

# DoS e DDos

Ataque de Negação de Serviço

Viana R.  
Santos R.

# O que é?

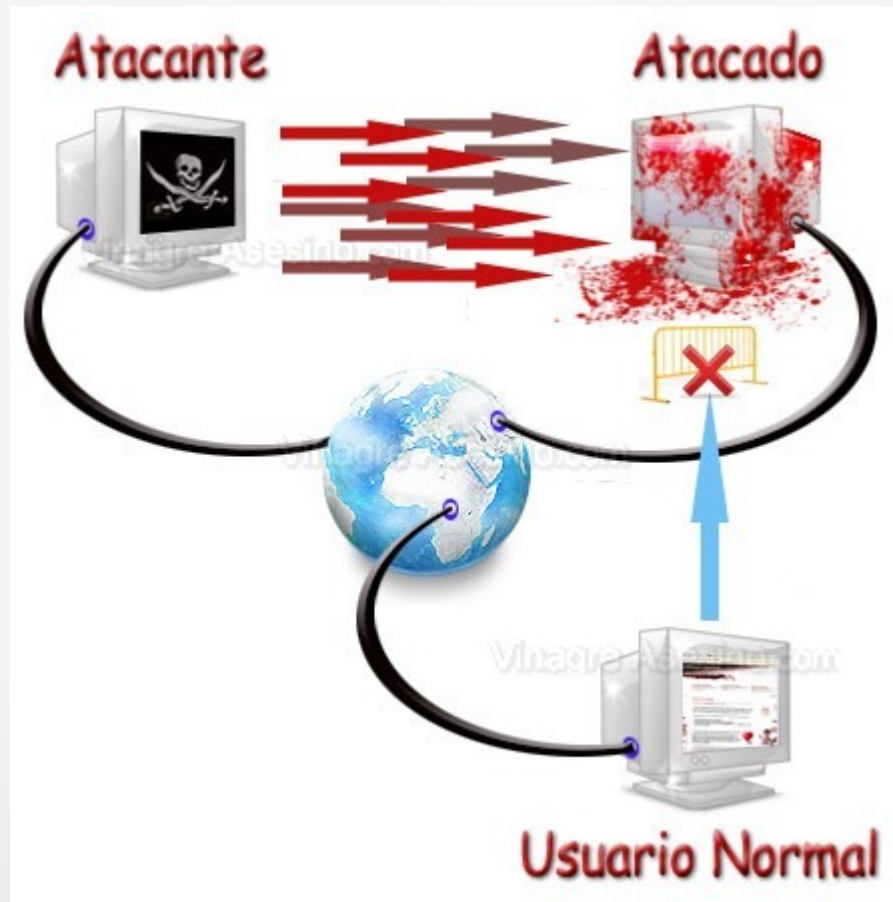
Diferentemente da maioria dos ataques da Internet, um ataque de negação de serviço **(Denial of Service)** ou **Distributed Denial of Service** não visa invadir um computador para extrair informações confidenciais, como números de cartões de crédito e senhas bancárias, e nem para modificar o conteúdo armazenado neste computador, como sítios da Internet. Tais ataques têm como objetivo tornar inacessíveis os serviços providos pela vítima a usuários legítimos.

# Como Funciona?

Para que um ataque DoS ou DDoS seja bem sucedido, um atacante deve gerar mensagens a uma taxa superior à taxa na qual a vítima, ou a sua infra-estrutura de rede, consegue tratar estas mensagens, ou apenas explorar uma vulnerabilidade da vítima.

# Como Funciona?

## DoS



# Como Funciona?

DDoS



# Classificação dos Ataques

Diversos fatores, como o número de atacantes envolvidos e o tipo de recurso explorado na vítima, podem ser usados para classificar os ataques de negação de serviço. Os ataques são classificados em:

- Inundação.
- Refletor.
- Infra-estrutura.
- Vulnerabilidades.
- Distribuídos.

# Classificação dos Ataques

- Inundação
  - Protocolos
    - TCP ACK, entre outros protocolos.
  - Recursos Afetados
    - Processamento.
    - Memória.
  - Soluções
    - Regras de Firewall.
    - Redirecionamento de Fluxo de Dados.
    - Entre diversas soluções a mais eficiente e a elaboração de um filtro de IP.

# Classificação dos Ataques

- Refletor(Amplificação)
  - Protocolos
    - ICMP entre outros protocolos.
  - Recursos Afetados
    - Processamento.
    - Memória.
  - Soluções
    - Regras de Firewall.
    - Redirecionamento de Fluxo de Dados.
    - Entre diversas soluções a mais eficiente e a elaboração de um filtro de IP.



# Classificação dos Ataques

- Distribuidos
  - Protocolos
    - TCP ACK, ICMP entre outros protocolos.
  - Recursos Afetados
    - Processamento.
    - Memória.
  - Soluções
    - Entre diversas soluções a mais eficiente e a elaboração de um filtro de IP.

# Classificação dos Ataques

- Vulnerabilidade
  - Protocolos
    - Qualquer protocolo vulnerável.
  - Recursos Afetados
    - O travamento da vítima.
  - Soluções
    - Sempre estar com o sistema atualizado para evitar alguma vulnerabilidade explorável.

# Classificação dos Ataques

- Infraestrutura
  - Protocolos
    - Qualquer protocolo com a infraestrutura comprometida.
  - Recursos Afetados
    - Recurso alvo.
  - Soluções
    - Estudo na codificação do recurso.

# Como Evitar Ataques

- Uma boa fornecedora de serviços de hospedagem e dns.
- Uma boa codificação do serviço/recurso disponível.
- Regras de Firewall
  - Sistema de isolamento de usuário por filtragem de IP.
- Não ser um alvo.

# Referências

- DDOS/DOS

<https://www.gta.ufrj.br/ftp/gta/TechReports/LMVB05a.pdf>

Acessado 15/06/2017

NEGAÇÃO DE SERVIÇOS

- <http://ieeexplore.ieee.org/abstract/document/5735752/>

Acessado 12/06/2017