# FACULDADES SPEI

Curso: **Bacharel em Sistemas de Informação**
Professor: **Paulo Cezar de Oliveira**
Disciplina: **Rede de Computadores** Turma:_____
Aluno(a): Data: 24/03/2016

**Observações:**

- LEIA ATENTAMENTE AS INSTRUÇÕES E O ENUNCIADO ANTES DE INICIAR O EXERCÍCIO.
- Deve ser entregue por email (paulocezar@spei.br) e em dupla até o término da aula de hoje.
- As respostas descritivas devem ser enviadas no formato .doc, docx ou odt.
    - No **assunto do email** coloque a **turma e o período**.
- Não se esqueça de identificar a atividade com nome e turma.
    - No **nome do arquivo** coloque o **primeiro nome de cada envolvido**
- As respostas copiadas não serão consideradas, tanto de quem copiou quanto de quem forneceu o original.
- Não será aceito atraso na entrega do trabalho.

## 5ª Lista de Exercícios

Para filtrar tráfegos ao IP desejado basta inserir no filtro o endereço IP, se desejar algum protocolo também é necessário iserí-lo no filtro. Exemplo: ip.addr==10.0.0.2 and http

## Monitoramento de pacotes com Wireshark
## Estudo dos protocolos UDP,TCP, ICMP, ARP.

Comece a captura de tráfego na rede;
Utilize a Internet normalmente;
Pare a captura do Wireshark;
Aplique um filtro aos pacotes capturados de forma a visualizar apenas os pacotes UDP do seu computador ( ip.addr == “ IP” and udp);

**Questões gerais**

1. Quais os campos existentes no cabeçalho de um segmento UDP?
2. Explique o funcionamento do handshake triplo com base nos tráfego que analisou na captura efetuada.
3. Descreve algumas portas do computador e os protocolos que a utilizam.
4. Explique a diferença entre os protocolos TCP e UDP. Indique as razões para uma aplicação utilizar o UDP em vez de TCP?
5. Indique duas aplicações que usem TCP e outras duas que utilizem o UDP?

**TCP**

Antes de explorar o protocolo TCP, vamos obter uma captura de uma transferência TCP de um arquivo da sua estação para um servidor remoto. Vamos entrar num site que nos permita entrar com o nome de um arquivo armazenado no seu computador contendo um texto ASCII e depois transferir este arquivo usando o método HTTP POST enquanto fazemos a captura.
Através do seu browser, salve uma cópia do arquivo http://gaia.cs.umass.edu/ethereal-labs/alice.txt
Entre na página http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html
Informe o caminho para o arquivo alice.txt
Inicie uma captura com o Wireshark.
Clique no botão “upload alice.txt file”.
Aguarde o browser exibir a página de congratulações.
Pare a captura.

Filtre os pacotes com a expressão “tcp”.

1. Quantos pacotes foram enviados e recebidos no handshake inicial entre a sua estação e gaia.cs.umass.edu?

2. Qual é o número sequencial usado pelo cliente no segmento SYN que inicia a conexão? O que o identifica como um segmento SYN ?
3. Qual é o número sequencial do segmento SYN-ACK enviado pelo servidor em resposta ao SYN do cliente? Qual é o número sequencial do campo “acknowledgement” neste segmento? O que identifica este segmento como SYN-ACK?
4. Após o handshake deve ter ocorrido uma mensagem HTTP POST dividida em vários segmentos TCP, intercalados com mensagens ACK enviadas pelo servidor remoto.
5. Qual o número sequencial do segmento contendo o comando HTTP POST?

**ICMP**
Nesta seção exploraremos o formato e o conteúdo de mensagens ICMP geradas pelo programa ping.
Exemplo de uso do ping (envia 10 mensagens ICMP echo request para hostname):
No Linux: ping -c 10 hostname
No Windows: ping -n 10 hostname

Inicie uma captura com o Wireshark.
Envie 10 pedidos de eco para algum host, por exemplo, www.ust.hk (Hong Kong University of Science and Technology).
Pare a captura. Filtre os pacotes com a expressão “icmp”.
Selecione um dos pacotes ICMP echo request e examine o cabeçalho ICMP. Quais informações há neste cabeçalho?
1. Examine e descreva as informações contidas no cabeçalho do pacote ICMP echo reply.
2. Há informação do número das portas de origem e de destino? Por quê?
3. Qual o intervalo de tempo de envio entre as mensagens ICMP echo request? Quantos pacotes foram enviados e quantos foram respondidos?

**ARP**
Analisar informações do protocolo ARP.
– Execute o Wireshark
– Inicie a captura de pacotes
– Execute um comando “ping” em uma máquina da rede local (máximo de 4 tentativas)
– Finalize a captura de pacotes
– Filtre as requisições com o protocolo “arp”
1. Execute o comando arp -a (Windows ou Linux), descreva o significado dos valores retornados.
2. Descreva os valores dos campos apresentados em uma requisição ARP.
3. Descreva os valores dos campos apresentados na resposta de uma requisição ARP.
4. Nessas mensagem é empacotado alguma informação nos protocolos de rede, transporte (TCP ou UDP) ou aplicação? Justifique.