Pontifícia Universidade Católica do Rio Grande do Sul
Escola Politécnica

Trabalho Final
Redes II e Laboratório de Redes

Implementação do ataque TCP SYN Flooding com IPv6

Objetivo

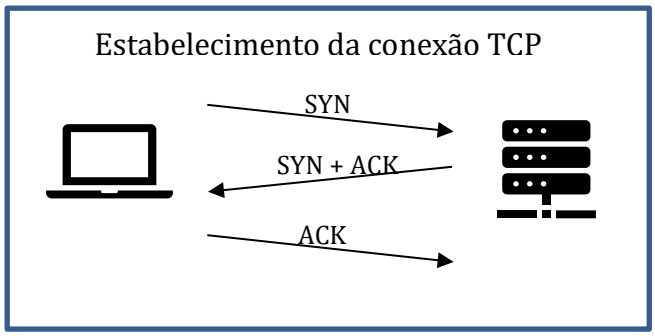
Este trabalho possui os seguintes objetivos:

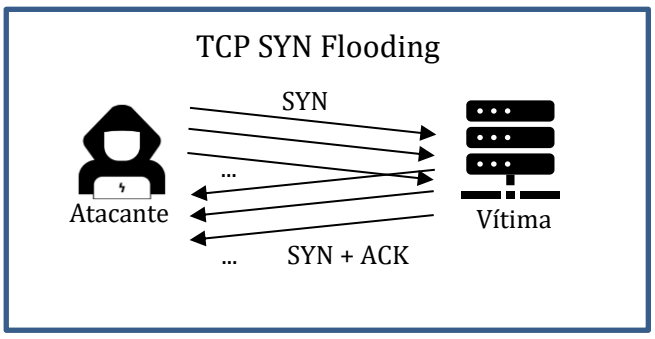
- implementar um programa faça um ataque de TCP SYN flooding usando IPv6; e,
- implementar outro programa que receba a resposta enviada pela vítima.

Descrição

O TCP SYN flooding tem por objetivo realizar um ataque de negação de serviço em algum servidor. Esse ataque explora uma parte do estabelecimento da conexão do protocolo TCP, consumindo recursos na máquina que está sendo atacada, tornando-a indisponível.

As figuras seguir representam como é realizado o estabelecimento da conexão do TCP e um exemplo de como realizar o TCP SYN flooding.





A ideia do ataque consiste nos seguintes passos:

- o atacante envia muitos pedidos de estabelecimento de conexão TCP (pacotes com o bit SYN setado) mais rápido do que o destino consiga processar, sobrecarregando-o;

- ao receber um pedido de estabelecimento de conexão, a vítima aceita a conexão e fica esperando o ACK final, sendo que este ACK nunca é enviado pelo atacante e a conexão é encerrada por timeout.

Para o flooding acontecer, o atacante envia muitas mensagens de estabelecimento de conexão, de forma que o destino não consiga fazer mais nada.

Sendo assim, o trabalho final da disciplina consiste na implementação de dois programas:

- o primeiro deve enviar muitas mensagens de TCP com o bit SYN setado, encapsulado em protocolo IPv6 através de ***socket RAW***;
- o segundo deve imprimir na tela as informações do pacote ACK enviado pela vítima, na tentativa de realizar a conexão. Essa impressão deve seguir o seguinte formato:

MAC Origem – MAC Destino – IPv6 Origem – IPv6 Destino – Flags do Cabeçalho do TCP

Para realizar o ataque, será necessário instalar algum serviço na vítima ou descobrir alguma porta aberta nesta máquina.

A implementação tanto do envio quanto da recepção do cabeçalho das mensagens deverá ter os **campos** dos protocolos de **nível 2 (Ethernet)**, **3 (IPv6)** e **4 (TCP)** preenchidos pela **aplicação** a ser desenvolvida, não sendo permitido deixar que a pilha de protocolos da máquina realize o preenchimento "*default*".

Resultados e Entrega

Os itens que devem ser enviados em um arquivo compactado (.zip ou .tar.gz) na respectiva sala de entrega no Moodle são descritos abaixo:

- código-fonte do programa;
- relatório explicando a organização da implementação (módulos/classes) e o processo de validação.

Os trabalhos serão apresentados no Zoom na mesma data da entrega e todos os componentes devem estar presentes e participar da apresentação.

Grupos: até 3 alunos
Data de entrega e apresentação: 25/11/2021

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.