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)

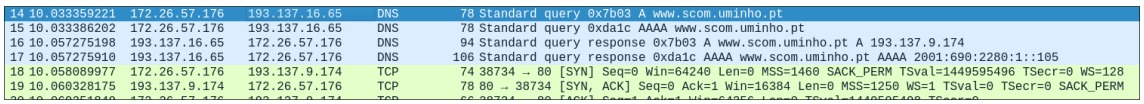
Pedro Augusto Camargo (A102504)

Novembro 2023

Contents

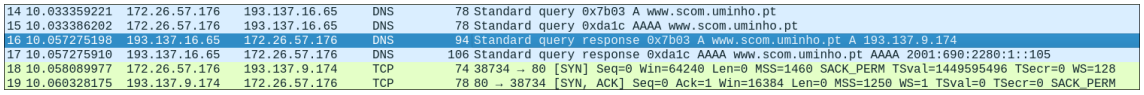
1 Nível aplicacional

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



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



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:

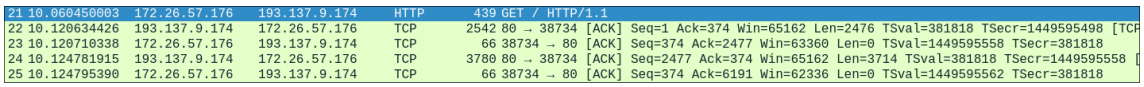
Obtemos que o servidor DNS que forneceu a resposta, tem por hostname: dns3.uminho.pt

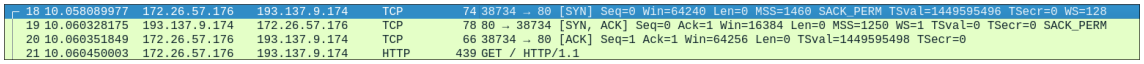
1.3 Aplique o filtro aos protocolos http // tcp. Identifique os endereços IP do cliente e do servidor HTTP

- 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.





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?

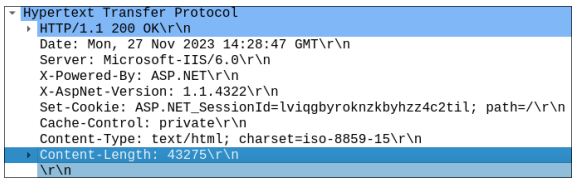
O campo host do cabeçalho do pedido HTTP indica o nome colocado no url do browser, que serve para identificar o website que se pretende aceder, em caso de um servidor conter vários websites diferentes.

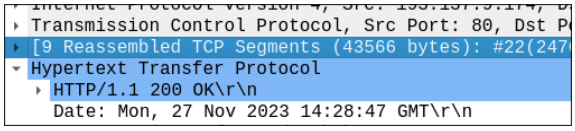
1.9 Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.

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?

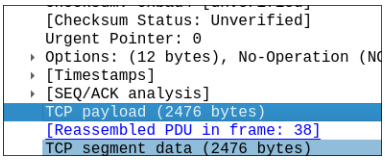
A razao pela qual o trafego HTTP nao é identificado como tal no Wireshark, é porque o trafego HTTP está a ser feito sobre o protocolo TLS, que é um protocolo de segurança que encripta o trafego HTTP, de forma a que este não seja visivel a terceiros. O Wireshark sabe que se trata de uma ligação http-over-tls,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



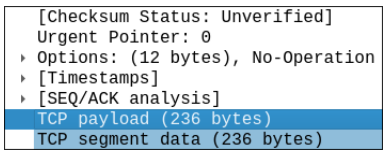


1.11 Diga, justificando, quais dos seguintes elementos uma comunicação HTTPS permite manter ocultos dum atacante: i) o endereço IP do cliente, ii) o endereço IP do servidor web, iii) o nome do servidor web, iv) o tamanho da mensagem trocada entre o cliente o servidor, v) a identificação da página acedida 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.



(a) Primeiro Segmento



(b) Último Segmento

Figure 1: 2 Figures side by side