Pontifícia Universidade Católica do Rio Grande do Sul
Escola Politécnica
Laboratório de Redes de Computadores
Redes de Comunicação II

Trabalho Final

Objetivo

Implementar dois programas: um que envia mensagens de varredura TCP e outro que faz a detecção das mesmas, ambos utilizando usando IPv6.

Descrição

O trabalho consiste na implementação de dois programas, um que que envia mensagens de varredura TCP (*port scanning*), como o objetivo de descobrir portas abertas no sistema, e outro que faz a detecção dos ataques, ambos utilizando usando IPv6.

O programa que faz o *port scanning* deve implementar os seguintes ataques de varreduda:

- **TCP connect:**
  - uma mensagem de SYN é enviada para uma determinada porta;
  - se a porta estiver aberta, um SYN/ACK deve ser recebido;
  - a fase de handshake do TCP deve ser concluída com o envio de um ACK.
- **TCP half-opening:**
  - uma mensagem de SYN é enviada para uma determinada porta;
  - se a porta estiver aberta, um SYN/ACK deve ser recebido;
  - um pacote de RST é enviado para fechar a conexão.
- **Stealth scan ou TCP FIN:**
  - uma mensagem FIN é enviada para a uma determinada porta;
  - se a porta estiver fechada, um RST deve ser recebido; senão a porta está aberta.
- **SYN/ACK:**
  - uma mensagem de SYN/ACK é enviada para uma determinada porta;
  - se a porta estiver aberta, um RST deve ser recebido; senão a porta está fechada.

Esses ataques devem verificar o range de portas que o usuário informa, como, por exemplo, de 25 a 80, e informar sempre que foi possível realizar a verificação com sucesso.

O programa que faz a detecção dos ataques, deve indicar quando os ataques dos tipos anteriores estiverem sendo realizados na máquina monitorada. Este programa deve indicar de qual IP vem o ataque e qual o tipo de ataque encontrado.

Quanto ao tipo de *sockets* a ser utilizado na aplicação para a comunicação entre processos, deve-se observar que a comunicação deve ser implementada com *socket* RAW, para envio e recebimento das mensagens. Neste caso, devem ser preenchidas as informações dos *headers* de nível de enlace, rede e transporte, ou, no caso do recebimento, lidas e tratadas por nível.

Apresentação: a apresentação consiste em utilizar o *port scanning* implementado pelo grupo, com o programa que faz a detecção de outro grupo. Desta forma, os protocolos e as formas de ataque e detecção devem estar corretamente implementados.

Resultados e Entrega

Grupos: Até 3 alunos.

Data da Entrega e Apresentação: 13/06/2016
Obs.: Todos participantes devem estar presentes

IMPORTANTE: Não serão aceitos trabalhos entregues fora do prazo. Trabalhos que não compilam ou que não executam não serão avaliados. Todos os trabalhos serão analisados e comparados. Caso seja identificada cópia de trabalhos, todos os trabalhos envolvidos receberão nota ZERO.