O que é DoS e DDoS

Na Internet a comunicação é feita através de fluxo de pacotes de dados. Mas o que acontece quando uma máquina emissora envia mais dados do que a maquina destino consegue lidar? A máquina destino irá recusar os novos pacotes, pois ela possui uma enorme quantidade de informação para processar e, portanto, ficará indisponível.
Por isso esse ataque ganhou o nome de Denial Of Services (DoS) que em português significa Negação De Serviços.

Já o Distributed Denial Of Services (DDoS) que em português significa Negação De Serviços Distribuída, é mais potente. Um cracker invade vários servidores e instala um programa para ataques DoS em cada um deles, fazendo dos mesmos maquinas zumbis.
Do computador central, o cracker envia um comando e os Zumbis começam a enviar o máximo de pacotes ao alvo fazendo um ataque sincronizado. Como ele utiliza muitos zumbis o ataque fica muito mais eficiente e dificilmente a vítima não cai. Embora para o ataque se concretizar não seja preciso que a máquina caia, ele apenas deve deixá-la lenta o suficiente para que o cliente abandone o serviço.
Esses ataques ganharam mais importância entre os administradores de redes quando foram usados em grandes sites como a UOL e Yahoo entre outros.

Como surgiu o DDoS

Diz a lenda que o uso de DoS originou-se nas salas de bate-papo do IRC (Internet Relay Chat). Jovens que queriam tomar o controle do canal usavam desse método para sobrecarregar a máquina alheia.

Como funciona o DDoS

Nomenclatura dos componentes de um ataque DDoS segundo Esther, Cicilini e Piccolini:
Atacante: Quem efetivamente coordena o ataque.(na maioria dos casos é um cracker)

Máster: Máquina que recebe os parâmetros para o ataque e comanda os zumbis.

Agente: Máquina que concretiza o ataque DoS contra uma ou mais vítimas.

Vítima: Alvo do ataque. Máquina que é "inundada" por um volume enorme de pacotes, ocasionando um extremo congestionamento da rede e resultando na paralisação dos seus serviços.

Cliente: Aplicação que reside no máster e que efetivamente controla os ataques enviando comandos aos daemons.

Daemons: Processo que roda no zumbi, responsável por receber e executar os comandos enviados pelo cliente.

OBS: (Neste trabalho optei por chamar os agentes de zumbis e muitas vezes me refiro ao atacante como cracker).

Passo 1: Intrusão em massa

É passado um scanner que verifica as vulnerabilidades nos sistemas, o cracker explora essas vulnerabilidades encontradas para obter acesso total nas máquinas.
Depois da invasão, é feita uma lista com os endereços IPs das máquinas violadas para construir a rede do ataque.

Passo2: Instalação de software DDoS

Nessa fase, em cada uma das máquinas é instalado o software necessário para efetuar o ataque propriamente dito. Todavia, antes das ferramentas de automatização do ataque existirem, era preciso que o cracker se conectasse a cada máquina que ele fosse usar para lançar o ataque. Usando um telnet, por exemplo, ele dispararia o comando para causar o flood na máquina alvo. Para tanto, o comando ping nos hosts já serviria.

Uma vez instalado e executado o daemons DDoS, os zumbis anunciam sua presença aos masters e ficam aguardando ordens.O programa DDoS cliente, que roda nos masters, registra em uma lista o IP das máquinas zumbis ativas. Esta lista pode ser acessada pelo atacante.
Com a comunicação automatizada dos masters e dos zumbis são feitos os ataques.

Passo 3: Disparando o ataque

O cracker controla uma ou mais máquinas máster, estas, podem controlar várias máquinas zumbis. É a partir dos zumbis que é disparado o flood de pacotes que concretiza o ataque. Os zumbis aguardam instruções dos masters para atacar uma ou mais vítimas, pelos seus endereços IP's, por um período específico de tempo.

Quando o ataque é ordenado, uma ou mais máquinas alvos são bombardeadas por um imenso volume de pacotes, resultando principalmente na paralisação dos seus serviços.

Outras características do DDoS

Existem ferramentas para apagar os rastros do ataque e tornando-o ainda mais poderoso. Para despistar, esses programas falsificam o endereço de origem do pacote, pois esta é uma deficiência no protocolo da internet.
Logo, todo os sistemas conectados à Internet que estejam equipados com serviços de rede baseados em TCP estão sujeitos ao DDoS.
"Vulnerabilidades do TCP/IP são a chave para o desenvolvimento de novos programas, cada vez mais poderosos nesses ataques".(Nogueira 2001)

FERRAMENTAS DE DDoS

Esther, Cicilini e Piccolini relacionaram em seu artigo: "Tudo o que você precisa Saber sobre os ataques DDoS", as seguintes ferramentas:

1. Fapi (1998) ;

2. Blitznet ;
3. Trin00 (jun/99) ;
4. TFN (ago/99) ;
5. Stacheldraht(set/99) ;
6. Shaft;
7. TFN2K(dez/99) ;
8. Trank ;
9. Trin00 win version.

Trin00

Esta ferramenta lança ataques DoS sincronizados. Ideal para redes de ataque com poucos másters e muitos zumbis.
O máster controla remotamente os zumbis através da conexão TCP. Depois de se conectar, o atacante deve fornecer uma senha.
O máster que está com o Trin00 se comunica com os zumbis pelo UDP usando a porta 27444/udp ou por pacotes TCP na porta 1524/tcp. A senha padrão para usar os comandos é "l44adsl" e somente comandos com a sub string "l44" são processados.

Já a comunicação entre os zumbis com o máster Trin00 é apenas por pacotes UDP, mas em outra porta, a 31335/udp.Quando um daemon é startado, ele diz ao máster que está disponível, mandando uma mensagem "*HELLO*" ao máster, que adiciona o IP desse zumbi a uma lista dos IPs das máquinas zumbis ativas, que ele atualmente controla.

TFN – TRIBE FLOOD NETWORK

Esta ferramenta é usada para ataques DoS sincronizados a uma ou várias máquinas alvo, a partir de várias máquinas zumbis.
Ela torna possível forjar o endereço de origem dos pacotes lançados às vítimas, dificultando assim qualquer tentativa de identificação do atacante.

O máster TFN controla remotamente os zumbis através de comandos executados pelo programa cliente. O estabelecimento da conexão entre o atacante e o cliente pode ser realizado usando um, telnet por exemplo. Não precisa de senha para executar o cliente, mas é necessária a lista dos IPs das máquinas zumbis ativas. A comunicação entre o cliente TFN e os daemons é feita via pacotes ICMP_ ECHOREPLY. Não existindo comunicação TCP ou UDP entre eles.

Stacheldraht (arame farpado em alemão)

É uma combinação das ferramentas Trin00 e TFN, com alguns aspectos próprios, como: criptografia da comunicação entre o atacante e o máster e atualização automática dos zumbis.

A idéia de criptografia da comunicação entre o atacante e o máster surgiu exatamente porque era uma das deficiências encontradas no TFN onde a conexão entre atacante e

máster era completamente desprotegida. O Stacheldraht inclui um utilitário o "telnet criptografado" na distribuição do código.

A atualização dos daemons instalados nos zumbis pode ser realizada instruindo o daemon a apagar a sua imagem e trocá-la por uma nova cópia.

Uma rede Stacheldraht é composta por um pequeno número de masters onde rodam os programas clientes (comumente encontrados sob o nome de mserv, e um grande número de zumbis, onde rodam os processos daemons (comumente encontrados sob o nome de leaf ou td).

Diferencialmente do que ocorre com o Trinoo, que utiliza pacotes UDP na comunicação entre os masters e os zumbis, e do TFN, que utiliza apenas pacotes ICMP_ ECHOREPLY, o Stacheldraht utiliza pacotes TCP (porta padrão 65000/tcp) e ICMP (ICMP_ECHOREPLY).

TFN2K - TRIBLE FLOOD NETWORK 2000

É considerada uma atualização do TFN. Ambas ferramentas foram criadas pela mesma pessoa, Mixter.

O máster controla remotamente os zumbis através de comandos via pacotes TCP, UDP, ICMP ou os três de modo aleatório. Estes pacotes estão criptografados usando o algoritmo CAST.

Diferente do TFN, não existe confirmação (ACK) da recepção dos comandos, a comunicação de controle é em uma única direção. Ao invés do ACK, o cliente envia 20 vezes cada comando confiando em que, ao menos uma vez, o comando chegue com sucesso.

O máster utilizar um endereço IP falso.

A tabela abaixo foi retirada do artigo: “Tudo o que você precisa Saber sobre os ataques DDoS” – por Esther, Cicilini e Piccolini. Ela resume de forma comparativa, como é realizada a comunicação entre as partes de um típico ataque DDoS, para cada uma das ferramentas:

	TRIN00	TFN	STACHELDRAHT	TFN2K
Atacante →Máster	1524/tcp	27665/tcp	icmp_ echoreply	16660/tcp icmp/udp/tcp
Master → Zumbi	27444/udp	icmp_echoreply	65000/tcp	icmp_echoreply icmp/udp/tcp
Zumbi → Master	31335/udp	icmp_echoreply	65000/tcp	icmp_echoreply icmp/udp/tcp

Como detectar o ataque

Existem dois tipos de tráfego que são gerado por DDoS:

- Tráfego de controle (entre o cliente e o servidor).
- Tráfego ´flood´ (entre o servidor DDoS e a vítima).

Para habilitar uma eficiente detecção deve-se procurar por anomalias que possam sinalizar a ocorrência deste tipo de ataque como:

- **Excesso de tráfego**: A utilização da banda excede o seu limite, com número de acessos bem acima do esperado.
- **Pacotes UDP e ICMP de tamanho acima do normal**: As sessões UDP utilizam pacotes pequenos de dados. As mensagens ICMP também são pequenas e não excedem a faixa entre 64 e 128 bytes. Pacotes cujo tamanho seja superior a esses números são considerados suspeitos de conterem mensagens de controle, destinadas a cada um dos zumbis que está participando do ataque. Apesar do conteúdo dos pacotes estar cifrado, o endereço do destino é o correto, desta forma pode-se localizar um dos zumbis que estão realizando o ataque baseado no seu fluxo de mensagens.
- **Ping Of Death ou Ping da Morte**: Consiste em enviar um pacote IP com tamanho maior que o máximo permitido (65500 bytes), para a máquina que se deseja atacar. O pacote é enviado na forma de fragmentos (a razão é que nenhum tipo de rede permite o tráfego de pacotes deste tamanho por causa da Unidade Máxima de Transferência (MTU)) e quando a máquina destino tenta reagrupar estes fragmentos, na maioria da máquinas travam, outras abortam e mostram mensagens de erro, etc.
- **Pacotes TCP e UDP não fazem parte de uma conexão**: Alguns tipos de DDOS utilizam aleatoriamente vários protocolos (incluindo protocolos orientados a conexão) para enviar dados sobre canais não orientados a conexão. Isto pode ser detectado utilizando-se firewalls que mantenham o estado das conexões (statefull-firewalls). Outro ponto importante é que estes pacotes costumam destinar-se a portas acima de 1024.
- **Os tipos de pacotes devem ser analisado:** Se os dados de pacotes recebidos forem em binário e seu destino for diferente às portas de ftp ou de http, estes devem ser descartados.
- **Vários pacotes de um mesmo endereço:** Quando forem enviados vários pacotes com o mesmo endereço IP, estes passam a ser considerados suspeitos.

Ferramentas de detecção específicas de DDoS

O National Infraestructure Protection Center (NIPC) possui uma ferramenta de auditoria, a "find_ddos" que vasculha no filesystem os binários do cliente e daemon das principais ferramentas usadas pelo DDoS, o Trin00, TFN, Stacheldraht e TFN2K.

Como evitar um ataque

“É virtualmente impossível bloquear um ataque DDoS. O que se pode fazer é tentar minimizar seu impacto”. (Nogueira 2001)
Existem precauções simples que podem ser tomadas para reduzir o risco de um ataque de DDoS. Por exemplo, desativar a resposta ICMP para proteger de um ataque do tipo Smurf ou configurar um roteador para filtrar e verificar se um IP recebido de uma fonte externa tem um IP externo (ou vice-versa) para evitar ataques do tipo TFN.

Instalar atualizações, pois os sistemas invadidos para executar ataques DDoS são comumente escolhidos por vulnerabilidades conhecidas. Assim, recomenda-se manter os sistemas sempre atualizados.

Aplicar filtros "anti-spoofing". Durante os ataques DDoS, os intrusos tentam esconder seus endereços IP verdadeiros usando o mecanismo de spoofing, que basicamente consisti em forjar o endereço origem, o que dificulta a identificação da origem do ataque.

“Limitar banda por tipo de tráfego. Alguns roteadores permitem limitar a banda consumida por tipo de tráfego na rede. Nos roteadores Cisco, por exemplo, isto é possível usando CAR (Commited Access Rate). No caso específico de um ataque DDoS que lança um flood de pacotes ICMP ou TCP SYN, por exemplo, você pode configurar o sistema para limitar a banda que poderá ser consumida por esse tipo de pacotes”.(Esther,Cicilini, Piccolini 2000)

Prevenir que a rede seja usada como "amplificadora". O envio de pacotes a endereços de broadcasting faz com que esses pacotes sejam enviados para todos os hosts da rede. Os roteadores devem saber controlar o recebimento de pacotes endereçados a tais endereços.

Tipos de Ataques de DDoS

Consumo de Largura de Banda:
Ou o atacante possui uma banda maior que a da vítima, ou ele utiliza outros computadores para que juntos, disparem o ataque, amplificando seu efeito e consumindo a largura de banda do computador vítima.

Consumo dos Recursos
Esgotando os recursos do sistema, como memória, cpu , etc., os processos irão travar e o sistema para.

Ataques a Servidores de Nomes de Domínios (DNS) e a Roteadores
O atacante manipula a tabela de roteamento para negar serviço a quem consultá-la, explorando as falhas dos protocolos de roteamento. Com isso, o atacante pode direcionar todo tráfego para a máquina dele, ou mesmo para uma rede que não existe (buraco negro). O ataque a DNS também permite redirecionar o tráfego. Contudo, esses ataques, em sua maioria, consistem em armazenar endereços falsos servidor da vítima.

Exemplos de Ataques DDoS

SMURF

O ataque Smurf é um dos mais perigosos. Envolve uma vítima, um atacante e uma rede auxiliar, funcionando da seguinte maneira: são enviados pacotes ICMP echo para a rede auxiliar. Só que a origem desses pacotes é forjada como sendo o endereço da vítima e quando os pacotes chegam a rede auxiliar, eles são multiplicados e, portanto, a vítima será inundada com quantos pacotes forem ecoados na rede.

SYN FLOOD

Para compreender este ataque é preciso entender primeiro como funciona uma conexão TCP entre duas máquinas A e B, esta é realizada em 3 etapas. Primeiro, a máquina A envia um pacote SYN (pedido de conexão) para a máquina B. A máquina B então responde com um outro pacote SYN/ACK que ao chegar a máquina A, reenvia um pacote ACK e então a conexão é estabelecida. A vulnerabilidade que é explorada é que os sistemas alocam uma quantidade finita de recursos para cada conexão em potencial. E mesmo que um servidor seja capaz de atender a muitas conexões concorrentes para uma porta específica (a porta 80 por exemplo), o que o atacante explora é que apenas um pequeno número de conexões potenciais são tratáveis. Para iniciar o ataque, o cracker envia um pacote SYN com origem falsa (buraco negro), o que deixará a vítima procurando por algum tempo de onde veio esse SYN para lhe enviar o pacote SYN/ACK. Sendo assim, esta possível conexão fica aguardando na fila, que é limitada. Sendo assim, o atacante enviando vários pacotes SYN falsificados em um curto espaço de tempo, a vítima lotará sua fila e com certeza negará o serviço a outras solicitações mesmo que sejam autênticas.

Considerações Finais

O DDoS não dá ao atacante acesso aos dados da vítima, ele é utilizado para impedir acesso de usuários legítimos ao sistema. Então porque eles seriam usados hoje em dia?
Suponhamos que um indivíduo seja exposto em um site,e ele passe a odiar esse site tanto que queria ver ele offline, se ele não for um hacker provavelmente não sabe como fazer isso. Então ele paga pra um hacker fazer isso.

Na Internet ocorre bastante guerra entre sites. Por exemplo entre portais rivais.
O administrador de um site paga um hacker derrubar o site do rival e assim os acessos do rival offline vão logicamente para o que está online. Com isso eles faturam mais grana dos patrocinadores uma vez que eles aumentam seus acessos!
Enquanto existirem concorrência e pessoas mal intencionadas, os ataques DDoS também existirão.

Sites Relacionados

- ALR-01/2000: Recentes ataques de DoS
  por CAIS - Centro de Atendimento de Incidentes de Segurança
  http://www.rnp.br/arquivos/ALR-012000.txt

- Lockabit - Portal de Segurança da Informação
  http://www.lockabit.ufrj.br

- CERTs (http://www.cert.org ou http://www.cert-rs.tche.br)

Bibliografia

- CICILINI, Renata & PICCOLINI, Jacomo & ESTHER, Liliana - "Tudo que você precisa saber sobre os ataques DDoS" (2000).
- NOGUEIRA, José – "Ataque DDoS: ninguém está a salvo" (2001).
- MAIA, Luiz Paulo – "Ataques Distributed Denial of Service (DDoS)"

Distributed Denial Of Services (DdoS)

Aluno: George Hilton de Andrade Frey
Professor: Marco Antônio
15 de outubro de 2003