Diferenças entre ataque DoS e DDoS

21 DE ABRIL DE 2015

Vemos muitas pessoas que estão começando a estudar métodos hacking cometerem um erro bobo. Muitos sabem que alguns hackers são conhecidos por aplicar ataques DDoS em servidores e acabarem derrubando o site, impedindo que usuários entrem no site atacado.

Mais recentemente tivemos o ataque a PSN (serviço da Sony) e a Live (serviço da Microsoft) aonde seus servidores foram atacados com uma ferramenta do grupo hacker chamado LizardSquad. Ataques DDoS são muito famosos pela internet. Muitos querem saber como aplicar mas acabam se confundindo em dizer que fizeram ataque DDoS com ataques DoS. E você? Sabe a diferença sobre eles?

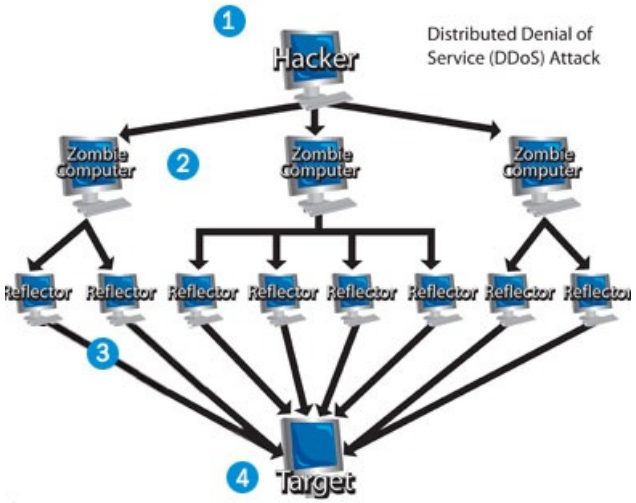
Primeiro vamos começar explicando o que é *'negação de serviço'* (Denial of Service. Mais conhecido como DoS). Um ataque de negação de serviço não é feito para roubar dados pessoais, ele consiste em sobrecarregar o servidor de um site com o envio de muitos pacotes, fazendo assim, muitas requisições de uma só vez para o servidor. Quando o servidor é enxurrado por tantas requisições de uma só vez, ele acaba sobrecarregando e parando de responder as outras requisições feitas. Isto impede de outros usuários se conectarem ao servidor e de ele responder a você. Imagine uma fila em que tem 50 pessoas para entrar em uma loja. Se todas essas 50 pessoas decidirem entrar ao mesmo tempo por apenas 1 porta de entrada, iria causar um congestionamento e dificilmente todos entrariam. Mas vamos supor que mesmo demorando, todos eles consigam entrar. Agora, imagine 300 pessoas tentando entrar ao mesmo tempo por aquela única porta de entrada. Difícil, né? E se acabasse chegando mais gente depois para entrar, elas não conseguiriam ser atendidas do lado de dentro pois nem conseguiriam chegar á porta. Devido a alta demanda de pessoas querendo ser atendidas, ia chegar uma hora em que a loja não iria aceitar mais ninguém querendo entrar e acabaria parando de atender as outras pessoas que chegassem depois. É basicamente isso que acontece quando se aplica um ataque de negação de serviço. Existem muito mais coisa envolvida nestes processos que ocorrem se a gente for estudar a fundo como funciona. Essa foi apenas uma analogia feita para que vocês pudessem entender mais ou menos como funciona.

Agora vamos ás diferenças entre ataques DoS e DDoS.

Ataques DDoS

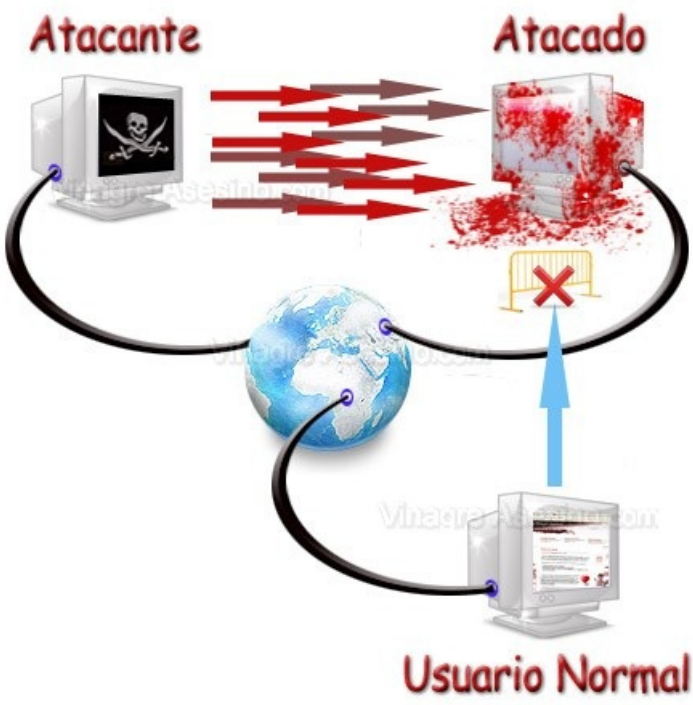
Os famosos ataques DDoS sempre tem um atacante, porém, não é ele que ataca. O atacante geralmente invade o computador de uma vítima e o torna "mestre" de vários outros computadores, que são chamados de "zumbis". Esse ataque geralmente é o mais efetivo na hora de derrubar um site, pois ele acaba tendo um maior "poder de fogo" na hora de atacar a vítima, fazendo milhões de requisições ao mesmo tempo. Isso seria como se tivessem milhões de pessoas clicando no ícone de

atualizar a página ou apertando a tecla F5 para recarregar a página em seus navegadores. Este tipo de ataque também é mais seguro para o atacante já que ele não vai atacar diretamente, ele vai enviar comandos para os computadores mestres e esses computadores mestres vão falar para os computadores zumbis atacarem a vítima, escondendo assim, o real atacante por traz do congestionamento causado no servidor.



Esta imagem acima representa um perfeito esquema de ataques DDoS. Temos com personagem principal o “atacante” que controla seus computadores “mestres”. Estes computadores mestres enviam os comandos para os computadores “zumbis” atacarem a vítima.

Ataques DoS



Por serem parecidos (este é o problema) muita gente confunde na hora de dizer que realizou um ataque de negação de serviço. Ataque DoS são realmente muito parecidos por terem a mesma finalidade e quase o mesmo nome. Então pessoas leigas no assunto podem acabar dizendo de forma

errada, o que é perfeitamente normal. Afinal, ninguém nasceu sabendo de tudo.

O método de ataque DoS é realizado por apenas uma pessoa, o atacante. Ele quem direciona o ataque a tal vítima com o objetivo de derrubar a mesma. Este tipo de ataque é bem fácil de ser prevenido com algumas regras no Firewall pois não é tão complexo de se fazer o ataque e porque dependendo do servidor o atacante não irá conseguir derrubar a vítima. Essa é a principal diferença entre ataques DoS e DDoS.

É necessário também uma internet boa e um computador razoável para poder enviar muitos pacotes ao mesmo tempo para uma vítima.

Então da próxima vez que você fizer um ataque deste tipo, lembre-se de dizer o tipo correto do ataque que você fez.

Como realizar ataques de negação de serviço

Existem muitas ferramentas por aí em vários formatos de arquivos. A maioria são scripts feitos em linguagem Perl. Eu estou publicando aqui a mais nova versão do CannonBytes (0.9.1) que eu mesmo criei. Não é só para divulgar mas também para mostrar como funciona um ataque de negação de serviço. Ela já foi testada e se usada as configurações corretas de ataque, você pode derrubar um servidor pequeno ou local. Esta versão inclui o uso de threads (que é a possibilidade de usar mais de uma função ao mesmo tempo em Perl. Coisa que a linguagem em si não possui) e algumas outras coisinhas. Vale a pena dar uma olhada para saber como funciona um script DoS feito em Perl.

Lembrando que, ataque de negação de serviço é considerado crime aqui no Brasil e em outros países. O atacante estará sujeito as penalidades que lhe forem cabidas caso seja condenado. Ninguém do Ciência Hacker apoia o uso deste tipo de ataques e nem nos responsabilizamos por eventuais ataques feitos por outras pessoas. Eu estou divulgando minha ferramenta para estudo. Conhecimento deve ser livre e de todos!

Link para Github –> GitHub
Link para download no MEGA –> MEGA

Como evitar ser atacado e/ou não ser “mestre” nem “zumbi”

Existem muitos vírus que tornam seu computador “mestre” ou “zumbi”. Uma das maneiras corretas de se evitar isso é nunca baixando arquivos em sites não confiáveis e nunca baixando arquivos com nomes estranhos como: “MyPenis” e “MyBalls”. Esses são nomes de alguns vírus que controlam seu computador para praticar este tipo de ataque.

Caso você ache que seu computador esteja sendo usado como cobaia para ataques, configure bem

seu Firewall e use um bom antivírus.

Agora se você esta sendo vítima de ataques deste tipo, ligue para a empresa de seu provedor e solicite um IP novo e diga que você esta sofrendo ataques DoS ou DDoS que eles podem resolver seu problema, já que ataques deste tipo são direcionados a IPs externos.

Espero que tenha ajudado a tirar dúvidas e a esclarecer como funcionam este tipo de ataque.
Este foi meu primeiro post no site e estou sujeito a críticas construtivas.
Deixem comentários e digam o que gostaram e o que deveria mudar no meu tipo de postagem.

Artigos, DOS / DDOS, Segurança da Informação

DOS DDOS DISTRIBUIÇÃO DE NEGAÇÃO DE SERVIÇO