

Universidade do Minho

LICENCIATURA EM CIÊNCIAS DA COMPUTAÇÃO SISTEMAS DE COMUNICAÇÕES E REDES

Ensaio Escrito Aplicações e Camada de Transporte

Grupo 28

Davide Santos (A102938) Edgar Araújo (A102946)

Pedro Augusto Camargo (A102504)

Novembro 2023

Contents

1	Nív	el aplicacional	2
	1.1	Identifique o endereço IP da estação que formulou a query DNS e o tipo de query realizada	2
	1.2	Localize a trama com a resposta à query DNS formulada. Identifique nesta trama o endereço IP do servidor web. Identifique também o servidor de nomes que forneceu a resposta, através do seu IP e nome	2
	1.3	Aplique o filtro aos protocolos http://tcp. Identifique os endereços IP do cliente e do servidor HTTP	2
	1.4	Identifique os segmentos TCP correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP. Qual o o tamanho máximo de segmento (MSS) que o servidor aceita receber?	2
	1.5	Identifique a resposta HTTP do servidor respeitante ao primeiro pedido GET efetuado pelo cliente. Quantos bytes de dados aplicacionais contém essa resposta HTTP?	3
	1.6	A resposta HTTP identificada na alínea anterior foi transmitida em quantos segmentos TCP? Apresente também uma estimativa teórica para essa quantidade	3
	1.7	A partir da informação contida nos cabeçalhos dos protocolos IP e TCP, determine o número de bytes de dados enviados no primeiro e no último segmento TCP respeitantes à resposta HTTP.	3
	1.8	Observe a informação apresentada no campo host do cabeçalho do pedido HTTP e diga qual o seu interesse?	3
	1.9	Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.	3
	1.10	Aceda a https://www.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark. Porque razão o tráfego HTTP não é identificado como tal no Wireshark? Apesar disso, pode detetar-se qual o protocolo aplicacional. Como	
	1.11	é que o Wireshark sabe que se trata duma ligação http-over-tls?	3
		a frequência das conexões estabelecidas entre o cliente e o servidor, vii) os dados da aplicação trocados entre o servidor e o cliente	4

1 Nível aplicacional

1.1 Identifique o endereço IP da estação que formulou a query DNS e o tipo de query realizada.

14 10.033359221	172.26.57.176	193.137.16.65	DNS	78 Standard query 0x7b03 A www.scom.uminho.pt
15 10.033386202	172.26.57.176	193.137.16.65	DNS	78 Standard query 0xda1c AAAA www.scom.uminho.pt
16 10.057275198	193.137.16.65	172.26.57.176	DNS	94 Standard query response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17 10.057275910	193.137.16.65	172.26.57.176	DNS	106 Standard query response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18 10.058089977	172.26.57.176	193.137.9.174	TCP	74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19 10.060328175	193.137.9.174	172.26.57.176	TCP	78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM

O endereço IP da estação que formulou a query DNS: 172.26.57.176 (O meu computador) Foram enviadas 2 querys dns, uma do tipo A (endereço IPv4) e outra do tipo AAAA (endereço IPv6)

1.2 Localize a trama com a resposta à query DNS formulada. Identifique nesta trama o endereço IP do servidor web. Identifique também o servidor de nomes que forneceu a resposta, através do seu IP e nome

14 10.033359221 172.26.57.176	193.137.16.65 DN	78 Standard query	0x7b03 A www.scom.uminho.pt
15 10.033386202 172.26.57.176	193.137.16.65 DN		v 0xda1c AAAA www.scom.uminho.pt
16 10.057275198 193.137.16.65	172.26.57.176 DN		response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17 10.057275910 193.137.16.65	172.26.57.176 DN	106 Standard query	response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18 10.058089977 172.26.57.176	193.137.9.174 TC	74 38734 → 80 [SY	N] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19 10.060328175 193.137.9.174	172.26.57.176 TC	78 80 → 38734 [SY	N, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM

O endereço IP do servidor web que respondeu a query DNS: 193.137.16.65 De forma a identificar o servidor de nomes que forneceu a resposta, poderia ter sido usado o utilitario nslookup, como tambem o servico WEB https://whatismyipaddress.com/ip/<ip>, para o ip anterior:



Obtemos que o servidor DNS que forneceu a resposta, tem por hostname: dns3.uminho.pt

- 1.3 Aplique o filtro aos protocolos http // tcp. Identifique os endereços IP do cliente e do servidor HTTP
 - Temos o endereco IP do cliente, vindo do HTTP GET Request: 172.26.57.176
 - Que tem como destino o IP do servidor: 193.137.9.174
- 1.4 Identifique os segmentos TCP correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP. Qual o o tamanho máximo de segmento (MSS) que o servidor aceita receber?

Tal como mostra a imagem, os pacotes 18 e 19 correspondem aos pactoes SYN do cliente e SYN-ACK do servidor, respetivamente. Logo ambos tem oportunidade nestes pacotes de solicitar um MSS, que no caso do servidor é de 1250 bytes.

21 10.060450003	172.26.57.176	193.137.9.174	HTTP	439 GET / HTTP/1.1
22 10.120634426	193.137.9.174	172.26.57.176	TCP	2542 80 → 38734 [ACK] Seq=1 Ack=374 Win=65162 Len=2476 TSval=381818 TSecr=1449595498 [TCF
23 10.120710338	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=374 Ack=2477 Win=63360 Len=0 TSval=1449595558 TSecr=381818
24 10.124781915	193.137.9.174	172.26.57.176	TCP	3780 80 → 38734 [ACK] Seq=2477 Ack=374 Win=65162 Len=3714 TSval=381818 TSecr=1449595558 [
25 10.124795390	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=374 Ack=6191 Win=62336 Len=0 TSval=1449595562 TSecr=381818

L 18 10.058089977	1/2.26.5/.1/6	193.137.9.174	TCP	74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=1449595496 TSecr=0 WS=128
19 10.060328175	193.137.9.174	172.26.57.176	TCP	78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
20 10.060351849	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595498 TSecr=0
21 10.060450003	172.26.57.176	193.137.9.174	HTTP	439 GET / HTTP/1.1

1.5 Identifique a resposta HTTP do servidor respeitante ao primeiro pedido GET efetuado pelo cliente. Quantos bytes de dados aplicacionais contém essa resposta HTTP?

A resposta HTTP do servidor é do tipo 200 OK, e contem 43275 bytes de dados aplicacionais, tal como indica o campo Content-Length.

1.6 A resposta HTTP identificada na alínea anterior foi transmitida em quantos segmentos TCP? Apresente também uma estimativa teórica para essa quantidade.

A resposta HTTP foi transmitida em 9 segmentos. A estimativa teórica para essa quantidade é de 43566/1460 = 29.8, ou seja, 30 segmentos.

1.7 A partir da informação contida nos cabeçalhos dos protocolos IP e TCP, determine o número de bytes de dados enviados no primeiro e no último segmento TCP respeitantes à resposta HTTP.

No primeiro segmento TCP, o número de bytes de dados enviados é de 2476 bytes. No último segmento TCP, o número de bytes de dados enviados é de 236 bytes.

1.8 Observe a informação apresentada no campo host do cabeçalho do pedido HTTP e diga qual o seu interesse?

O campo host do cabeçalho do pedido HTTP indica o nome colocado no url do browser, que serve para identificar o website que se pretende aceder, em caso de um servidor conter vários websites diferentes.

1.9 Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.

O servidor HTTP está a funcionar em modo de conexão persistente, pois nenhum dos segmentos TCP tem a flag FIN ativa, entre GET Requests.

1.10 Aceda a https://www.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark. Porque razão o tráfego HTTP não é identificado como tal no Wireshark? Apesar disso, pode detetar-se qual o protocolo aplicacional. Como é que o Wireshark sabe que se trata duma ligação http-over-tls?

A razao pela qual o trafego HTTP nao é identificado como tal no Wireshark, é porque o trafego HTTP está a ser feito sobre o protocolo TLS, que é um protocolo de segurança que encripta o trafego HTTP, de forma a que este não seja visivel a terceiros. O Wireshark sabe que se trata de uma ligação http-over-tls, porque o protocolo TLS é identificado no campo Protocol do pacote.

```
Hypertext Transfer Protocol
HTTP/1.1 200 0K\r\n
Date: Mon, 27 Nov 2023 14:28:47 GMT\r\n
Server: Microsoft-IIS/6.0\r\n
X-Powered-By: ASP.NET.SessionId=lyliggbyroknzkbyhzz4c2til; path=/\r\n
Set-Cookie: ASP.NET.SessionId=lyliggbyroknzkbyhzz4c2til; path=/\r\n
Cache-Control: private\r\n
Content-Type: text/html; charset=iso-8859-15\r\n
Content-Length: 43275\r\n
\r\n
**Transmission Control Protocol, Src Port: 80, Dst P
**Internet Frotocot Version 4, Src. 133:137:317, D
**Transmission Control Protocol, Src Port: 80, Dst P
**Internet Frotocot Version 4, Src. 133:137:317, D
**Transmission Control Protocol, Src Port: 80, Dst P
**Internet Frotocot Version 4, Src. 133:137:317, D
**Transmission Control Protocol, Src Port: 80, Dst P
**Internet Frotocot Version 4, Src. 133:137:317, D
**Internet Frotocot Version 4, Src. 133:137, D
**Internet Frotocot Version 4, Src.
```

- 1.11 Diga, justificando, quais dos seguintes elementos uma comunicação HTTPS permite manter ocultos dum atacante: i) o endereço IP do cliente, ii) o endereço IP do servidor web, iii) o nome do servidor web, iv) o tamanho da mensagem trocada entre o cliente o servidor, v) a identificação da página acedida no servidor web, vi) a frequência das conexões estabelecidas entre o cliente e o servidor, vii) os dados da aplicação trocados entre o servidor e o cliente
 - i) O endereço IP do cliente não é oculto, pois é necessário para que o servidor saiba para onde enviar a resposta.
 - ii) O endereço IP do servidor web não é oculto, pois é necessário para que o cliente saiba para onde enviar o pedido.
 - iii) O nome do servidor web não é oculto, pois é necessário para que o servidor saiba para que website enviar o pedido.
 - iv) O tamanho da mensagem trocada entre o cliente e o servidor não é oculto, pois é necessário para que o cliente saiba se recebeu a mensagem completa.
 - v) A identificação da página acedida no servidor web não é oculto. O caminho do URL é
 parte da solicitação HTTP e, embora a comunicação seja criptografada, a estrutura básica
 da solicitação permanece visível.
 - vi) A frequência das conexões estabelecidas entre o cliente e o servidor não é oculto, pois é necessário para que o servidor saiba se o cliente está a tentar fazer um ataque de negação de serviço.
 - vii) Os dados da aplicação trocados entre o servidor e o cliente SÃO ocultos, isso garante que o conteúdo da mensagem, incluindo informações sensíveis, não seja visível para um atacante que possa interceptar a comunicação.

```
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NO)
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (2476 bytes)
[Reassembled PDU in frame: 38]
TCP segment data (2476 bytes)
```

(a) Primeiro Segmento

[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation
[Timestamps]
[SEQ/ACK analysis]
TCP payload (236 bytes)
TCP segment data (236 bytes)

(b) Último Segmento

Figure 1: 2 Figures side by side

```
TCP payload (368 bytes)

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: 193.137.9.174\r\n

User-Agent: Mozilla/5.0 (X11; Linux

Accept: text/html,application/xhtml-
Accept-Language: en-US.en:g=0.5\r\n
```