Pontifícia Universidade Católica do Rio Grande do Sul
Escola Politécnica
Redes de Computadores Avançadas

Exercício TCP/UDP

Questões

Utilizando um *sniffer* de pacotes (wirehark)g monitore o tráfego na sua rede para responder as questões a seguir.

1) Monitore o handshake de estabelecimento de conexão TCP e verifique:
    a. Quais os pacotes de controle foram trocados entre origem e destino;
    b. Quais opções do TCP foram negociadas no estabelecimento da conexão e o que elas significam;
    c. Qual o tamanho da janela negociado pela origem e pelo destino;
    d. Qual o Roud Trip Time (RTT) das mensagens.
2) Monitore o processo de encerramento de conexão TCP e verifique:
    a. Quais pacotes de controle foram trocados entre origem e destino;
    b. Quais as opções do TCP foram utilizadas no encerramento da conexão e o que elas significam;
    c. Se ocorre envio de dados no processo de *half-close*, para a aplicação que você está usando;
    d. Qual o Roud Trip Time (RTT) das mensagens.
3) Monitore o processo de transmissão de dados com protocolo TCP e verifique:
    a. O tamanho das janelas negociadas e o momento em que são negociadas;
    b. A ocorrência de possíveis retransmissões. Quais mensagens são trocadas? Qual o tempo entre o envio do primeiro pacote e do pacote retransmitido?
    c. O retorno do ACK. Ele ocorre sempre sozinho? Em que situações ele ocorreu junto com pacote de dados? Qual a diferença de tempo na resposta de uma situação e outra?

d. Como é utilizada a janela de transmissão, de acordo com a aplicação que você está utilizando? Ocorre a transmissão de mais de um pacote na janela, sem ter ocorrido ACK do anterior? Por quê?

4) Tente estabelecer conexão com um serviço que não está ativo em uma máquina vizinha e/ou da Internet. Por exemplo, usando telnet tente conectar em porta que não está ativa na máquina, ou utilize o nmap para fazer uma varredura de portas. Verifique qual a mensagem de resposta da máquina destino para esta solicitação de conexão.

5) Gere tráfego UDP na rede com o comando *nmap* e teste as portas UDP que estão abertas ou fechadas. Verifique quais mensagens são geradas para as portas que não se encontram abertas na máquina destino; e quais são geradas para as portas que estão abertas.