Folha de exercícios nº 3

Análise do protocolo HTTP na pilha TCP/IP
Utilização da ferramenta Wireshark

Introdução

Nesta observação necessitará da ferramenta wireshark (que pode obter em http://www.wireshark.org/). Esta ferramenta permite capturar tráfego observado numa interface de rede do seu computador. Com a ferramenta, poderá capturar o tráfego trocado numa transação HTTP GET/Response entre o browser e um servidor web, de modo a poder analisar todo o fluxo de objetos transferidos entre o browser e o servidor. A captura exigirá que a ferramenta esteja a ser usada no seu computador e sistema operativo, com privilégios adequados ("root", ou "Administrador"), para que a captura possa ser possível.

Na captura pode selecionar os protocolos que se pretendem observar, podendo assim observar e analisar tráfego de diversos protocolos. Para uma utilização completa ou mais avançada da ferramenta poderá consultar a informação disponível, que inclui as várias opções de configuração da ferramenta para os diferentes protocolos, diferentes configurações de filtros para análise específica de certos padrões de tráfego, bem como possibilidade de relacionar o tráfego com uma visão integrada do encapsulamento da pilha TCP/IP (desde o nível aplicação até ao nível *data-link*). Uma das possibilidades de uso da ferramenta é capturar amostras de tráfego observado, sendo estas amostras guardados em ficheiros (que contêm os pacotes capturados). Estes ficheiros podem depois ser carregados para análises posteriores.

A ferramenta disponibiliza várias ajudas, e existe muita informação, acessível na internet sobre uso da ferramenta. Para o efeito pode procurar, por exemplo, em:

http://www.wireshark.org/
http://www.wireshark.org/faq.html
Páginas de manual (opção HELP na ferramenta)
http://wiki.wireshark.org/SampleCaptures

Utilização na aula

Para os objectivos da aula, serão disponibilizados dois ficheiros com amostras de capturas previamente efectuadas, nomeadamente:
• ex3-1.pcap
• ex3-3.pcap

Deverá obter estes ficheiros, disponibilizados como material da aula.
A captura **ex3-1.pcap** vai ser usada para as **questões 1 e 2**.
A captura **ex3-3.pcap** será usada para a **questão 3**.

Após o carregamento dos ficheiros deverá conseguir identificar, na análise do tráfego observado, os diferentes protocolos suportados na rede.

Questão 1.

Nesta questão vamos focar a análise nos protocolos HTTP, TCP, IP e ARP.
Para o efeito, é importante saber o papel desses protocolos na pilha TCP/IP, bem como o nível na pilha em que cada um dos protocolos opera.

Depois das observações iniciais do tráfego capturado em **ex3-1.pcap**, tente interpretar o tráfego, respondendo às seguintes questões:

1. Identifique como o tráfego HTTP é encapsulado em mensagens TCP, envolvendo os portos do cliente e do servidor (web).
2. Verifique que as mensagens TCP resultantes do tráfego HTTP estão encapsuladas em pacotes IP, com endereços origem e destino associados aos computadores em causa (cliente, onde executa o browser) e servidor web.
3. Tente identificar numa mensagem HTTP o cabeçalho do pedido e o cabeçalho de uma resposta.
4. Tente identificar numa mensagem TCP os campos do cabeçalho TCP. Tente encontrar por exemplo, os campos onde estão os portos origem e destino, os números de sequência e os demais campos do cabeçalho.
5. Tente identificar tráfego TCP associado à abertura e ao fecho de conexões TCP.
6. Tente identificar num pacote IP os campos do cabeçalho IP. Tente encontrar, por exemplo, o endereço do emissor e do receptor, o TTL ou outros campos do cabeçalho IP.
7. Identifique a existência de ARP *queries* e respostas. Verifique que os pacotes ARP estão encapsulados em *frames* Ethernet. Verifique que é mesmo possível saber qual os endereços MAC origem e destino ao nível das frames ethernet que transportam os pacotes IP.
8. Tente identificar nos pacotes ARP identificados, quem é que está a fazer o pedido ARP ? Em que consiste esse pedido ? Quem respondeu ? O que respondeu ?
9. Tente identificar queries de DNS. Consegue identificar que o protocolo DNS (query/reponse) está suportado em UDP ? Que endereços IP (máquinas) e portos estão envolvidos nas quesries e respostas DNS ?
10. Verifique qual o computador (endereço) que está a fazer a interrogação, que pergunta está a ser feita ? Qual o servidor DNS que está a ser usado ? Que resposta foi dada ? Analise o formato das mensagens DNS nas interrogações e respostas.
11. Concentre-se agora na análise de segmentos TCP. Em todo o tráfego observado na captura, quantos pacotes dizem respeito à abertura e fecho de conexões TCP ? Consegue identificar o protocolo *handshake* associado ao estabelecimento de uma conexão TCP ?
12. Consegue verificar o tamanho da janela proposto pelo cliente e servidor na abertura de conexões TCP ? Verifique o estado das flags do header do segmento TCP na abertura e aceitação de conexões. Quais os hosts que estão envolvidos na abertura e estabelecimento da conexão ? Consegue identificar qual o propósito do estabelecimento da conexão (pelos portos que questão envolvidos ?)
13. Tente verificar em detalhe o processamento dos números de sequencia em todos os segmentos da abertura de conexão TCP ? Lembra-se do que estudou

na teoria sobre como evoluem esses números de sequencia ? O que observa está de acordo com a sua expectativa ?

14. Verifique complementarmente os parâmetros MSS bem como os valores das janelas nos segmentos TCP. Tente identificar a variação da dimensão da janela numa conexão TCP. Aumenta ? Diminui ? O que quer isso dizer ?
15. Verifique os pacotes trocados no fecho da conexão TCP.
16. Quantos pacotes dizem respeito a transações HTTP ? Tente identificar o número de pedidos HTTP e respostas HTTP, e tente compreender o fluxo de um pedido HTTP e da consequente resposta HTTP.
17. Verifique que no pedido, o URL inicialmente pedido pelo cliente é corrigido pelo servidor. Qual o verdadeiro URL mostrado pelo browser? O que terá acontecido ?
18. O Browser está a usar HTTP 1.0 ou 1.1 ? E o servidor ?
19. Qual é o endereço IP do computador cliente e o do servidor ?
20. Qual a dimensão em bytes do primeiro objecto retornado e em que formato está representado esse objecto ?
21. É possível saber pela informação do cabeçalho HTTP quando foi esse objecto modificado pela última vez no servidor ?

Questão 2.

Far-se-á agora a observação de uma sequencia completa de pedidos HTTP a partir de um pedido inicial.

1. Observe que os números de sequência aparecem ao longo dos pedidos (aparentemente) de acordo com saltos (incrementos com diferentes valores). Porquê ? Qual a lógica desse sequenciamento dos segmentos TCP que transportam as mensagens HTTP ?
2. Na sequência de pedidos o cliente obteve alguma resposta HTTP com erro ? Tente identificar esse erro e perceber o que terá acontecido.
3. Quantos objectos foi o Browser buscar e a que endereços IP quando fez o pedido?
4. Quantas transacções HTTP GET/Reply foram realizada? Identifique quantas e transacções e quantas foram feitas sobre servidores distintos.
5. O Browser foi buscar os objectos em paralelo ou em sequência? Porquê ? Faz sentido face ao que sabe da teoria do protocolo HTTP ?

Questão 3.

Observação de um pedido HTTP com resposta condicional
(Conditional GET/Reponse)

Com base na captura **ex3-3.pcap**, que deverá ser observada como estando na base de uma operação de RELOAD (ou *refresh*), por parte do browser do mesmo pedido da página associada à captura **ex4-1.pcap**, responda às seguintes questões:

1. Observe que diferenças nota no pedido da página (após RELOAD), comparativamente à captura observada anteriormente. Explique porque é que neste caso é diferente.
2. O browser continuou a abrir uma conexão com o servidor. Isto faz sentido,

uma vez que o browser já tinha antes na sua cache os conteúdos que recebeu na captura anterior? Porquê? Verifique em que moldes o pedido é feito neste contexto ?

3. Após RELOAD da página, o browser mostrou garantidamente a última versão da página, mesmo que não a tenha transferido ? Porquê ?
4. Obtenha uma visão global do fluxo de pacotes com a opção "Flow Graph" (tag STATISTICS) da ferramenta Wireshark. A informação será útil para perceber e avaliar os tempos da transferência dos diversos objectos que tiveram que ser transferidos como resultados do pedido do browser.
5. Explore agora as estatísticas que pode obter na opção HTTP.

Sugestão final

Agora que compreendeu algum do potencial da utilização de uma ferramenta como o Wireshark, tente aumentar a sua autonomia no uso da ferramenta como instrumento prático para complementar o estudo teórico dos protocolos da pilha TCP/IP, nomeadamente o que aprendeu sobre protocolos do nível aplicação, transporte (TCP, UDP), nível rede (IP, ARP ou RARP), ou do nível de ligação de dados (Ethernet), observando na prática a estrutura e o formato das mensagens, segmentos, pacotes ou frames Ethernet e a lógica do seu encapsulamento na pilha TCP/IP.

Para elaboração do trabalho prático nº 3, a ferramenta Wireshark será também de uma grande utilidade para o ajudar a monitorar o tráfego HTTP trocado entre browsers, um proxy HTTP que vai ter que desenvolver e os servidores WEB finais com os quais o seu proxy vai ter que conseguir comunicar, de forma transparente em relação aos pedidos dos browsers e respostas obtidas por estes.