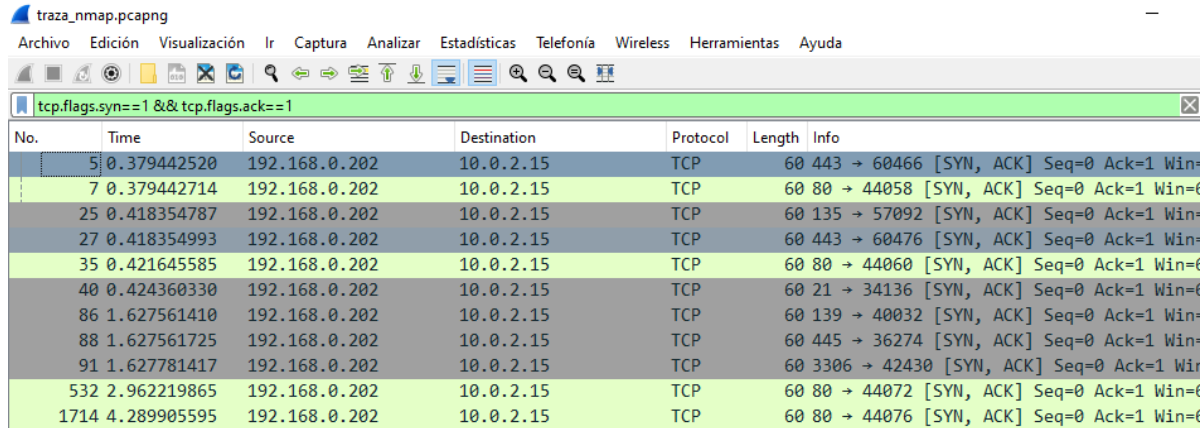


INSTRUCCIONES TURNO 1: COPIA LAS PREGUNTAS EN UN DOCUMENTO Y RESPONDE EN COLOR AZUL. UNA VEZ TERMINADO, SUBE TU DOCUMENTO AL AULA VIRTUAL EN PDF con el nombre NOMBREAPELLIDO_1.pdf 14/12/2022 NOMBRE:

1-La traza llamada “traza_nmap”, es la que encontramos cuando lanzamos un nmap a una IP. Investígala y:

1. Enumera qué puertos hay abiertos.(1 punto)

80,443,135,139,3306



No.	Time	Source	Destination	Protocol	Length	Info
5	0.379442520	192.168.0.202	10.0.2.15	TCP	60	443 → 60466 [SYN, ACK] Seq=0 Ack=1 Win=0
7	0.379442714	192.168.0.202	10.0.2.15	TCP	60	80 → 44058 [SYN, ACK] Seq=0 Ack=1 Win=0
25	0.418354787	192.168.0.202	10.0.2.15	TCP	60	135 → 57092 [SYN, ACK] Seq=0 Ack=1 Win=0
27	0.418354993	192.168.0.202	10.0.2.15	TCP	60	443 → 60476 [SYN, ACK] Seq=0 Ack=1 Win=0
35	0.421645585	192.168.0.202	10.0.2.15	TCP	60	80 → 44060 [SYN, ACK] Seq=0 Ack=1 Win=0
40	0.424360330	192.168.0.202	10.0.2.15	TCP	60	21 → 34136 [SYN, ACK] Seq=0 Ack=1 Win=0
86	1.627561410	192.168.0.202	10.0.2.15	TCP	60	139 → 40032 [SYN, ACK] Seq=0 Ack=1 Win=0
88	1.627561725	192.168.0.202	10.0.2.15	TCP	60	445 → 36274 [SYN, ACK] Seq=0 Ack=1 Win=0
91	1.627781417	192.168.0.202	10.0.2.15	TCP	60	3306 → 42430 [SYN, ACK] Seq=0 Ack=1 Win=0
532	2.962219865	192.168.0.202	10.0.2.15	TCP	60	80 → 44072 [SYN, ACK] Seq=0 Ack=1 Win=0
1714	4.289905595	192.168.0.202	10.0.2.15	TCP	60	80 → 44076 [SYN, ACK] Seq=0 Ack=1 Win=0

2. Nombra al menos tres servicios que sepas que usan esos puertos (en formato protocolo: puerto) (1 punto)

http:80

https:443

MySQL:3306

ftp:21

3. Indica al menos 2 de las aplicaciones (nombre y versión, p.ej: Apach 3.2) que nmap detecta. (1 punto)

Apache 2.4.46

traza_nmap.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
4447	11.499263373	10.0.2.15	192.168.0.202	HTTP	72	GET / HTTP/1.0
4510	11.515552297	192.168.0.202	10.0.2.15	HTTP	419	HTTP/1.1 302 Found (text/html)
4677	16.507504840	192.168.0.202	10.0.2.15	HTTP	544	HTTP/1.1 400 Bad Request (text/html)
4681	16.507667717	10.0.2.15	192.168.0.202	HTTP	72	GET / HTTP/1.0
4684	16.508538731	192.168.0.202	10.0.2.15	HTTP	567	HTTP/1.1 503 Service Unavailable (text/)
4737	17.610899611	10.0.2.15	192.168.0.202	HTTP	72	GET / HTTP/1.0
4738	17.610947440	10.0.2.15	192.168.0.202	HTTP	234	GET /nmaplowercheck1669635121 HTTP/1.1
4739	17.610977264	10.0.2.15	192.168.0.202	HTTP	229	GET /nmaplowercheck1669635121 HTTP/1.1
4740	17.611011656	10.0.2.15	192.168.0.202	HTTP	676	POST /sdk HTTP/1.1
4747	17.611213579	10.0.2.15	192.168.0.202	HTTP	72	GET / HTTP/1.0
4748	17.611256364	10.0.2.15	192.168.0.202	HTTP	671	POST /sdk HTTP/1.1
4757	17.613468829	192.168.0.202	10.0.2.15	HTTP	567	HTTP/1.1 503 Service Unavailable (text/)
4760	17.613469060	192.168.0.202	10.0.2.15	HTTP	567	HTTP/1.1 503 Service Unavailable (text/)

<

> Frame 4510: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface enp0s3, id 0000 08 00 27 3

> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_38:1f:cd (08:00:27:38:1f:cd) 0010 01 95 11 6

> Internet Protocol Version 4, Src: 192.168.0.202, Dst: 10.0.2.15 0020 02 0f 00 5

> Transmission Control Protocol, Src Port: 80, Dst Port: 44086, Seq: 1, Ack: 19, Len: 365 0030 ff ff 6e e

> Hypertext Transfer Protocol 0040 30 32 20 4

> HTTP/1.1 302 Found\r\n 0050 4d 6f 6e 2

Date: Mon, 28 Nov 2022 11:31:55 GMT\r\n 0060 20 31 31 3

Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3\r\n 0070 65 72 76 e

X-Powered-By: PHP/8.0.3\r\n 0080 34 2e 34 3

Location: http://dashboard/\r\n 0090 6e 53 53 4

> Content-Length: 115\r\n 00a0 38 2e 30 2

Connection: close\r\n 00b0 2d 42 79 3

Content-Type: text/html; charset=UTF-8\r\n 00c0 4c 6f 63 6

\r\n 00d0 7f 7f 6d f

Filezilla 0.9.41

traza_nmap.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length	Info
2904	5.495923291	192.168.0.202	10.0.2.15	FTP	202	Response: 220-FileZilla Server version 0.9.41 be

2-¿Qué contiene la “traza_servidor_web”? Responde a las preguntas:

1. ¿Qué navegador inicia la conexión? (1 punto)

La IP de origen es 192.168.0.202

traza_servidor_web.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.1	255.255.255.255	UDP	398	45748 → 29810 Len=356
2	-3597.806468...	192.168.0.147	185.125.190.57	NTP	90	NTP Version 4, client
3	-3597.772598...	185.125.190.57	192.168.0.147	NTP	90	NTP Version 4, server
4	3.511186574	192.168.0.202	192.168.0.147	TCP	66	54193 → 80 [SYN] Seq=0 Win=64240 Len=0
5	3.511222333	192.168.0.147	192.168.0.202	TCP	66	80 → 54193 [SYN, ACK] Seq=0 Ack=1 Win=6
6	3.511186767	192.168.0.202	192.168.0.147	TCP	66	54194 → 80 [SYN] Seq=0 Win=64240 Len=0
7	3.511249683	192.168.0.147	192.168.0.202	TCP	66	80 → 54194 [SYN, ACK] Seq=0 Ack=1 Win=6
8	3.511683394	192.168.0.202	192.168.0.147	TCP	60	54193 → 80 [ACK] Seq=1 Ack=1 Win=131328
9	3.512011071	192.168.0.202	192.168.0.147	TCP	60	54194 → 80 [ACK] Seq=1 Ack=1 Win=131328
10	3.517169636	192.168.0.202	192.168.0.147	HTTP	508	GET / HTTP/1.1
11	3.517214450	192.168.0.147	192.168.0.202	TCP	54	80 → 54193 [ACK] Seq=1 Ack=455 Win=6412

Busco el GET que hace el cliente en el protocolo http, pues en ese GET el cliente “se presenta”:

traza_servidor_web.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
10	3.517169636	192.168.0.202	192.168.0.147	HTTP	508	GET / HTTP/1.1
12	3.517549246	192.168.0.147	192.168.0.202	HTTP	709	HTTP/1.1 200 OK (text/html)
18	15.040295671	192.168.0.202	192.168.0.147	HTTP	681	POST /login.php HTTP/1.1 (application/...
20	15.040674677	192.168.0.147	192.168.0.202	HTTP	788	HTTP/1.1 405 Not Allowed (text/html)

<

> Frame 10: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface enp0s3, id 0
 > Ethernet II, Src: EIZO_32:c6:fb (00:90:93:32:c6:fb), Dst: PcsCompu_05:56:44 (08:00:27:05:56:44)
 > Internet Protocol Version 4, Src: 192.168.0.202, Dst: 192.168.0.147
 > Transmission Control Protocol, Src Port: 54193, Dst Port: 80, Seq: 1, Ack: 1, Len: 454
 > Hypertext Transfer Protocol
 > GET / HTTP/1.1\r\n
 Host: 192.168.0.147\r\n
 Connection: keep-alive\r\n
 Cache-Control: max-age=0\r\n
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Sa
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: es-ES,es;q=0.9\r\n
 \r\n

NOTA: Si el pantallazo muestra el User-Agent, lo pondré bien aunque pongais Mozilla, Chrome....

2. ¿Qué servidor responde?(1 punto)

Esto lo veré en la respuesta del servidor:

nginx 1.18.0

traza_servidor_web.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
10	3.517169636	192.168.0.202	192.168.0.147	HTTP	508	GET / HTTP/1.1
12	3.517549246	192.168.0.147	192.168.0.202	HTTP	709	HTTP/1.1 200 OK (text/html)
18	15.040295671	192.168.0.202	192.168.0.147	HTTP	681	POST /login.php HTTP/1.1 (application/x-www
20	15.040674677	192.168.0.147	192.168.0.202	HTTP	788	HTTP/1.1 405 Not Allowed (text/html)

<

> Frame 12: 709 bytes on wire (5672 bits), 709 bytes captured (5672 bits) on interface enp0s3, id 0
 > Ethernet II, Src: PcsCompu_05:56:44 (08:00:27:05:56:44), Dst: EIZO_32:c6:fb (00:90:93:32:c6:fb)
 > Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.202
 > Transmission Control Protocol, Src Port: 80, Dst Port: 54193, Seq: 1, Ack: 455, Len: 655
 > Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n
 Server: nginx/1.18.0 (Ubuntu)\r\n
 Date: Wed, 30 Nov 2022 10:18:30 GMT\r\n
 Content-Type: text/html\r\n
 Last-Modified: Wed, 30 Nov 2022 10:13:51 GMT\r\n
 Transfer-Encoding: chunked\r\n
 Connection: keep-alive\r\n
 ETag: W/"63872cdf-28c"\r\n
 Content-Encoding: gzip\r\n
 \r\n
 [HTTP response 1/2]
 [Time since request: 0.000379610 seconds]
 [Request in frame: 10]
 [Next request in frame: 18]
 [Next response in frame: 20]

3. ¿Puedes ver el nombre de alguna de las páginas que ve el cliente? (1 punto)
 Parece que ve login.php, porque le hace POST y no devuelve ningún “No encontrado”.

traza_servidor_web.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
10	3.517169636	192.168.0.202	192.168.0.147	HTTP	508	GET / HTTP/1.1
12	3.517549246	192.168.0.147	192.168.0.202	HTTP	709	HTTP/1.1 200 OK (text/html)
18	15.040295671	192.168.0.202	192.168.0.147	HTTP	681	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
20	15.040674677	192.168.0.147	192.168.0.202	HTTP	788	HTTP/1.1 405 Not Allowed (text/html)

4. ¿Qué puerto usa el cliente para ver las páginas? (1 punto)
 El cliente ve las páginas por el 54193

traza_servidor_web.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
10	3.517169636	192.168.0.202	192.168.0.147	HTTP	508	GET / HTTP/1.1
12	3.517549246	192.168.0.147	192.168.0.202	HTTP	709	HTTP/1.1 200 OK (text/html)
18	15.040295671	192.168.0.202	192.168.0.147	HTTP	681	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
20	15.040674677	192.168.0.147	192.168.0.202	HTTP	788	HTTP/1.1 405 Not Allowed (text/html)

<

> Frame 12: 709 bytes on wire (5672 bits), 709 bytes captured (5672 bits) on interface enp0s3, id 0

> Ethernet II, Src: PcsCompu_05:56:44 (08:00:27:05:56:44), Dst: EIZ0_32:c6:fb (00:90:93:32:c6:fb)

> Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.202

> Transmission Control Protocol, Src Port: 80, Dst Port: 54193, Seq: 1, Ack: 455, Len: 655

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Server: nginx/1.18.0 (Ubuntu)\r\n

Date: Wed, 30 Nov 2022 10:18:30 GMT\r\n

Content-Type: text/html\r\n

Last-Modified: Wed, 30 Nov 2022 10:13:51 GMT\r\n

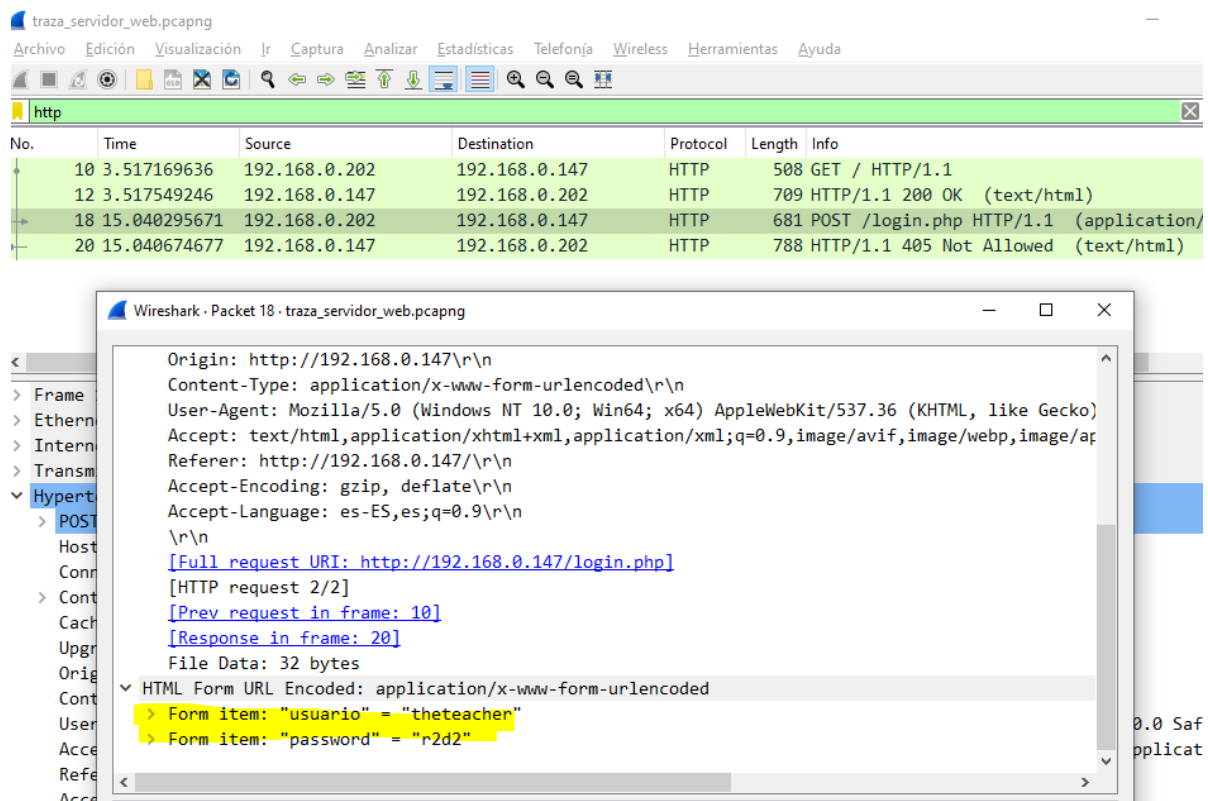
Transfer-Encoding: chunked\r\n

Connection: keep-alive\r\n

ETag: W/"63872cdf-28c"\r\n

Content-Encoding: gzip\r\n

5. ¿Se transmite algún dato privado en la conexión?. (1 punto)
 Cuando el cliente envía los datos por POST, como es protocolo plano, se ve:



En los dos ejercicios, a la respuesta debe acompañarse el pantallazo con el que se ha descubierto; si no están, no se dará por válida la respuesta.

3-Responde a las preguntas:

- 1-¿En qué cabecera/-s existe el TTL?, ¿cuántos bits ocupa? (0.5 puntos) IP, 8bits
- 2-¿En qué cabecera/-s aparece el puerto destino?, ¿cuántos bits ocupa?, ¿qué campo tiene antes? (0.5 puntos) TCPy UDP, 16 bits, El anterior es el puerto origen
- 3-Nombra los últimos 6 flags de TCP (0.5 puntos) URG, ACK, PSH, RST, SYN, FIN
- 4- Nombra dos campos de cabecera que existan en TCP y no en UDP. (0.5 puntos) Sequence number, Ack number, sindow size, los flags...