DDoS Contramedidas

Igor T. Martins

Redes de Computadores 2
TCC-00186

Motivação

- Aprender sobre o funcionamento de um DDoS e as medidas defensivas usadas.

- A dificuldade de evitar ou reduzir os danos de um DDoS.

Objetivos

- Explicar o funcionamento de um ataque de negação de serviço.
- Apresentar algumas técnicas usadas em ataques.
- Apresentar as medidas defensivas usadas.

DoS

- Ataque de negação de serviço.
- Tem como finalidade consumir os recursos da vítima.
- É difícil diferenciar o ataque de usuários da vítima.

DoS: Ataque por Inundação

Objetivo:

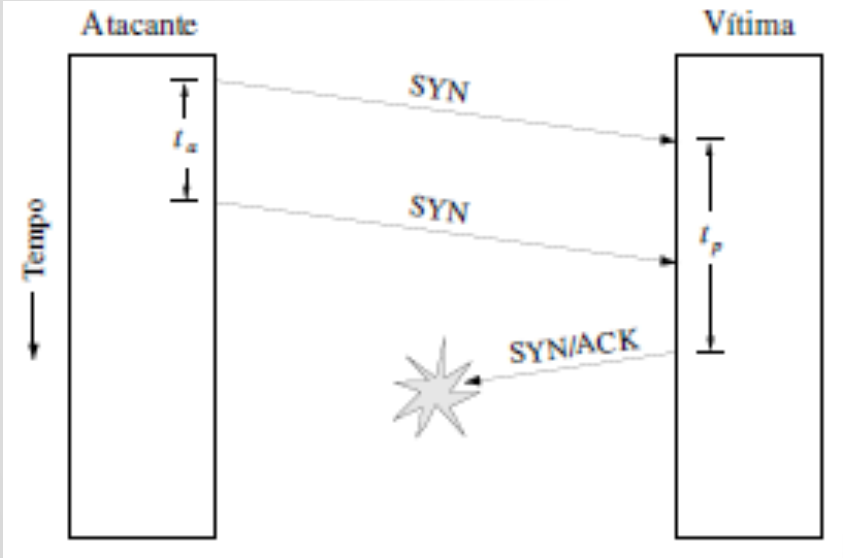
- Sobrecarregar o processamento ou memória da vítima.

Técnica:

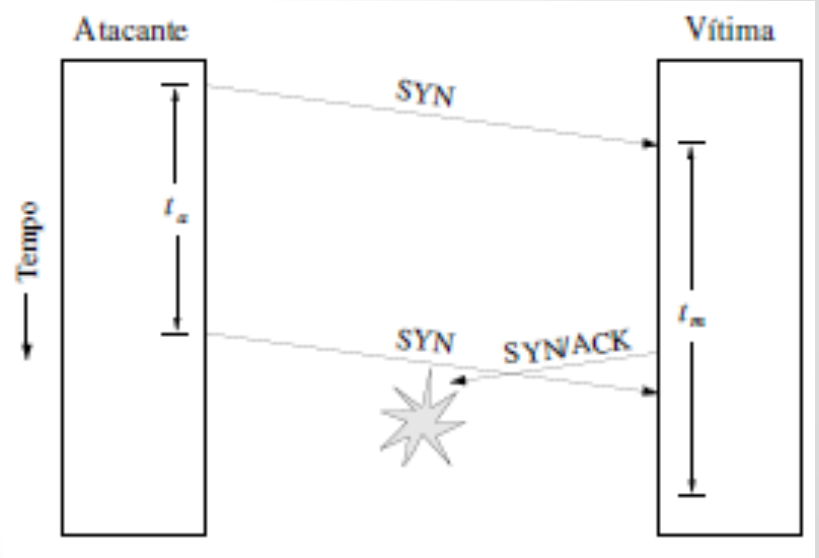
- Envia segmentos TCP SYN.
- Não envia ACK de resposta.

DoS: Ataque por Inundação

Processamento



Memória



fonte: ”Negação de Serviço: Ataques e Contramedidas”

DoS: Ataque por Refletor

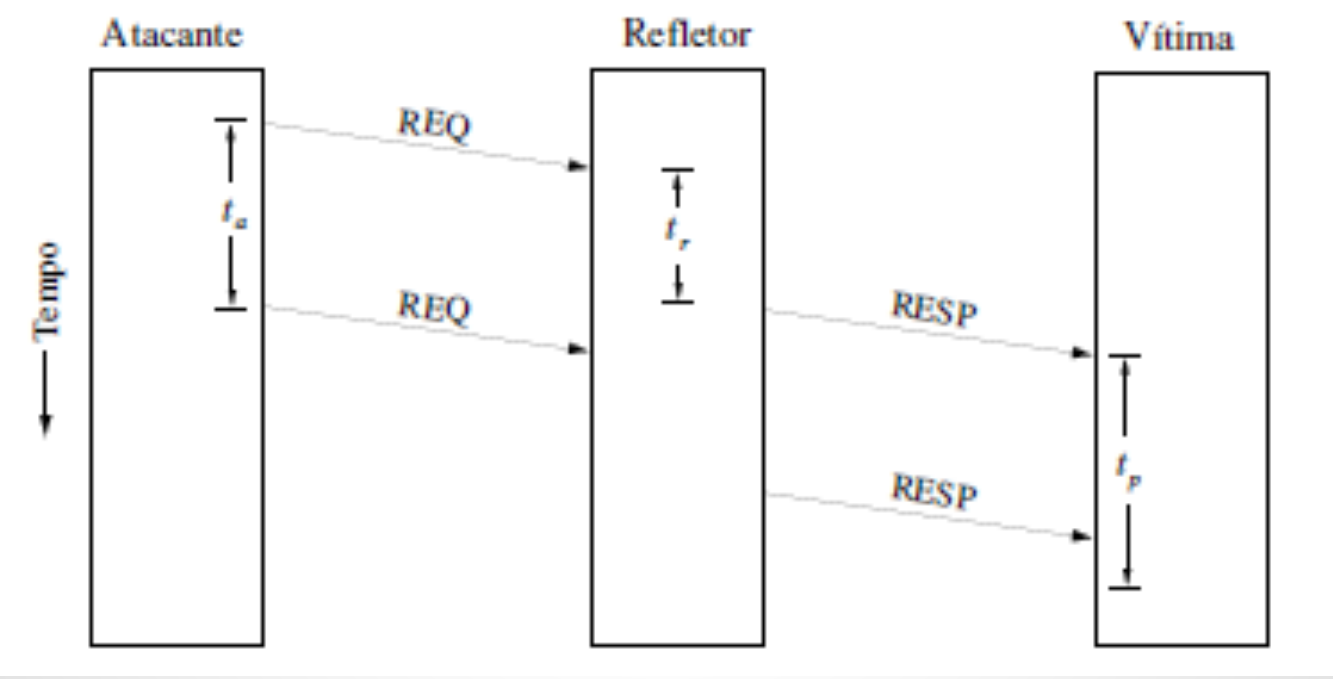
Objetivo:

- Sobrecarregar a vítima.

Técnica:

- Atacar a vítima usando um refletor.
- Envia uma requisição com o IP da vítima ao refletor.
- O refletor envia a resposta à vítima.

DoS: Ataque por Refletor



fonte: ”Negação de Serviço: Ataques e Contramedidas”

DDoS

- Ataque distribuído de negação de serviço.
- O atacante usa várias estações.
- Geralmente há o uso de **botnets**, rede de computadores infectados.

DDoS: Contramedidas

Medidas Preventivas:

- Manutenção do sistema
- Filtragem dos dados recebidos pela vítima.

Medidas Reativas:

- Rastreamento de pacotes.
- Redução da taxa de transmissão do atacante.

DDoS: Manunteção do Sistema

- Minimiza os ataques por vulnerabilidade.
- Dificulta que o atacante domine o sistema.

DDoS: Filtragem de Dados

- Evita que pacotes com IP forjados trafeguem na rede.
- Implementada nos roteadores.
- Os roteadores comparam o IP dos pacotes com faixa de endereços da rede.

DDoS: Filtragem de Dados

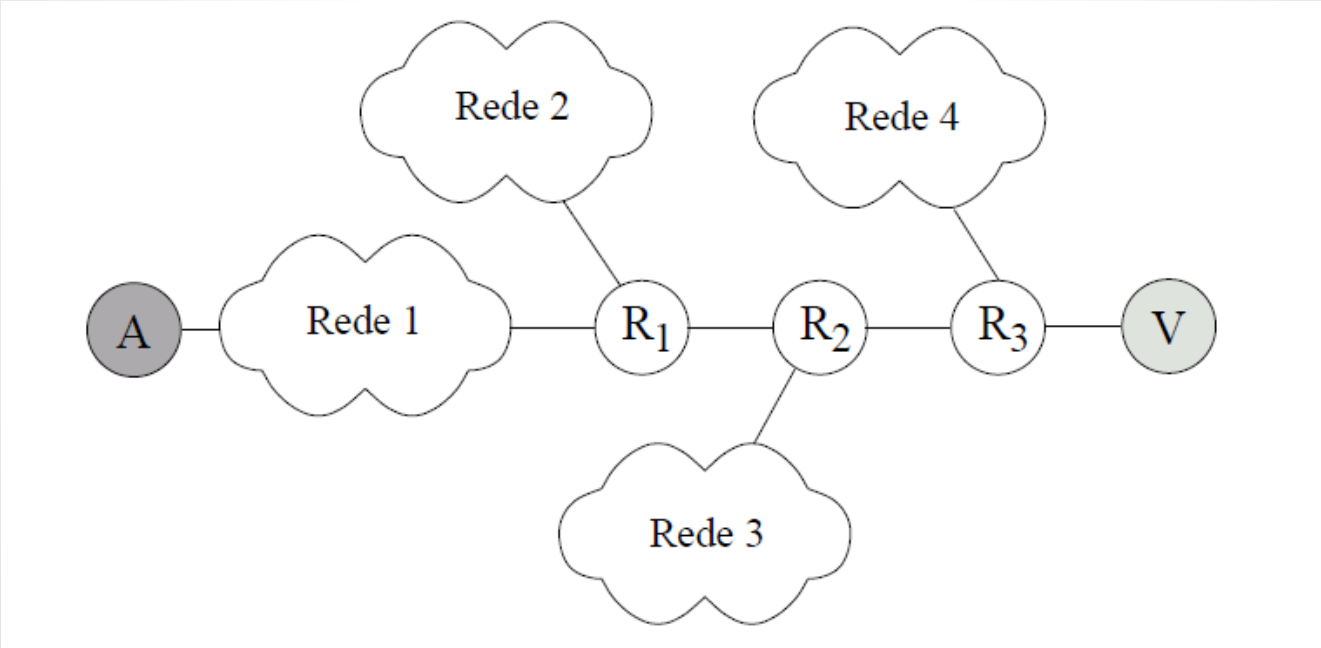
Vantagem:

- Técnica simples.

Desvantagem:

- Precisa ser implementada em muitos roteadores.
- Processamento adicional.

DDoS: Filtragem de Dados



fonte: “Negação de Serviço: Ataques e Contramedidas”

DDoS: Rastreamento de Pacotes

- Descobrir a origem e a rota de ataque.
- Necessária para uma análise mais detalhada do ataque.
- Usada por outros métodos para prover uma melhor defesa.

DDoS: Rastreamento de Pacotes

Rastreamento sem estado.

- Mais simples, pois não há armazenamento de dados.

Desvantagem:

- Só pode ser utilizada durante o ataque.
- É necessário testar os enlaces da rede.
- Não consegue detectar um ataque.

DDoS: Rastreamento de Pacotes

Rastreamento com auditoria.

- Coleta informações sobre os pacotes que trafegam na rede.
- Análise contínua do tráfego.

Desvantagem:

- É necessário armazenar as informações.
- Acréscimo de processamento nos roteadores.

DDoS: Limitação de Taxa

- Ao identificar a rota de ataque, uma mensagem de alerta é enviada aos nós da rede.

- Os nós limitam a taxa de transmissão do atacante.

DDoS: Limitação de Taxa

Vantagem:

- Reduz o dano causado.
- Permite que a vítima consiga atender seus usuários.

Desvantagem:

- Deve haver a correta identificação do atacante.
- Não impede totalmente o ataque.

Conclusão

- Os DDoS ainda são um desafio de segurança.
- São muito usados devido a simplicidade.
- São eficiente por tirarem proveito dos protocolos usados na Internet.

Perguntas

1. Qual a vantagem do rastreamento de pacotes?

2. Qual a principal característica de um DDoS ?

Respostas

1. Descobrir a origem e a rota do ataque, permitindo que seja feita a filtragem correta do tráfego de ataque.

2. O uso de várias estações para inundar a vítima.

Referências

Laufer, R. P., Moraes, I. M., Velloso, P. B., Bicudo, M. D. D., Campista, M. E. M., Cunha, D. O., Costa, L. H. M. K., Duarte, O. C. M. B. "Negação de Serviço: Ataques e Contramedidas", in Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais SBSeg' 2005. Florianópolis, Brazil, pp. 163, September 2005.

Debajyoti Mukhopadhyay, ByungJun Oh, SangHeon Shim, YoungChon Kim “ A Study on Recent Approaches in Handling DDoS Attacks”, arXiv:1012.2979, December 2010.

Saravanan Kumarasamy, R. Asokan “Distributed Denial of Service (DDoS) Attacks Detection Mechanism”, arXiv:1201.2007, January 2012