Universidade do Minho
Licenciatura em Ciências da Computação
Sistemas de Comunicações e Redes

TP3: Aplicações e Camada de Transporte (2 aulas)

1. Objetivo

Este trabalho tem como objetivo a familiarização com protocolos e ferramentas do nível aplicacional, e análise dos protocolos de transporte em uso. Para tal, deve usar a sua **máquina nativa** (preferencialmente com o sistema operativo Linux), e não a máquina virtual.

2. Nível aplicacional

Ligue-se à rede Eduroam e proceda da seguinte forma. Ative um browser na sua máquina e certifique-se que não tem outras instâncias *web* ativas. Ative o Wireshark, certificando-se que está em modo privilegiado (*root*), e proceda à captura de tráfego na interface de rede *wi-fi* em uso. Aceda à página ***http://www.sas.uminho.pt*** e espere que o conteúdo seja carregado. Pare a captura no Wireshark e grave-a para eventual uso posterior. Para localizar mais facilmente o tráfego correspondente ao acesso *web* realizado, comece por filtrar pelo protocolo *dns*. Para tal, introduza *dns* na caixa do *display filter* e aplique o filtro. (Também pode usar "Edit > Find Packet..." (ou CTRL+F) para encontrar os pacotes contendo *strings* relativas ao nome do servidor). Localize a resolução do nome do servidor *www.sas.uminho.pt*.

1. Identifique o endereço IP da estação que formulou a *query* DNS e o tipo de *query* realizada. (Nota: Caso não consiga encontrar a referida *query*, limpe a cache DNS da sua máquina, executando num terminal do Ubuntu: *sudo systemd-resolve --flush-caches*; ou *sudo /etc/init.d/dns-clean restart*. No Windows deve executar o comando: *ipconfig /flushdns*).

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 (sugestão: consulte o *Additional Records*).

HTTP e TCP

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

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?

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

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

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.

8. Observe a informação apresentada no campo *host* do cabeçalho do pedido HTTP e diga qual o seu interesse? Experimente aceder à mesma página *web* através de *http://endereço_IP*, em que *endereço_IP* é o respeitante a *www.sas.uminho.pt* (identificado na alínea 2). Justifique o comportamento observado.

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.

10. Aplique o filtro apenas ao protocolo *http*. O *hard refresh* permite limpar a cache do browser para uma determinada página, forçando o browser a carregar a última versão da página existente no servidor. Normalmente o *hard refresh* duma página faz-se com CTRL+F5 ou SHIFT+*page reload* (caso não funcione, procure na Internet a forma de fazer *hard refresh* no seu *browser*). Coloque o Wireshark a capturar tráfego e faça *hard refresh* da página indicada anteriormente. Depois volte a aceder à mesma página mas sem fazer *hard refresh*. Pare a captura de tráfego. Identifique a principal diferença observada no tráfego HTTP entre carregar a referida página com e sem *hard refresh*. Qual a principal vantagem e desvantagem inerente ao *hard refresh*?

HTTPS

11. Aceda a *https://elearning.uminho.pt*, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark.
    a. De que forma o seu *browser* assinala que o utilizador está perante, ou não, uma ligação HTTP ao servidor segura? Apresente uma captura de écran com essa indicação.
    b. 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*?

12. 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.

3. Consultas ao serviço de resolução de nomes DNS

A maioria dos sistemas operativos (Windows, Linux, etc) inclui um cliente DNS genérico designado por *nslookup*. No entanto este cliente tem vindo a ser preterido a favor de outros como o *dig* e o *host*. O package *dnsutils* inclui todos. Se no Linux não conseguir usar nenhum deles tente reinstalar o *package* com o comando: *sudo apt-get install dnsutils.*

A base de dados dum servidor DNS é constituida por registos de diversos tipos, como por exemplo: *A, AAAA, NS, SOA, MX, PTR*. Usando o *nslookup* ou o *dig* e com base nos seus manuais (*man nslookup* ou *man dig*) procure responder às seguintes questões, devendo incluir os resultados que sustentam as suas respostas:

1. Se estiver a usar o Linux, observe o conteúdo do ficheiro */etc/resolv.conf.* Se estiver a usar o Windows, abra uma janela de comandos e execute *nslookup*. Indique qual o servidor de nomes que a sua máquina está a usar?

2. Usando o registo do tipo *A*, identifique os endereços IPv4 dos servidores *www.sas.uminho.pt*, *marco.uminho.pt* e *www.google.com*? Usando o registo *AAAA*, identifique o endereço IPv6 do servidor *www.fccn.pt*.

3. Experimente fazer uma *query* aos registos *PTR* para os nomes 240.9.136.193.in-addr.arpa. e 7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa. Comente os resultados face aos obtidos na alínea anterior.

4. Usando os registo *NS*, identifique os servidores de nomes definidos para os domínios: "uminho.com.", "sas.uminho.pt.", "pt." e "." (*root*). *i*) Perante a informação obtida, diga, justificando, se os servidores de nomes de diferentes domínios podem coexistir numa mesma máquina física. *ii*) Encontra domínios geridos por servidores de nomes localizados em redes IP distintas? Se sim, apresente esses domínios e diga qual a vantagem resultante desse procedimento?

5. Usando o registo *SOA*, identifique o servidor DNS primário definido para os domínios "uminho.pt.", "pt." e "." ? Em que difere o servidor primário de um servidor secundário e qual o significado dos parâmetros temporais associados ao servidor primário?

6. Usando o registo *MX*, diga qual(quais) o(s) servidor(s) de email do domínio *edu.ulisboa.pt* ? A que sistema são entregues preferencialmente as mensagens dirigidas a *geral@edu.ulisboa.pt*?

7. Usando o registo *CNAME*, diga qual(quais) o(s) *aliases* do nome *www.ebay.com*? O que é que isso significa?

8. Qual a diferença entre uma resposta adjetivada como *non-authoritative answer* ("não-autoritativa") e uma resposta "autoritativa" para uma determinada *query*?

4. Uso da camada de transporte por parte das aplicações

Verifique se na sua máquina de trabalho tem disponíveis as seguintes aplicações ou ferramentas: clientes *ftp*, *ssh*, *traceroute* (*tracert* em Windows), *ping* e *telnet*, senão instale. Corra novamente o Wireshark. Capturando o tráfego nos momentos que considere adequados, observe atentamente como as várias aplicações utilizam o serviço de transporte, quando é efetuado:

a. Acesso via *browser* a *http://www.sas.uminho.pt*
b. Acesso via *browser* a *https://elearning.uminho.pt*
c. Acesso em *ftp* para *ftp.di.uminho.pt* (login: *anonymous*)
d. *ping cisco.di.uminho.pt*
e. Acesso *ssh* para *marco.uminho.pt*
f. *nslookup www.fccn.pt*
g. traceroute router-di.uminho.pt
h. telnet freechess.org

1. Preencha a seguinte tabela com base nos resultados que obteve:

Comando/aplicação	Canal seguro?	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)
browser http://			
browser https://			
ftp			
ping			
ssh			
nslookup / dig			
traceroute			
telnet			

Inclua todos os extratos dos *outputs* que lhe permitem chegar às conclusões acima.

2. Comente as principais diferenças entre os protocolos TCP e UDP. Relacione-as com as experiências realizadas onde observou os campos dos cabeçalhos respetivos e o *overhead* protocolar. Em particular, identifique os campos do TCP responsáveis pelo controlo de fluxo, ordenação e fiabilidade do protocolo.

Relatório do trabalho

O relatório final deste trabalho deve incluir apenas:
- título e identificação do grupo;
- uma secção "Questões e Respostas" relativas ao enunciado acima (formato: transcrição da questão, resposta, ...);
- uma secção de "Conclusões" que autoavalie (de forma completa) os resultados da aprendizagem decorrentes das várias vertentes estudadas no trabalho.

O relatório deve seguir preferencialmente o formato LNCS (Springer, existem *templates* .tex e .docx) e ser submetido obrigatoriamente na plataforma de ensino com o nome SCR-TP3-Gxx.pdf (por exemplo, SCR-TP3-G11.pdf para o grupo G11) até final do dia previsto para a conclusão do trabalho.