Exercício Avaliativo Wireshark

1)Escreva quantos pacotes foram capturados ao todo pelo wireshark.

Foram capturados 75207 pacotes

2) Filtre os pacotes UDP que contenham as seguintes palavras: youtube yahoo unipac

Qual o protocolo da camada de aplicação desses pacotes?

Não foi encontrado nenhum pacote UDP para youtube

Não foi encontrado nenhum pacote UDP para google

Protocolo DNS para yahoo

3) Filtre os pacotes TCP que contenham as mesmas palavras acima: youtube yahoo unipac

Qual o protocolo da camada de aplicação desses pacotes? Os protocolos são diferentes para cada uma dessas pesquisas? Se sim, por que você acha que isso ocorreu?

YouTube apareceu o TLSV1.3

Google apareceu o TCP, TLSV1.3, TLSV1.2

Yahoo apareceu TCP, TLSV.3, TLSV1.1, TLSV1.2

O motivo principal para leitor de paginas,um para leitor de arquivos.

4) Com relação ao protocolo DNS, você consegue tirar alguma conclusão de como é feito o seu tráfego na rede?

Basicamente, o meu tráfego na rede é feito 99% por domínios DNS, ou seja, o mesmo busca, consulta o servidor DNS, e em seguida ele irá recebera resposta com o endereço IP, que irá se repetir para cada site por exemplo que eu vou querer acessar.

5) Filtre todos os pacotes que não são TCP e responda, quantos pacotes foram apresentados?

70980 pacotes não são TCP

6) Filtre os pacotes que não são UDP e que contenham a palavra youtube. Responda, quantos pacotes foram apresentados?

1 pacote foi apresentado

7) Observe os IPs que foram apresentados na busca da questão 6, insira alguns desses IPs no navegador e responda: Esses IPs levam até o site do youtube.com? Se não, para onde eles levam?

O IP me levou para o site do google, não diretamente para o youtube.

8) Faça um filtro para mostrar todos os pacotes UDP que usem a porta 47199, no mesmo filtro devem ser mostrados os pacotes TCP que usam a porta 43206. Escreva o filtro:

udp.port==47199 || tcp.port==43206

9) Faça um filtro que mostre todos os pacotes cuja porta UDP do transmissor seja 53 ou a porta tcp de destino seja 43206, porém, só devem ser mostrados os pacotes cujo IP da fonte seja 172.217.30.99. Escreva o filtro:

ip.src==172.217.30.99 && (udp.srcport==53 || tcp.dstport==43206)

10)) **Filtre todos os pacotes que contenham um arquivo jpg, quantos pacotes foram mostrados? Escreva o filtro:**

frame contains “jpg”.

2 pacotes foram encontrados.

11**) Faça um filtro para mostrar se houve algum pacote com problema na transmissão TCP quando o destino do pacote foi a sua máquina. Escreva o filtro e responda quantos pacotes foram apresentados?**

tcp.analysis.retransmission. Foram perdidos 33 pacotes

12) Qual filtro você deve utilizar para mostrar os pacotes que não puderam ser encontrados? (Page not found)

http.responde.code == 404.