd
mkdir: Access failed: 550 Create directory operation failed. (xd)
lftp yoda@192.168.50.3:/var/www/intranet.hoth.ally> quit
si2@debian:~$ lftp -u windu ftps://192.168.50.3
Clave:
lftp windu@192.168.50.3:~> cd /var/www/hoth.ally/
lftp windu@192.168.50.3:/var/www/hoth.ally> cd ../
lftp windu@192.168.50.3:/var/www> cd intranet.hoth.ally/
lftp windu@192.168.50.3:/var/www/intranet.hoth.ally> mkdir prueba
mkdir ok, `prueba' creado
lftp windu@192.168.50.3:/var/www/intranet.hoth.ally>
```

3.3-Client configuration

apt-get install lftp

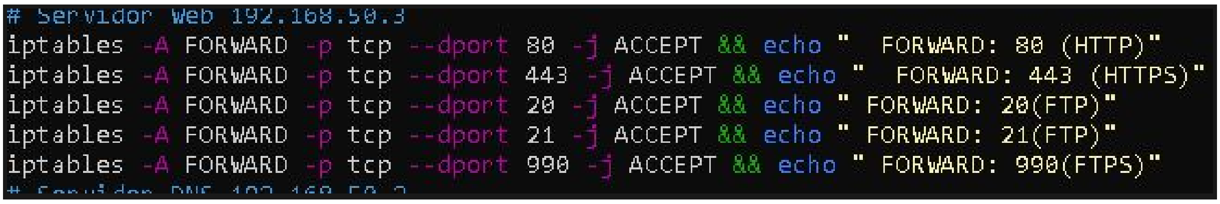
We configure in the home directory of the user that is going to connect this file: nano .lftprc so that ssl connection works properly.

```
~/.lftprc

set ftp:ssl-auth TLS

set ftp:ssl-force true

set ftp:ssl-protect-list yes

set ftp:ssl-protect-data yes

set ftp:ssl-protect-fxp yes

set ssl:verify-certificate no
```

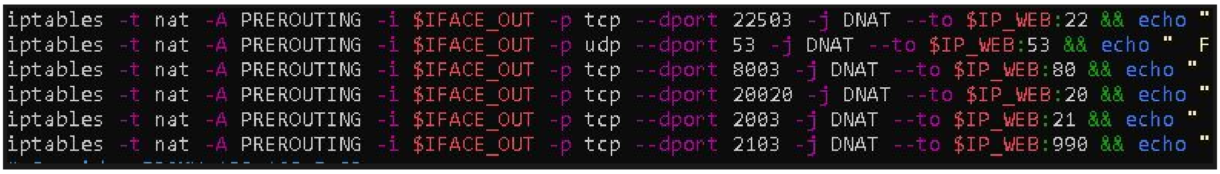

mail 2 prueba julen ibon [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Activar Windows
Ve a Configuración para activar Windows.
CTRL DERECHA
12:49
19/12/2019

```
si2@debian:~$ lftp -u yoda ftps://192.168.50.3
Clave:
lftp yoda@192.168.50.3:~> ls
-rwxr-xr-x    1 2001     5001          495 Dec 16 10:16 crearart.SQL
-rw-r--r--    1 2001     5001          107 Dec 17 12:58 creargrupo.ldif
-rw-r--r--    1 2001     5001          337 Dec 17 13:01 crearusuario.ldif
drwxr-xr-x    3 2001     0            4096 Dec 16 11:40 home_html
lftp yoda@192.168.50.3:~>
```

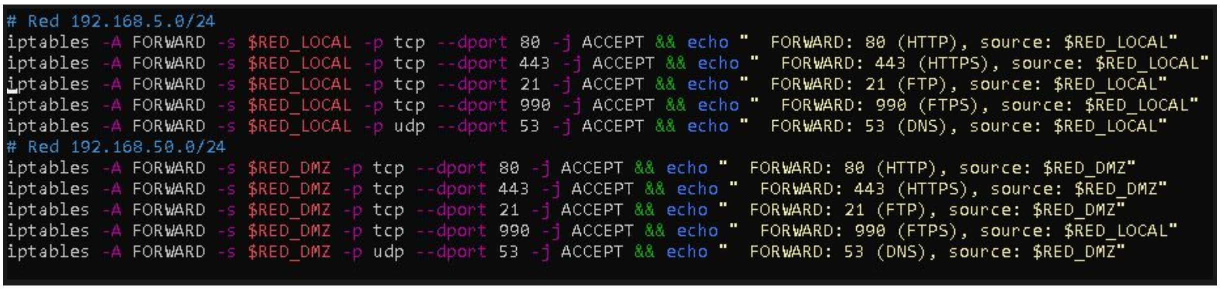
3.4- Firewall configuration



```
# Servidor Web 192.168.50.3
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT && echo "  FORWARD: 80 (HTTP)"
iptables -A FORWARD -p tcp --dport 443 -j ACCEPT && echo "  FORWARD: 443 (HTTPS)"
iptables -A FORWARD -p tcp --dport 20 -j ACCEPT && echo " FORWARD: 20(FTP)"
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT && echo " FORWARD: 21(FTP)"
iptables -A FORWARD -p tcp --dport 990 -j ACCEPT && echo " FORWARD: 990(FTPS)"
# Servidor DNS 192.168.50.3
```



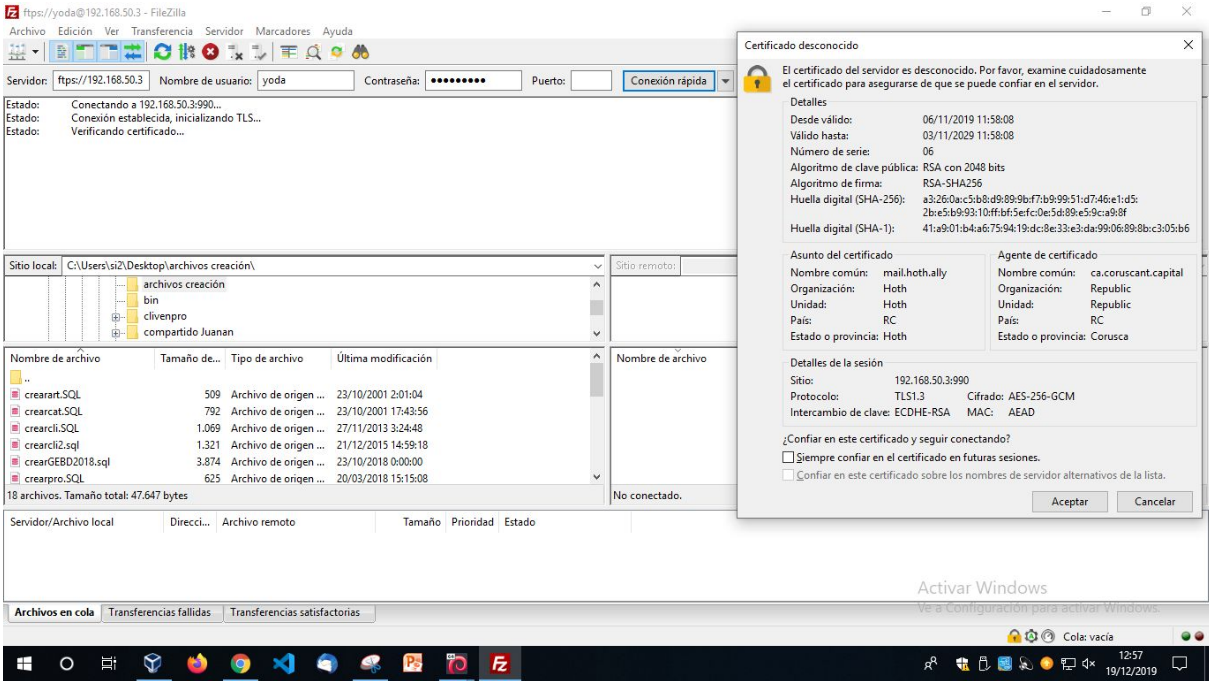
```
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 22503 -j DNAT --to $IP_WEB:22 && echo "
iptables -t nat -A PREROUTING -i $IFACE_OUT -p udp --dport 53 -j DNAT --to $IP_WEB:53 && echo "  F
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 8003 -j DNAT --to $IP_WEB:80 && echo "
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 20020 -j DNAT --to $IP_WEB:20 && echo "
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 2003 -j DNAT --to $IP_WEB:21 && echo "
iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 2103 -j DNAT --to $IP_WEB:990 && echo "
```



```
# Red 192.168.5.0/24
iptables -A FORWARD -s $RED_LOCAL -p tcp --dport 80 -j ACCEPT && echo "  FORWARD: 80 (HTTP), source: $RED_LOCAL"
iptables -A FORWARD -s $RED_LOCAL -p tcp --dport 443 -j ACCEPT && echo "  FORWARD: 443 (HTTPS), source: $RED_LOCAL"
iptables -A FORWARD -s $RED_LOCAL -p tcp --dport 21 -j ACCEPT && echo "  FORWARD: 21 (FTP), source: $RED_LOCAL"
iptables -A FORWARD -s $RED_LOCAL -p tcp --dport 990 -j ACCEPT && echo "  FORWARD: 990 (FTPS), source: $RED_LOCAL"
iptables -A FORWARD -s $RED_LOCAL -p udp --dport 53 -j ACCEPT && echo "  FORWARD: 53 (DNS), source: $RED_LOCAL"
# Red 192.168.50.0/24
iptables -A FORWARD -s $RED_DMZ -p tcp --dport 80 -j ACCEPT && echo "  FORWARD: 80 (HTTP), source: $RED_DMZ"
iptables -A FORWARD -s $RED_DMZ -p tcp --dport 443 -j ACCEPT && echo "  FORWARD: 443 (HTTPS), source: $RED_DMZ"
iptables -A FORWARD -s $RED_DMZ -p tcp --dport 21 -j ACCEPT && echo "  FORWARD: 21 (FTP), source: $RED_DMZ"
iptables -A FORWARD -s $RED_DMZ -p tcp --dport 990 -j ACCEPT && echo "  FORWARD: 990 (FTPS), source: $RED_LOCAL"
iptables -A FORWARD -s $RED_DMZ -p udp --dport 53 -j ACCEPT && echo "  FORWARD: 53 (DNS), source: $RED_DMZ"
```

3.5-Checkings

Asks for SSL connection and our user yoda can go back from his home directory.



ftps://yoda@192.168.50.3 - FileZilla

Servidor: ftps://192.168.50.3 Nombre de usuario: yoda Contraseña: ••••••••• Puerto:

```
Estado:    Conectando a 192.168.50.3:990...
Estado:    Conexión establecida, inicializando TLS...
Estado:    Verificando certificado...
```

Sitio local: C:\Users\si2\Desktop\archivos creación\

archivos creación
bin
clivenpro
compartido Juanan

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..			
creurart.SQL	509	Archivo de origen ...	23/10/2001 2:01:04
crearcat.SQL	792	Archivo de origen ...	23/10/2001 17:43:56
crearcli.SQL	1.069	Archivo de origen ...	27/11/2013 3:24:48
crearcli2.sql	1.321	Archivo de origen ...	21/12/2015 14:59:18
crearGEBD2018.sql	3.874	Archivo de origen ...	23/10/2018 0:00:00
crearpro.SQL	625	Archivo de origen ...	20/03/2018 15:15:08

18 archivos. Tamaño total: 47.647 bytes

Sitio remoto:

Nombre de archivo

No conectado.

Certificado desconocido

El certificado del servidor es desconocido. Por favor, examine cuidadosamente el certificado para asegurarse de que se puede confiar en el servidor.

Detalles

Desde válido:	06/11/2019 11:58:08
Válido hasta:	03/11/2029 11:58:08
Número de serie:	06
Algoritmo de clave pública:	RSA con 2048 bits
Algoritmo de firma:	RSA-SHA256
Huella digital (SHA-256):	a3:26:0a:c5:b8:d9:89:9b:f7:b9:99:51:d7:46:e1:d5: 2b:e5:b9:93:10:ff:bf:5e:fc:0e:5d:89:e5:9c:a9:8f
Huella digital (SHA-1):	41:a9:01:b4:a6:75:94:19:dc:8e:33:e3:da:99:06:89:8b:c3:05:b6

Asunto del certificado		Agente de certificado	
Nombre común:	mail.hoth.ally	Nombre común:	ca.coruscant.capital
Organización:	Hoth	Organización:	Republic
Unidad:	Hoth	Unidad:	Republic
País:	RC	País:	RC
Estado o provincia:	Hoth	Estado o provincia:	Corusca

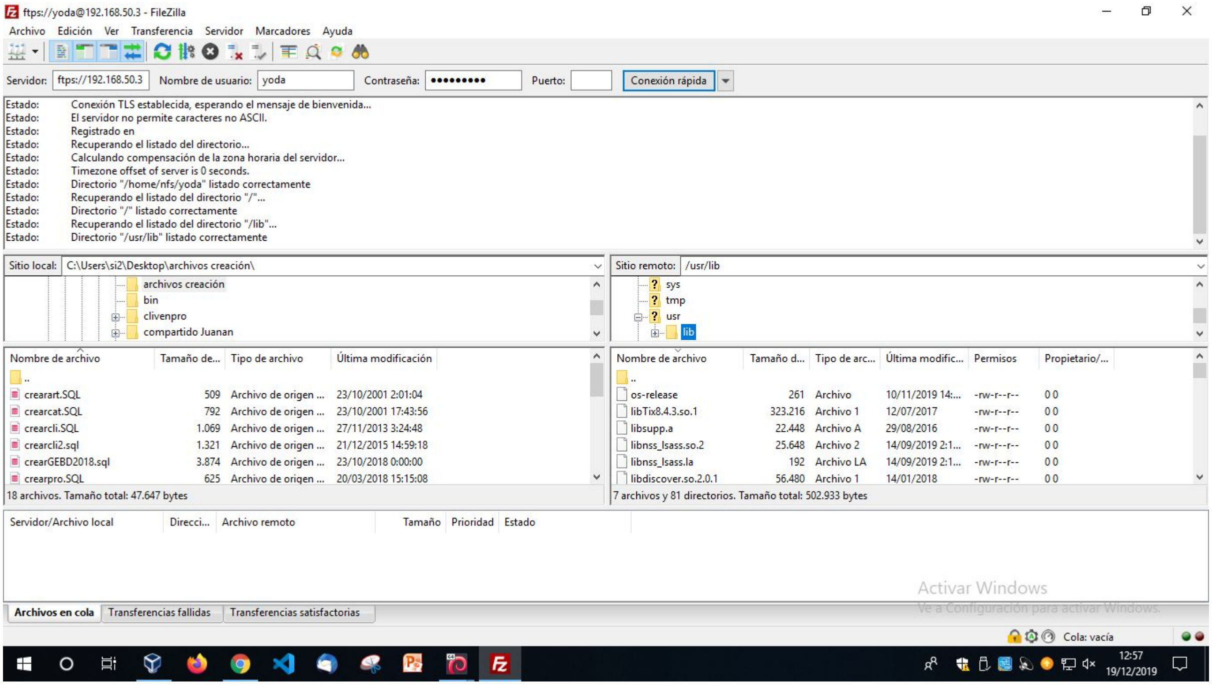
Detalles de la sesión

Sitio: 192.168.50.3:990
Protocolo: TLS1.3 Cifrado: AES-256-GCM
Intercambio de clave: ECDHE-RSA MAC: AEAD

¿Confiar en este certificado y seguir conectando?

☐ Siempre confiar en el certificado en futuras sesiones.

☐ Confiar en este certificado sobre los nombres de servidor alternativos de la lista.



ftps://yoda@192.168.50.3 - FileZilla

Servidor: ftps://192.168.50.3 Nombre de usuario: yoda Contraseña: ••••••••• Puerto:

```
Estado:     Conexión TLS establecida, esperando el mensaje de bienvenida...
Estado:     El servidor no permite caracteres no ASCII.
Estado:     Registrado en
Estado:     Recuperando el listado del directorio...
Estado:     Calculando compensación de la zona horaria del servidor...
Estado:     Timezone offset of server is 0 seconds.
Estado:     Directorio "/home/nfs/yoda" listado correctamente
Estado:     Recuperando el listado del directorio "/"...
Estado:     Directorio "/" listado correctamente
Estado:     Recuperando el listado del directorio "/lib"...
Estado:     Directorio "/usr/lib" listado correctamente
```

Sitio local: C:\Users\si2\Desktop\archivos creación\

archivos creación
bin
clivenpro
compartido Juanan

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..			
creart.SQL	509	Archivo de origen ...	23/10/2001 2:01:04
crearcat.SQL	792	Archivo de origen ...	23/10/2001 17:43:56
crearcli.SQL	1.069	Archivo de origen ...	27/11/2013 3:24:48
crearcli2.sql	1.321	Archivo de origen ...	21/12/2015 14:59:18
crearGEBD2018.sql	3.874	Archivo de origen ...	23/10/2018 0:00:00
crearpro.SQL	625	Archivo de origen ...	20/03/2018 15:15:08

18 archivos. Tamaño total: 47.647 bytes

Sitio remoto: /usr/lib

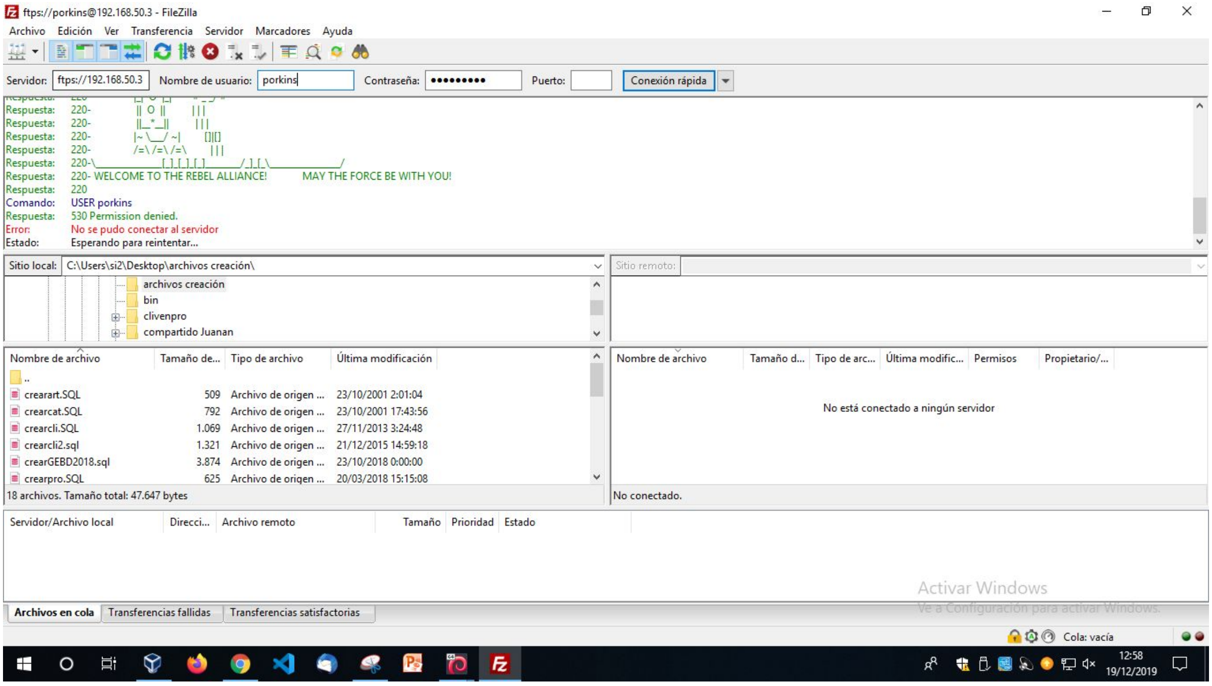
sys
tmp
usr
lib

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...
..					
os-release	261	Archivo	10/11/2019 14:...	-rw-r--r--	0 0
libTix8.4.3.so.1	323.216	Archivo 1	12/07/2017	-rw-r--r--	0 0
libsupp.a	22.448	Archivo A	29/08/2016	-rw-r--r--	0 0
libnss_lsass.so.2	25.648	Archivo 2	14/09/2019 2:1...	-rw-r--r--	0 0
libnss_lsass.la	192	Archivo LA	14/09/2019 2:1...	-rw-r--r--	0 0
libdiscover.so.2.0.1	56.480	Archivo 1	14/01/2018	-rw-r--r--	0 0

7 archivos y 81 directorios. Tamaño total: 502.933 bytes

Servidor/Archivo local	Direcci...	Archivo remoto	Tamaño	Prioridad	Estado

User porkins cannot connect and the welcome banner.



ftps://porkins@192.168.50.3 - FileZilla

Servidor: ftps://192.168.50.3 Nombre de usuario: porkins Contraseña: ••••••••• Puerto:

```
Respuesta:  220-         || O ||       | | |
Respuesta:  220-         ||__*__||      | | |
Respuesta:  220-         |~ \___/ ~|      []|[]
Respuesta:  220-         /=\ /=\ /=\      | | |
Respuesta:  220-\____________[_]_[_]_[_]______/_]_[_\____________/
Respuesta:  220- WELCOME TO THE REBEL ALLIANCE!        MAY THE FORCE BE WITH YOU!
Respuesta:  220
Comando:    USER porkins
Respuesta:  530 Permission denied.
Error:      No se pudo conectar al servidor
Estado:     Esperando para reintentar...
```

Sitio local: C:\Users\si2\Desktop\archivos creación\

archivos creación
bin
clivenpro
compartido Juanan

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..			
creart.SQL	509	Archivo de origen ...	23/10/2001 2:01:04
crearcat.SQL	792	Archivo de origen ...	23/10/2001 17:43:56
crearcli.SQL	1.069	Archivo de origen ...	27/11/2013 3:24:48
crearcli2.sql	1.321	Archivo de origen ...	21/12/2015 14:59:18
crearGEBD2018.sql	3.874	Archivo de origen ...	23/10/2018 0:00:00
crearpro.SQL	625	Archivo de origen ...	20/03/2018 15:15:08

18 archivos. Tamaño total: 47.647 bytes

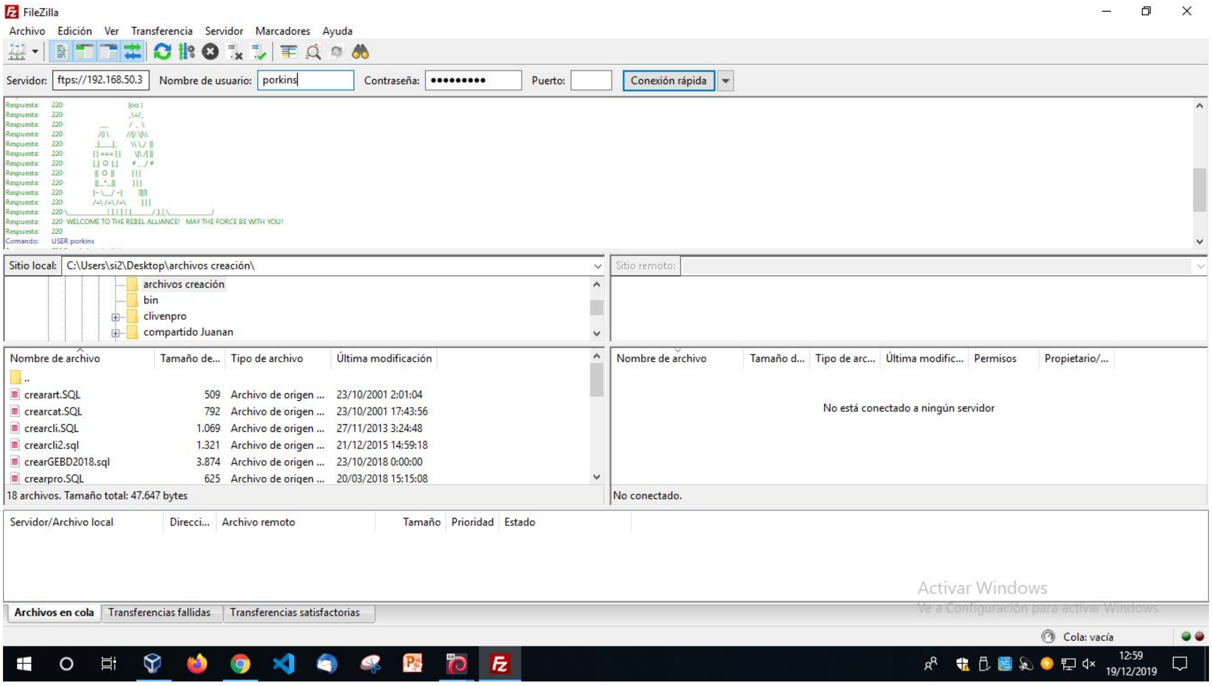
Sitio remoto:

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...

No está conectado a ningún servidor

No conectado.

Servidor/Archivo local	Direcci...	Archivo remoto	Tamaño	Prioridad	Estado



Servidor: ftps://192.168.50.3 Nombre de usuario: porkins Contraseña: ●●●●●●●●● Puerto:

```
Respuesta:  220-                    |oo )
Respuesta:  220-                    _\=/_
Respuesta:  220-          ___      /  _  \
Respuesta:  220-         /()\     //|/.\|\\
Respuesta:  220-       _|_____|_   \\ \_/ ||
Respuesta:  220-      | | === | |   \|\ /| ||
Respuesta:  220-      |_|  O  |_|   # _ _/ #
Respuesta:  220-       ||  O  ||     | | |
Respuesta:  220-       ||__*__||     | | |
Respuesta:  220-      |~ \___/ ~|    []|[]
Respuesta:  220-      /=\ /=\ /=\    | | |
Respuesta:  220-\________[_]_[_]_[_]______/_]_[_\_____________/
Respuesta:  220- WELCOME TO THE REBEL ALLIANCE!   MAY THE FORCE BE WITH YOU!
Respuesta:  220
Comando:    USER porkins
```

Sitio local: C:\Users\si2\Desktop\archivos creación\

- archivos creación
- bin
- clivenpro
- compartido Juanan

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..			
creararat.SQL	509	Archivo de origen ...	23/10/2001 2:01:04
crearcat.SQL	792	Archivo de origen ...	23/10/2001 17:43:56
crearcli.SQL	1.069	Archivo de origen ...	27/11/2013 3:24:48
crearcli2.sql	1.321	Archivo de origen ...	21/12/2015 14:59:18
crearGEBD2018.sql	3.874	Archivo de origen ...	23/10/2018 0:00:00
crearpro.SQL	625	Archivo de origen ...	20/03/2018 15:15:08

18 archivos. Tamaño total: 47.647 bytes

Sitio remoto:

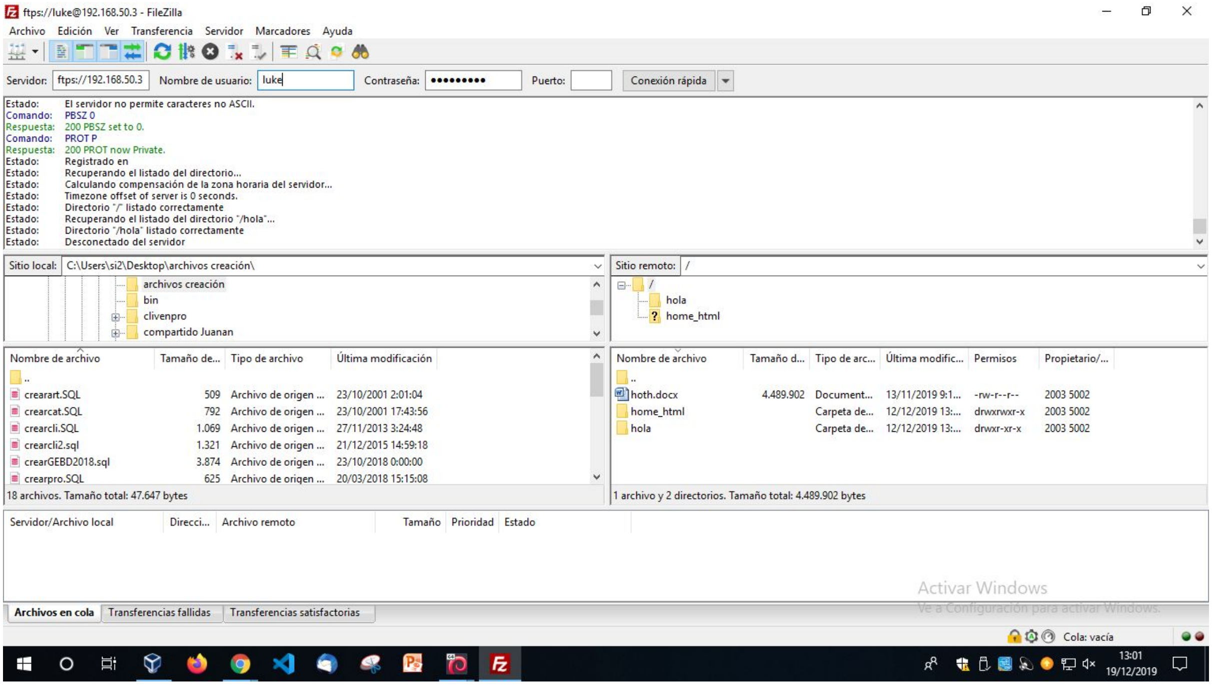
Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...

No está conectado a ningún servidor

No conectado.

Servidor/Archivo local	Direcci...	Archivo remoto	Tamaño	Prioridad	Estado

Luke is restricted to his home directory



Servidor: ftps://192.168.50.3 Nombre de usuario: luke Contraseña: ●●●●●●●●● Puerto:

```
Estado:     El servidor no permite caracteres no ASCII.
Comando:    PBSZ 0
Respuesta:  200 PBSZ set to 0.
Comando:    PROT P
Respuesta:  200 PROT now Private.
Estado:     Registrado en
Estado:     Recuperando el listado del directorio...
Estado:     Calculando compensación de la zona horaria del servidor...
Estado:     Timezone offset of server is 0 seconds.
Estado:     Directorio "/" listado correctamente
Estado:     Recuperando el listado del directorio "/hola"...
Estado:     Directorio "/hola" listado correctamente
Estado:     Desconectado del servidor
```

Sitio local: C:\Users\si2\Desktop\archivos creación\

- archivos creación
- bin
- clivenpro
- compartido Juanan

Sitio remoto: /

- /
  - hola
  - home_html

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..			
crearart.SQL	509	Archivo de origen ...	23/10/2001 2:01:04
crearcat.SQL	792	Archivo de origen ...	23/10/2001 17:43:56
crearcli.SQL	1.069	Archivo de origen ...	27/11/2013 3:24:48
crearcli2.sql	1.321	Archivo de origen ...	21/12/2015 14:59:18
crearGEBD2018.sql	3.874	Archivo de origen ...	23/10/2018 0:00:00
crearpro.SQL	625	Archivo de origen ...	20/03/2018 15:15:08

18 archivos. Tamaño total: 47.647 bytes

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...
..					
hoth.docx	4.489.902	Document...	13/11/2019 9:1...	-rw-r--r--	2003 5002
home_html		Carpeta de...	12/12/2019 13:...	drwxrwxr-x	2003 5002
hola		Carpeta de...	12/12/2019 13:...	drwxr-xr-x	2003 5002

1 archivo y 2 directorios. Tamaño total: 4.489.902 bytes

Servidor/Archivo local	Direcci...	Archivo remoto	Tamaño	Prioridad	Estado

4-PROXY

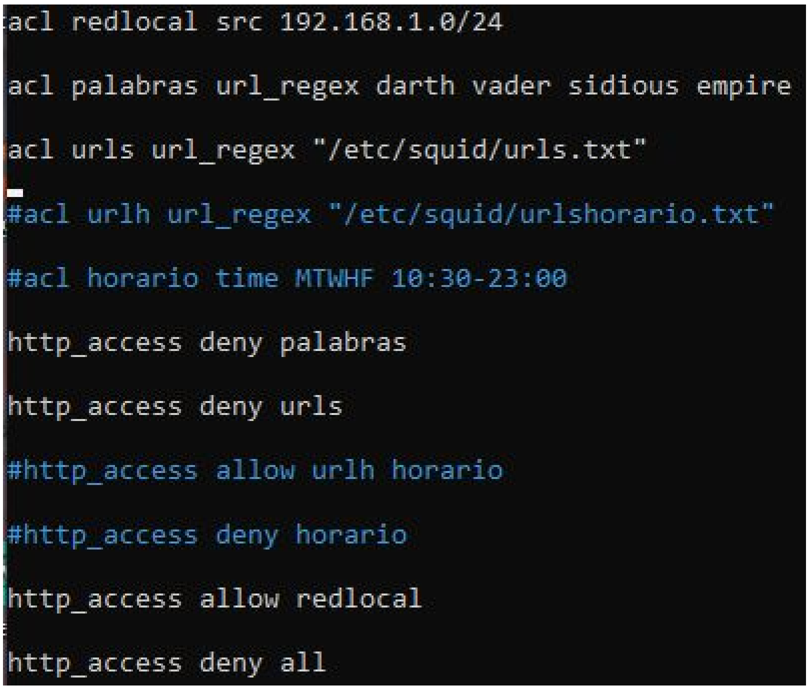
4.1-Introduction

Finally, we want our rebel allies in xxxx.local network not to be entertained when browsing the web and not to access to some websites, so we will install and configure a web proxy server (squid3) with the following features: Establishing a proxy server in clients is compulsory for being able to browse and will be set through domain directives. Due to save the last resources visited by clients, will be configured as cache web proxy server, with a store space of 150 MB. Visiting the **f**ollowing websites will be forbidden:
starwars.fandom.com/wiki/Death_Star
starwars.fandom.com/wiki/Death_Star_II
starwars.fandom.com/wiki/Death_Star_III
Will also be forbidden visiting websites that content any of these words:
Darth Vader Sidious Sith Empire
From Monday to Friday, from 10:30 to 13:00, it will be permitted browsing only the following webpages (Active Directory device has not got this restriction):
starwars.fandom.com/wiki/Alliance_to_Restore_the_Republic
starwars.fandom.com/wiki/Resistance

A proxy server acts as a gateway between you and the internet. It’s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you’re using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.

4.2-ACL Configuation



```
acl redlocal src 192.168.1.0/24

acl palabras url_regex darth vader sidious empire

acl urls url_regex "/etc/squid/urls.txt"

#acl urlh url_regex "/etc/squid/urlshorario.txt"

#acl horario time MTWHF 10:30-23:00

http_access deny palabras

http_access deny urls

#http_access allow urlh horario

#http_access deny horario

http_access allow redlocal

http_access deny all
```

4.3-SQUID PROXY SERVER

The first step is to install the service in our proxy machine, in the local area of our network, for this we can use this command:
apt-get install squid

Then we go to the folder where the configuration file is:
cd /etc/squid

In order to edit the configuration file we will use any editor and the file's name.

squid.conf

This is the whole configuration file:

```
acl SSL_ports port 443
acl Safe_ports port 80        # http
acl Safe_ports port 21        # ftp
acl Safe_ports port 443       # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

################## REGLAS PROXY HOTH##################
#Acl red local y equipoad
acl redlocal src 192.168.50.0/24
acl equipoad src 192.168.5.92

#Acl archivo de URL prohibidas:
acl webs url_regex "/etc/squid/webs.txt"

#Acl palabras prohibidas
acl palabras url_regex darth vader sidious sith empire

#Acls Horario
acl webshorario url_regex "/etc/squid/webshorario.txt"

acl horario time MTWHF 10:30-13:00

#Permitimos acceso total al equipoad antes de denegar ninguna otra regla.

http_access allow equipoad

#Denegar acceso a las palabras y webs prohibidas

http_access deny palabras

http_access deny webs

#Permitir acceso desde redlocal restringido en horario
http_access allow horario webshorario

http_access allow !horario redlocal

#########################################################
include /etc/squid/conf.d/*

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

http_port 3128

#visible_hostname proxy.hoth.local

cache_store_log stdio:/var/log/squid/store.log

cache_mem 512 MB

cache_dir ufs /var/spool/squid 512 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
```

We should make a copy of the conf file in case we need it again, and if we want we can also download a clean template of this file.
cp /etc/squid/squid.conf{,.original}

Then we are going to start configuring squid using the conf file:
nano /etc/squid/squid.conf

In order to set the port that our proxy is going to be using we use the line (in our case we will use the default one):
http_port 3128

There are some default parameters in the config file that we don’t have to change:

For the cache configuration we use these commands:
cache_store_log stdio:/var/log/squid/store.log
cache_mem 512 MB
cache_dir ufs /var/spool/squid 512 16 256

Created acls and rules for our proxy:

An access-control list (ACL), is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

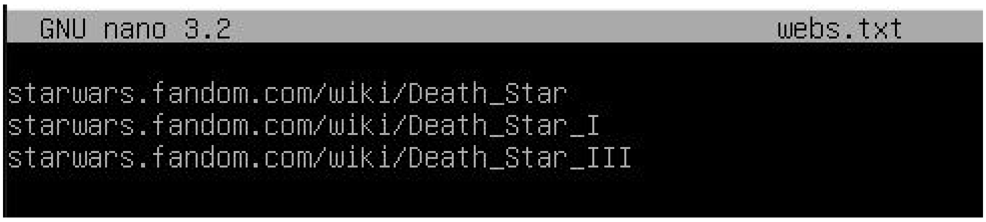
We are going to define two acl’s, one for our class network and one for our active directory server:

#Acl local network and equipoad
acl redlocal src 192.168.50.0/24
acl equipoad src 192.168.5.92

Here we define two acl’s for the forbidden webs and words:

#Acl archivo de URL prohibidas:

acl webs url_regex "/etc/squid/webs.txt"

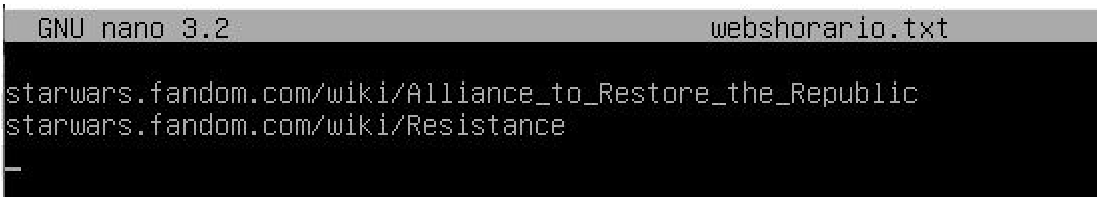


```
 GNU nano 3.2                                    webs.txt

starwars.fandom.com/wiki/Death_Star
starwars.fandom.com/wiki/Death_Star_I
starwars.fandom.com/wiki/Death_Star_III
```

#Acl palabras prohibidas
acl palabras url_regex darth vader sidious sith empire

We define an schedule from monday to friday and from 10:30 to 13:00 and the web pages that are only accessible in that schedule:

#Acls Horario
acl webshorario url_regex "/etc/squid/webshorario.txt"



```
 GNU nano 3.2                                webshorario.txt

starwars.fandom.com/wiki/Alliance_to_Restore_the_Republic
starwars.fandom.com/wiki/Resistance
```

acl horario time MTWHF 10:30-13:00

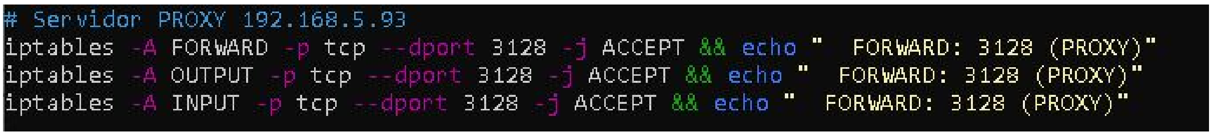
Using “http_access” we are going to deny everything forbidden:

#Denegar acceso a las palabras y webs prohibidas

http_access deny palabras

Firewall Rules

With these rules we will accept any packet that comes to the router, comes out of it or just passes through it with destination port 3128 (proxy’s port).

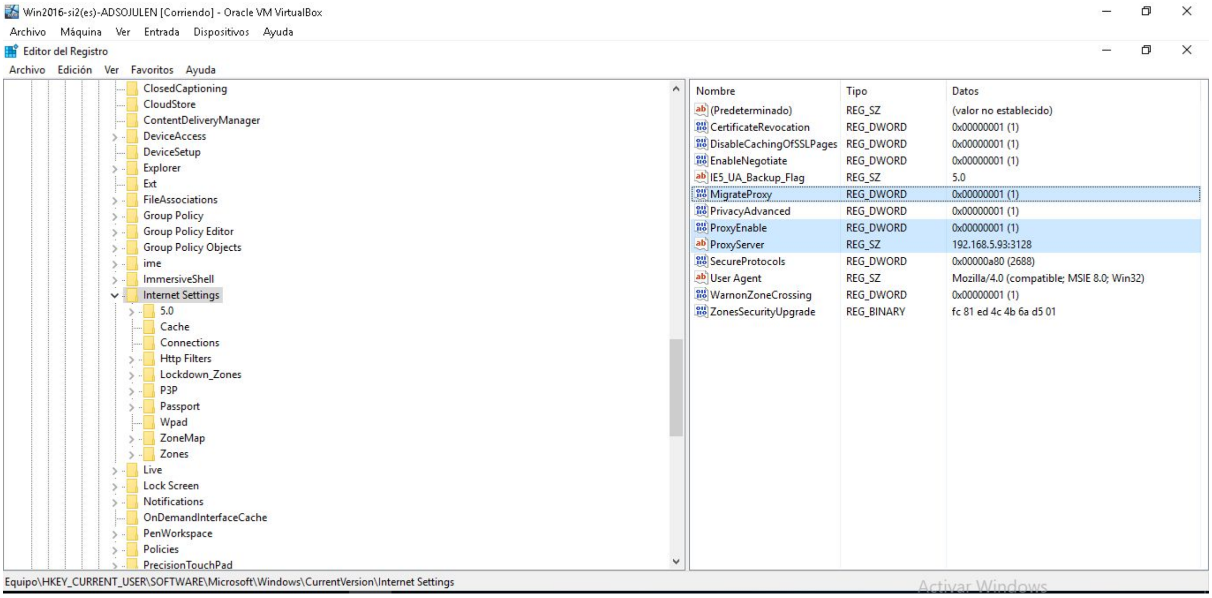


```
# Servidor PROXY 192.168.5.93
iptables -A FORWARD -p tcp --dport 3128 -j ACCEPT && echo "  FORWARD: 3128 (PROXY)"
iptables -A OUTPUT -p tcp --dport 3128 -j ACCEPT && echo "  FORWARD: 3128 (PROXY)"
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT && echo "  FORWARD: 3128 (PROXY)"
```

To configure the proxy server settings on a client computer, create the following .reg file to populate the registry with the proxy server information:

This is how we can set the proxy server configuration in a pc.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings]
"MigrateProxy"=dword:00000001
"ProxyEnable"=dword:00000001
"ProxyServer"="http://ProxyServername:80"
```

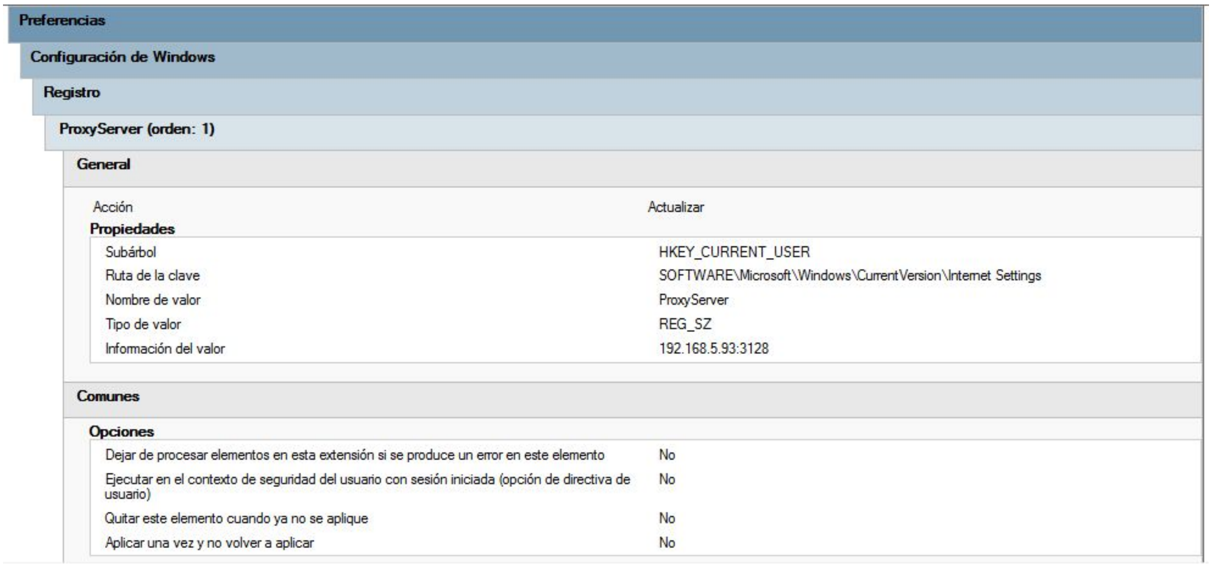


Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
CertificateRevocation	REG_DWORD	0x00000001 (1)
DisableCachingOfSSLPages	REG_DWORD	0x00000001 (1)
EnableNegotiate	REG_DWORD	0x00000001 (1)
IE5_UA_Backup_Flag	REG_SZ	5.0
MigrateProxy	REG_DWORD	0x00000001 (1)
PrivacyAdvanced	REG_DWORD	0x00000001 (1)
ProxyEnable	REG_DWORD	0x00000001 (1)
ProxyServer	REG_SZ	192.168.5.93:3128
SecureProtocols	REG_DWORD	0x00000a80 (2688)
User Agent	REG_SZ	Mozilla/4.0 (compatible; MSIE 8.0; Win32)
WarnonZoneCrossing	REG_DWORD	0x00000001 (1)
ZonesSecurityUpgrade	REG_BINARY	fc 81 ed 4c 4b 6a d5 01

Equipo\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

These are the values that we have to change in order to set the proxy server in any client, but we need a directive so that we can set them every time a client logins.

With this regedit directive we can set those values.



Preferencias

Configuración de Windows

Registro

ProxyServer (orden: 1)

General

Acción	Actualizar

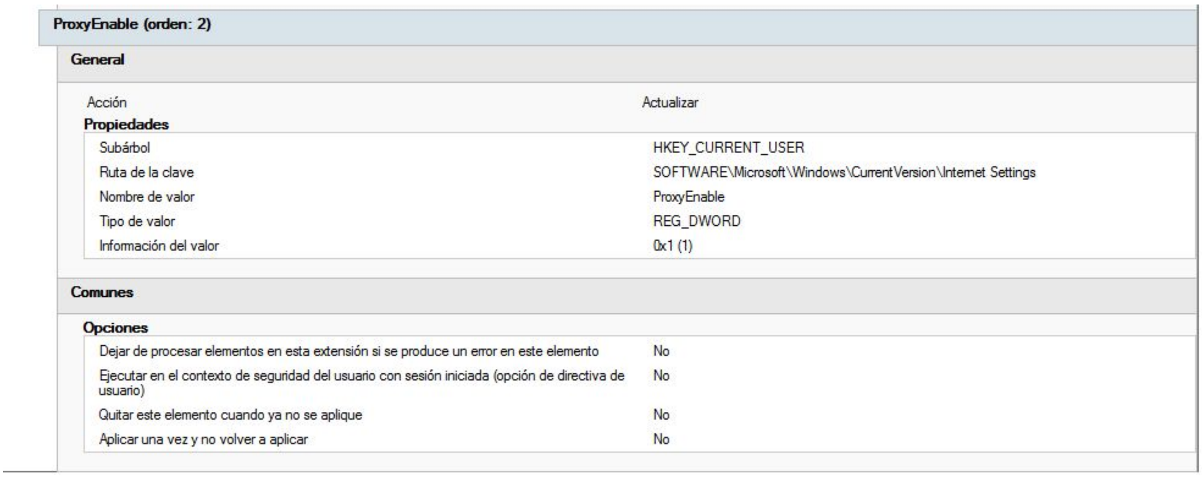
Propiedades

Subárbol	HKEY_CURRENT_USER
Ruta de la clave	SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Nombre de valor	ProxyServer
Tipo de valor	REG_SZ
Información del valor	192.168.5.93:3128

Comunes

Opciones

Dejar de procesar elementos en esta extensión si se produce un error en este elemento	No
Ejecutar en el contexto de seguridad del usuario con sesión iniciada (opción de directiva de usuario)	No
Quitar este elemento cuando ya no se aplique	No
Aplicar una vez y no volver a aplicar	No



ProxyEnable (orden: 2)

General

Acción	Actualizar

Propiedades

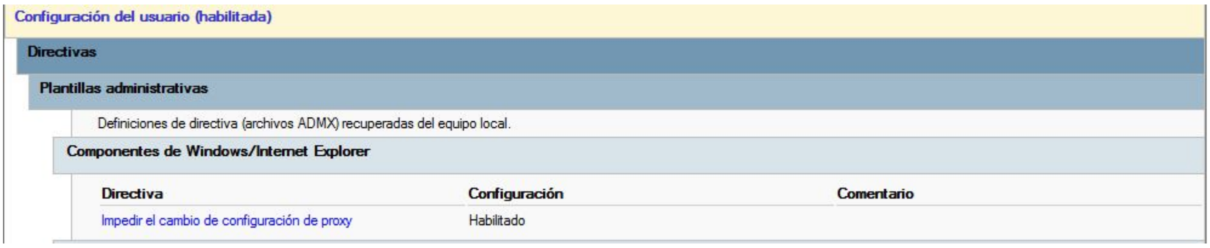
Subárbol	HKEY_CURRENT_USER
Ruta de la clave	SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Nombre de valor	ProxyEnable
Tipo de valor	REG_DWORD
Información del valor	0x1 (1)

Comunes

Opciones

Dejar de procesar elementos en esta extensión si se produce un error en este elemento	No
Ejecutar en el contexto de seguridad del usuario con sesión iniciada (opción de directiva de usuario)	No
Quitar este elemento cuando ya no se aplique	No
Aplicar una vez y no volver a aplicar	No

Now, in order to forbid our clients from changing this configuration we can use another active directory directive:



Configuración del usuario (habilitada)

Directivas

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

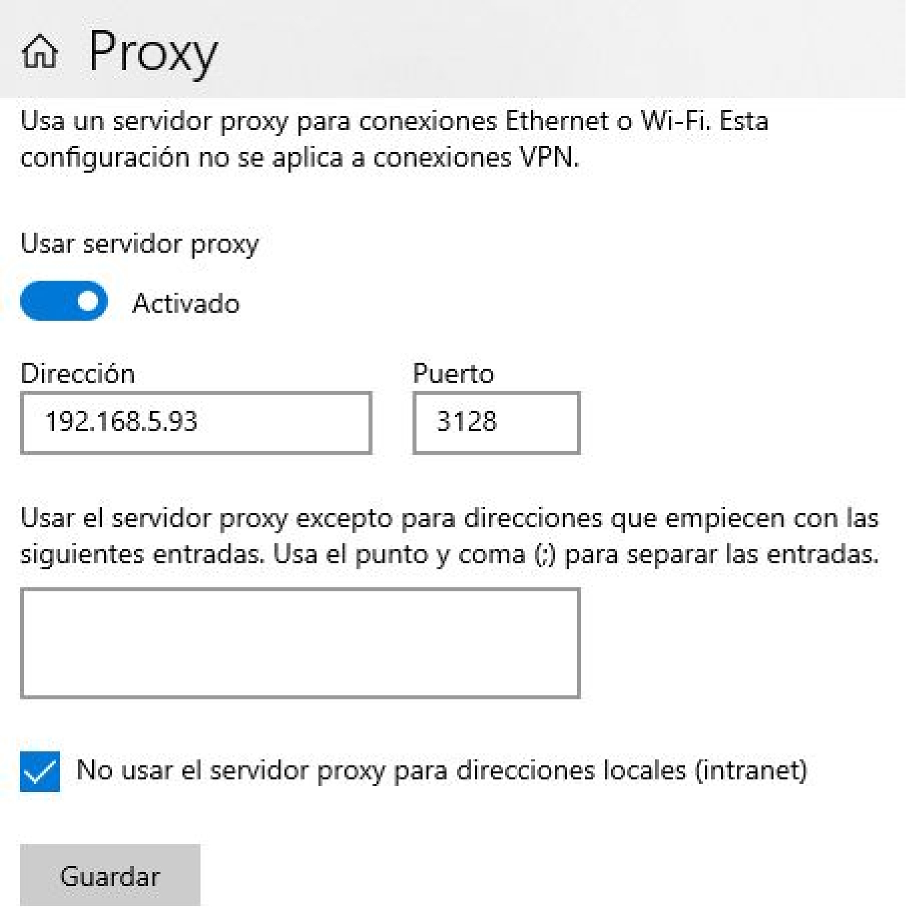
Componentes de Windows/Internet Explorer

Directiva	Configuración	Comentario
Impedir el cambio de configuración de proxy	Habilitado	

4.5-Checkings

The first step is to set the proxy in our machines configuration, in the case of windows 10, we will just access the proxy configuration of the system, we can access this option by going into advanced settings of our browser, or just searching for proxy in the windows search bar.

Set the proxy's ip and port and then turn it on, then click on "Guardar" in order to save the apply the changes.



Proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Usar servidor proxy

● Activado

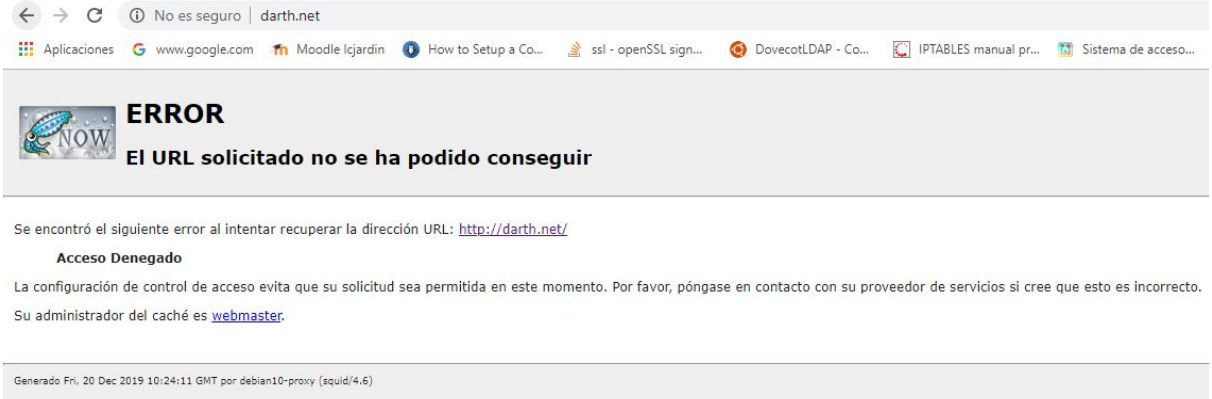
Dirección: 192.168.5.93

Puerto: 3128

Usar el servidor proxy excepto para direcciones que empiecen con las siguientes entradas. Usa el punto y coma (;) para separar las entradas.

☑ No usar el servidor proxy para direcciones locales (intranet)

The checkings for the forbidden webs only works if we try to access them using http and not https.



ERROR

El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: http://darth.net/

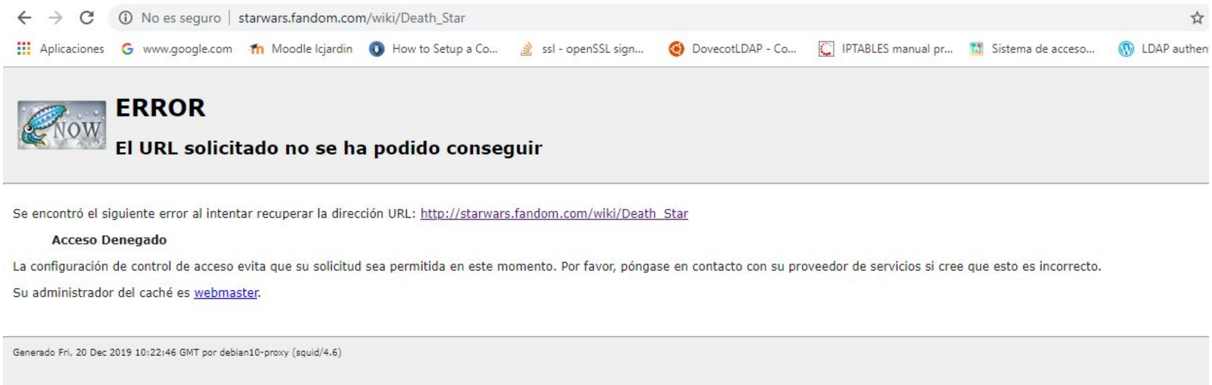
Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto.

Su administrador del caché es webmaster.

Generado Fri, 20 Dec 2019 10:24:11 GMT por debian10-proxy (squid/4.6)

http_access deny webs



ERROR

El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: http://starwars.fandom.com/wiki/Death_Star

Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto.

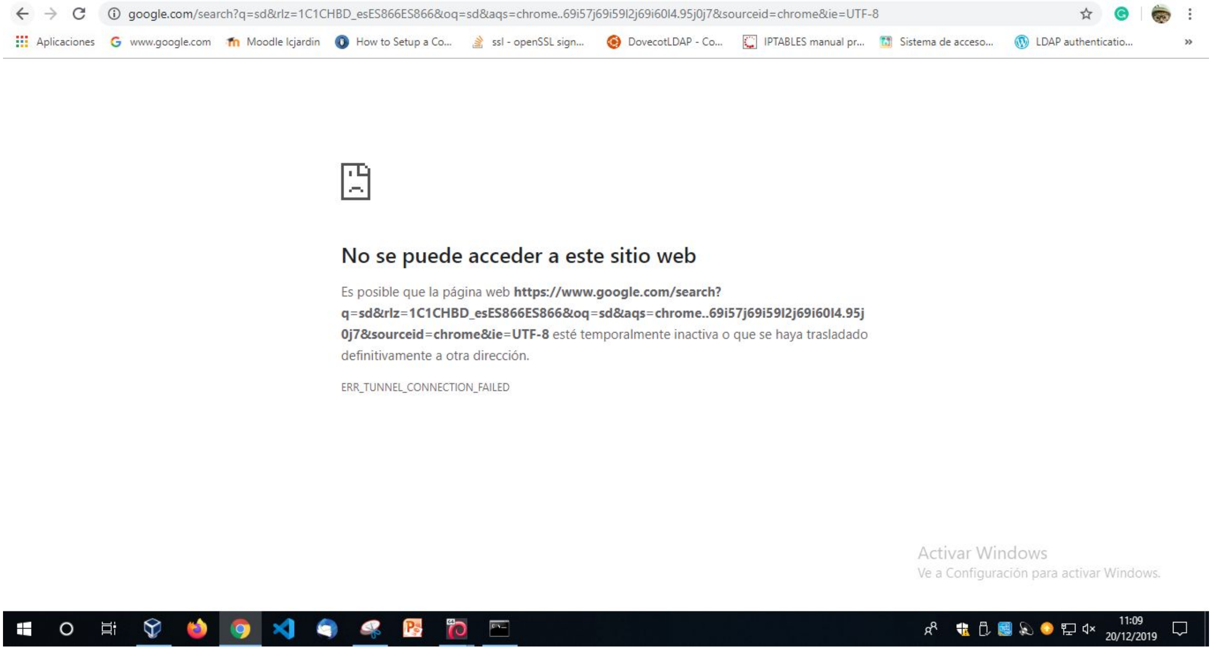
Su administrador del caché es webmaster.

Generado Fri, 20 Dec 2019 10:22:46 GMT por debian10-proxy (squid/4.6)

We allow visiting the webs defined for the schedule only in schedule time and we deny anything else in that schedule:

```
#Permitir acceso desde redlocal restringido en horario
http_access allow horario webshorario

http_access allow equipoad

http_access allow !horario redlocal
```

If you are inside the schedule defined you won't be able to access any web pages but the ones defined in the “webshorario” acl:



No se puede acceder a este sitio web

Es posible que la página web **https://www.google.com/search?q=sd&rlz=1C1CHBD_esES866ES866&oq=sd&aqs=chrome..69i57j69i59l2j69i60l4.95j0j7&sourceid=chrome&ie=UTF-8** esté temporalmente inactiva o que se haya trasladado definitivamente a otra dirección.

ERR_TUNNEL_CONNECTION_FAILED

5-Webgraphy

VPN

https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-10
https://moodle.icjardin.com/pluginfile.php/97056/mod_folder/content/0/guia_vpn.pdf?forcedownload=1

PROXY

https://www.juanluramirez.com/servidor-proxy-cache-squid/
https://linuxize.com/post/how-to-install-and-configure-squid-proxy-on-debian-10/
https://www.cyberciti.biz/faq/howto-linux-unix-view-squid-log-files/
https://wiki.squid-cache.org/SquidFaq/SquidLogs
https://socifi-doc.atlassian.net/wiki/spaces/SC/pages/5308677/SQUID+Proxy+-+Local+Cache+as+the+local+storage+Mikrotik+Linux

HTTP

https://askubuntu.com/questions/184791/how-to-disable-non-ssl-connection-on-apache-2-2
https://www.digitalocean.com/community/tutorials/como-instalar-el-servidor-web-apache-en-ubuntu-18-04-es
https://httpd.apache.org/docs/trunk/es/howto/
https://www.linux.com/news/apache-authentication-and-authorization-using-ldap/

FTP

https://www.server-world.info/en/note?os=Ubuntu_16.04&p=ftp&f=1
https://serverfault.com/questions/318622/vsftpd-ldap-pam