



Realizada por Benjamin Gordo Cortés

Contenido

Índice de ilustraciones.....	2
Esquema de red.....	4
Configuración del router.	4
Comprobación a nivel de red.	5
Reglas en router Mikrotik	6
Creación de usuario y directorios para VSFTPD.	7
Configuración de CENTOS	8
Instalación y configuración del VSFTP en CENTOS.....	9
Instalación y configuración DNS.....	9
Pruebas de funcionamiento	12
DNS.....	12
Realizar una petición de transferencia de zona.	12
Consulta directa.	12
Zona indirecta.....	12
Consulta a ftp.zona.tech	12
FTP.....	13
Conexión al ftp a través del FQDN desde la red interna 1.....	13
Accediendo al ftp a través de su IP.	13
Subir ficheros con el usuario evil.....	14
Subir ficheros con el usuario andrea.....	15
Alternativo: Acceder desde internet con DNAT	16

Índice de ilustraciones

Ilustración 1 Esquema de red.....	4
Ilustración 2 Menú Winbox para configurar interfaces	4
Ilustración 3 configuración de las interfaces del router	4
Ilustración 4 ping red interna 1 a internet	5
Ilustración 5 ping red interna 1 a red interna 2	5
Ilustración 6 ping de internet a red interna 1	5
Ilustración 7 ping de internet a red interna 2	5
Ilustración 8 ping de servidor a red interna 1	6
Ilustración 9 ping de servidor a red interna 1	6
Ilustración 10 regla para no permitir conexión de internet con la red interna parte 1.....	6
Ilustración 11 comprobación regla en Mikrotik filtrado ICMP	6
Ilustración 12 creación de directorios de usuarios	7
Ilustración 13 creación de usuario evil.....	7
Ilustración 14 creación de usuario andrea.....	7
Ilustración 15 configuración de contraseña usuario andrea.....	7
Ilustración 16 configuración de contraseña usuario evil	7
Ilustración 17 asignación de dueño y grupo a los directorios.....	7
Ilustración 18 añadir shell	7
Ilustración 19 interfaz de red CENTOS.....	8
Ilustración 20 regla de filtrado de ICMP.....	8
Ilustración 21 ping realizado desde un host en internet	8
Ilustración 22 ping realizado desde una maquina en la red interna 1.....	8
Ilustración 23 inicio automático del servicio.....	9
Ilustración 24 parar el firewall de CENTOS	9
Ilustración 25 deshabilitar el firewall de CENTOS.....	9
Ilustración 26 instalación del paquete Bind	9
Ilustración 27 configuración de las zonas del DNS.....	9
Ilustración 28 copia del archivo named.empty para la zona directa	10
Ilustración 29 copia del archivo named.empty para la zona inversa.....	10
Ilustración 30 cambio de dueño a la configuración de zonas	10
Ilustración 31 contenido de db.zona.tech zona directa.....	10
Ilustración 32 contenido de db.0.2.0.10 zona inversa	10
Ilustración 33 error al iniciar el servicio una vez instalado	11
Ilustración 34 configuración del archivo para solucionar el error	11
Ilustración 35 transferencia de zona con DIG	12
Ilustración 36 consulta al servidor DNS consulta directa.....	12
Ilustración 37 consulta al servidor DNS consulta indirecta.....	12
Ilustración 38 consulta a ftp.zona.tech	12
Ilustración 39 conexión al ftp por su FQDN desde la red interna 1	13
Ilustración 40 accediendo al FTP a través de su IP.....	13
Ilustración 41 análisis de tráfico de una conexión segura ftp.....	13
Ilustración 42 metadatos del tráfico con Network Miner.....	13
Ilustración 43 análisis de tráfico de una conexión no segura ftp.....	13
Ilustración 44 directorio ftp del usuario evil	14
Ilustración 45 fichero subido al directorio ftp del usuario evil	14
Ilustración 46 directorio ftp de la usuaria andrea.....	15

Ilustración 47 fichero subido al directorio ftp del usuario evil	15
Ilustración 48 regla DNAT puerto de control y dirección parte 1	16
Ilustración 49 regla DNAT puerto de control y dirección parte 1	16
Ilustración 50 regla DNAT puertos pasivos parte 1.....	16
Ilustración 51 regla DNAT puertos pasivos parte 2.....	16
Ilustración 52 comprobación regla DNAT	17

Esquema de red.

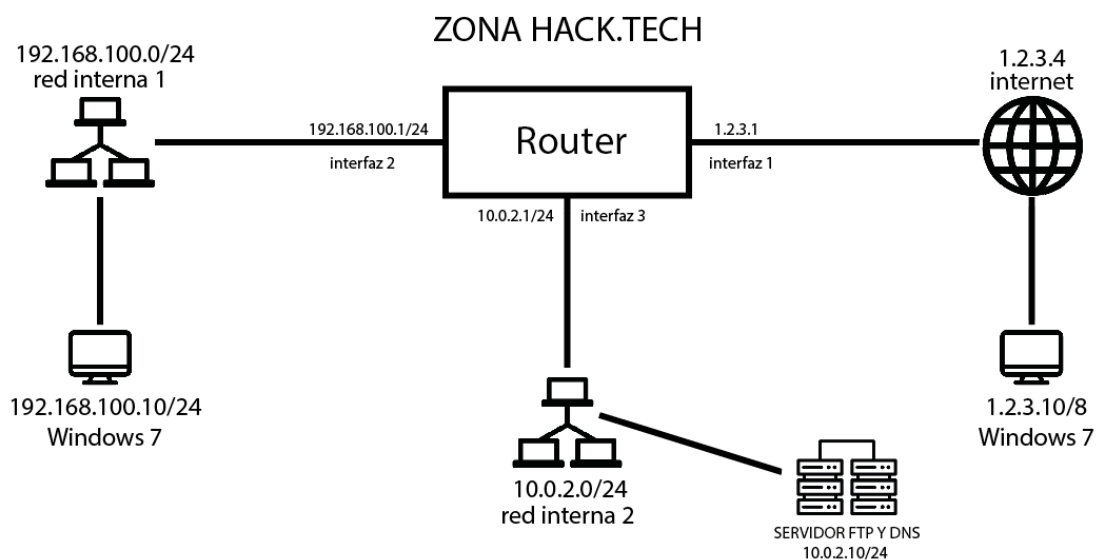


Ilustración 1 Esquema de red

Configuración del router.

Nos iremos a nuestro Winbox y seleccionaremos nuestro router. Una vez seleccionado nos vamos a la pestaña de IP > Addresses para agregar las IP a las interfaces de red.

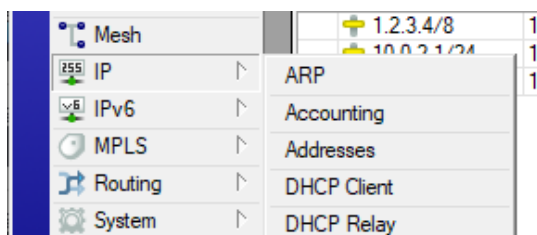


Ilustración 2 Menú Winbox para configurar interfaces

Address List			
Address	Network	Interface	
1.2.3.4/8	1.0.0.0	ether1	
10.0.2.1/24	10.0.2.0	ether3	
192.168.100.1...	192.168.100.0	ether2	

Ilustración 3 configuración de las interfaces del router

Comprobación a nivel de red.

Antes de realizar todas las demás configuraciones y el montaje del servidor pondremos máquinas en las diferentes redes para comprobar que hay conexión a nivel de red entre ellas y evitar posibles problemas después.

Máquina en red interna 1:

```
C:\Users\win7>ping 1.2.3.10

Pinging 1.2.3.10 with 32 bytes of data:
Reply from 1.2.3.10: bytes=32 time<1ms TTL=63
Reply from 1.2.3.10: bytes=32 time<1ms TTL=63
Reply from 1.2.3.10: bytes=32 time<1ms TTL=63
Reply from 1.2.3.10: bytes=32 time<1ms TTL=63

Ping statistics for 1.2.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 4 ping red interna 1 a internet

```
C:\Users\win7>ping 10.0.2.10

Pinging 10.0.2.10 with 32 bytes of data:
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63

Ping statistics for 10.0.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 5 ping red interna 1 a red interna 2

Máquina en red interna 2:

```
C:\Users\win7>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:
Reply from 192.168.100.10: bytes=32 time=1ms TTL=127
Reply from 192.168.100.10: bytes=32 time<1ms TTL=127
Reply from 192.168.100.10: bytes=32 time<1ms TTL=127
Reply from 192.168.100.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ilustración 6 ping de internet a red interna 1

```
C:\Users\win7>ping 10.0.2.10

Pinging 10.0.2.10 with 32 bytes of data:
Reply from 10.0.2.10: bytes=32 time=1ms TTL=63
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63
Reply from 10.0.2.10: bytes=32 time=1ms TTL=63
Reply from 10.0.2.10: bytes=32 time<1ms TTL=63

Ping statistics for 10.0.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ilustración 7 ping de internet a red interna 2

Server en red interna 2:

```
[root@localhost benja]# ping 192.168.100.10 -c 2
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=127 time=0.856 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=127 time=0.837 ms
```

Ilustración 8 ping de servidor a red interna 1

```
[root@localhost benja]# ping 10.0.2.10 -c 2
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.
64 bytes from 10.0.2.10: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 10.0.2.10: icmp_seq=2 ttl=64 time=0.062 ms
```

Ilustración 9 ping de servidor a red interna 1

Reglas en router Mikrotik .

En el apartado de firewall de Mikrotik debemos crear esta regla:

- Desde la red internet no se podrá acceder a la red interna 1 (192.168.100.0/24).

Iremos al apartado del router IP > firewall e iremos a “Filter Rules” y configuraremos la regla. Ahí configuraremos que desde internet no se pueda acceder a la red interna 1 .

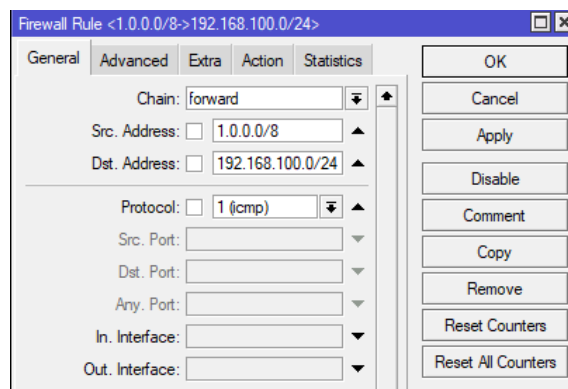
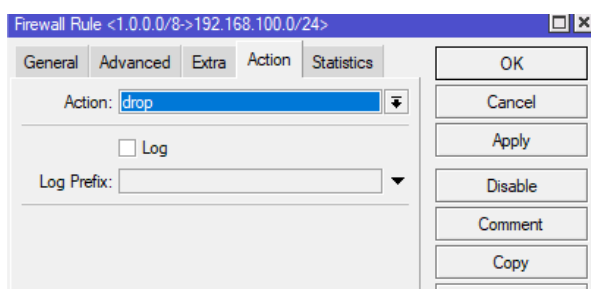


Ilustración 10 regla para no permitir conexión de internet con la red interna parte 1



Ahora haremos un ping desde la red Internet hacia la red interna 1

```
C:\Windows\system32\cmd.exe

C:\Users\win7>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 11 comprobación regla en Mikrotik filtrado ICMP

Creación de usuario y directorios para VSFTPD.

Crearemos los usuarios evil y Andrea que tendrán sus directorios en home (/home/ evil, /home/andrea). Primero crearemos los directorios pertenecientes a los usuarios.

```
[root@localhost home]# mkdir evil
[root@localhost home]# mkdir andrea
```

Ilustración 12 creación de directorios de usuarios

Luego crearemos los usuarios .

```
[root@localhost home]# useradd evil -d /home/evil/ -s /bin/ftp -G ftp -c "evil"
```

Ilustración 13 creación de usuario evil

```
[root@localhost home]# useradd andrea -d /home/andrea/ -s /bin/ftp -G ftp -c "andrea"
```

Ilustración 14 creación de usuario andrea

Les asignaremos unas contraseñas.

```
[root@localhost home]# passwd andrea
```

Ilustración 15 configuración de contraseña usuario andrea

```
[root@localhost home]# passwd evil
```

Ilustración 16 configuración de contraseña usuario evil

Ahora cambiaremos el dueño y grupo de sus directorios.

```
[root@localhost home]# chown andrea:ftp -R andrea/
[root@localhost home]# chown evil:ftp -R evil/
[root@localhost home]# ls -l
total 4
drwxr-xr-x. 15 andrea ftp    244 dic 29 10:58 andrea
drwx----- 15 benja  benja 4096 ene 15 17:38 benja
drwxr-xr-x.  4 evil   ftp    49 ene 15 13:30 evil
[root@localhost home]#
```

Ilustración 17 asignación de dueño y grupo a los directorios

Y agregaremos la Shell en */etc/shells*

```
GNU nano 2.9.8 /etc/shells
/bin/sh
/bin/bash
/usr/bin/sh
/usr/bin/bash
/bin/ftp
```

Ilustración 18 añadir shell

Configuración de CENTOS

La configuración de red de CENTOS será:

```
GNU nano 2.9.8 /etc/sysconfig/network-scripts/ifcfg-enp0s3
BOOTPROTO=static
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
IPADDR=10.0.2.10
PREFIX=24
GATEWAY=10.0.2.1
DNS1=10.0.2.10
```

Ilustración 19 interfaz de red CENTOS

Aplicaremos una regla en iptables para dropear todos los mensajes de tipo icmp 8 cuyo origen sea la red interna 1 (192.168.100.0/24) e internet (interfaz 1.2.3.4) y comprobamos que la regla funciona.

```
[root@localhost benja]# iptables -A INPUT -p icmp --icmp-type 8 -j DROP
```

Ilustración 20 regla de filtrado icmp en CENTOS

También deberemos hacer persistente la regla para que cuando se reinicie el sistema permanezca la regla.

```
[root@localhost ~]# iptables-save > reglas
```

Ilustración 21 regla iptables persistente parte 1

Una vez hagamos esto iremos al archivo oculto .bashrc y añadiremos al final iptables-restore reglas

```
iptables-restore reglas
```

Ilustración 22 regla iptables persistencia parte 2

Reiniciaremos y comprobaremos la regla.

Ilustración 23 regla de filtrado de ICMP

```
C:\Users\win7>ping 10.0.2.10
Pinging 10.0.2.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 24 ping realizado desde un host en internet

```
C:\Users\win7>ping 10.0.2.10
Pinging 10.0.2.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 25 ping realizado desde una maquina en la red interna 1

Instalación y configuración del VSFTP en CENTOS.

En primer lugar, instalaremos el paquete con el comando `yum install vsftpd` y realizaremos una copia de archivo de configuración con el comando `cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.confbak`. Una vez tengamos la copia de seguridad tenemos que se ejecute el servicio al iniciar la máquina.

```
[root@localhost benja]# systemctl enable --now vsftpd
```

Ilustración 26 inicio automático del servicio

Después debemos desactivar el firewall.

```
[root@localhost benja]# systemctl stop firewalld
```

Ilustración 27 parar el firewall de CENTOS

Y también deshabilitaremos el firewall para así evitar que una vez iniciemos la maquina se vuelve a activar el firewall.

```
[root@localhost benja]# systemctl disable firewalld
```

Ilustración 28 deshabilitar el firewall de CENTOS

En el archivo de configuración `/etc/vsftpd/vsftpd.conf` tendremos que tener estas líneas:

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list (en este archivo pondremos al
usuario evil)
allow_writeable_chroot=YES
listen_ipv6=YES
```

Una vez tenemos estas directivas reiniciamos el servicio podremos acceder al ftp.

Instalación y configuración DNS.

En primer lugar, instalaremos el paquete bind para poder tener el servicio DNS.

```
[root@localhost benja]# yum install bind
```

Ilustración 29 instalación del paquete Bind

Ahora iremos a al archivo de configuración de las zonas situado en `/etc/named.conf`

```
zone "zona.tech"{
    type master;
    file "/var/named/db.zona.tech";
    allow-query{192.168.100.0/24;};
    allow-transfer{none;};
};
zone "10.2.0.10.in-addr.arpa"{
    type master;
    file "/var/named/db.10.2.0.10";
    allow-query{192.168.100.0/24;};
    allow-transfer{none;};
};
```

Ilustración 30 configuración de las zonas del DNS

Ahora crearemos los archivos que contendrán la configuración de las zonas.

```
[root@localhost var]# cp /var/named/named.empty /var/named/db.zona.tech
```

Ilustración 31 copia del archivo named.empty para la zona directa

```
[root@localhost var]# cp /var/named/named.empty /var/named/db.10.2.0.10
```

Ilustración 32 copia del archivo named.empty para la zona inversa

Una vez cambiado el dueño o el grupo por named para que se pueda iniciar con el servicio, pasaremos a configurar los archivos.

```
[root@localhost benja]# ls -l /var/named/
total 24
drwxrwx---. 2 named named 49 ene 12 17:41 data
-rw-r-----. 1 named root 211 dic 31 12:36 db.10.2.0.10
-rw-r-----. 1 named root 201 dic 31 12:10 db.zona.tech
drwxrwx---. 2 named named 60 ene 14 09:24 dynamic
-rw-r-----. 1 root named 2253 ago 24 19:31 named.ca
-rw-r-----. 1 root named 152 ago 24 19:31 named.empty
-rw-r-----. 1 root named 152 ago 24 19:31 named.localhost
-rw-r-----. 1 root named 168 ago 24 19:31 named.loopback
drwxrwx---. 2 named named 6 ago 24 19:31 slaves
[root@localhost benja]#
```

Ilustración 33 cambio de dueño a la configuración de zonas

Zona directa:

```
GNU nano 2.9.8 /var/named/db.zona.tech
$TTL 3H
@      IN SOA  @ zona.tech. (
                                0      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

      NS      @
      NS      evil.zona.tech.
      A       127.0.0.1
      AAAA    ::1
evil     A     10.0.2.10
ftp      A     10.0.2.10
```

Ilustración 34 contenido de db.zona.tech zona directa

Zona indirecta:

```
GNU nano 2.9.8 /var/named/db.10.2.0.10
$TTL 3H
@      IN SOA  @ zona.tech. (
                                0      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

      NS      @
      NS      evil.zona.tech.
      A       127.0.0.1
      AAAA    ::1
10       PTR   evil.zona.tech
10       PTR   ftp.zona.tech
```

Ilustración 35 contenido de db.0.2.0.10 zona inversa

Si nos sale este fallo para solucionarlo tendremos que modificar el archivo `/etc/sysconfig/named` y poner `OPTIONS="-4"`, reiniciando el servicio se corregirá el error.

```
[root@localhost benja]# service named status
Redirecting to /bin/systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-12-31 11:53:09 CET; 12s ago
     Process: 2910 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
     Process: 2916 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -c /etc/named.conf; fi (code=exited, status=0/SUCCESS)
    Main PID: 2921 (named)
      Tasks: 5 (limit: 11323)
     Memory: 67.0M
    CGroup: /system.slice/named.service
            └─2921 /usr/sbin/named -u named -c /etc/named.conf

dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/A/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/AAAA/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/A/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/AAAA/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/A/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/AAAA/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/A/IN': 2.11.4.4:53
dic 31 11:53:22 localhost.localdomain named[2921]: network unreachable resolving '2.centos.pool.ntp.org/AAAA/IN': 2.11.4.4:53
```

Ilustración 36 error al iniciar el servicio una vez instalado

```
GNU nano 2.9.8 /etc/sysconfig/named

# BIND named process options
# ~~~~~
# OPTIONS="whatever" -- These additional options will be passed to named
#                      at startup. Don't add -t here, enable proper
#                      -chroot.service unit file.
#
OPTIONS="-4"
# NAMEDCONF=/etc/named/alternate.conf
```

Ilustración 37 configuración del archivo para solucionar el error

Una vez hayamos puesto `OPTIONS="-4"` y reiniciemos el servicio no nos saldrá el error.

Pruebas de funcionamiento

DNS

Realizar una petición de transferencia de zona.

```
root@kali:~# dig @evil.zona.tech zona.tech AXFR

; <<>> DiG 9.11.4-P2-3-Debian <<>> @evil.zona.tech zona.tech AXFR
; (1 server found)
;; global options: +cmd
; Transfer failed.
root@kali:~#
```

Ilustración 38 transferencia de zona con DIG

Consulta directa.

```
C:\Users\win7>nslookup zona.tech
10.2.0.10.in-addr.arpa
primary name server = 10.2.0.10.in-addr.arpa
responsible mail addr = zona.tech
serial = 0
refresh = 86400 <1 day>
retry = 3600 <1 hour>
expire = 604800 <7 days>
default TTL = 10800 <3 hours>
Server: Unknown
Address: 10.0.2.10

Name: zona.tech
Addresses: ::1
           127.0.0.1
```

Ilustración 39 consulta al servidor DNS consulta directa

Zona indirecta.

```
C:\Users\win7>nslookup 10.0.2.10
10.2.0.10.in-addr.arpa
primary name server = 10.2.0.10.in-addr.arpa
responsible mail addr = zona.tech
serial = 0
refresh = 86400 <1 day>
retry = 3600 <1 hour>
expire = 604800 <7 days>
default TTL = 10800 <3 hours>
Server: Unknown
Address: 10.0.2.10
```

Ilustración 40 consulta al servidor DNS consulta indirecta

Resolución a ftp.zona.tech

```
C:\Users\win7>nslookup ftp.zona.tech
10.2.0.10.in-addr.arpa
primary name server = 10.2.0.10.in-addr.arpa
responsible mail addr = zona.tech
serial = 0
refresh = 86400 <1 day>
retry = 3600 <1 hour>
expire = 604800 <7 days>
default TTL = 10800 <3 hours>
Server: Unknown
Address: 10.0.2.10

Name: ftp.zona.tech
Address: 10.0.2.10
```

Ilustración 41 consulta a ftp.zona.tech

FTP

Conexión al ftp a través del FQDN desde la red interna 1.

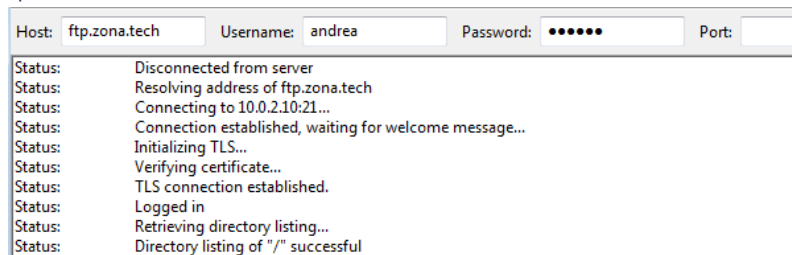


Ilustración 42 conexión al ftp por su FQDN desde la red interna 1

Accediendo al ftp a través de su IP.

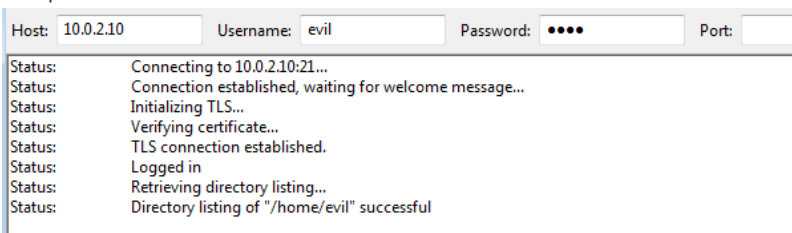


Ilustración 43 accediendo al FTP a través de su IP

Si al acceder al ftp usamos un analizador de tráfico veremos que está cifrado.

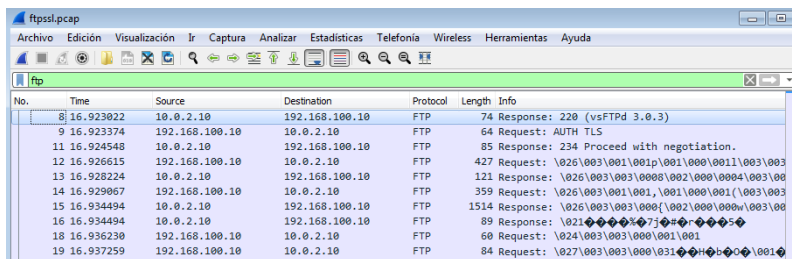


Ilustración 44 análisis de tráfico de una conexión segura ftp

También podemos usar Network Miner para analizar los metadatos y ver claramente que no hay credenciales.

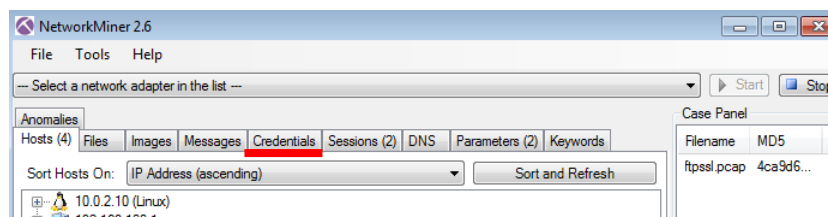


Ilustración 45 metadatos del tráfico con Network Miner

Para poder ver la diferencia esto es lo que saldría sin el SSL, el usuario y la clave en texto claro.

Source	Destination	Protocol	Length	Info
10.0.2.10	192.168.100.10	FTP	74	Response: 220 (vsFTPd 3.0.3)
192.168.100.10	10.0.2.10	FTP	64	Request: AUTH TLS
10.0.2.10	192.168.100.10	FTP	92	Response: 530 Please login with USER and PASS.
192.168.100.10	10.0.2.10	FTP	64	Request: AUTH SSL
10.0.2.10	192.168.100.10	FTP	92	Response: 530 Please login with USER and PASS.
192.168.100.10	10.0.2.10	FTP	65	Request: USER evil
10.0.2.10	192.168.100.10	FTP	88	Response: 331 Please specify the password.
192.168.100.10	10.0.2.10	FTP	65	Request: PASS evil

Ilustración 46 análisis de tráfico de una conexión no segura ftp

Subir ficheros con el usuario evil

Estableceremos conexión con el FTP y subiremos el fichero dentro de la carpeta ftp.

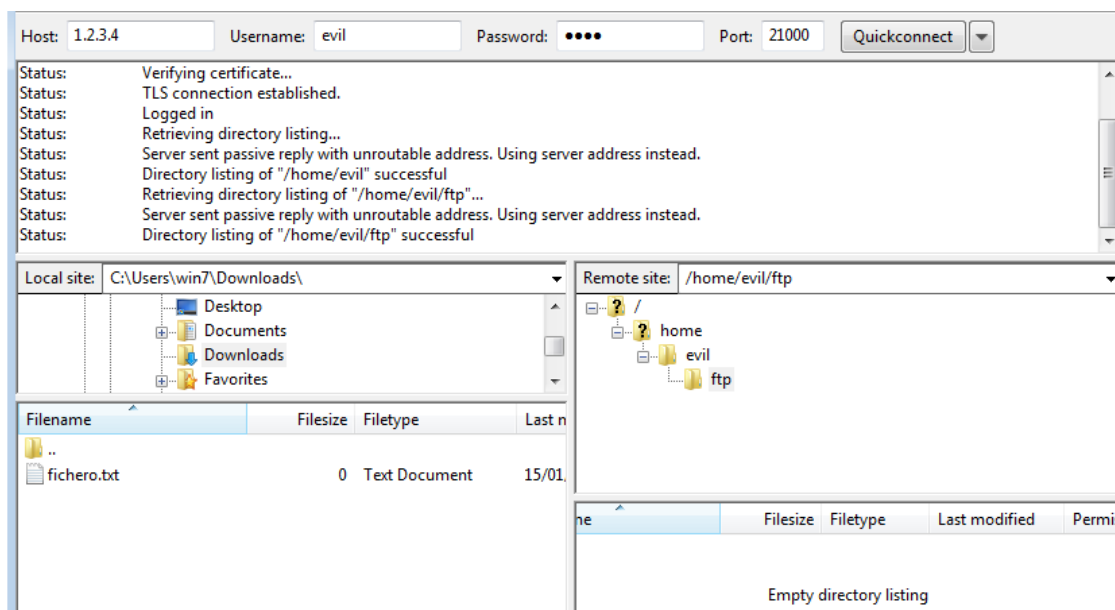


Ilustración 47 directorio ftp del usuario evil

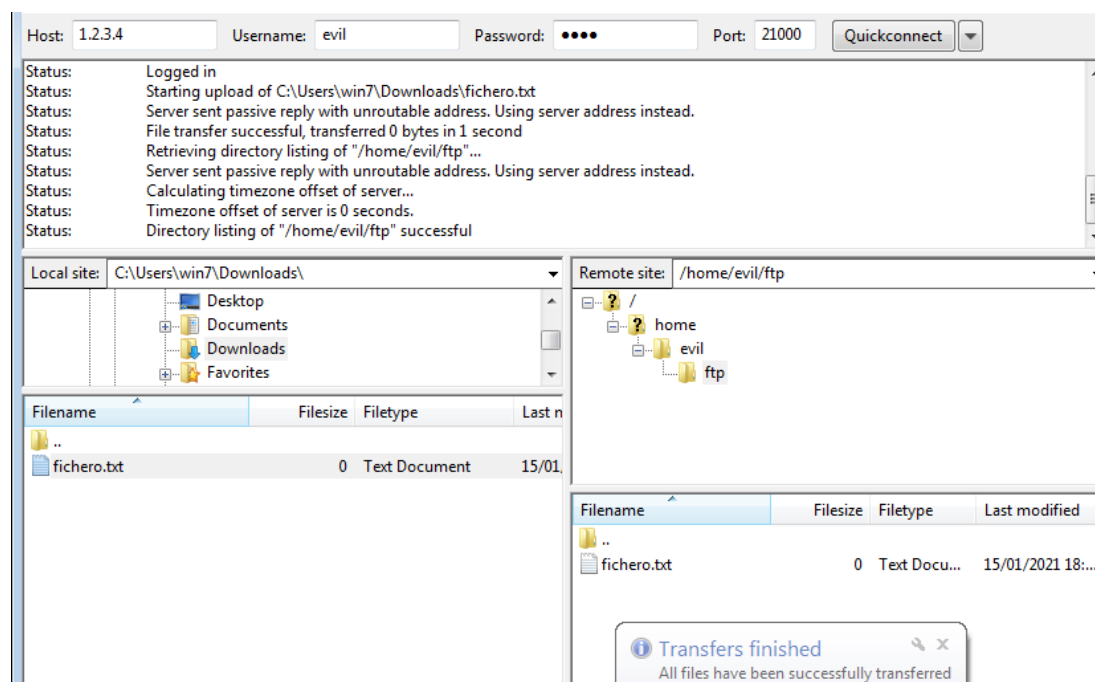


Ilustración 48 fichero subido al directorio ftp del usuario evil

Subir ficheros con el usuario andrea.

Estableceremos conexión con el FTP y subiremos el fichero dentro de la carpeta ftp.

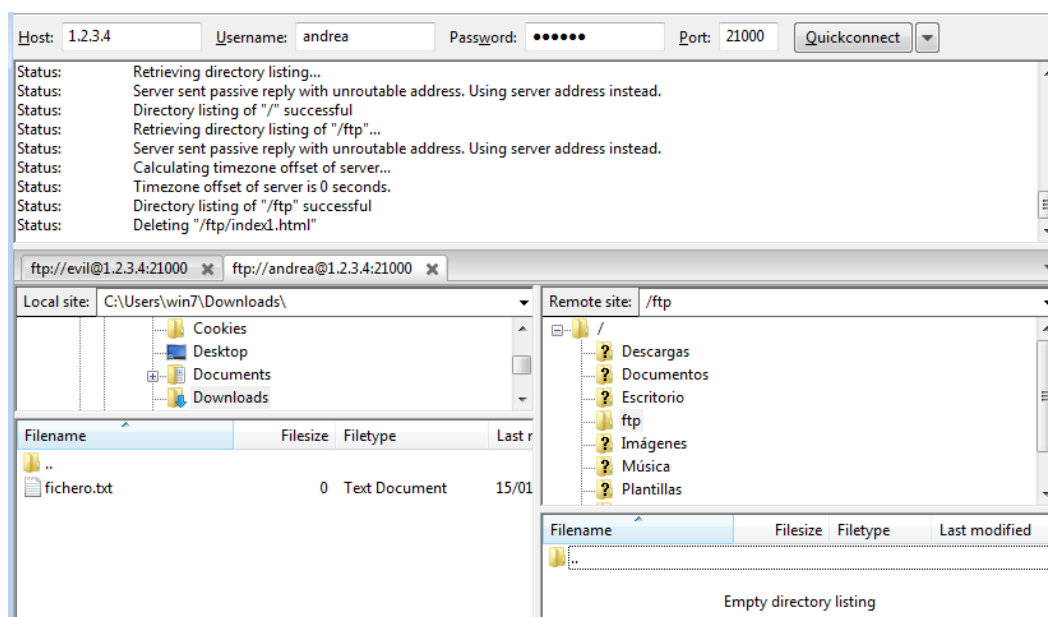


Ilustración 49 directorio ftp de la usuaria andrea

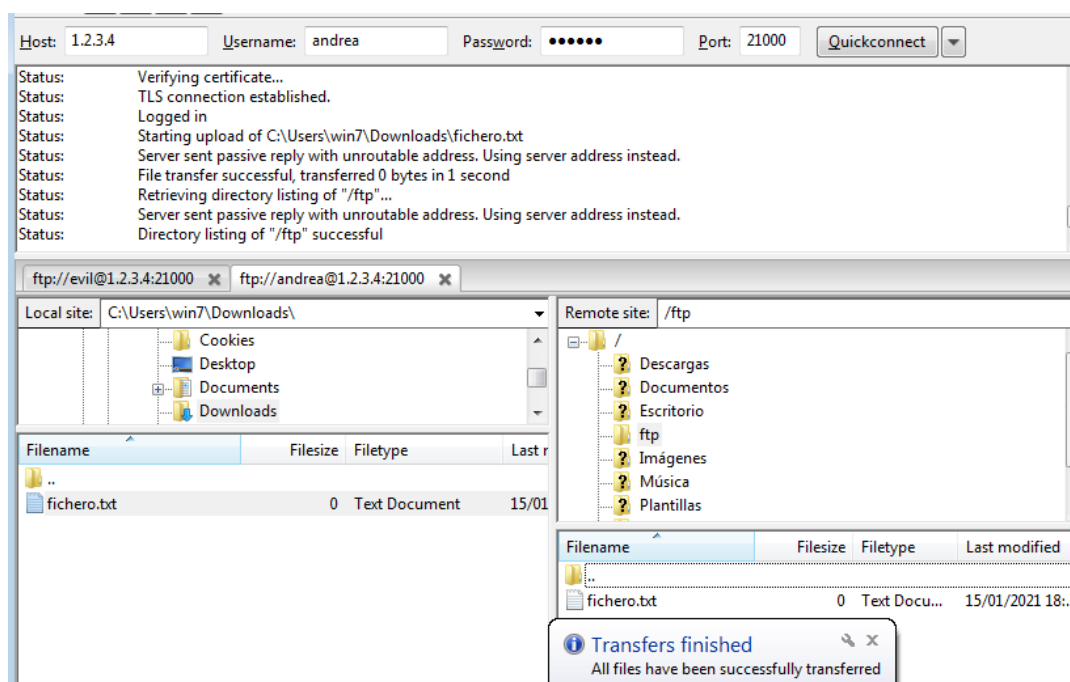


Ilustración 50 fichero subido al directorio ftp del usuario evil

Alternativo: Acceder desde internet con DNAT

Para poder acceder al FTP desde internet y poder mantener el anonimato de nuestra red interna 2, debemos añadir al router una regla DNAT para definir la dirección y el puerto de control (1.2.3.4:21000) y otra regla para habilitar los puertos pasivos.

The screenshot shows the 'General' tab of a NAT Rule configuration window titled 'NAT Rule <1.2.3.4:21000>'. The 'Chain' is set to 'dstnat'. The 'Dst. Address' is '1.2.3.4'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '21000'. The 'Src. Address' and 'Src. Port' fields are empty. The right side of the window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

Ilustración 51 regla DNAT puerto de control y dirección parte 1

The screenshot shows the 'Action' tab of the same NAT Rule configuration window. The 'Action' is 'dst-nat'. There is an unchecked 'Log' checkbox. The 'Log Prefix' is empty. The 'To Addresses' is '10.0.2.10'. The 'To Ports' is '21'. The right side of the window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', and 'Copy'.

Ilustración 52 regla DNAT puerto de control y dirección parte 2

The screenshot shows the 'General' tab of a NAT Rule configuration window titled 'NAT Rule <1.2.3.4:23000-25000>'. The 'Chain' is 'dstnat'. The 'Dst. Address' is '1.2.3.4'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '23000-25000'. The 'Src. Address' and 'Src. Port' fields are empty. The right side of the window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

Ilustración 53 regla DNAT puertos pasivos parte 1

The screenshot shows the 'Action' tab of the same NAT Rule configuration window. The 'Action' is 'dst-nat'. There is an unchecked 'Log' checkbox. The 'Log Prefix' is empty. The 'To Addresses' is '10.0.2.10'. The 'To Ports' is empty. The right side of the window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Ilustración 54 regla DNAT puertos pasivos parte 2

También al fichero de configuración del vsftpd (/etc/vsftpd/vsftpd.conf) debemos añadir estas líneas.

```
Pasv_enable=YES
pasv_min_port=23000
pasv_max_port=25000
```

Abriremos FileZilla en la máquina que tenemos desde internet y comprobaremos que al poner la dirección 1.2.3.4 y puerto 21000 tenemos conexión.

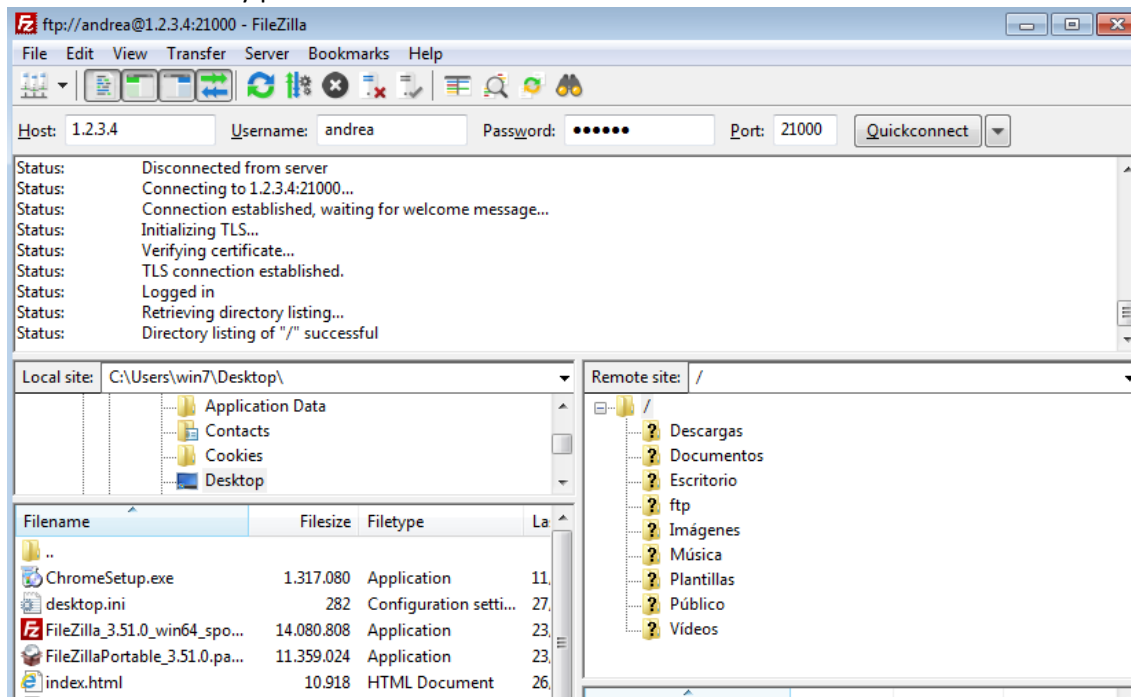


Ilustración 55 comprobación regla DNAT