Capítulo 11

DoS - Denial of Service

DDoS - Distributed Denial of Service

DRDoS - Distributed Reflection Denial of Service

DoS

- Principio de funcionamento do DoS é o consumo dos recursos do sistema;
- Tem como objetivo tirar de atividade um serviço ou um servidor por completo;
- Permite que um cracker deixe um sistema inutilizável ou consideravelmente lento para os usuários legítimos;
- Podem explorar falhas dos protocolos ou utilizar força bruta para inundação (flooding).

DoS

- Locais
- Remotos

DoS Remotos

- Flood de pacotes
  - Ataques Diretos;
  - Ataques com Spoofing;
  - Ataques em Loop.
- Excesso de conexões em determinados serviços;

DoS – Ataques Diretos

- Flood de pacotes em que o atacante inunda o servidor com pacotes, utilizando o IP real de sua maquina.

DoS – Ataques com Spoofing

- Flood de pacotes em que o atacante inunda o servidor com pacotes, utilizando uma técnica de geração de um IP de origem falsificado.

DoS – Ataques em Loop

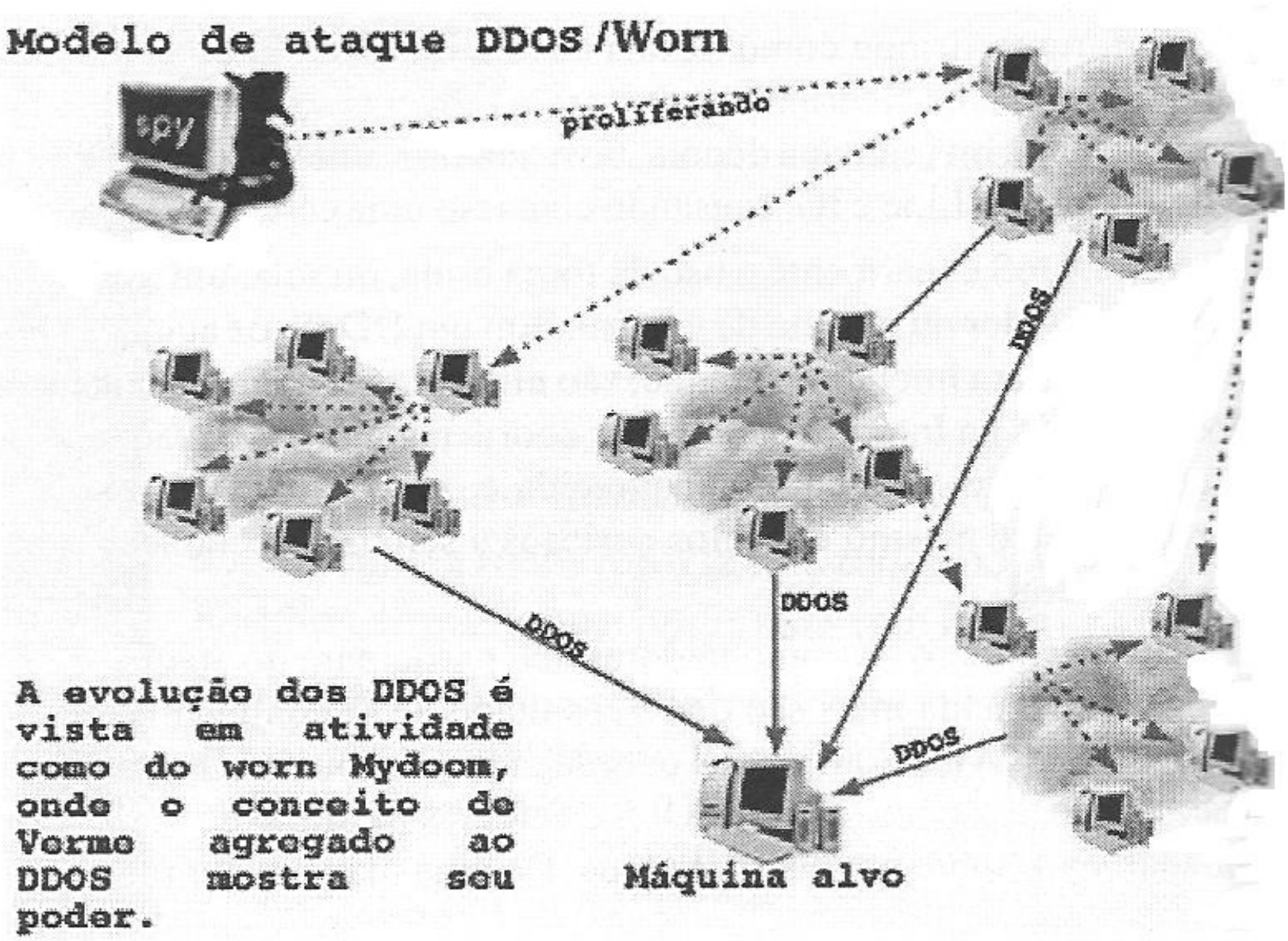
- Flood de pacotes utilizando IP Spoofing, mas com a característica de que o IP falsificado recebe o endereço igual ao do destino (alvo);

DoS – Ataques Diretos

- Beer;
- Kkill.c

DoS – Ataques com Spoofing

- 1234;
- Bloop.c;
- Jolt.c;
- Jolt2.c;
- Nestea.c;
- Newtear.c

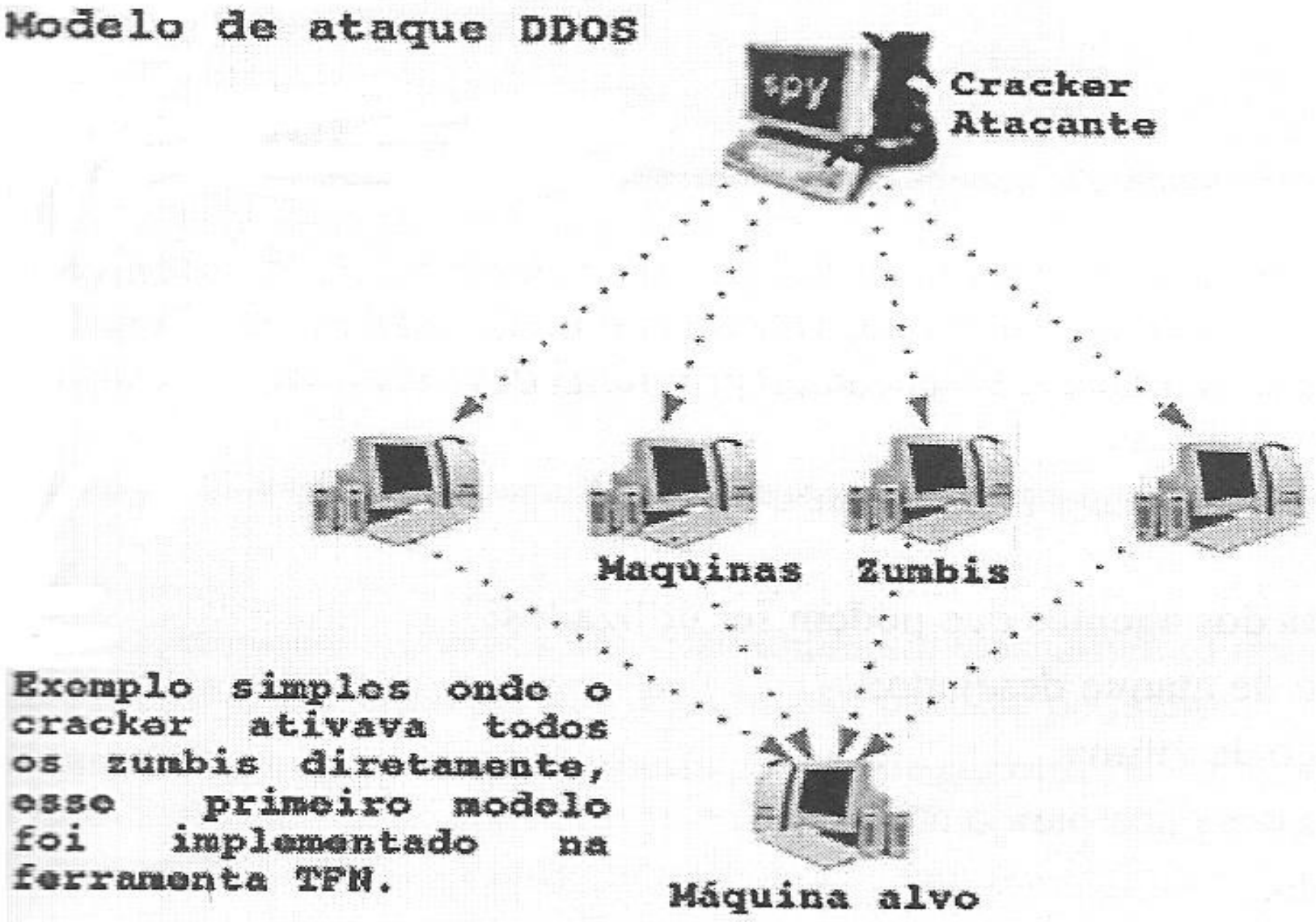


um ataque DDoS combinado com a técnica de worm

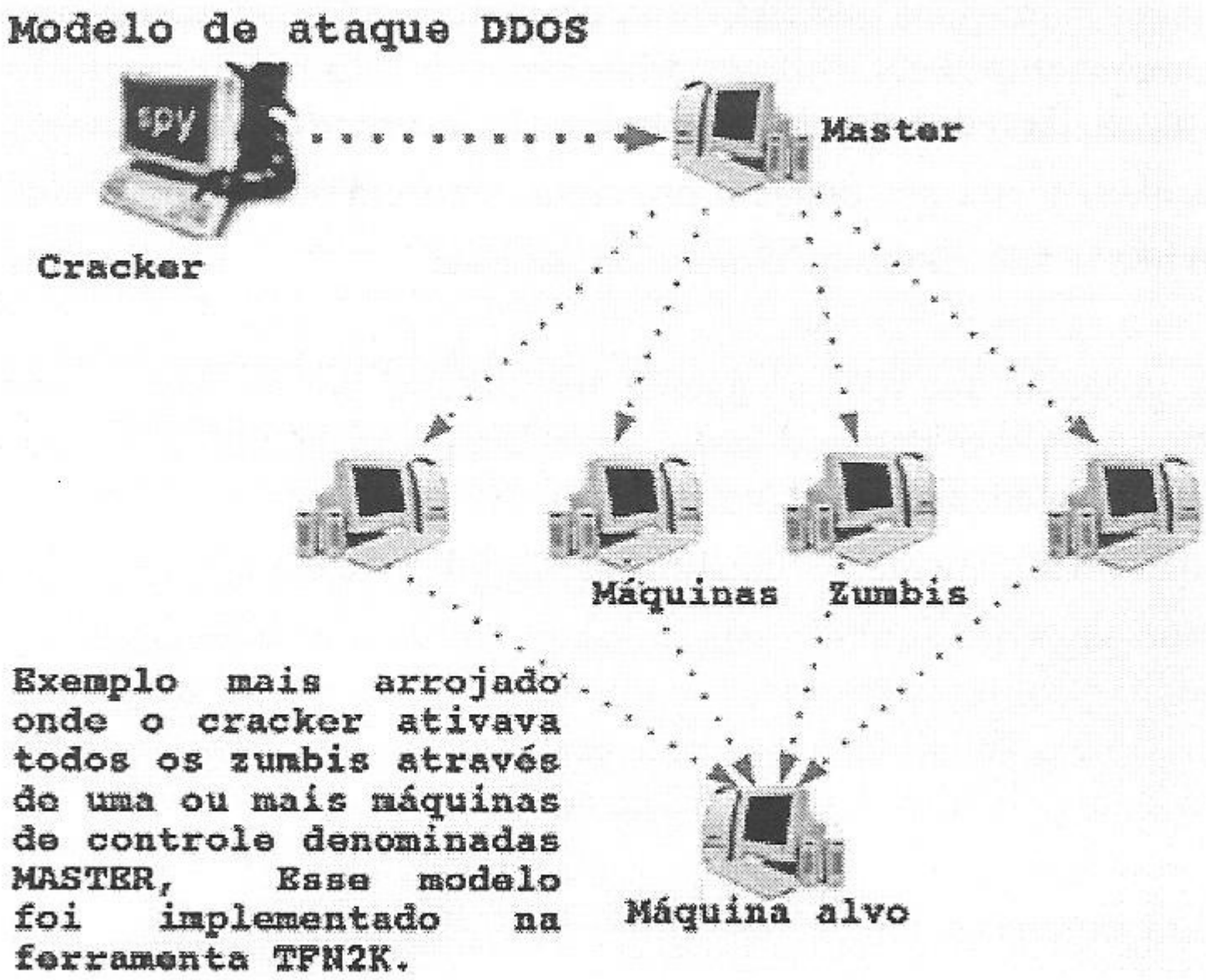
Ferramentas de DDoS

- Fapi – 1998;
- Blitznet – 1999;
- Trin00 – 1999;
- TFN (Tribe Flood Network) – 1999;
- Stacheldraht – 1999;
- Shaft – 1999;
- TFN2K – 1999
- Trank
- TFN

} **Windows**

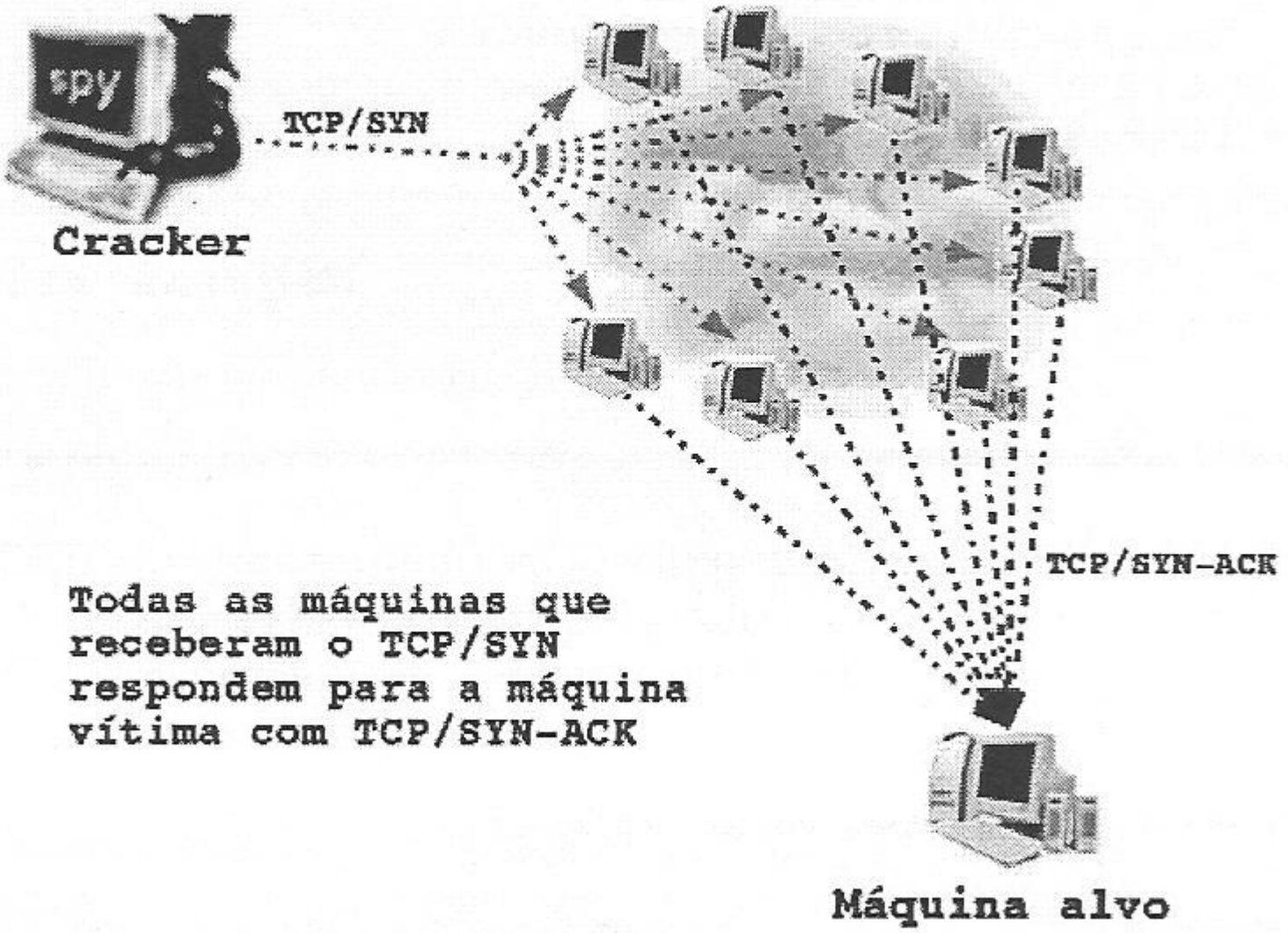


Um ataque DDoS em 3 camadas.

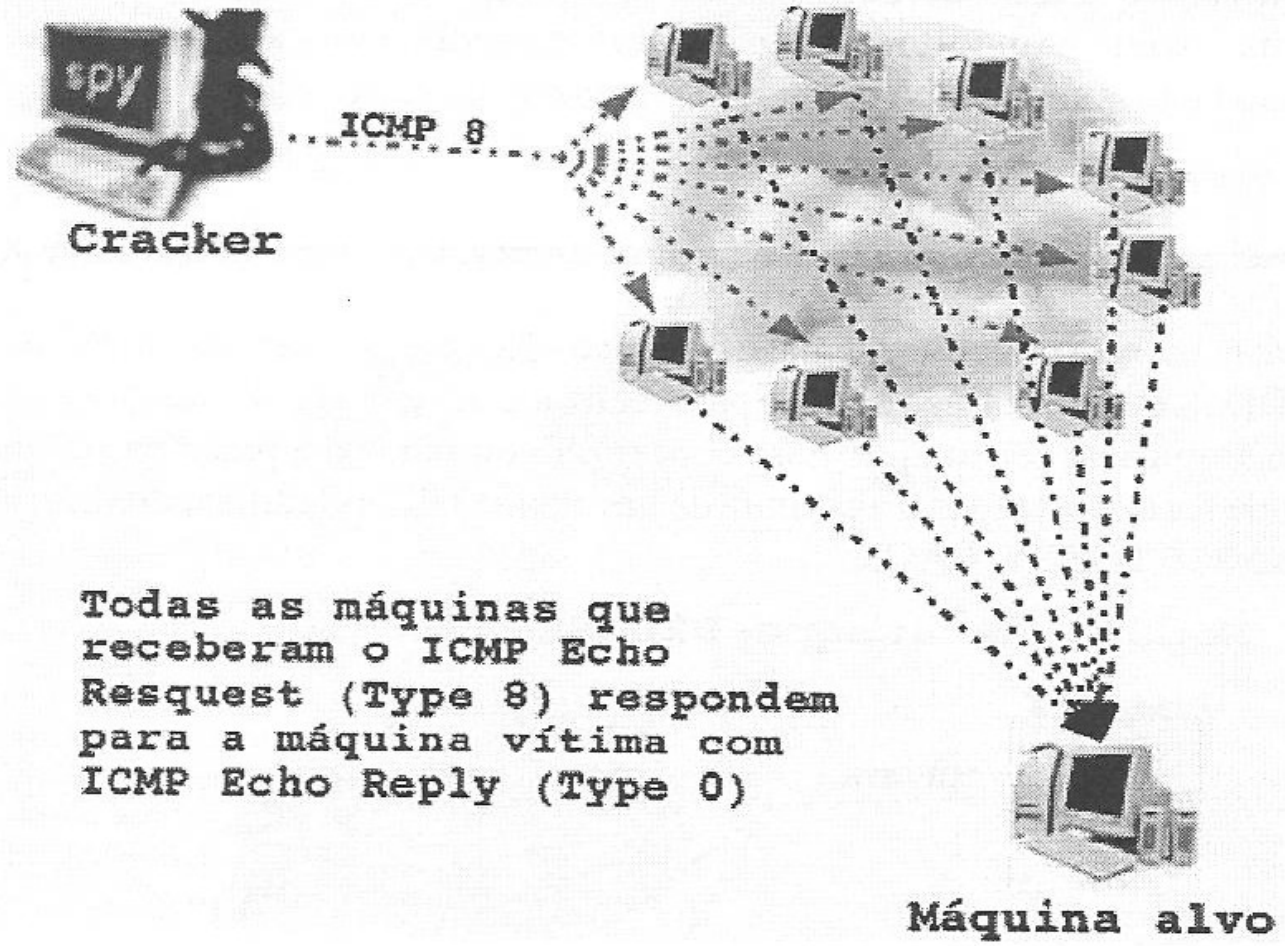


Um ataque DDoS em 4 camadas.

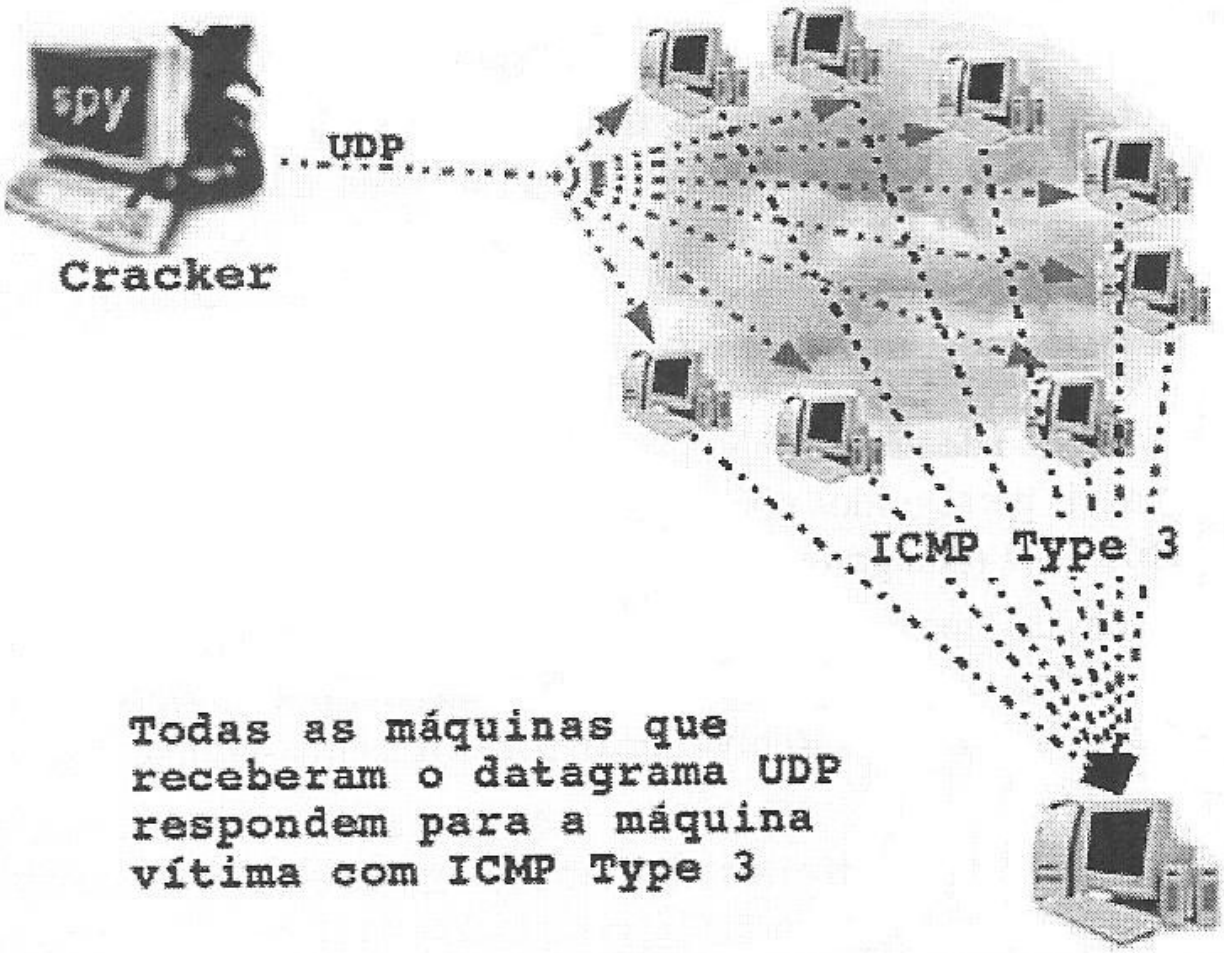
Modelo de ataque DRDOS



Modelo de ataque Smurf



Modelo de ataque Fraggle



Todas as máquinas que receberam o datagrama UDP respondem para a máquina vítima com ICMP Type 3

Contramedida

- Estabelecer uma política de segurança rígida em relação as atividades dos usuários;
- Configurar o roteador de perímetro para filtrar trafego recebido e enviado, controlando ataques com inundação de pacotes ICMP e TCP/ SYN;
- Manter o ambiente atualizado para proteger a maquina de ataques vinculados a vulnerabilidade da pilha TCP/ IP, que o S.O. utiliza;
- Configurar o Firewall com política bem planejada, para evitar ataques DoS;