

Tarea 3

Nombre: Univ. Mamani Chavez Carla Vanesa	CI: 9124602 LP
Docente : Ms.c Gallardo Portanda Franz Ramiro	Fecha : 15/03/2020

1. Con los comandos nmap y nestat captura cualquier búsqueda que realices con Google donde se determinen los puertos de los servicios que se abren en la dirección remota y en la dirección de la red local.

```

C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : 
    Dirección IPv6 . . . . . : ::f064:ce7b:37bc:afed
    Dirección IPv6 temporal . . . . . : ::b14c:b3e5:facc:2c5f
    Vínculo: dirección IPv6 local. . . . . : fe80::f064:ce7b:37bc:afedz11
    Dirección IPv4. . . . . : 192.168.1.20
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de Ethernet VirtualBox Host-Only Network:

    Sufijo DNS específico para la conexión. . . : 
    Dirección IPv4 de configuración automática: 169.254.110.15
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada . . . . . : 

Adaptador de túnel isatap.{21CECB84-00D3-4803-BBD7-5B63AF2F0EA6}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : 

Adaptador de túnel isatap.{3DBFABDC-DA4B-4D36-8386-638085B4367F}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : 

C:\Windows\system32>
  
```

Figura 1.

Con el analizador de protocolos WIRESHARK se utilizó en S.O. Windows se capturo y analizo los paquetes de Facebook así mismo de la red Local.

No.	Time	Source	Destination	Protocol	Length	Info
608	13.064981	8.8.8.8	192.168.1.20	DNS	106	Standard query response 0x8086 A scontent.flpbl-2.fna.fbcdn.net A 190.129.240.84
671	13.552619	192.168.1.20	8.8.8.8	DNS	82	Standard query 0x179e A edge-chat.facebook.com
674	13.598849	8.8.8.8	192.168.1.20	DNS	122	Standard query response 0x179e A edge-chat.facebook.com CNAME star.c10r.facebook.com A 157.240.204.17
755	14.011616	192.168.1.20	8.8.8.8	DNS	78	Standard query 0x3e8f A graph.facebook.com
825	14.770464	192.168.1.20	8.8.8.8	DNS	81	Standard query 0x9204 A scontent.xx.fbcdn.net
827	14.817701	8.8.8.8	192.168.1.20	DNS	97	Standard query response 0x9204 A scontent.xx.fbcdn.net A 157.240.204.15
839	15.010945	192.168.1.20	8.8.8.8	DNS	78	Standard query 0x3e8f A graph.facebook.com
915	16.011003	192.168.1.20	8.8.8.8	DNS	78	Standard query 0x3e8f A graph.facebook.com
917	16.059970	8.8.8.8	192.168.1.20	DNS	136	Standard query response 0x3e8f A graph.facebook.com CNAME api.facebook.com CNAME star.c10r.facebook.com A 157.240.204.15
1817	20.001591	192.168.1.20	8.8.8.8	DNS	79	Standard query 0x2ec2 A clients4.google.com
1828	20.055046	8.8.8.8	192.168.1.20	DNS	199	Standard query response 0x2ec2 A clients4.google.com CNAME clients.l.google.com A 172.217.192.102 A 172.217.192.138 A 172.217.192.144 A 172.217.192.160
1837	20.071749	192.168.1.20	8.8.8.8	DNS	87	Standard query 0x3de6 A video.flpbl-2.fna.fbcdn.net
1872	20.116169	8.8.8.8	192.168.1.20	DNS	103	Standard query response 0x3de6 A video.flpbl-2.fna.fbcdn.net A 190.129.240.82
2700	20.232823	192.168.1.20	8.8.8.8	DNS	78	Standard query 0x3e8f A graph.facebook.com

Frame 401: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{F055E037-F260-4194-9CFD-0142BAEC3F80}, id 0
 Ethernet II, Src: IntelCor_c2:b5:5f (b4:b6:76:c2:b5:5f), Dst: HuaweiTe_9d:37:32 (04:02:1f:9d:37:32)
 Source: IntelCor_c2:b5:5f (b4:b6:76:c2:b5:5f)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.1.20, Dst: 8.8.8.8
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 76
 Identification: 0x3c6b (15467)
 Flags: 0x0000
 Fragment offset: 0
 Time to live: 128
 Protocol: UDP (17)
 Header checksum: 0x2c6a [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.20
 Destination: 8.8.8.8
 User Datagram Protocol, Src Port: 52130, Dst Port: 53

Figura 2

2. Mediante opciones del comando nmap, mostrar un reporte en la que viene asociada la información del fabricante del producto.

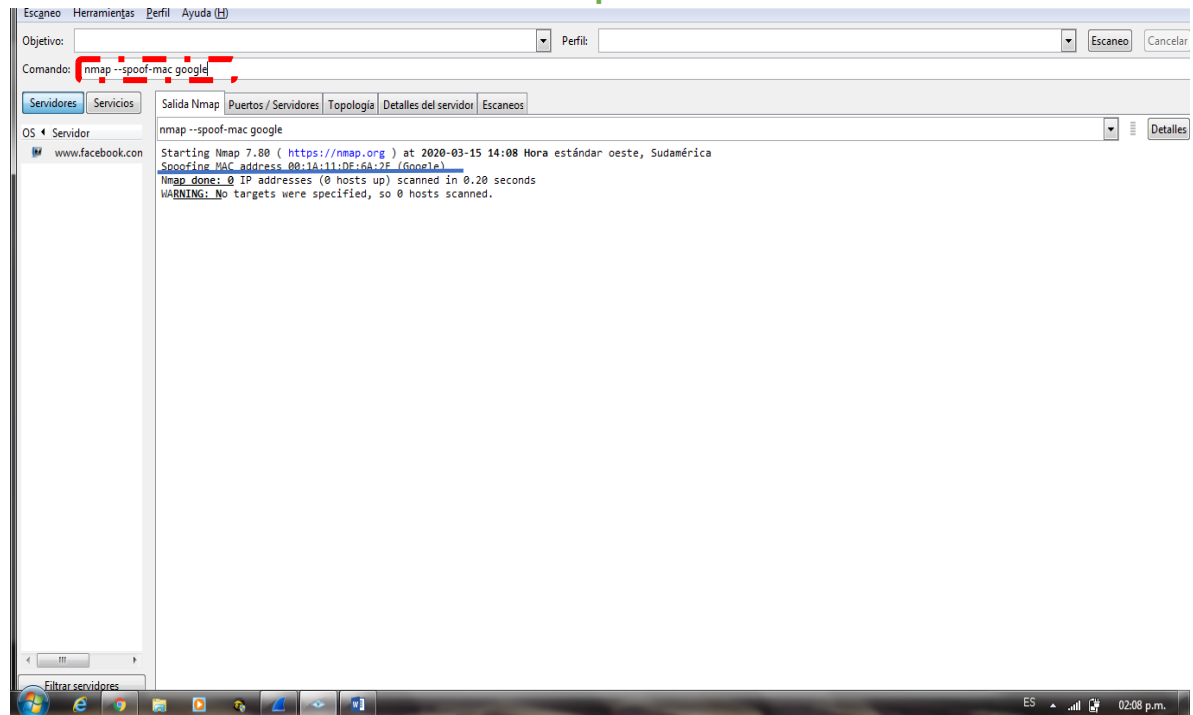


Figura 3

3. Si su host se encuentra conectado a internet, mostrar con reportes lo siguiente:

a) A través de cuál interface?

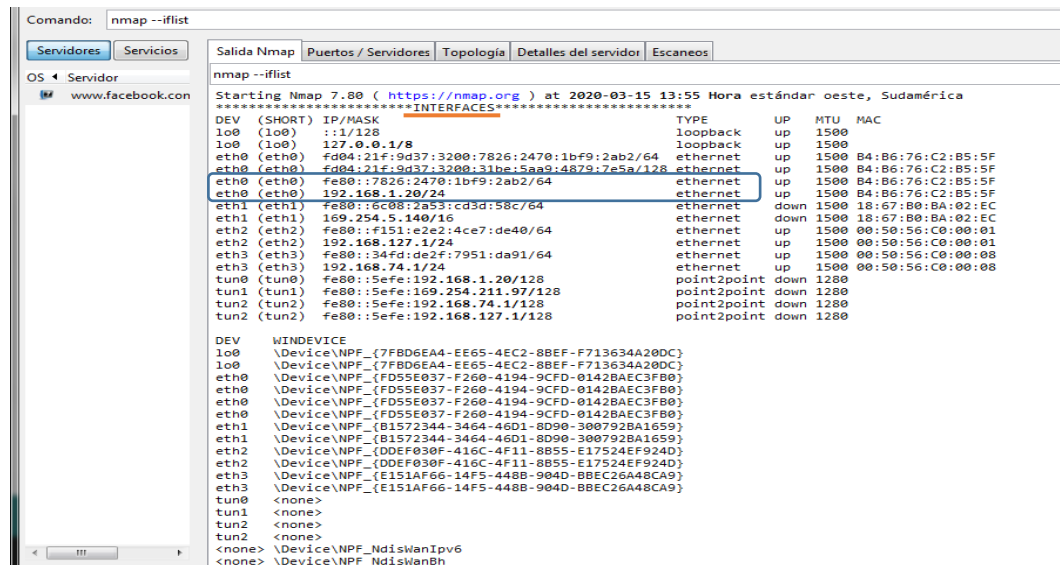


Figura 4

b)Cuál es el trayecto o ruta que recorre para llegar al servidor de Facebook.

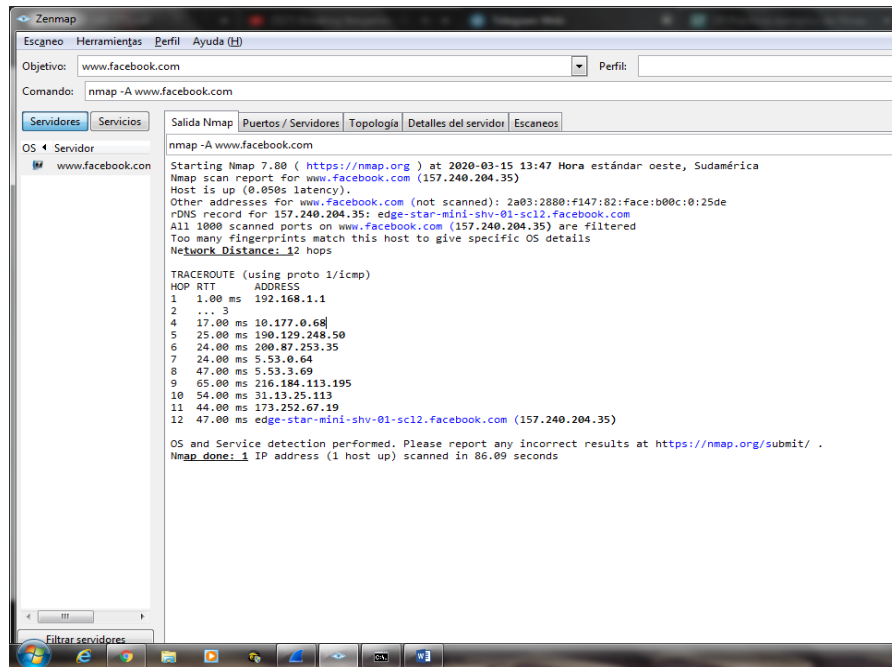


Figura 5

4. Interprete el siguiente reporte

En el reporte se analiza toda una subred, la cual puede escanearse toda una subred o rango de direcciones IP usando Nmap proporcionado con el comodín * el cual se muestra con el cuadro verde.

El resultado del reporte se puede ver que nmap escanea toda una subred y da toda la información sobre el hosts que están en la red.

En el cuadro se muestra los puertos como por ejemplo:

El puerto 80/ tcp en estado abierto y del tipo servicio http, el cual pertenece a la capa de aplicación del servicio web.



Figura 6

5. Para cada uno de los incisos las expresiones que deberían utilizarse para capturar:

a) Tráfico que tenga como origen y/o destino la red 192.168.80.0/24

Se utilizó el filtro → **(IP.ADDR == 192.168.80.0)**

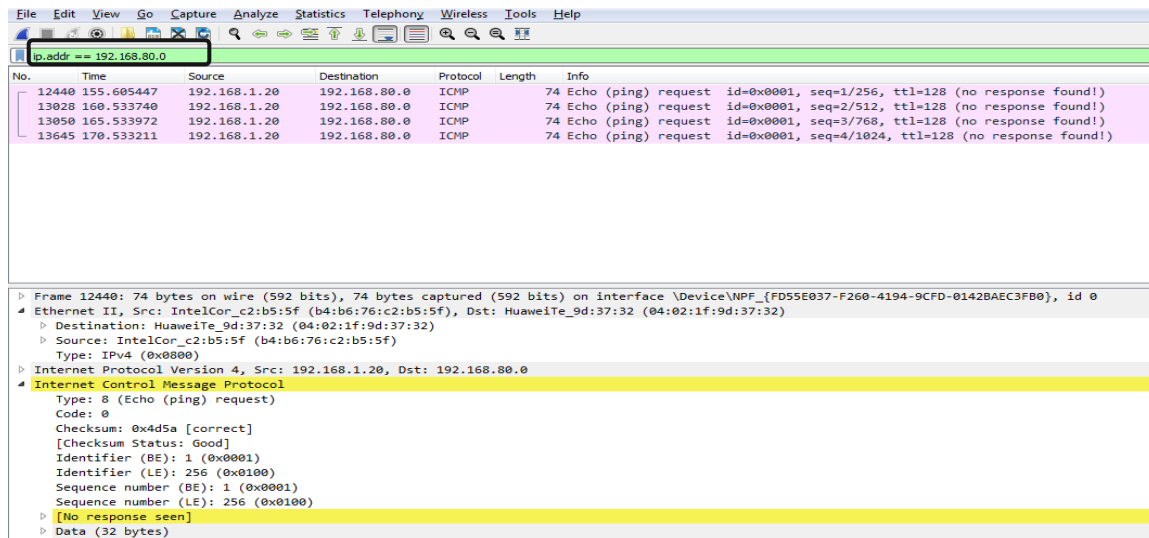


Figura 7

b) Que no sea ni HTTP ni DNS

Se utilizó el filtro → **(NOT DNS AND NOT HTTP)**

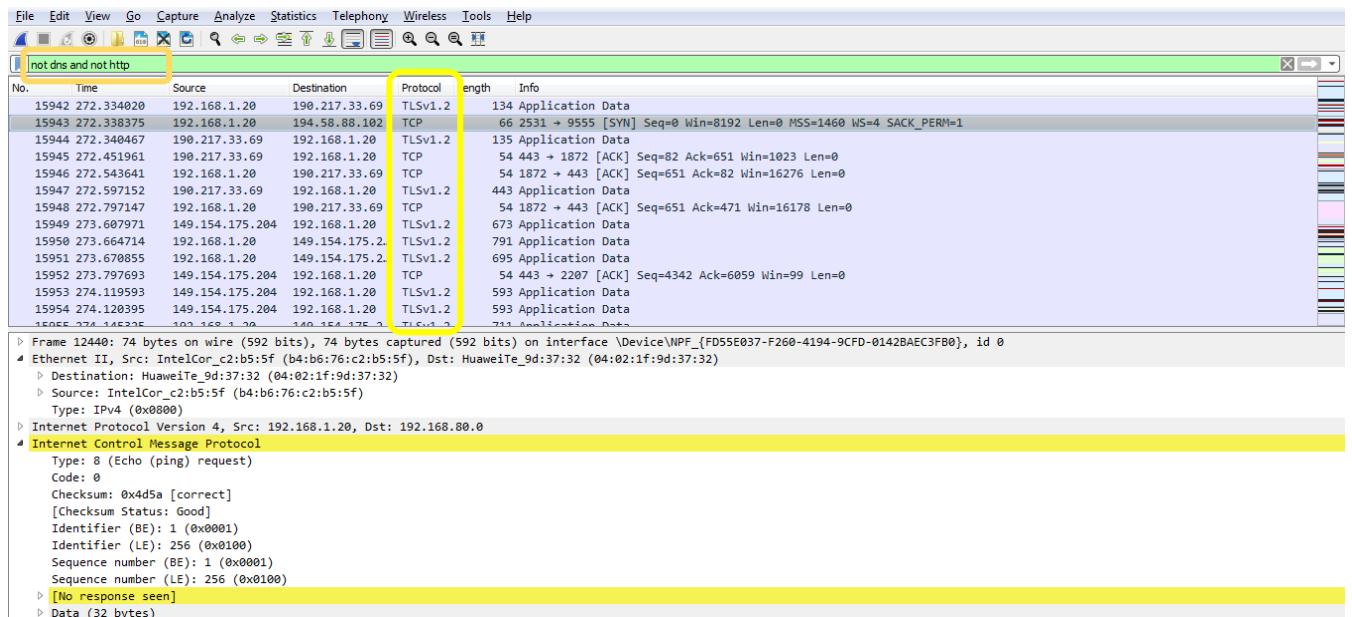


Figura 8

c) Que involucre a un rango de puertos como ser: 1000 a 1150

Se utilizó el filtro → **(NOT DNS AND NOT HTTP)**

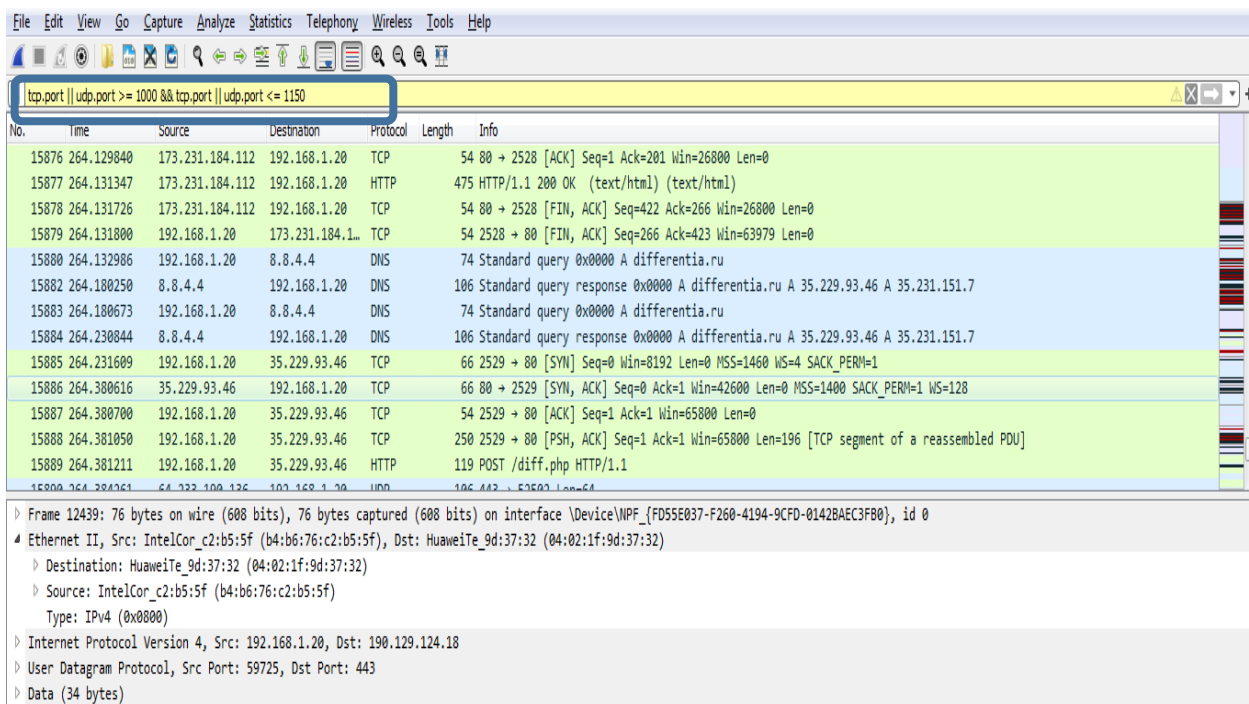


Figura 9

d) Solo tráfico únicas

Se utilizó el filtro → **(GNUTELLA OR BITTORRENT OR EDONKEY)**

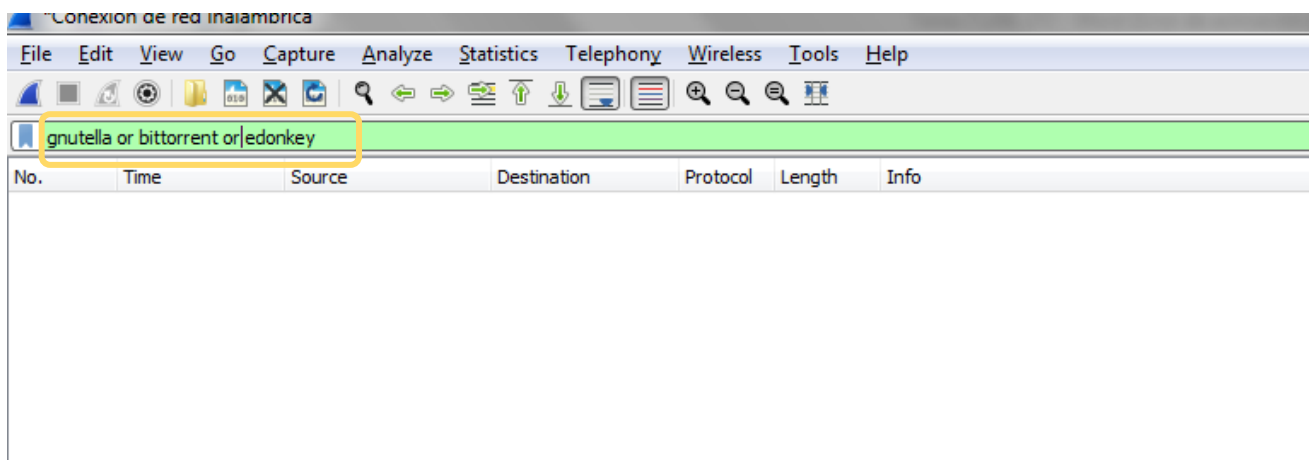


Figura 10