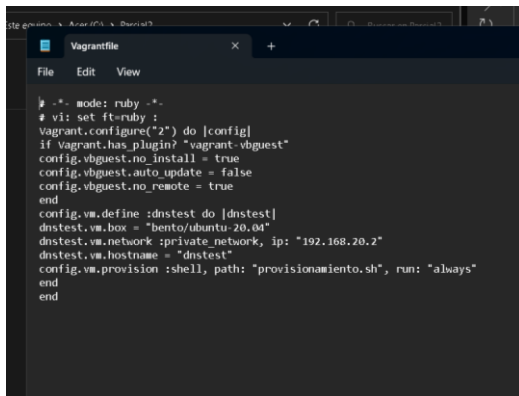
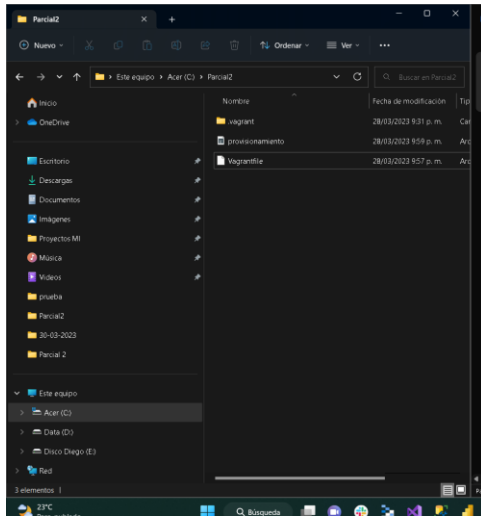


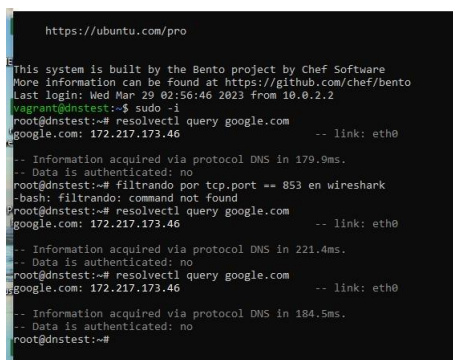
2. DNS over TLS

Para esta prueba se uso una maquina llamada dnstest

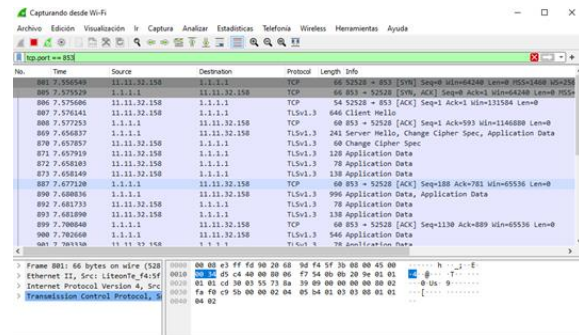
Configuración vagrantfile:



Comando resolvf a Google.com



Trama wireshark:



Los diferentes apartados que aparecen al tomar 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.

3. RichRules

Para esta práctica se usó una maquina servidor 2.

Configuración lista dmz:

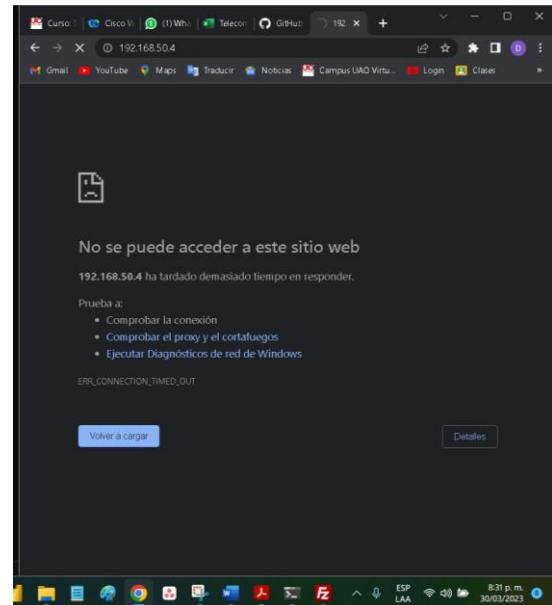
```
root@servidor2:~# firewall-cmd --zone=dmz --list-all
dmz (active)
target: default
icmp-block-inversion: no
interfaces: eth0 eth1
sources:
services: http ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
  rule family="ipv4" port port="80" protocol="tcp" drop
root@servidor2:~#
```

```
root@servidor2:~# service httpd status
Redirecting to /bin/systemctl status httpd.service
* httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2023-03-31 00:28:11 UTC; 1h 0min ago
     Docs: man:httpd.service(8)
    Main PID: 3433 (httpd)
   Status: "Total requests: 3; Idle/Busy workers 180/0; Requests/sec: 0.000821; Bytes served: 0"
    Tasks: 213 (limit: 2749)
   Memory: 21.2M
    CGroup: /system.slice/httpd.service
            └─3433 /usr/sbin/httpd -DFOREGROUND
            └─3434 /usr/sbin/httpd -DFOREGROUND
            └─3435 /usr/sbin/httpd -DFOREGROUND
            └─3436 /usr/sbin/httpd -DFOREGROUND
            └─3437 /usr/sbin/httpd -DFOREGROUND

Mar 31 00:28:11 servidor2 systemd[1]: Starting The Apache HTTP Server...
Mar 31 00:28:11 servidor2 httpd[3433]: AH00548: NameVirtualHost has no effect and will be removed in the future.
Mar 31 00:28:11 servidor2 httpd[3433]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, setting 'Servidor2'
Mar 31 00:28:11 servidor2 httpd[3433]: Server configured, listening on: port 80
root@servidor2:~# service firewall status
Redirecting to /bin/systemctl status firewall.service
* firewall.service - firewall - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewall.service; disabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-03-31 01:07:42 UTC; 21min ago
     Docs: man:firewalld(1)
    Main PID: 3732 (firewalld)
   Tasks: 2 (limit: 2749)
   Memory: 23.5M
    CGroup: /system.slice/firewalld.service
            └─3732 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Mar 31 01:07:42 servidor2 systemd[1]: Starting firewall - dynamic firewall daemon...
Mar 31 01:07:42 servidor2 systemd[1]: Started firewall - dynamic firewall daemon.
Mar 31 01:07:42 servidor2 firewalld[3732]: WARNING: AllowZoneDrifting is enabled. This is not recommended for production environments.
root@servidor2:~#
```

Evidencia



Una vez desactivado el servicio firewalld si deja acceder a la página httpd

