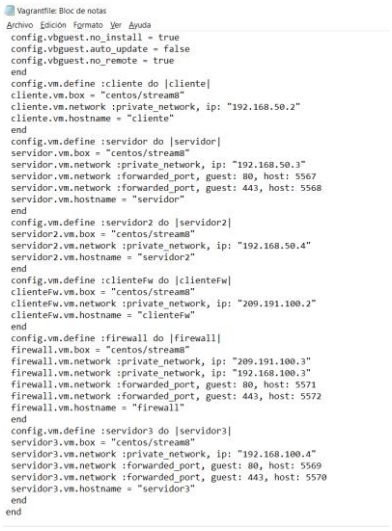
Oscar David Quiñones Franco

Cod: 2215738

## 1. FTP Seguro protegido por firewall

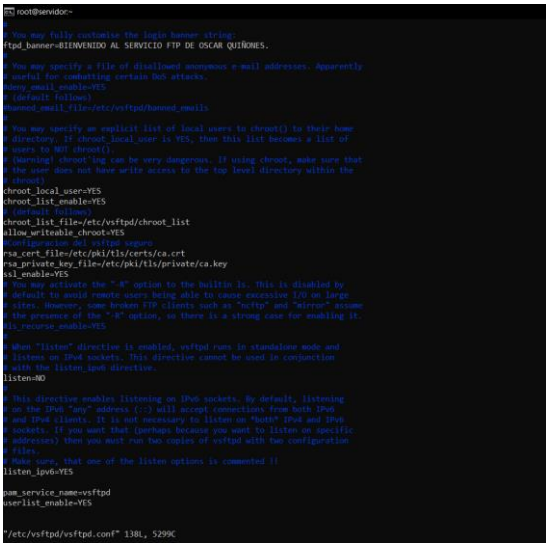
Para esta prueba se usaron dos maquinas: servidor y firewall.

Configuración vagrantfile:



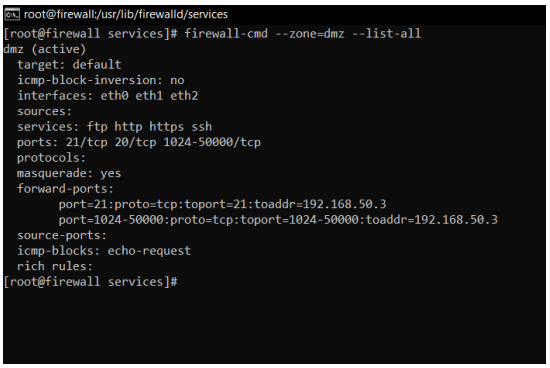
```
Vagrantfile: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
 config.vbguest.no_install = true
 config.vbguest.auto_update = false
 config.vbguest.no_remote = true
 end
 config.vm.define :cliente do |cliente|
 cliente.vm.box = "centos/stream8"
 cliente.vm.network :private_network, ip: "192.168.50.2"
 cliente.vm.hostname = "cliente"
 end
 config.vm.define :servidor do |servidor|
 servidor.vm.box = "centos/stream8"
 servidor.vm.network :private_network, ip: "192.168.50.3"
 servidor.vm.network :forwarded_port, guest: 80, host: 5567
 servidor.vm.network :forwarded_port, guest: 443, host: 5568
 servidor.vm.hostname = "servidor"
 end
 config.vm.define :servidor2 do |servidor2|
 servidor2.vm.box = "centos/stream8"
 servidor2.vm.network :private_network, ip: "192.168.50.4"
 servidor2.vm.hostname = "servidor2"
 end
 config.vm.define :clienteFw do |clienteFw|
 clienteFw.vm.box = "centos/stream8"
 clienteFw.vm.network :private_network, ip: "209.191.100.2"
 clienteFw.vm.hostname = "clienteFw"
 end
 config.vm.define :firewall do |firewall|
 firewall.vm.box = "centos/stream8"
 firewall.vm.network :private_network, ip: "209.191.100.3"
 firewall.vm.network :private_network, ip: "192.168.100.3"
 firewall.vm.network :forwarded_port, guest: 80, host: 5571
 firewall.vm.network :forwarded_port, guest: 443, host: 5572
 firewall.vm.hostname = "firewall"
 end
 config.vm.define :servidor3 do |servidor3|
 servidor3.vm.box = "centos/stream8"
 servidor3.vm.network :private_network, ip: "192.168.100.4"
 servidor3.vm.network :forwarded_port, guest: 80, host: 5569
 servidor3.vm.network :forwarded_port, guest: 443, host: 5570
 servidor3.vm.hostname = "servidor3"
 end
end
```

Vsftpd.conf servidor:



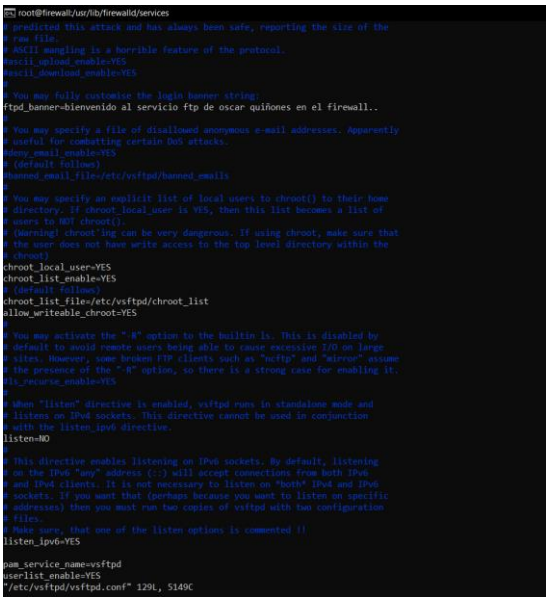
```
root@servidor:~
#
# You may fully customise the login banner string:
ftpd_banner=BIENVENIDO AL SERVICIO FTP DE OSCAR QUIÑONES.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
deny_email_enable=YES
# (default follows)
banned_email_file=/etc/vsftpd/banned_emails
#
# 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)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
#configuracion de ssl vsftpd seguro
rsa_cert_file=/etc/pki/tls/certs/ca.crt
rsa_private_key_file=/etc/pki/tls/private/ca.key
ssl_enable=YES
# 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
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES


"/etc/vsftpd/vsftpd.conf" 138L, 5299C
```

Configuración firewall lista dmz:



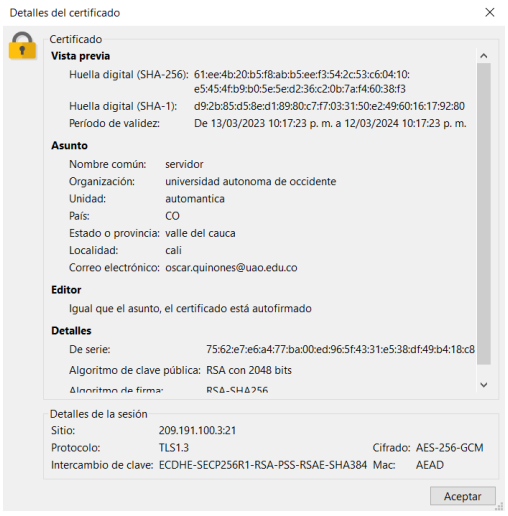
```
root@firewall:/usr/lib/firewalld/services
[root@firewall services]# firewall-cmd --zone=dmz --list-all
dmz (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1 eth2
  sources:
  services: ftp http https ssh
  ports: 21/tcp 20/tcp 1024-50000/tcp
  protocols:
  masquerade: yes
  forward-ports:
        port=21:proto=tcp:toport=21:toaddr=192.168.50.3
        port=1024-50000:proto=tcp:toport=1024-50000:toaddr=192.168.50.3
  source-ports:
  icmp-blocks: echo-request
  rich rules:
[root@firewall services]#
```

Configuración vsftpd.conf firewall:



```
root@firewall:/usr/lib/firewalld/services
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# 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=bienvenido al servicio ftp de oscar quiñones en el firewall..
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# 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)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
#
# 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
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
"/etc/vsftpd/vsftpd.conf" 129L, 5149C
```

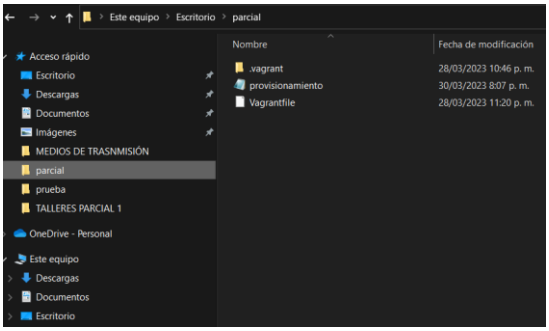
Certificado FTP seguro:



2. **DNS over TLS**

Para esta prueba se uso una maquina llamada dnstest

Configuración vagrantfile:

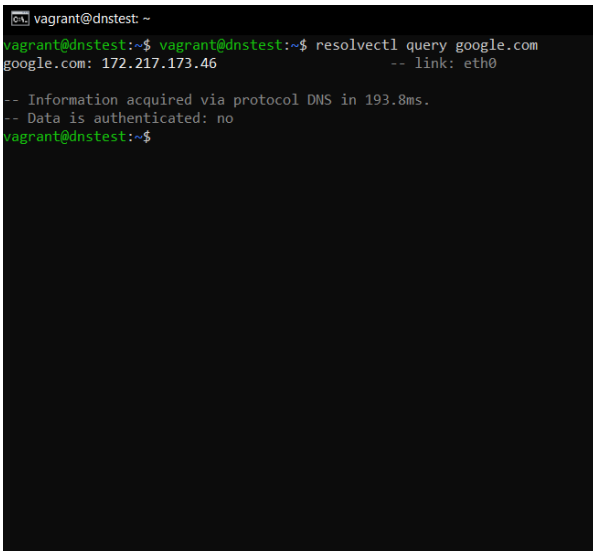



Vagrantfile: Bloc de notas

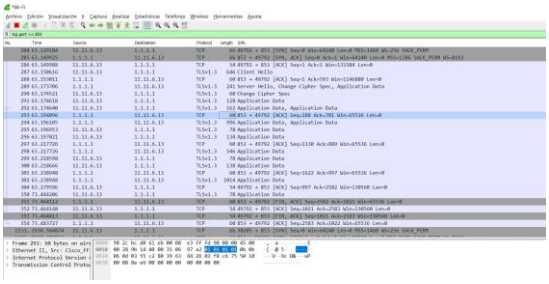
Archivo Edición Formato Ver Ayuda

```
# -*- mode: ruby -*-
# vi: set ft=ruby :
Vagrant.configure("2") do |config|
 if Vagrant.has_plugin? "vagrant-vbguest"
 config.vbguest.no_install = true
 config.vbguest.auto_update = false
 config.vbguest.no_remote = true
 end
 config.vm.define :dnstest do |dnstest|
 dnstest.vm.box = "bento/ubuntu-20.04"
 dnstest.vm.network :private_network, ip: "192.168.20.2"
 dnstest.vm.hostname = "dnstest"
 config.vm.provision :shell, path: "provisionamiento.sh", run: "always"
 end
end
```

Comando resolvf a Google.com




Trama wireshark:



Los apartados que se registran al realizar una trama por filtrado tcp.port == 853 utilizando un analizador de protocolos como Wireshark son los siguientes:

No.: Número de la trama en la secuencia de captura.

Time: Tiempo transcurrido desde el inicio de la captura hasta que se capturó esta trama.

Source: Dirección IP del origen de la trama.

Destination: Dirección IP del destino de la trama.

Protocol: Protocolo utilizado para la trama (en este caso, TCP).

Length: Longitud en bytes de la trama capturada.

Info: Información adicional sobre la trama, como el puerto de origen y destino, la secuencia y el número de reconocimiento, entre otros detalles específicos del protocolo TCP.