MAC0352 - Redes de Computadores e Sistemas Distribuídos - 2s2023
EP0
Entrega até 8:00 de 28/8/2023
(INDIVIDUAL)

Prof. Daniel Macêdo Batista

1 Problema

Quando utilizamos aplicativos que se comunicam via Internet, esses aplicativos realizam a comunicação por meio de conjuntos de dados chamados de mensagens. Para que essas mensagens sejam propagadas pela Internet, elas precisam ser transformadas no que se chama de pacote. Muitas vezes uma única mensagem precisa ser dividida em mais de um pacote. Isso ocorre por exemplo se a mensagem for muito grande. Para que esses pacotes possam trafegar na Internet e possam ser unidos para reconstruir a mensagem original, é necessário incluir informações extra além da mensagem propriamente dita. A mensagem propriamente dita é chamada de *payload* ou carga útil. As informações extra necessárias para que a mensagem possa trafegar pela Internet constitui o que é chamado de cabeçalho do pacote. Portanto, quando falamos sobre tráfego na Internet, estamos falando de um conjunto de pacotes que estão sendo transferidos entre várias entidades como computadores, *smartphones*, roteadores, *switches* [1], etc...

Neste EP (que nem deveria ser chamado de EP, já que não há programação envolvida) você deverá capturar o tráfego de rede no seu computador em duas situações e responder dois conjuntos de perguntas. A captura será feita com o `Wireshark`[2]. O `Wireshark` é um *sniffer*. Um *sniffer* é um software capaz de capturar todo o tráfego que passa por uma interface de rede. A depender de como a rede esteja configurada, isso pode permitir a captura do tráfego de todos os computadores da rede.

2 Requisitos

2.1 Ambiente de Software

Você precisa instalar o `Wireshark` no seu computador. Na página do software há versões para diversos sistemas operacionais. Caso você vá instalar em um computador com GNU/Linux, recomenda-se que o `Wireshark` seja instalado pelo gerenciador de pacotes da distribuição que você utiliza.

Para que a captura funcione da melhor forma possível, o `Wireshark` precisa rodar em um modo

[1] Estudaremos roteadores e *switches* no decorrer da disciplina

[2] `https://www.wireshark.org/`

chamado modo "promíscuo" em que quadros[3] da camada de enlace percorrem toda a pilha da arquitetura Internet do sistema operacional do seu computador mesmo que esses quadros não tenham o seu computador como origem ou destino. Para funcionar em modo "promíscuo", o `Wireshark` precisará de permissões a nível de super usuário. Preste atenção às mensagens relacionadas a isso quando você instalar o software e siga as instruções do instalador.

Você também precisará instalar algum software que faça download de conteúdo via HTTPS no shell, como o `curl`[4] ou o `wget`[5]. Recomenda-se que eles sejam instalados pelo gerenciador de pacotes do seu sistema operacional mas antes verifique se eles já estão instalados. Em boa parte dos sistemas operacionais, pelo menos um desses dois já costuma vir instalado.

2.2 Perguntas

Ligue o seu computador e abra todos os programas que você costuma usar de forma simultânea no seu dia-a-dia, incluindo o navegador web com abas nos sites que você mais utiliza. Não interaja com nenhum desses programas por 3 minutos. Abra o `Wireshark` e capture o tráfego na interface de rede do seu computador que esteja conectada à Internet por 10 segundos (Ao abrir o software, ele vai mostrar uma lista de todas as interfaces de rede do seu computador). Depois de capturar o tráfego por 10 segundos, interrompa a captura e salve o arquivo de *trace* como `pergunta1.pcapng`. Esse arquivo poderá ser usado para continuar a realizar este EP em outro momento. Para acessar o arquivo em outro momento, abra o `Wireshark` e selecione o arquivo indo no menu **File ->** **Open** ou **Arquivo ->** **Abrir**.

Responda as perguntas abaixo num arquivo `respostas.txt` (Não escreva as perguntas no arquivo. Escreva **apenas** as respostas):

Escolha dois quadros quaisquer que foram capturados e responda: qual software ou site foi responsável por esses segmentos? Como você descobriu? Na sua resposta informe para cada segmento: endereço IP fonte, endereço IP destino, endereço MAC de origem, endereço MAC de destino e protocolo da camada de aplicação, caso haja algum protocolo da camada de aplicação. Todas essas informações são exibidas no Wireshark. Basta clicar sobre o segmento e obter as informações no painel exibido no meio da janela principal.

Feche o navegador web e todos os programas que você acha que fazem algum acesso à Internet. Aguarde 3 minutos, abra o `Wireshark` e no campo de filtro de captura escreva:

```
host 200.144.244.77
```

Com esse filtro, apenas os quadros que tenham o servidor web do IME-USP como origem ou destino serão capturados. Inicie a captura do `Wireshark`.

Responda as perguntas abaixo no mesmo arquivo `respostas.txt` onde as perguntas anteriores foram respondidas:

Abra um terminal e faça download do arquivo `https://www.ime.usp.br/~batista/234800947` com o wget ou com o curl (Esse arquivo é um arquivo em texto simples). Espere 3 minutos e encerre a captura pelo Wireshark. Salve o trace da captura com o nome pergunta2.pcapng. Esse arquivo terá

[3] A depender da camada na arquitetura Internet, o pacote tem um nome diferente: segmento na camada de transporte, datagrama na camada de rede e quadro na camada de enlace

[4] `https://curl.se/`

[5] `https://www.gnu.org/software/wget/`

que ser entregue no e-Disciplinas. Considerando o instante do primeiro quadro e o instante do último quadro da comunicação com o servidor do IME exibidos no Wireshark, quando tempo foi necessário para fazer a transferência do arquivo? Considerando o tamanho real do arquivo em bytes após ele ter sido copiado do servidor do IME-USP e a quantidade de bytes que foram enviados do servidoor para o seu computador de acordo com o Wireshark, pode-se dizer que a transferência via HTTPS gerou uma sobrecarga de quantos '%' a mais de bytes? Explique como você fez esse cálculo.

Entregas sem o *trace* da segunda pergunta não serão corrigidas e receberão nota ZERO.

3 Entrega

Você deverá entregar um arquivo .tar.gz contendo os seguintes itens:

- .txt com as respostas;
- .pcapng com o *trace* da segunda pergunta.

O desempacotamento do arquivo .tar.gz deve produzir um diretório contendo os itens. O nome do diretório deve ser ep0-seu_nome. Por exemplo: ep0-joao_dos_santos.

A entrega do .tar.gz deve ser feita no e-Disciplinas.

O EP deve ser feito individualmente.

Obs.1: Serão descontados 2,0 pontos de EPs com arquivos que não estejam nomeados como solicitado ou que não criem o diretório com o nome correto após serem descompactados.

Obs.2: A depender da qualidade do conteúdo que for entregue, o EP pode ser considerado como não entregue, implicando em MF=0,0. Isso acontecerá por exemplo se for enviado um .tar.gz ou um .pcapng corrompido ou um .txt vazio.

Obs.3: O prazo de entrega expira às 8:00:00 do dia 28/8/2023.

4 Avaliação

Os critérios detalhados da correção serão disponibilizados apenas quando as notas forem liberadas.