DoS – Denial of Service

# Índice

1. O que é?
2. Formas de Ataques
   1. Ataques de Força Bruta
   2. Ataques de Protocolo
3. Principais Tipos de Ataques
   * 1. *UDP Flood*
     2. *HTTP Flood*
     3. Ataques *Smurf*
     4. Ataques *Fraggle*
     5. *SYN Flooding*
     6. Ping da Morte
     7. *Ataques de Amplificação DNS*

# O que é?

Os ataques de *Denial of Service*, ou Negação de Serviço, são, como o nome diz, um tipo de ataque cujo objetivo é interromper ou prejudicar o fornecimento de um serviço. Por exemplo, um ataque DoS pode ser realizado para sobrecarregar uma rede, tornando-a lenta, tornar serviços de e-mail instáveis ou para tornar uma página da Internet inacessível.

Nesses ataques, são exploradas vulnerabilidades dos sistemas operacionais e dos protocolos de rede usados pela máquina-alvo, de modo a sobrecarregar o seu alvo. Dessa forma, usuários legítimos ficam impedidos de acessar o serviço, pois o servidor não consegue processar suas requisições.

Ataques DoS podem ser feitos de duas formas em relação ao endereço IP do atacante. Uma delas é um ataque de forma direta, ou seja, sem disfarçá-lo. Essa forma de ataque é facilmente interrompida adicionando-se um filtro de IP ao *firewall*. A outra alternativa é fazer o chamado *IP Spoofing*, ou seja, o mascaramento de endereços IP, aproveitando-se do fato de que não há verificação do remetente nos comutadores da rede. Para fazer isso, o atacante deve inserir cabeçalhos de TCP e IP válidos nos pacotes, ou seja, deve usar endereços IP válidos. Pode-se usar um único endereço de alguma máquina que não vai enviar um ACK de resposta porque ela não existe ou por causa de alguma propriedade da rede ou usar vários endereços de uma lista, esperando que as máquinas de alguns desses endereços não respondam, ou o endereço IP da vítima quando as respostas às requisições poderem ser aproveitadas no ataque à vítima. A desvantagem de usar um único IP é que, novamente, pode-se usar um filtro de IPs para evitar o ataque.

# Formas de Ataques

Considerando as vulnerabilidades exploradas nos ataques, classificamos os ataques DoS em dois tipos principais: ataques de protocolo e ataques de força-bruta. Alguns ataques DoS têm características das duas formas de ataque.

## Ataques de Força-Bruta

Esse tipo de ataque é realizado iniciando-se uma grande quantidade de requisições que são aparentementemente legítimas. A ideia é congestionar a rede da vítima com um grande volume de dados, impedindo que ela forneça o serviço de maneira adequada.

## Ataques de Protocolo

Os ataques de protocolo exploram alguma funcionalidade específica ou algum erro de implementação de um protocolo de rede para consumir uma quantidade maciça de recursos da máquina vítima.

# Principais Tipos de Ataques

## UDP Flooding

Esse ataque explora a ausência de apresentação do protocolo UDP, também aproveitada nos ataques de amplificação DNS. Por não requerer essa autenticação, os pacotes UDP possuem um menor cabeçalho, permitindo transferências de dados com menor *overhead*. Como não há um limite estabelecido para a taxa de transmissão e não há especificações sobre o tamanho e formato dos pacotes no UDP, atacantes podem criar pacotes grandes (geralmente por volta de 8 KB), preenchê-los com informações aleatórias e enviá-los rapidamente para portas aleatórias da máquina-alvo. Quando a vítima recebe esses pacotes, ela procura aplicações que estejam monitorando essas portas. Como ela não irá encontrar nenhuma aplicação usando essas portas, ela envia um pacote do ICMP de volta ao endereço IP do remetente que transmite a informação de que o destino desses pacotes não pôde ser alcançado (*destination unreachable*). Com o envio de um número grande de pacotes, a vítima esgota seus recursos recebendo, procurando aplicações usando as portas e enviando as respostas. Para o atacante não receber as respostas, ele pode mascarar seu endereço IP com o endereço de outra máquina qualquer. Além disso, alguns ataques desse tipo utilizam amplificação, utilizando mensagens de resposta de outras máquinas direcionadas à vítima.

## HTTP Flooding

Esse ataque explora as requisições do HTTP (*Hypertext Transfer Protocol*), principalmente as requisições GET e POST para atacar um servidor web. As requisições GET são usadas para obter conteúdo estático, como texto e imagens, do servidor, enquanto as requisições POST são usadas para obter recursos gerados dinamicamente.

O objetivo do ataque é enviar várias requisições de processamento de conteúdo para o servidor, de forma a esgotar os recursos do alvo. Por isso, as requisições POST tendem a ser mais eficientes, uma vez que exigem processamento mais complexo por parte do servidor. No entanto, ataques por requisições GET são mais simples e mais escaláveis se forem distribuídos.

## Ataques *Smurf*

Esse ataque usa o *Internet Control Message Protocol* (ICMP), usado para troca de mensagens de controle, tratamento de erros e diagnósticos de rede. Esse protocolo pode ser usado para verificar se uma máquina da Internet está respondendo, enviando um pacote de “requisição de eco” (*echo request*). Ao receber esse pacote, a máquina responde com um pacote de resposta ao eco (*echo reply packet*). Uma implementação comum desse processo é o comando *ping*, implementado em vários sistemas operacionais e *softwares* relacionados a redes de computadores.

Essa funcionalidade pode ser explorada enviando-se vários pacotes de requisição de eco para o endereço IP de *broadcast*. Um pacote enviado para esse endereço é recebido por um comutador da rede local e retransmitido para todos os computadores dentro da rede local definida por esse endereço, e isso é possível de ser feito por uma máquina dentro ou fora da rede local. Esses pacotes têm o endereço IP do remetente mascarado com o endereço IP da máquina da vítima.

Ao receberem os pacotes de requisição de eco, todas as máquinas da rede local respondem com outro pacote de resposta ao eco. Como são feitas várias requisições, a rede fica congestionada. Além disso, como o endereço IP de remetente das requisições é o endereço da máquina vítima, a vítima recebe as respostas de todos os nós da rede, causando instabilidade e podendo impossibilitá-la de fornecer serviços.

O nome *Smurf* vem de um programa popular para realizar esse tipo de ataque.

## Ataques *Fraggle*

Esses ataques são variantes do ataque *Smurf* para o protocolo UDP (*User Datagram Protocol*). A diferença é que os pacotes UDP, depois de utilizado o *IP Spoofing*, são enviados para a porta 7 do protocolo (porta de eco). Ao receber esse pacote, o comutador da rede local retransmite o pacote de requisição para todos os nós da rede e as respostas são enviadas para a vítima.

## SYN Flooding

Os alvos desse tipo de ataque são máquinas que usam o TCP (*Transmission Control Protocol*), um dos protocolos usados na Internet, na camada de transporte. Esse ataque explora o processo do *handshake*, usado para iniciar uma conexão. Esse processo consiste no envio de três pacotes entre cliente e servidor: SYN, SYN-ACK e ACK. Além disso, o servidor usa uma estrutura de dados chamada *Transmission Control Block* (TCB) para armazenar os dados da conexão em sua memória.

Para estabelecer uma conexão normal, o cliente envia um pacote SYN para o servidor, solicitando a conexão. Ao receber esse pacote, o servidor responde com o SYN-ACK, uma confirmação de recebimento, e reserva um TCB para essa conexão no estado SYN-RECEIVED, que indica que a conexão está parcialmente aberta e que sua validade ainda não foi confirmada. Quando o cliente recebe o SYN-ACK, ele envia o pacote ACK para o servidor, que, recebendo-o, abre a conexão e muda o TCB para o estado ESTABLISHED (conexão estabelecida).

O ataque explora essa funcionalidade enviando vários pacotes SYN para a máquina-alvo, sem enviar os ACKs de resposta. Dessa forma, o alvo armazena TCBs até que sua memória é esgotada, ponto no qual ele não consegue processar mais requisições. Para evitar esse esgotamento que pode parar a máquina, os sistemas operacionais limitam a quantidade de TCBs armazenados no estado SYN-RECEIVED por um valor chamado de *backlog*. Porém, mesmo assim, o ataque impede a formação de novas conexões, pois o limite é alcançado.

A vantagem do SYN Flooding é que ele precisa do envio de menos pacotes do que um ataque de força bruta, uma vez que os TCBs são armazenados por um longo tempo até serem descartados.

## *Ping* da morte

O ataque do *ping* da morte utiliza as funcionalidades de fragmentação e remontagem dos pacotes, usadas na transmissão de dados. O tamanho máximo de um pacote IP, com cabeçalho, é 65535 bytes. A camada de enlace limita o tamanho dos quadros a um valor, que para uma rede Ethernet é de 1500 bytes. Assim, um pacote IP é dividido em vários pacotes IP (fragmentos) e enviados. No *ping* da morte, os dados são manipulados de forma que o receptor dos dados forma um pacote maior que 65535 bytes na remontagem, o que pode estourar *buffers* da memória e afetar variáveis do sistema, travando a máquina vítima.

Em 1996, *hackers* começaram a usar essa funcionalidade quando descobriram que era possível remontar um pacote maior que o limite dado pelo protocolo IP. Na época, muitos sistemas operacionais não tinham programada uma reação para um pacote maior que o limite, então muitos computadores eram vulneráveis. Outra razão para esse ataque ter se tornado popular é a facilidade de execução: só é necessário conhecer o IP da vítima. Já no final de 1997, várias produtoras de sistemas operacionais começaram a divulgar atualizações para evitar esses ataques.

Hoje em dia, a maioria dos sistemas operacionais já possuem medidas de evitar esse ataque, tanto para evitar que um *ping* malicioso cause uma pane no sistema, quanto para evitar que tais pacotes sejam enviados.

## Ataques de Amplificação DNS

O DNS (*Domain Name System*) é um sistema de gerenciamento de nomes para identificação de computadores, serviços ou qualquer recurso, usado na Internet e em redes locais. Ele associa nomes para endereços IP e endereços IP para nomes. Há servidores DNS autoritativos e recursivos. Os servidores autoritativos possuem armazenadas associações entre nomes de domínio e endereços IP, e os servidores recursivos recebem as requisições de um cliente e enviam requisições a outros servidores DNS para descobrir o endereço IP do domínio solicitado.

Em um ataque de amplificação DNS, é enviado um grande número de solicitações para um ou mais servidores de nomes, usando-se um endereço IP de origem mascarado com o IP da vítima. Com o IP de origem mascarado, o servidor envia as respostas à vítima. Essas respostas são de tamanhos maiores que as requisições. Com a adoção das DNSSEC (*DNS Security Extensions*), as respostas dos servidores DNS passaram a carregar chaves criptográficas e assinaturas digitais, o que aumenta o tamanho da resposta. O tamanho da resposta é ainda maior se a requisição for do tipo “ANY”. Tal solicitação solicita todas as informações sobre uma zona DNS, que é a parte de um domínio sob administração de alguma entidade. Dessa forma, mesmo que os atacantes tenham baixas larguras de banda, eles podem causar grandes impactos na máquina-alvo e na rede que ela está utilizando.

Para enviar essas requisições, é usado o protocolo UDP (*User Datagram Protocol*), que não é orientado à conexão, ou seja, que não possui confirmações de entrega e confirmação do remetente por apresentação (*handshake*). O uso desse protocolo combinado com o fato de que há vários servidores recursivos que aceitam requisições de qualquer IP, chamados de resolvedores abertos (ou *open resolvers*), na Internet, torna difícil bloquear esse tipo de ataque.

Fontes usadas:

[16] Jelena Mirkovic, Janice Martin e  Peter Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms  
<http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf>

[23] Wesley M. Eddy, Defenses Against TCP SYN Flood Attacks. Obtido em <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html>

[24] *Request for Comments 4987 – Internet Engineering Task Force (IETF). Obtido em* <https://tools.ietf.org/html/rfc4987>

[25] *Smurf IP Denial of Service Attacks* - DIvisão CERT - Instituto de Engenharia de Software da Universidade Carnegie Mellon. Obtido em http://www.cert.org/historical/advisories/ca-1998-01.cfm?

[26] *DDoS Attacks* - Incapsula. Obtido em https://www.incapsula.com/ddos/ddos-attacks/

[28] David Cornell, *DNS Amplification Attacks* - OpenDNS Security Labs. Obtido em <https://labs.opendns.com/2014/03/17/dns-amplification-attacks/>

[29] Greg Lindsay, *DNSSEC and DNS Amplification Attacks* - Technet (Microsoft). Obtido em: <https://technet.microsoft.com/en-us/security/hh972393.aspx>

[30] Thijs Rozekrans, Javy de Koning, *Defending against DNS reflection amplification attacks*. Obtido em: https://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf

[31] UDP Flood - DDoS Attack Glossary - Incapsula. Obtido em <https://www.incapsula.com/ddos/attack-glossary/udp-flood.html>

[32] *DNS Amplification Attacks* - DIvisão CERT - Instituto de Engenharia de Software da Universidade Carnegie Mellon. https://www.us-cert.gov/ncas/alerts/TA13-088A