

Nesta atividade prática, compreenderemos o funcionamento do protocolo TCP usando o software Wireshark.

THREE-WAY HANDSHAKE: Estabelecendo uma conexão TCP

- Feche o seu cliente web (navegador);
- Inicialize o software Wireshark;
- No software Wireshark, inicie uma Nova Captura na interface de rede cabeada (`Eth0` ou `Conexão Local`) do seu host;
- Inicialize o seu cliente web (navegador);
- No cliente web, acesse o servidor web localizado no endereço: `gaia.cs.umass.us`

(se houver conectividade de rede entre o seu host e o host remoto onde está sendo executado o servidor web, você deverá receber objetos web, como uma página HTML, enviados pelo servidor web)

- Pare a captura do Wireshark.
- 1) Na lista de mensagens capturadas pelo Wireshark, procure aquela contém `[SYN]` na coluna `Info`. Abra a mensagem para identificar os dados contidos nos cabeçalhos dos protocolos desta mensagem. Analisando os **cabeçalhos do segmento TCP**, pergunta-se:
 - a) Qual é a porta TCP usada pelo seu cliente web para estabelecer a conexão TCP com o servidor web?
 - b) Quais flags estão setados com o valor 1?
 - 2) Na lista de mensagens capturadas pelo Wireshark, procure aquela contém `[SYN,ACK]` na coluna `Info`. Abra a mensagem para identificar os dados contidos nos cabeçalhos dos protocolos desta mensagem. Analisando os **cabeçalhos do segmento TCP**, pergunta-se:
 - a) Qual é a porta TCP usada pelo servidor web para estabelecer a conexão TCP com o seu cliente web?
 - b) Quais flags estão setados como valor 1?

- 3) Na lista de mensagens capturadas pelo Wireshark, procure aquela contém [ACK] na coluna Info. Abra a mensagem para identificar os dados contidos nos cabeçalhos dos protocolos desta mensagem. Analisando os **cabeçalhos do segmento TCP**, pergunta-se:
- a) Identifique, respectivamente, as portas TCP da fonte e do destino.

ENCAPSULAMENTO

- 4) Na lista de mensagens capturadas pelo Wireshark, procure aquela contém [SYN] na coluna Info. Abra a mensagem para identificar os dados contidos nos cabeçalhos dos protocolos desta mensagem. Pergunta-se:
- a) Que PDU encapsula o segmento TCP?
 - b) Identifique, respectivamente, os endereços IP do seu host e do host remoto (onde está sendo executado o servidor web).
 - c) Identifique, respectivamente, os endereços MAC da interface de rede do seu host e a interface de rede do próximo salto do quadro Ethernet.
 - d) Pode-se afirmar que o endereço MAC do próximo salto do quadro é o endereço MAC da interface do host `gaia.cs.umass.us`? Justifique a sua resposta.
- 5) Na lista de mensagens capturadas pelo Wireshark, procure aquela contém [SYN,ACK] na coluna Info. Abra a mensagem para identificar os dados contidos nos cabeçalhos dos protocolos desta mensagem. Pergunta-se:
- a) No cabeçalho do protocolo IP, qual é o valor do cabeçalho TTL?
 - b) No cabeçalho do quadro Ethernet, qual é o valor do tipo do protocolo encapsulado?