Negação de Serviço, Negação de Serviço Distribuída e *Botnets*

Gabriel Augusto Amim Sab, Rafael Cardoso Ferreira e Rafael Gonsalves Rozendo

Engenharia de Computação e Informação - UFRJ

EEL878 – Redes de Computadores I (DEL) – 2013.1

Professor Otto Carlos Muniz Bandeira Duarte

1. Introdução

Conceitos

- O que é Negação de Serviço?
- O que é Negação de Serviço Distribuído?
- O que são *Botnets* ?

1. Introdução

Denial of Service (Negação de Serviço)

•Ataques DoS (Denial of Service), que são também conhecidos como ataques de negação de serviços, são ataques à computadores – como por exemplo, servidores WEB – que tem como objetivo torna-los indisponíveis para seus usuários.

•Normalmente, esses ataques se utilizam de vulnerabilidades no sistema de algum servidor, para que ao se fazer um grande número de requisições, os recursos do servidor, como banda ou memória, sejam esgotados e assim, os serviços prestados pelo servidor, se tornem não mais acessíveis.

1. Introdução

Distributed Denial of Service (Ataque Distribuído de Negação de Serviço)

- Ataques DDoS (Distributed Denial of Service), também conhecidos como ataque distribuído de negação de serviço, são ataques como os DoS, porém, muito mais potentes, uma vez que estes utilizam não somente uma máquina para atacar, mas dezenas, centenas e as vezes, até milhares de computadores, todos acessando um único servidor ao mesmo tempo.

1. Introdução

Botnets

- Para se entender o conceito de *botnet*, inicialmente deve-se entender o conceito de *bot*. Dizemos que um computador é um *bot* – abreviação da palavra em inglês *robot* – quando ele é infectado por algum software mal-intencionado. Esse software adquire controle sobre certas funções do computador, sem que o usuário saiba, e pode fazer com o que o computador execute tarefas via internet.

- Quando falamos em botnets, falamos em grandes quantidades de computadores infectados (bots), de tal forma que eles formem uma rede. Essa rede é controlada por um computador (chamado de mestre). Com a rede sobre seu controle, é possível manipula-la, e utiliza-la para que ataques sejam cometidos.

1. Introdução

Rápido Histórico

- Final do anos 80 - ataques dos usuários do *AOL* e *IRC*
- Meio dos anos 90 – *WinNuke* e *Teardrop*
- Após se descobrir como se defender deles, os ataques começaram a se basear em inundar a banda de um servidor
- *Smurf Attacks (*Ataques utilizando *ICMP)*
- Por volta do ano 2000 – *Synfloods*
- Dias de hoje – ataques em escala global *(ex: Grupo Anonymous)*

2. Ataques

- Ataques por inundação (*flood attacks*)

  Envio contínuo e constante de pacotes até que a banda ou os recursos físicos do sistema alvo sejam completamente utilizados, impedindo pacotes legítimos de chegarem à vítima ou serem enviados pela mesma

- Ataques por amplificação

  Requisições são enviadas a vários sistemas pertencentes à rede a partir de um endereço IP mascarado. Tais requisições levam aqueles que as recebem a enviar a resposta ao endereço IP da vítima do ataque

- Ataques por exploração de protocolos

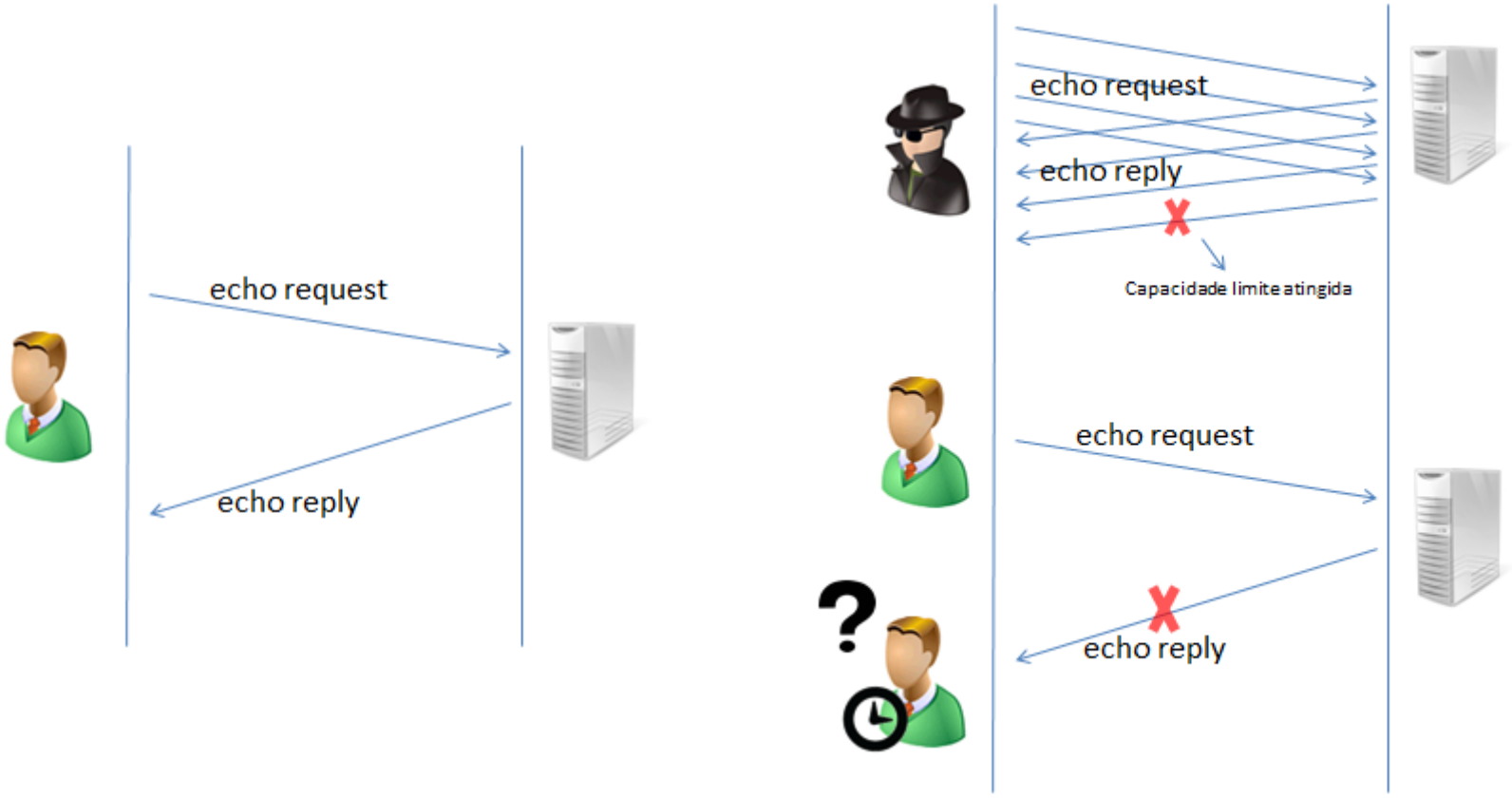
  Alguma característica ou falha de implementação de algum protocolo utilizado pelo alvo é explorada a fim de gerar um consumo excessivo dos recursos do mesmo

2. Ataques

Inundação por ICMP (*ICMP flood*)

- Também chamado de *ping flood*
- Atacante envia continuamente, a partir de um IP mascarado, uma grande quantidade de *echo requests* a fim de ultrapassar o limite de *requests* por segundo do alvo
- Ultrapassado esse limite, *requests* legítimos passam a ser ignorados
- Condição: banda do atacante >> banda do alvo (ex.: DSL vs *dial-up*)

2. Ataques

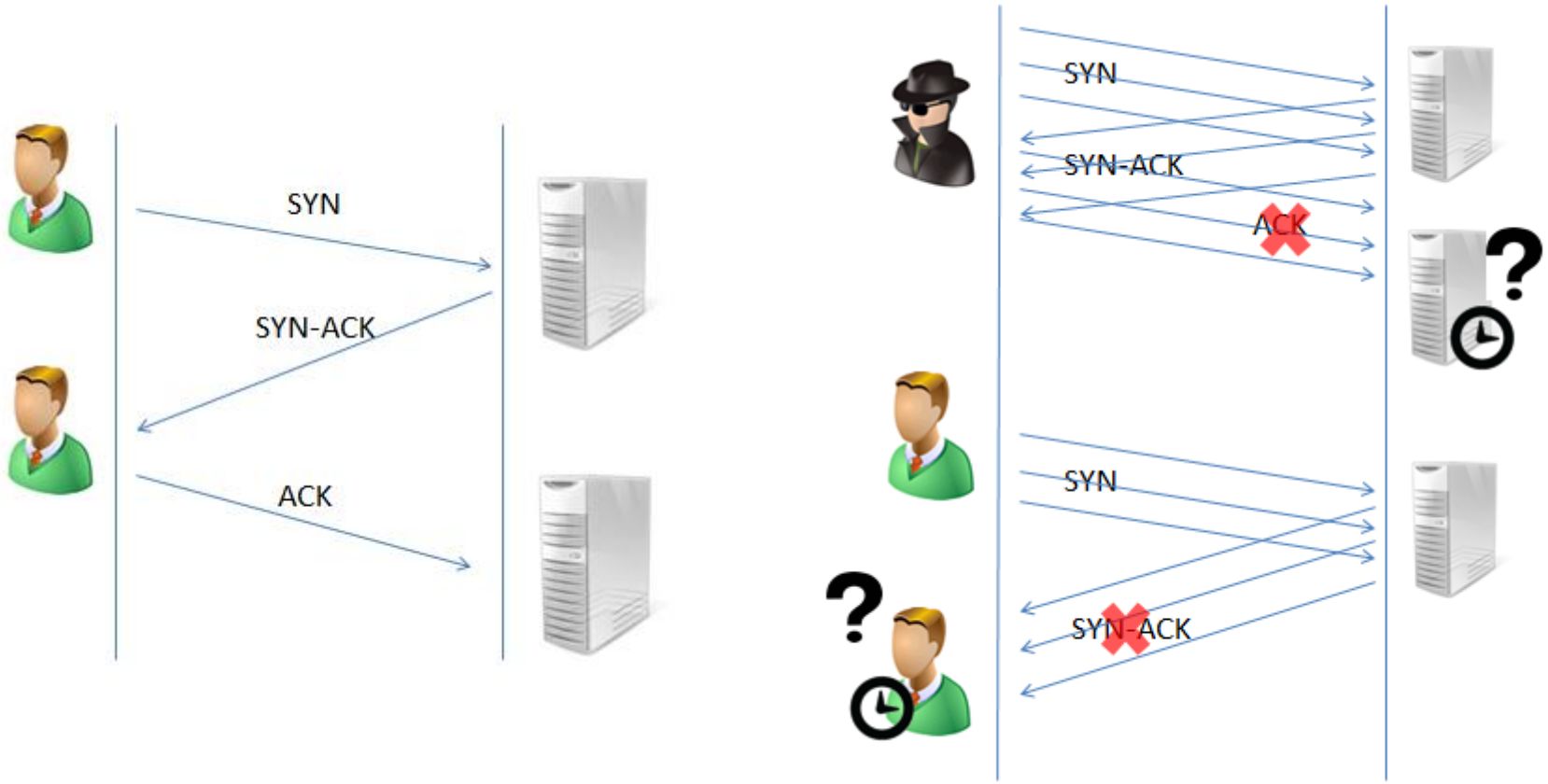

echo request
echo reply
echo request
echo reply
Capacidade limite atingida
echo request
echo reply

2. Ataques

Inundação SYN (*SYN flood*)

- Atacante inunda o alvo a partir de um IP mascarado com pacotes SYN
- Sistema alvo aloca determinada quantidade de memória, destinada à nova conexão prestes a ser estabelecida
- Sistema alvo envia pacotes SYN-ACK e espera por pacotes ACK como resposta para iniciar efetivamente a conexão
- Os pacotes ACK nunca são enviados à vítima
- Memória do alvo é completamente alocada, apenas com conexões parciais
- Impossível estabelecer novas conexões legítimas
- Atacante tem acesso a arquivos do alvo por meio das conexões parciais

2. Ataques

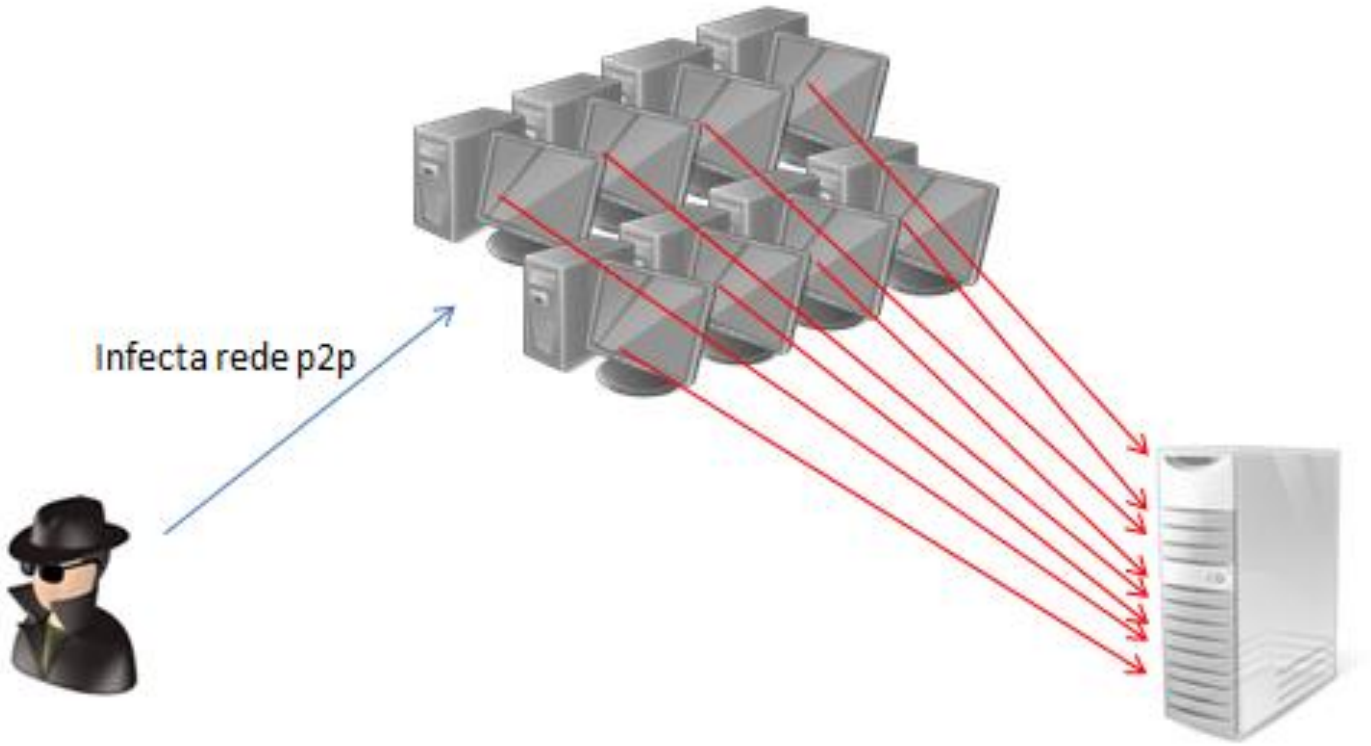


2. Ataques

Ataques *peer-to-peer*

- Atacante infecta rede p2p e passa a enviar instruções aos clientes da mesma
- Clientes se desconectam da rede e enviam requisições de conexão ao alvo do atacante
- Alvo é inundado

2. Ataques

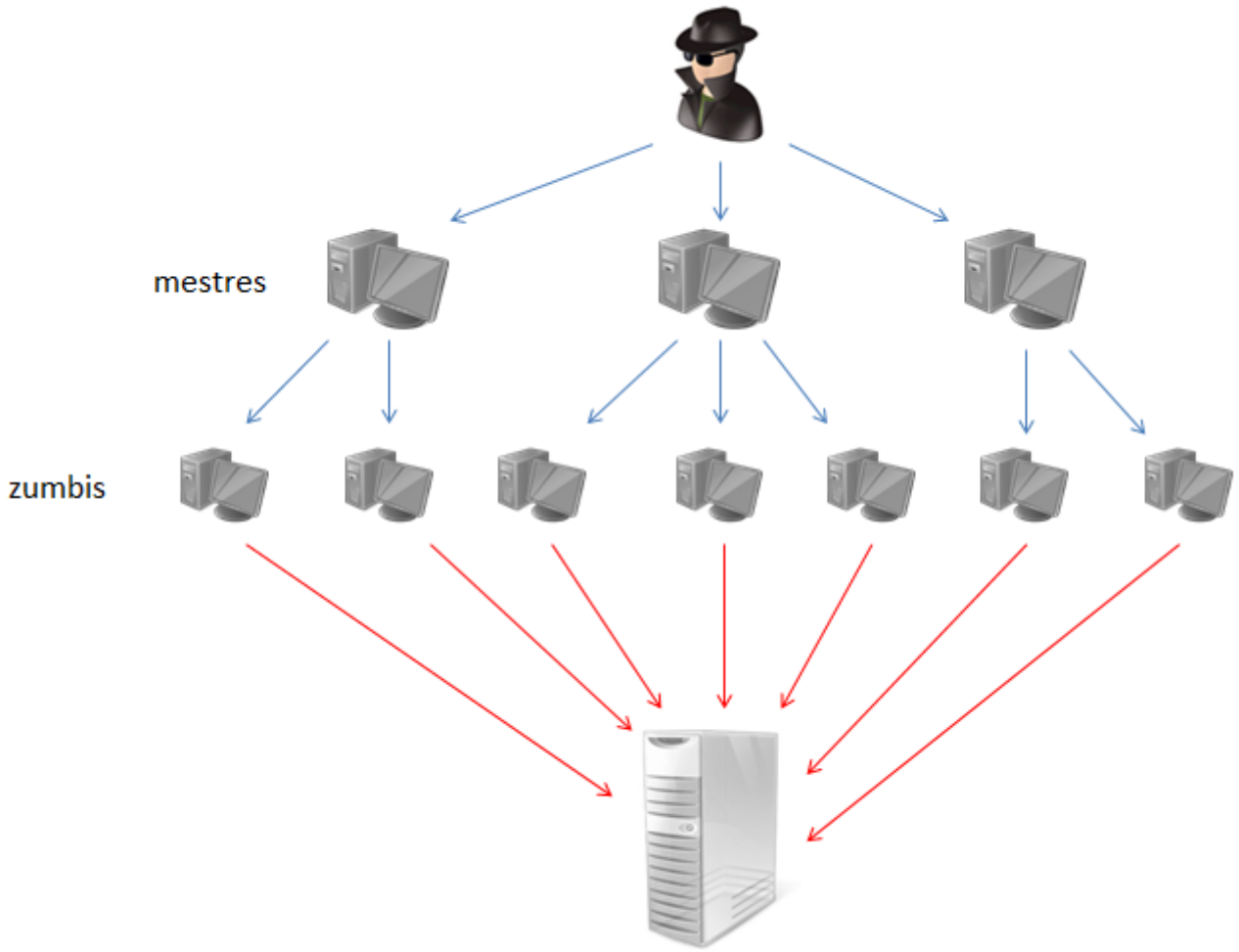


2. Ataques

Ataques distribuídos (DDoS)

- Atacante estabelece uma *botnet* por meio de um *malware* (ex.: *MyDoom*) ou *trojan*
- Com ou sem interação direta do atacante, instruções passadas aos *masters* fazem os mesmos instruírem os “zumbis” a efetuar o ataque
- Maior facilidade para geração de tráfego intenso
- Maior dificuldade para anulação do ataque

2. Ataques



2. Ataques

Ferramentas de execução

- *Stacheldraht*
  - Escrito em C para sistemas *Unix* e *Solaris*
  - Cria *botnets* para ataques DDoS
  - Geração automática de endereço IP mascarado
  - Inundação por UDP, inundação por ICMP, inundação SYN

- *trin00*
  - Conjunto de programas para execução de ataques DDoS por meio de botnets
  - Scripts executados em máquinas já afetadas automaticamente detectam e infectam novas máquinas
  - Máquinas infectadas atuam como *masters* ou *daemons*

2. Ataques

Como efetuar um ataque

- Alvo
  - Motivação
  - Determinar o alvo
  - Viabilidade de um ataque efetivo
- Planejamento do ataque
  - Determinar a forma e o tipo de ataque
  - Ferramenta(s) a ser(em) utilizada(s)
- Estabelecimento da rede de ataque
  - Determinar de que maneira, especificamente, a ferramenta escolhida será utilizada para executar o ataque (hora, data etc). Se o ataque exigir o estabelecimento de uma botnet, por exemplo, primeiro deve-se criá-la
- Atacar

3. Defesa

Considerações iniciais

- A defesa contra ataques de negação de serviço definitivamente não é uma tarefa simples. Entre os motivos estão o grande número de máquinas envolvidas e dificuldade de rastreamento devido à utilização de endereços IP forjados

- Medidas preventivas podem ser muito caras ou até mesmo inviáveis

- Medidas reativas podem ser trabalhosas, pouco eficientes e críticas, no sentido de que devem ser realizadas o mais rápido possível

3. Defesa

Medidas preventivas

- Prevenção contra ataques: eliminar a possibilidade da ocorrência do ataque. Isto se dá basicamente com o aumento da segurança do sistema, como remoção de bugs, atualização de protocolos etc.
  - Uma máquina segura é uma máquina que não sofrerá com ataques nem será utilizada para ataques distribuídos.

- Prevenção contra negação de serviço: possibilitar que a potencial vítima resista ao ataque sem negar serviço aos clientes legítimos.
  - Aumento de recursos: apenas dificulta o sucesso de um ataque. Pode ser uma solução muito cara, porém eficiente se o ataque passar a se tornar muito custoso.
  - Policiamento de recursos: gerencia a utilização de recursos pelos usuários. Necessita de identificação e autenticação.

3. Defesa

Medidas reativas

- Baseada em duas etapas fundamentais: detecção do ataque e resposta ao ataque.

- O objetivo da detecção é identificar toda tentativa de ataque DoS o mais rápido possível e com o menor número de falso-positivos.

- Após a detecção, a medida adequada de resposta pode ser tomada. Tais medidas podem incluir filtragem de pacotes, pedido de mais banda para suportar ao ataque, *blackholing*, entre outras.

3. Defesa

Medidas reativas

- As medidas reativas são classificadas de acordo com o seu mecanismo de detecção.

- Detecção por padrões: as assinaturas previamente conhecidas de atacantes são comparadas com as assinaturas de pacotes que estão chegando.

- Detecção de anomalias: o comportamento atual do sistema é comparado com o modelo de comportamento em condições normais.

- Detecção híbrida: utiliza tanto detecção por padrões quanto detecção de anomalias.

3. Defesa

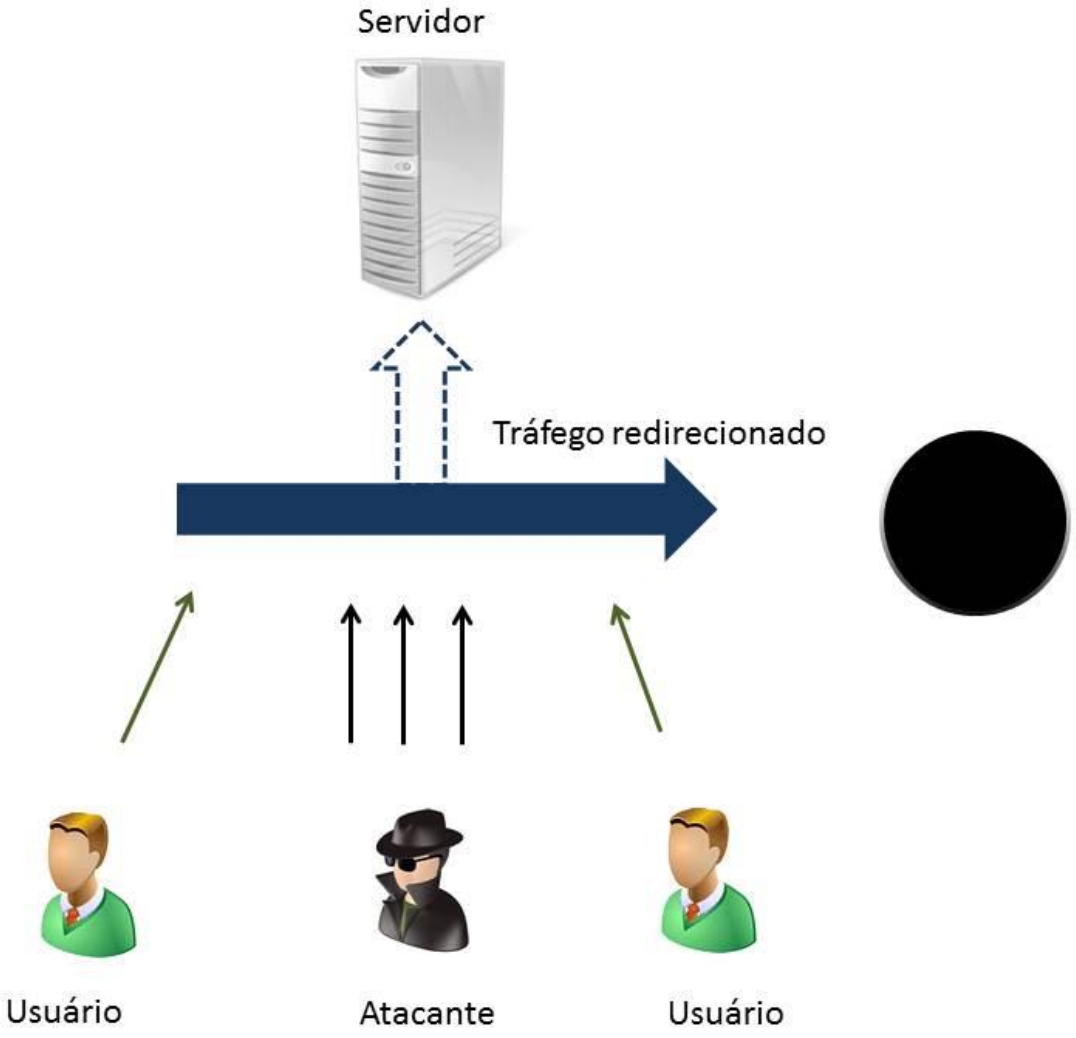
Blackholing

- Consiste em bloquear todo o tráfego direcionado a um servidor, redirecionando o tráfego a um “buraco negro” onde será descartado.

- Exemplos comuns de “buraco negro”:
  - Especificar o endereço IP de um servidor que não esteja rodando
  - Especificar um endereço IP que não esteja associado a nenhum servidor

- Esta solução não é muito boa, já que todo o tráfego é descartado (tanto do atacante como de um usuário legítimo)

3. Defesa


Servidor
Tráfego redirecionado
Usuário
Atacante
Usuário

3. Defesa

Roteadores

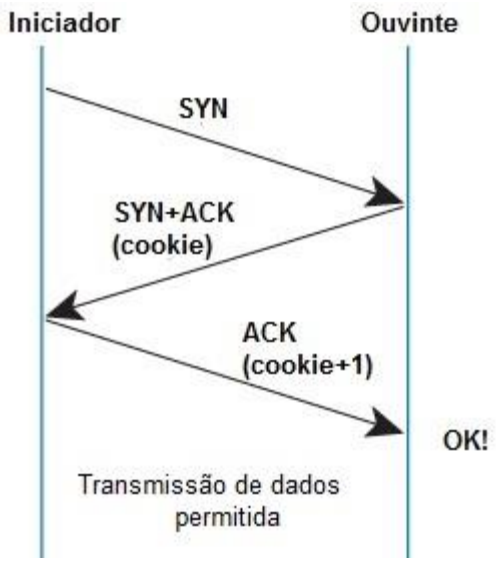
- Podem funcionar como uma primeira linha de defesa, pois possuem listas de controle de acesso que podem ser utilizadas para deter ataques DoS simples, como ataques de inundação por *ping*, filtrando protocolos não essenciais e endereços IP inválidos.

- Porém, os ataques DDoS mais sofisticados utilizam
  - Protocolos válidos e essenciais para o conexão com a Internet
  - Endereços IP mascarados *(spoofed),* porém válidos.

3. Defesa

SYN Cookies

- Contra ataques de inundação SYN
- Para estabelecer a conexão, o iniciador envia um pacote SYN ao ouvinte;
- O ouvinte responde enviando um SYN+ACK contendo um *cookie*. Este cookie é um número de sequência inicial calculado por técnicas criptográficas que utilizam inclusive o endereço IP e a porta utilizados pelo iniciador;
- O pacote SYN inicialmente enviado é descartado
- Condição para estabelecimento da conexão: iniciador responde com um ACK contendo o número de sequência *cookie*+1



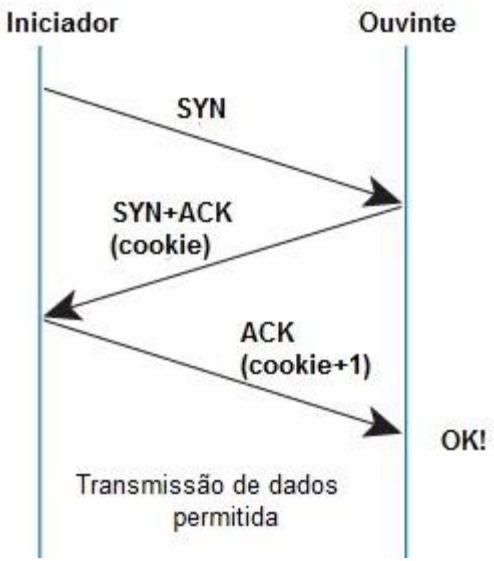
3. Defesa

SYN Cookies

- Caso o iniciador responda enviando um ACK, o ouvinte subtrai 1 de seu número de sequência e calcula novamente o valor do *cookie*. Se os resultados forem compatíveis, o pacote enviado foi válido e a conexão poderá ser estabelecida.

- Neste caso, o pacote SYN inicial (que havia sido descartado) pode ser recuperado decodificando informações contidas no *cookie* recebido

- Conclusão: o sistema alocou espaço para a conexão apenas após o envio de um ACK válido por parte do iniciador



3. Defesa

Firewalls

- Mecanismo de defesa eficiente contra ataques de inundação SYN, porém não muito eficiente contra ataques DDoS mais sofisticados

- Uma das técnicas possíveis de serem empregadas: mascarar os pacotes SYN+ACK enviados pelo servidor ao iniciador.

- Nesta técnica, o firewall funciona como um intermediário na conexão entre servidor e iniciador

3. Defesa

Firewalls

- Quando o iniciador envia um pacote SYN para iniciar a conexão, o *firewall* responde enviado um SYN+ACK mascarado ao iniciador sem que o servidor tenha conhecimento

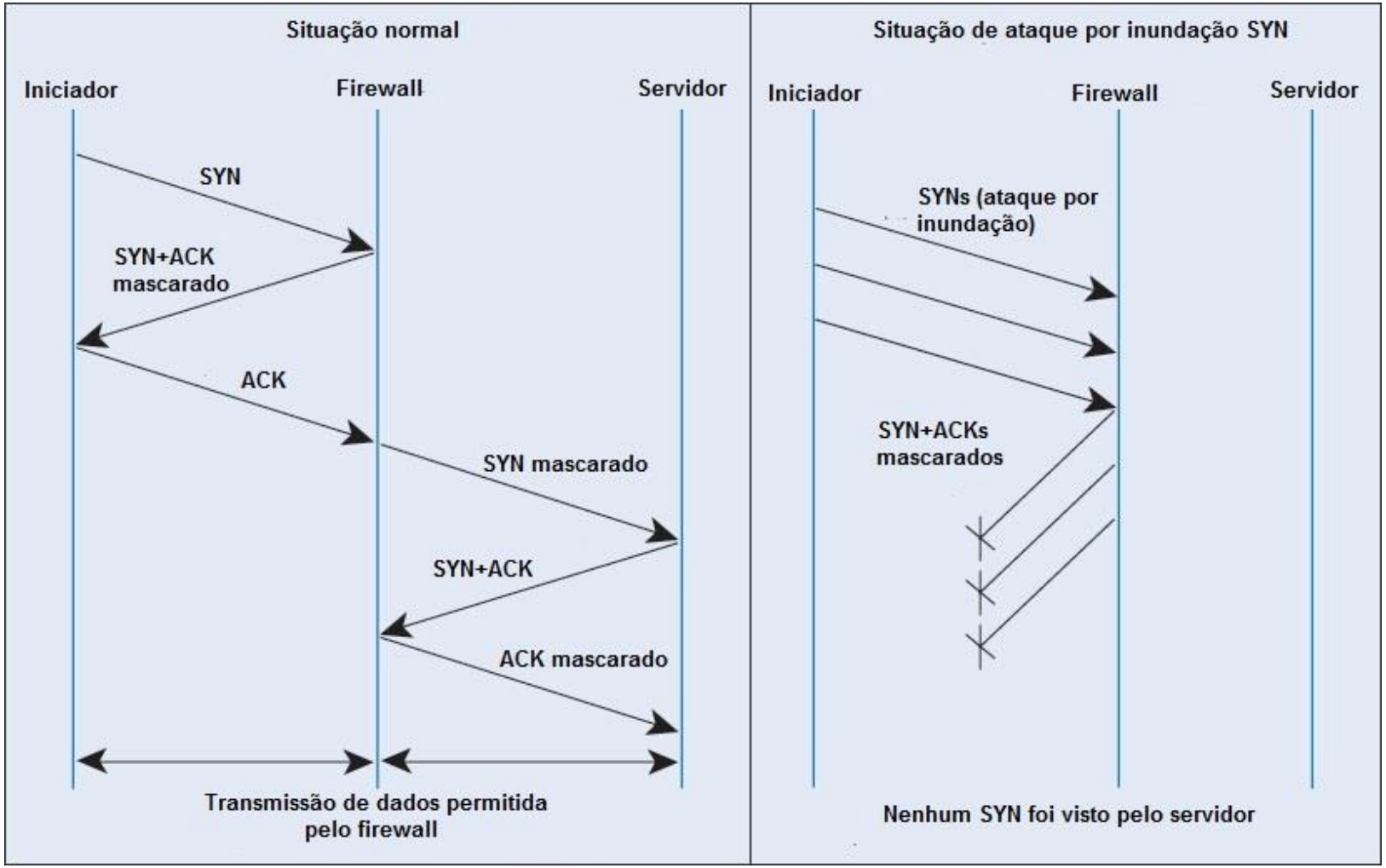
- Caso o iniciador responda enviado um ACK válido, o *firewall* irá iniciar uma conexão com o servidor. A partir dai, o *firewall* passa a funcionar como um intermediário na conexão entre iniciador e servidor, e a transmissão de dados é liberada.

- Caso o iniciador não responda enviando um ACK, o *firewall* simplesmente não inicia a conexão com o servidor.

- Esta técnica funciona desde que o *firewall* possua um mecanismo de defesa como o *SYN Cookie*

3. Defesa

Firewalls



3. Defesa

Firewalls

- Porém, *firewalls* não possuem mecanismos de defesa baseados em detecção de anomalias

- Quanto falamos de aplicações para a *Web,* o acesso deve ser liberado para alguns protocolos, como por exemplo o HTTP. Sendo assim, um atacante pode utilizar um destes protocolos para iniciar o ataque

- Como o firewall não detecta anomalias, o ataque passará despercebido

4. Implicaçoes Legais

Falta de Leis

- O Brasil, até muito pouco tempo atrás, não tinha leis que definissem de modo incisivo o que são crimes digitais e qual sua punição.

- Caso Carolina Dieckmann alavanca a criação da lei 12.737/12

4. Implicações Legais

Lei Carolina Dieckmann (12.737/12) e Lei Azeredo (12.735/12)

•Antes dessas leis, o invasor poderia ser punido por furto de dados ou por danos à imagem da pessoa, que são crimes já previstos no Código Penal; agora, ele terá punição específica pelos crimes eletrônicos

•Principais leis específicas para crimes digitais

•Lei Azeredo foi proposta em 1999, e só foi aprovada no ano de 2012.

•Projeto de lei muito polêmico – comparado ao *SOPA* nos EUA

•*DdoS* enquadra-se na Lei Carolina Dieckmann - " “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” rende de um a três anos de prisão, além de multa.”

Perguntas

1) Explique o que é um ataque de negação de serviço .

Perguntas

1) Explique o que é um ataque de negação de serviço .

Resposta:

São ataques a computadores com o objetivo de torná-los inacessíveis para outros usuários. Normalmente o ataque se dá através do consumo total dos recursos (banda, memória etc) do alvo.

Perguntas

2) Em que consiste um ataque por inundação SYN?

Perguntas

2) Em que consiste um ataque por inundação SYN?

Resposta:

- O atacante envia pacotes SYN ao alvo a partir de um endereço IP mascarado a fim de estabelecer diversas novas conexões
- O alvo responde enviando um pacote SYN-ACK para cada pacote SYN recebido e espera um pacote ACK como resposta;
- Os pacotes ACK esperados nunca são recebidos pelo alvo;
- A memória do alvo é completamente alocada, impedindo novas conexões, inclusive legítimas

Perguntas

3) Qual é a estrutura de um ataque distribuído de negação de serviço e quais suas vantagens em relação a ataques não-distribuídos?

Perguntas

3) Qual é a estrutura de um ataque distribuído de negação de serviço e quais suas vantagens em relação a ataques não-distribuídos?

Resposta:

Um DDoS consiste em um atacante e uma botnet, estabelecida pelo mesmo por meio do uso de alguma ferramenta adequada. Essa botnet é formada por masters, controlados diretamente pelo atacante, e daemons, controlados indiretamente pelo atacante por meio dos masters. Os daemons são quem realmente executam o ataque em si.

As vantagens de um DDoS são a maior facilidade para gerar um tráfego de ataque mais intenso e a maior dificuldade para o alvo anular o ataque.

Perguntas

4) Apresente os conceitos básicos do funcionamento do mecanismo *SYN Cookies.*

Perguntas

4) Apresente os conceitos básicos do funcionamento do mecanismo *SYN Cookies*.

Resposta:

- O iniciador envia um pacote SYN ao ouvinte para estabelecer uma conexão;
- O ouvinte responde enviando um pacote SYN+ACK e um cookie. O cookie é calculado através de técnicas criptográficas envolvendo diversas informações;
- O pacote SYN originalmente enviado pelo iniciador é descartado;
- Para que a conexão seja estabelecida, o iniciador deve responder enviando um ACK com o número de sequência cookie+1. Caso contrário, a conexão não é estabelecida e os recursos não são alocados pelo servidor.

Perguntas

5) Explique o conceito de *Blackholing*.

Perguntas

5) Explique o conceito de *Blackholing*.

Resposta:

Blackholing é uma técnica de defesa que consiste em bloquear todo o tráfego direcionado a um servidor, redirecionando o tráfego a um "buraco negro" onde será descartado. Porém, esta não é uma técnica muito adequada, já que todo tipo de tráfego será bloqueado - tanto o do atacante quanto o do usuário legítimo.