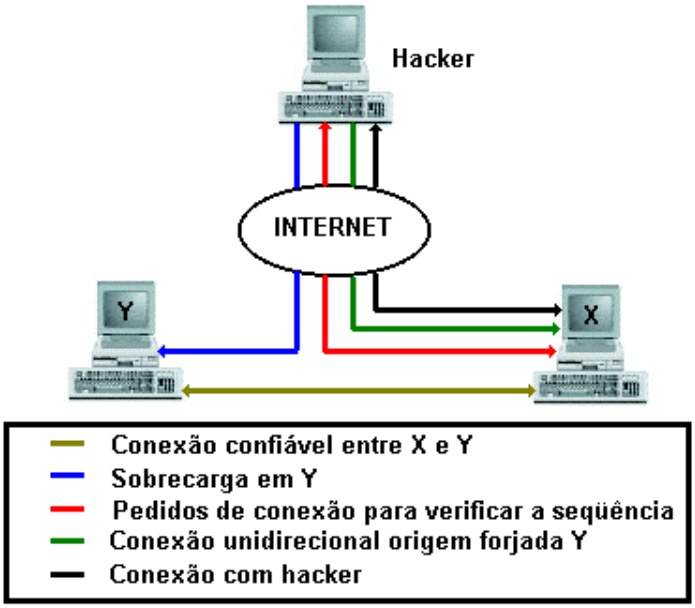
Ataque de Dicionário

- Trata-se de um ataque baseado em senhas que consiste na cifragem das palavras de um dicionário e posterior comparação com os arquivos de senhas de usuários.

IP Spoofing

- Falsificação de endereço IP
- Utilizada em conjunto com outros ataques para esconder a identidade do atacante.
- Consiste na manipulação direta dos campos do cabeçalho de um pacote para falsificar o número IP máquina que dispara a conexão.
- Quando um host X quer se conectar ao host Y, a identificação é feita através do número IP que está no cabeçalho
- Se o IP do cabeçalho enviado pelo host X for falsificado (IP de um host hacker), o host Y acredita estar falando com o host X



Os pacotes IP possuem um endereço destino e um endereço origem. Normalmente o endereço origem reflete a realidade, mas nada impede que um hacker altere este pacote para que ele pareça ter vindo de outro lugar.

Além de enganar o destino, neste caso o computador X, é necessário que se sobrecarregue o computador Y, para que ele não responda às mensagens de X, pois isso poderia cancelar a conexão.

Faz-se necessária, ainda, uma "previsão" do número de seqüência mandado por X. Este número é enviado por X ao originador da conexão (supostamente o Y). Mas Y não irá responder, devido à sobrecarga explicada anteriormente. Então o hacker deve prever o número de seqüência mandado por X para que seja enviado um novo pacote com estes números de seqüência, fingindo novamente ter sido enviado por Y, e forjando a autenticação.

A previsão deste número de seqüência é um processo demorado e criativo. Durante a negociação da conexão, os computadores trocam informações para efetuarem o "handshake" ou "aperto de mão". Dentre as informações trocadas estão os números de seqüência, que devem ser repetidos para o destino, para que este se certifique da autenticidade da conexão.

O que o invasor faz é o seguinte: enviar, através de um pacote legítimo e com o endereço de origem verdadeiro, vários pedidos de conexão à X. Este responde com um número de seqüência para que o invasor o repita e efetue a conexão, mas a máquina de origem (invasor) não tem privilégios e não lhe interessa fechar esta conexão. Então ele não responde a estes pacotes de X, apenas os guarda e verifica seu número de seqüência.

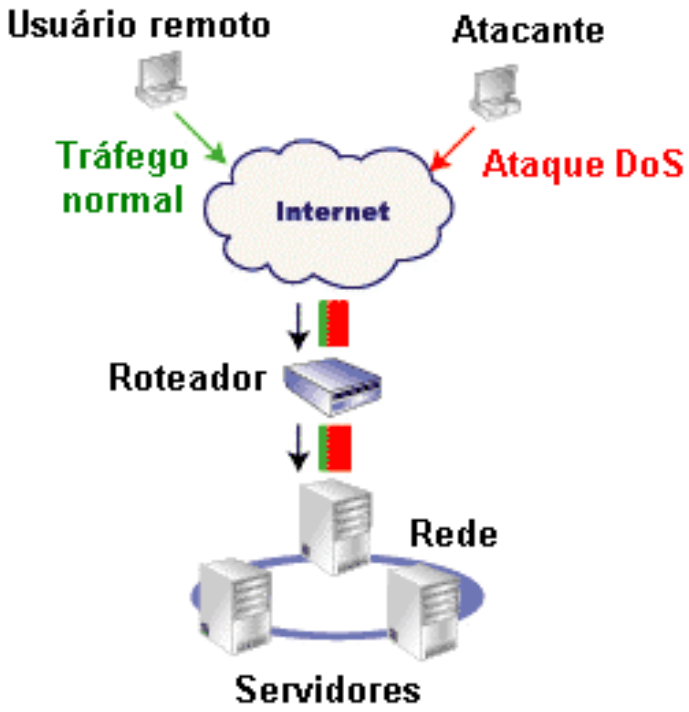
Após vários pedidos de conexão com X, o invasor pode "aprender" como X gera seus números e então mandar um pedido de conexão, desta vez com o endereço de origem sendo Y (o computador confiável). Obviamente, o invasor não vai receber os pacotes de X com os números de seqüência, pois estes irão para o endereço de origem (computador Y) que nesse momento deve estar sobrecarregado. Com base nos cálculos anteriores, o invasor prevê e manda o número de seqüência correto para o computador X, fechando a conexão.

Ataque de Negação de Serviços

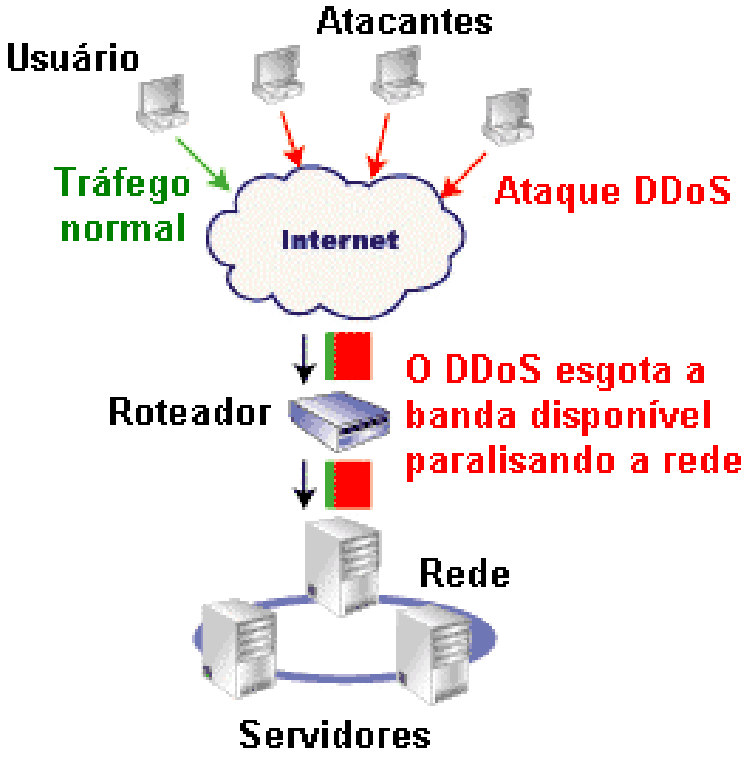
Os ataques de negação de serviço DoS (Denial of Service) têm como objetivos:

- Paralisar um serviço em um servidor;
- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível.

- **Denial of Service (Dos)**: Neste ataque, apenas uma máquina estranha a rede ataca a máquina alvo.



- **Distributed Denial of Service (DDos)**: Este ataque utiliza várias máquinas em conjunto para atacar uma máquina alvo. O objetivo do ataque é esgotar algum recurso da máquina alvo.

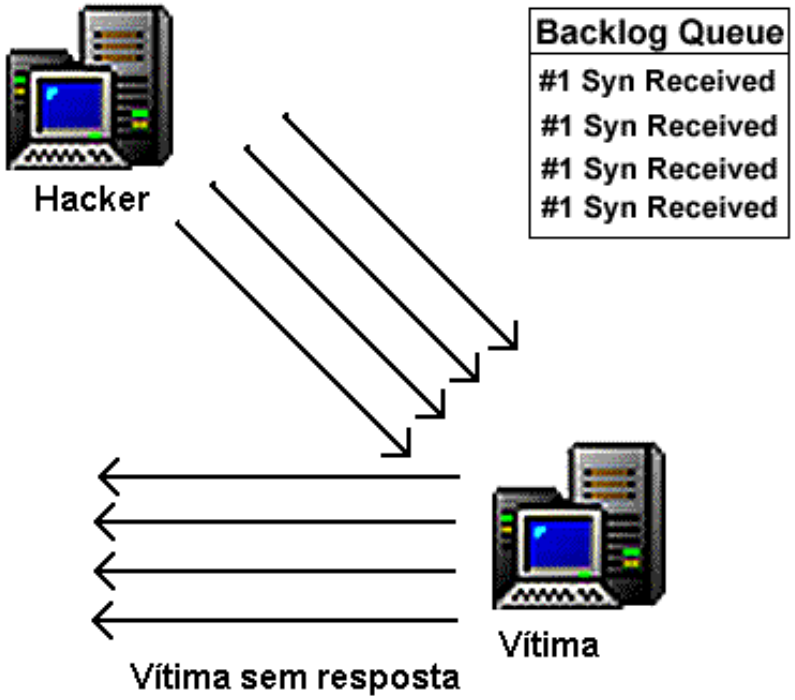


Vulnerabilidades Exploradas

- Falhas em softwares
- Falhas de Protocolo
- Esgotamento de recursos

SYN Flood

- Consiste no envio de um grande número de pacotes de abertura de conexão, com um endereço de origem forjado (IP Spoofing), para um determinado servidor.
- O servidor ao receber os pacotes, coloca uma entrada na fila de conexões em andamento, envia um pacote de resposta e fica aguardando uma confirmação da máquina cliente.
- Como o endereço de origem dos pacotes é falso, a confirmação nunca chega ao servidor.
- A fila de conexões no servidor fica lotada e, a partir daí, todos os pedidos de abertura de conexão são descartados e o serviço paralisado.
- A paralisação persiste até o tempo para o o servidor identificar a demora e remover a conexão em andamento da lista.



Ataque de LOOP

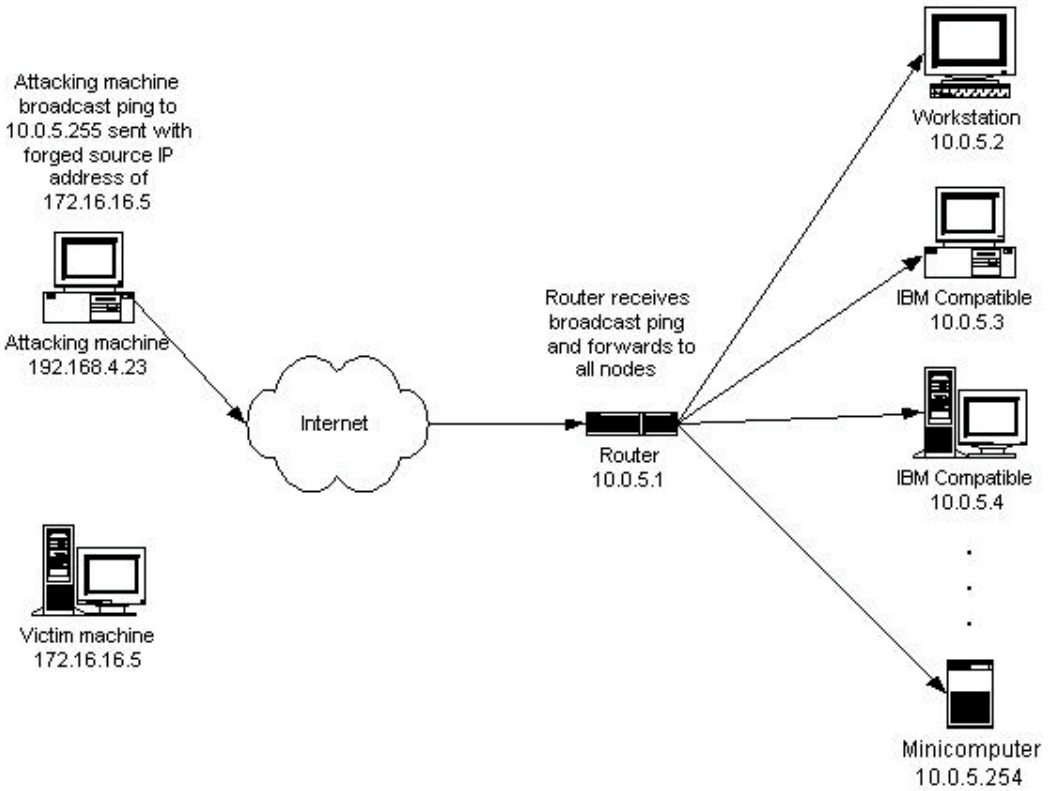
Consiste em mandar para um host um pacote IP com endereço de origem e destino iguais, ocasionando um loop na tabela de conexões de uma máquina atacada.

Ataques via ICMP

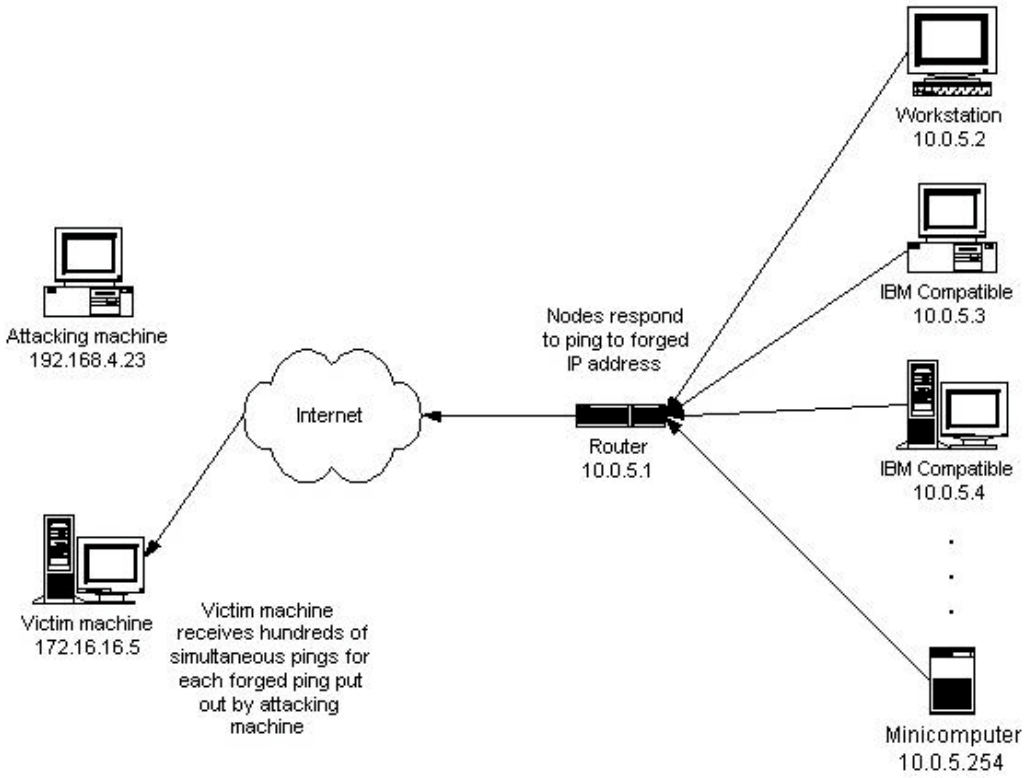
- O protocolo ICMP (Internet Control Message Protocol) é utilizado no transporte de mensagens de erro e de controle.
- O ICMP não tem garantias se a informação recebida é verdadeira, e por este motivo, um atacante pode utilizar as ICMP para interromper conexões já estabelecidas.

Ataque de Ping (Smurf Atack)

- Envia pacotes ICMP de echo request para um endereço de broadcast da rede



- Redireciona todas as respostas (através de IP Spoofing) para a máquina atacada, causando um volume grande de conexões de *echo reply* para a mesma.



Ataque de Ping of Death

- Consiste em enviar um pacote IP com tamanho maior que o máximo permitido (65.535 bytes) para a máquina atacada. O pacote é enviado na forma de fragmentos (porque nenhuma rede permite o tráfego de pacotes deste tamanho).
- O dano é causado quando uma máquina destino tenta montar os fragmentos.