Ficha do Trabalho Prático nº 4

Encapsulamento Protocolar

Descrição do Trabalho: Encapsulamento dos protocolos de ligação, rede, transporte e de aplicação. Visualização e interpretação do encapsulamento de PDUs capturados por um analisador de rede.

Entre num dos sistemas Linux com o seu username (cdr-g01 a cdr-g11) e password 3690147258

1. Aplicação de captura e análise de tráfego

As estações de trabalho PCx dispõem de um programa de captura e análise de tráfego de rede (vulgarmente designado por *sniffer*) denominado *ethereal*.

a) Explore este programa invocando-o através do comando **sudo ethereal**. Resuma as suas funcionalidades e o tipo de informação que ele é capaz de fornecer ao utilizador.
Nota: Coloque-o a capturar tráfego (Capture Start/Stop) e visualize o resultado da captura. Explore também a utilização de filtros na captura (Capture Filters) e na visualização (Analyze Filters).

Este programa captura pacotes que estejam a circular na rede num dado intervalo de tempo, em tempo real;

Podem ser aplicados filtros (TCP por exemplo), que apenas irá captura pacotes de protocolos dos níveis de Transporte e Aplicação (níveis superiores)).

Para cada pacote está disponível neste programa, informação detalhada referente a cada nível da camada protocolar TCP/IP.

Podem ser criados filtros (com a função Analyze Filters), que nos permitem identificar, tal como em "Captura Filters", determinados pacotes, (filtrando) sendo este filtro mais personalizado, permitindo filtrar pacotes detalhando mais informação do que nos filtros predefinidos (como comparação de comprimento em cada pacote, identificar pacotes relativos a certa porta, etc...).

Se não forem aplicados filtros o programa captura qualquer pacote, seja qual for o protocolo.

O Filtro analise é um filtro após a captura.

2. Análise de tráfego

Utilizando o analisador de rede capture uma trama *ethernet* que encapsule protocolos da pilha TCP/IP. Visualize e analise o encapsulamento dos PDU dos vários protocolos envolvidos.
Nota: se não conseguir obter esse tipo de informação, coloque o *ethereal* em modo de captura e force a geração de tráfego com uma aplicação apropriada.
ex1: arranque o browser mozilla e aceda à página da disciplina
ex2: aceda ao router-lab por telnet.

a) Para a trama capturada indique concretamente quais os protocolos encapsulados (desde o nível de aplicação ao nível físico) e transcreva a informação que lhe permitiu chegar a essa conclusão (os campos dos cabeçalhos e os seus valores).

Capturamos uma trama HTTP esta apresenta (pela encapsulação) os seguintes protocolos:
Ethernet (nível ligação lógica) → apresenta no cabeçalho o campo type do tipo IP;
IP (nível Rede) → apresenta no seu cabeçalho o campo protocol do tipo TCP;
TCP (nível Transporte) → apresenta a identificação do programa pelo seu nº de porta (Source: 3128, Destin: 3312[illegible])
HTTP (nível de aplicação) → apresenta apenas a informação (dados úteis)

b) Descreva o processo de desmultiplexagem protocolar nas máquinas equipadas com protocolos da pilha TCP/IP.

Neste processo os protocolos são desfeitos, filtrando apenas a informação protocolar relativa a protocolos situados num nível superior da pilha TCP/IP,
Começa com a chegada de uma trama ao Interface Ethernet (nível ligação lógica) é analisado o campo relativo ao protocolo do nível de rede do pacote respectivo, e é enviado a restante informação para o software relativo ao nível protocolar superior.
Aí, é analisado o campo referente ao nível de Transporte em IP (TCP ou UDP, conforme a fiabilidade pretendida na transmissão dos dados).
Finalmente, no nível de Transporte é analisado o nº da porta, identificando a aplicação respectiva, enviando a informação respectiva a essa aplicação.

c) Para a trama capturada, indique os vários endereços observados e os níveis protocolares a que se referem (MAC, IP, Transporte). Considerando a comunicação entre duas aplicações em redes IP distintas, descreva como são usados esses endereços no percurso fim-a-fim.

MAC: Source: 00:05:32:46:8D:C2
Destination: 00:50:FC:5E:EE:C9
} Ethernet Protocol

IP: Source: 193.136.19.08
Destination: 192.168.89.11

TCP: Source: port: squid (3128)
Destination: 33126

→ No percurso fim-a-fim, para a comunicação entre duas aplicações em redes IP distintas é utilizado um sistema intermediário → ROUTER; os endereços IP e TCP (Source e Destination respectivamente) são fixos, inalteráveis.
O endereço do MAC adress é relativo ao último nó da rede, por onde a trama passou, e o endereço destino do MAC adress é relativo à máquina ou nó para onde a trama vai ser enviada.

3. Segurança

a) Com um analisador de rede é possível encontrar as senhas que permitem aceder a sistemas ou recursos remotos.
Tente encontrar e capturar os *login* e as *password* que enviar através da rede ao efectuar **telnet router-lab** e **ssh kepler** (após a captura de tráfego, utilize a opção *Analyze/Follow TCP Stream* para facilitar a tarefa de visualização do *login* e *password*).
Em face do que observou comente sobre a vulnerabilidade de segurança de cada uma destas aplicações.

A aplicação telnet router-lab revelou-se vulnerável pois com a opção Analyse/Follow TCP facilmente obtemos o username e a password que inserimos. Verificamos que cada caracter da string de username e password é enviada numa trama diferente, e que a informação não se encontra encriptada.

A aplicação ssh kepler revelou-se segura, pois com a opção Analyse/Follow TCP não conseguimos obter nem o username nem a password dado que estes dados se encontram encriptados.

4. Efeitos do equipamento de rede

a) Como sabe, a rede do laboratório está equipada com um *switch*. Como é que este elemento da rede condiciona o tráfego que pode ser observado pelo analisador de rede a partir da sua estação de trabalho? Justifique a sua resposta, ilustrando com um exemplo se necessário.

O facto de existir um switch e não um repetidor, diminui o tráfego que chega à nossa máquina, pois os pacotes que chegam ao switch são enviados directamente para a máquina a que pertencem. No caso do repetidor, este envia para todas as máquinas a que está ligado todos os pacotes que recebe.

No nosso caso o tráfego observado não inclui tráfego com destino a outras máquinas diferentes da nossa, o que indica que a nossa máquina se encontra ligada a um switch e não a um repetidor.