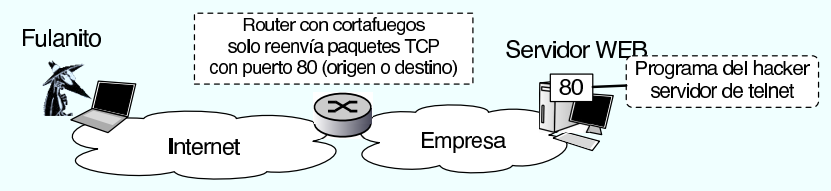
Problemas de Redes de Computadores.
Ingeniería Técnica en Informática de Gestión
Conjunto de problemas 2



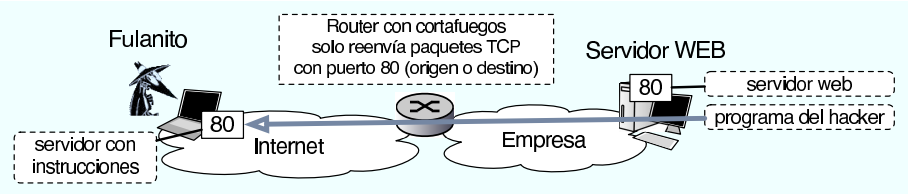
Pregunta 2.1: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un servidor de telnet que escucha en el puerto 80 de ese ordenador. Pero cuando intenta conectarse a su servidor de telnet no le funciona... ¿Por qué no funciona?

a) Porque telnet sólo puede funcionar en el puerto 23 como manda el RFC-854

b) Porque los usuarios remotos no sabrán que el servidor está en el puerto 80

c) Porque no se puede tener dos aplicaciones TCP escuchando en el puerto 80

d) Porque telnet usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP



Pregunta 2.2: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un programa que cada cierto tiempo establece una conexión con el puerto 80 de un servidor externo controlado por él y se descarga instrucciones por HTTP ¿Qué problema tiene esto?

a) Que HTTP no puede funcionar en el puerto 80 porque el puerto está reservado para la web

b) No tiene ningún problema y debería funcionar

c) Que no se puede tener una conexión TCP al puerto 80 y a la vez escuchar conexiones en el puerto 80

d) Que HTTP usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP

Problema 2.3: El host H1 se encuentra en una red en la que se filtran los paquetes que entran y sólo se permiten paquetes de conexiónes Web. El propietario de H1 quiere utilizar un programa peer-to-peer que utiliza normalmente el puerto TCP 6881 (aunque puede configurarse otro) pero no le funciona porque se eliminan los paquetes al no ser de conexiones web. ¿Cómo puede lograr que funcione el programa a pesar del filtro? ¿Puede conseguirlo si en H1 tiene activado el servidor Web? ¿Cómo cambia esto si el programa peer-to-peer utiliza UDP?

Problema 2.4: En una universidad el servidor oficial de correo se encuentra en el servidor S1. El administrador de la red de la universidad intenta evitar que se utilicen otros servidores de correo distintos de S1 en su red. Para ello, dado que el router de salida R1 tiene funcionalidades de firewall y permite aplicar reglas sobre los paquetes, añade una regla: R1 no reenviará paquetes TCP al exterior si tienen el puerto destino 25, salvo si su dirección IP origen es S1. ¿Evitará esto el uso de otros servidores?. Si un usuario del departamento B coloca un servidor de SMTP en un H3. Puede utilizarlo para enviar correo fuera sin usar el servidor S1? ¿Puede usarlo para recibir correo sin usar el servidor S1? Razone las respuestas. ¿Puede un usuario de la red B consultar su cuenta de correo de un servidor externo?¿Por que?

Problema 2.5: ¿Cuáles de estas funciones provoca el envío de algún paquete a la red?

```
socket()   connect()   recvfrom()   sendto()   bind()   listen()   accept()
```

Problema 2.6: ¿Como se detecta desde un programa que los datos entregados a un socket TCP pueden haber sufrido errores y no ser correctos?

Problema 2.7: El siguiente paquete capturado en la universidad es un paquete UDP

```
0x0000:  4500 003c 4f9a 0000 4011 0000 82ce a9b1  E..<O...@.......
0x0010:  82ce a66e c5c7 0035 0028 55f6 14f1 0100  ...n...5.(U.....
0x0020:  0001 0000 0000 0000 0377 7777 0667 6f6f  .........www.goo
0x0030:  676c 6503 636f 6d00 0001 0001            gle.com.....
```

¿A qué protocolo de nivel de aplicación pertenece? ¿Es una pregunta o una respuesta?

Problema 2.8: El siguiente paquete capturado en la universidad es un paquete UDP

```
0x0000:  4500 0138 0000 4000 3f11 e4f8 82ce a66e  E..8..@.?......n
0x0010:  82ce a9b1 0035 c5c7 0124 7ce0 14f1 8180  .....5...$|.....
0x0020:  0001 0007 0004 0004 0377 7777 0667 6f6f  .........www.goo
0x0030:  676c 6503 636f 6d00 0001 0001 c00c 0005  gle.com.........
0x0040:  0001 0003 5b28 0008 0377 7777 016c c010  ....[(...www.l..
0x0050:  c02c 0001 0001 0000 0110 0004 d155 e563  .,...........U.c
0x0060:  c02c 0001 0001 0000 0110 0004 d155 e567  .,...........U.g
0x0070:  c02c 0001 0001 0000 0110 0004 d155 e568  .,...........U.h
0x0080:  c02c 0001 0001 0000 0110 0004 d155 e569  .,...........U.i
0x0090:  c02c 0001 0001 0000 0110 0004 d155 e56a  .,...........U.j
0x00a0:  c02c 0001 0001 0000 0110 0004 d155 e593  .,...........U..
0x00b0:  c010 0002 0001 0000 a53d 0006 036e 7334  .........=...ns4
0x00c0:  c010 c010 0002 0001 0000 a53d 0006 036e  ...........=...n
0x00d0:  7331 c010 c010 0002 0001 0000 a53d 0006  s1...........=..
0x00e0:  036e 7332 c010 c010 0002 0001 0000 a53d  .ns2...........=
0x00f0:  0006 036e 7333 c010 c0b2 0001 0001 0000  ...ns3..........
0x0100:  ad7b 0004 d8ef 200a c0c4 0001 0001 0000  .{..............
0x0110:  ad7b 0004 d8ef 220a c0d6 0001 0001 0000  .{...."........
0x0120:  ad7b 0004 d8ef 240a c0a0 0001 0001 0000  .{....$.........
0x0130:  ad7b 0004 d8ef 260a                      .{....&.
```

¿A qué protocolo de nivel de aplicación pertenece? ¿Es una pregunta o una respuesta?

Problema 2.9: El siguiente paquete capturado en la universidad es un paquete TCP

```
0x0000:  4500 003c 0000 4000 3e06 ed8b 82ce 9fe2
0x0010:  82ce a9b1 024b ec0c d673 c9f2 b025 1c8a
0x0020:  a012 16a0 26c7 0000 0204 05b4 0402 080a
0x0030:  94c5 2654 40b6 6421 0103 0300
```

Indique cuales de los siguientes son correctos

a) Es un paquete de cliente a servidor

b) Es un paquete de servidor a cliente

c) El paquete transporta datos de aplicacion

d) Es un paquete de datos

e) Es un paquete de ACK

f) Es un paquete de establecimiento de conexión

e) Es un paquete de cierre de conexion

¿Cual debería ser el valor del campo ACK del paquete que confirme la recepción de este paquete mostrado?

Problema 2.10: Los siguientes paquetes pertenecen a una misma conexión TCP

```
0x0000:  4510 0045 115d 4000 4006 0000 82ce a9b1  E..E.]@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d997 5692 4a8f  .....:.n.,..V.J.
0x0020:  8018 ffff 4f6b 0000 0101 080a 40b6 8a50  ....Ok......@..P
0x0030:  d025 e50f 5553 4552 206d 696b 656c 2e69  .%..USER.mikel.i
0x0040:  7a61 6c0d 0a                             zal..
```

```
0x0000:  4500 0034 af72 4000 3e06 3e1e 82ce 9fe5  E..4.r@.>.>.....
0x0010:  82ce a9b1 006e ec3a 5692 4a8f a62c d9a8  .....n.:V.J..,..
0x0020:  8010 05a8 83b0 0000 0101 080a d025 f564  ............%.d
0x0030:  40b6 8a50                                @..P
```

```
0x0000:  4500 004c af74 4000 3e06 3e04 82ce 9fe5  E..L.t@.>.>.....
0x0010:  82ce a9b1 006e ec3a 5692 4a8f a62c d9a8  .....n.:V.J..,..
0x0020:  8018 05a8 808d 0000 0101 080a d025 f564  ............%.d
0x0030:  40b6 8a50 2b4f 4b20 5061 7373 776f 7264  @..P+OK.Password
0x0040:  2072 6571 7569 7265 642e 0d0a            .required...
```

```
0x0000:  4510 0034 5136 4000 4006 0000 82ce a9b1  E..4Q6@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d9a8 5692 4aa7  .....:.n.,..V.J.
0x0020:  8010 ffff 4f5a 0000 0101 080a 40b6 8a50  ....OZ......@..P
0x0030:  d025 f564                                .%.d
```

```
0x0000:  4510 0045 9a0d 4000 4006 0000 82ce a9b1  E..E..@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d9a8 5692 4aa7  .....:.n.,..V.J.
0x0020:  8018 ffff 4f6b 0000 0101 080a 40b6 8ab6  ....Ok......@...
0x0030:  d025 f564 5041 5353 2061 7361 6265 7263  .%.dPASS.asaberc
0x0040:  7561 6c0d 0a                             ual..
```

Indique cuales transportan datos y cuales son simplemente ACKs.

¿Cual es el siguiente numero de secuencia y ACK que esperaría encontrar en el siguiente paquete de servidor a cliente?

Identifique los datos del protocolo de nivel de aplicación del tercer paquete.

Problema 2.11: La siguiente traza ha sido capturada en la red de la universidad

```
 1 0.963491 IP 130.206.168.45.60905 > 193.252.23.108.110: S 2357731200:2357731200(0) win 65535
 2 0.964072 IP 193.252.23.108.110 > 130.206.168.45.60905: S 1061601894:1061601894(0) ack 2357731201 win 5792
 3 0.964129 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061601895 win 65535
 4 1.111168 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601895:1061601927(32) ack 2357731201 win 5792
 5 1.111753 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731201:2357731218(17) ack 1061601927 win 65535
 6 1.112349 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731218 win 5792
 7 1.200422 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601927:1061601956(29) ack 2357731218 win 5792
 8 1.200834 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731218:2357731232(14) ack 1061601956 win 65535
 9 1.201287 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731232 win 5792
10 1.711614 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601956:1061601991(35) ack 2357731232 win 5792
11 1.712040 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731232:2357731238(6) ack 1061601991 win 65535
12 1.712630 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731238 win 5792
13 1.861177 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601991:1061602000(9) ack 2357731238 win 5792
14 1.861596 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731238:2357731244(6) ack 1061602000 win 65535
15 1.862059 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731244 win 5792
16 2.064350 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061602000:1061602005(5) ack 2357731244 win 5792
17 2.065276 IP 130.206.168.45.60905 > 193.252.23.108.110: F 2357731244:2357731244(0) ack 1061602005 win 65535
18 2.065890 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731245 win 5792
19 2.065894 IP 193.252.23.108.110 > 130.206.168.45.60905: F 1061602005:1061602005(0) ack 2357731245 win 5792
20 2.065957 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061602006 win 65535
```

a) Indique a qué aplicación pertenece y qué acción del usuario ha causado esos paquetes

b) Indique cual es el cliente y cual el servidor en esta acción (con sus direcciones IP)

c) Haga una tabla para el cliente y otra para el servidor, indicando en qué estado de conexión estaba TCP al principio y en que estado ha quedado después de enviar o recibir cada paquete mostrado.