DDoS

Ataques Distribuídos de Negação de Serviço

Ataques de Negação de Serviço

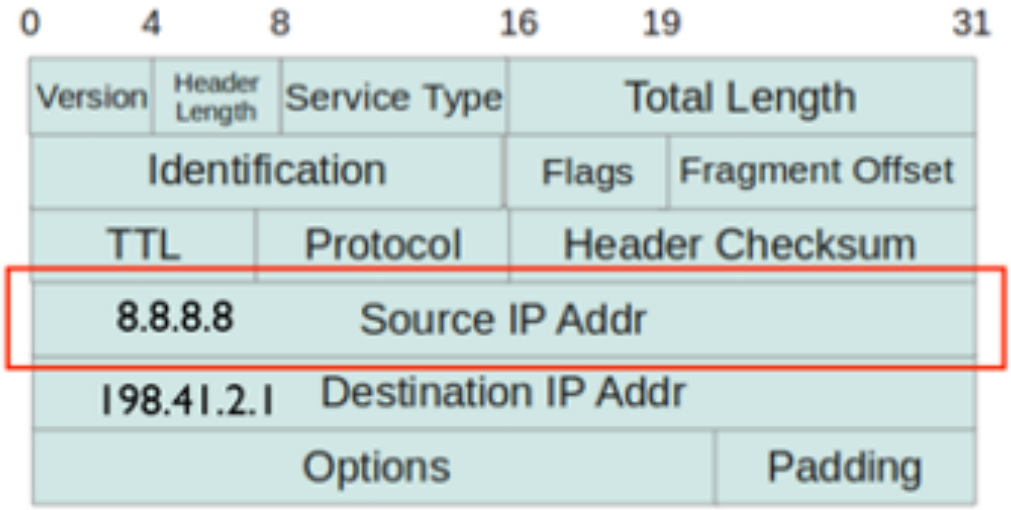
- Negação de serviço é uma forma de ataque contra a disponibilidade de algum serviço
  - Uma negação de serviço (DoS) é uma ação que impede ou prejudica o uso autorizado de redes, sistemas ou aplicações mediante a exaustão de recursos, como unidades centrais de processamento (Central Processing Unit — CPU), memória, largura de banda e espaço em disco.
  - categorias de recursos que poderiam ser atacados:
    - Largura de banda de rede
    - Recursos de sistema
    - Recursos de aplicações

Negação de serviço versus sobrecarga

- Negação de serviço: indisponibilidade por falha ou vulnerabilidade
  - Pacotes mal-formados.: ping of the death, teardrop
  - Violação de lógica de protocolo: SYN flood
- Sobrecarga: indisponibilidade por incapacidadede tratar todas as demandas
  - Ex.: ataque DDoS
  - Também conhecido como inundação/flooding

Falsificação de endereço de origem

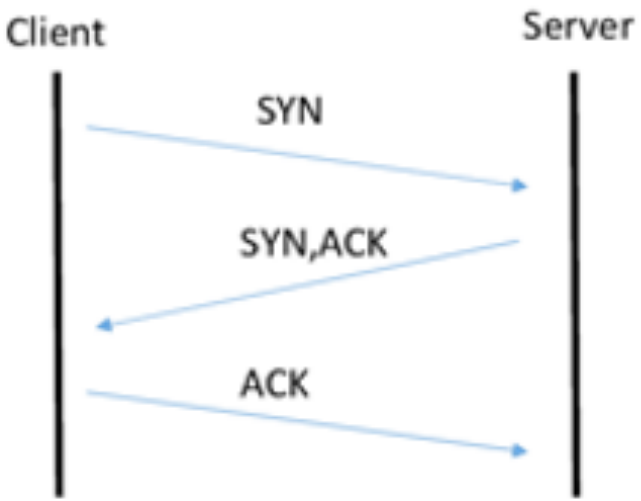
- Característica comum em muitos ataques DDoS
  - Particularmente frequente em ataques com "reflexão"
- Baseia-se em falhas (ou premissas fracas) nos processos de autenticação do TCP-IP



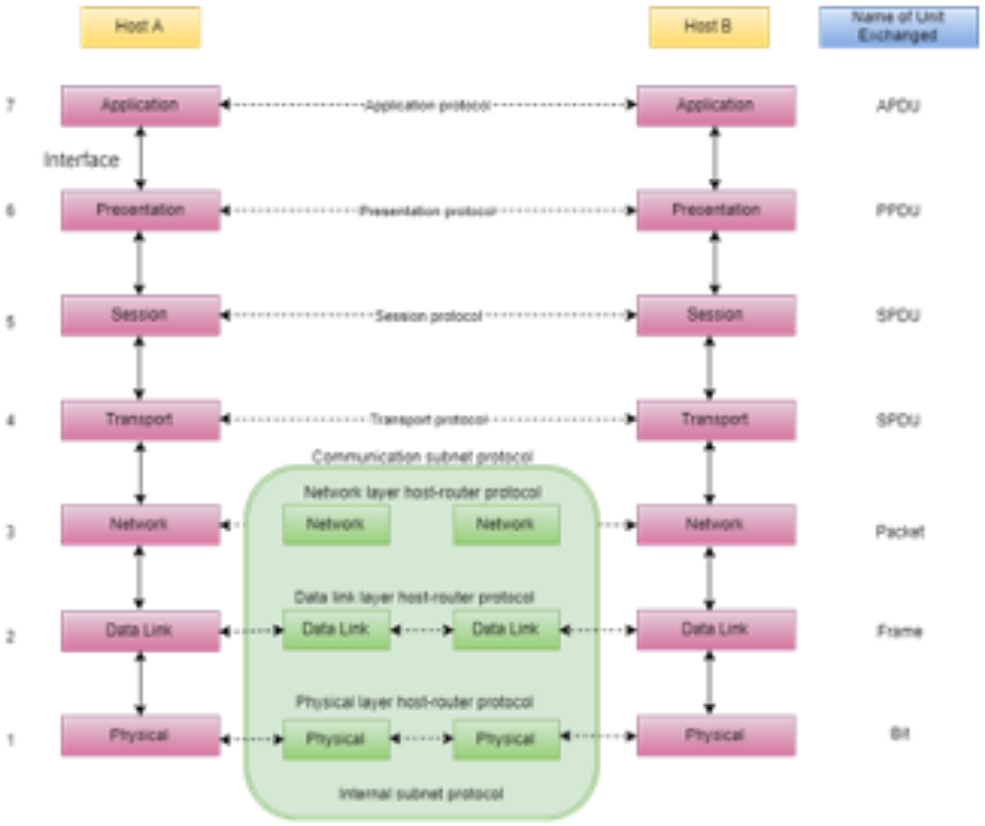
*Inversão de ordem

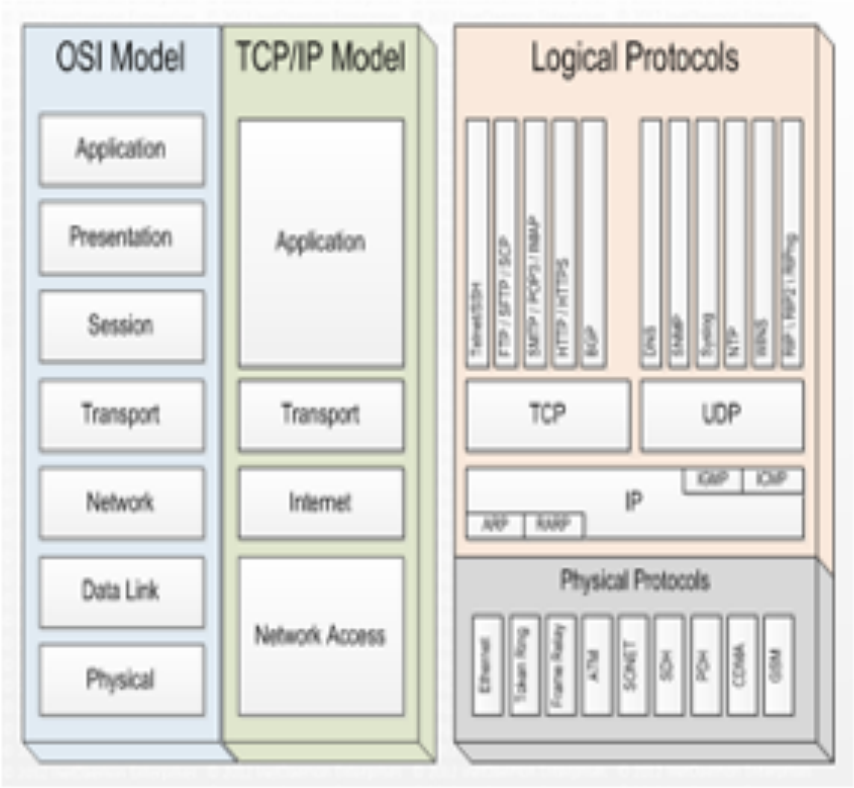
Three-way handshake

- Processo de estabelecimento de uma ”conexão TCP” entre dois participantes de um protocolo
  - UDP não estabelece conexão
  - Diferenças entre TCP e UDP
- Envio de três pacotes TCP: SYN, SYN,ACK, ACK



Modelo em camadas





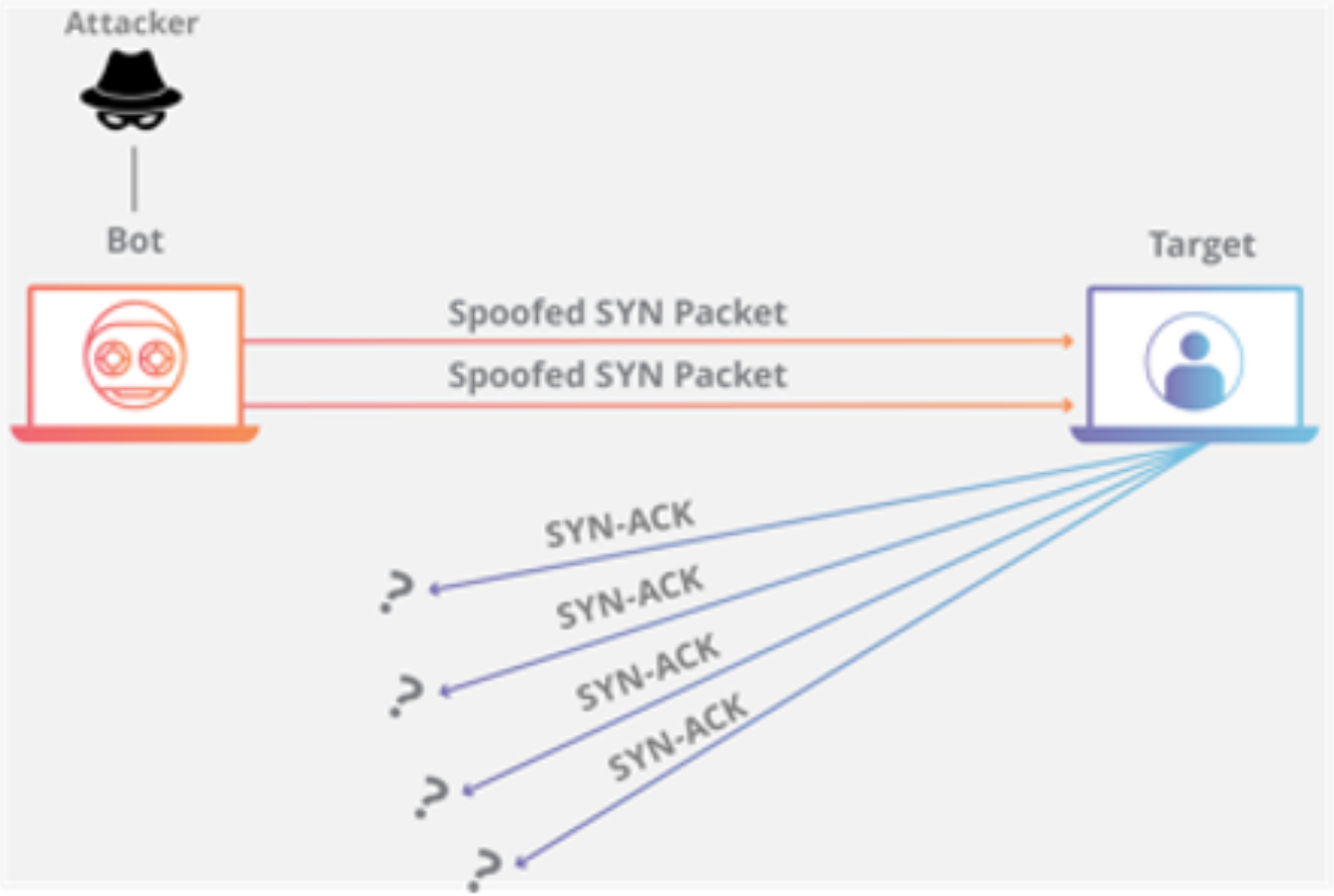
Ataques de inundação (flooding)

- Tentativa de degradação de serviço ou indisponibilidade de recurso a partir de sobrecarga
  - Recursos podem ser de comunicação ou de serviços
- Camada do ataque (protocolo) determina o recurso indisponível
  - Ataques em camadas inferiores (e.g. ICMP flood e SYN flood) comprometem recursos de comunicação (canais de comunicação e equipamentos de camadas 3 e 4)
  - Ataques em camadas superiores (e.g. HTTP flood, L7 attack) comprometem a disponibilidade e o desempenho de serviços

SYN Flooding

- Usa IP spoofing (mas não é conhecido como SYN spoofing)
- Envio de grande quantidade de requisições de conexões à máquina-alvo
- Como funciona:
  - O invasor envia um grande volume de pacotes SYN para o servidor de destino, geralmente com endereços IP falsificados.
  - O servidor responde a cada um dos pedidos de conexão e deixa uma porta aberta pronta para receber a resposta.
  - Enquanto o servidor aguarda o pacote ACK final, que nunca chega, o atacante continua a enviar mais pacotes SYN.
    - Cada novo pacote SYN faz com que o servidor mantenha temporariamente uma nova conexão de porta aberta por um determinado período de tempo e, uma vez que todas as portas disponíveis tenham sido utilizadas, o servidor deixa de funcionar normalmente.

SYN Flooding



SYN Flood – estratégia

- Não é um ataque ”volumétrico” em essência
  - Não precisa saturar infraestrutura de rede
  - Atacante só precisa superar a capacidade de backlog do sistema-alvo
  - Ataques parametrizados e com volumes relativamente baixos

SYN Flood – modos de ataque

- Ataque direto
  - Atacante não mascara IP – mais vulnerável a identificação
  - Atacante deve garantir que sua máquina não responde aos SYN/ACK – pode ser feito com firewall
  - Pouco usado – facilmente mitigado por bloqueio de IP
    - Pode ser usado quando se possui uma botnet
- Ataque forjado (spoofed)
  - Usa IP spoofing
  - Dificulta mitigação e identificação
    - Mas não é impossível, especialmente, com apoio do ISP
- Ataque distribuído (DDoS)
  - Usa botnet para alcançar grandes volumes e dificultar detecção

SYN Flood – mitigação

› Aumentar a capacidade de conexões half-open

› Reciclar (descartar) conexões half-open antigas

› SYN Cookies – liberar porta após enviar SYN/ACK

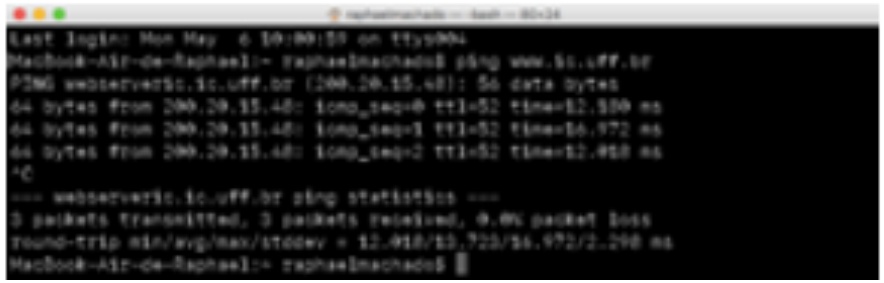
› Anycast – three-way handshake na nuvem

Ataques de Inundação

- Grande variedade de formas
- Em todos os casos, baseia-se no ”volume”
  - Sobrecarga de rede
  - Sobregarga de serviço
- Praticamente qualquer tipo de protocolo pode ser usado
  - ICMP
  - UDP
  - TCP (SYN)

ICMP Flood (Ping)

- Sobrecarrega o alvo com pacotes ICMP echo-request
- ICMP é usado por ferramentas de ”diagnóstico de rede”, tais como ping e traceroute
  - echo request e echo reply indicam saúde e conectividade de dispositivos
- Historicamente, atacantes forjavam IP (spoofing)
  - com uso de botnets, spoofing tornou-se desnecessário
- O ataque é ”simétrico



ICMP flood – mitigação

- Desabilitar ICMP
  - Serviços como ping e traceroute ficam indisponíveis
- Uso de serviços anti-DDoS na nuvem (anycast)

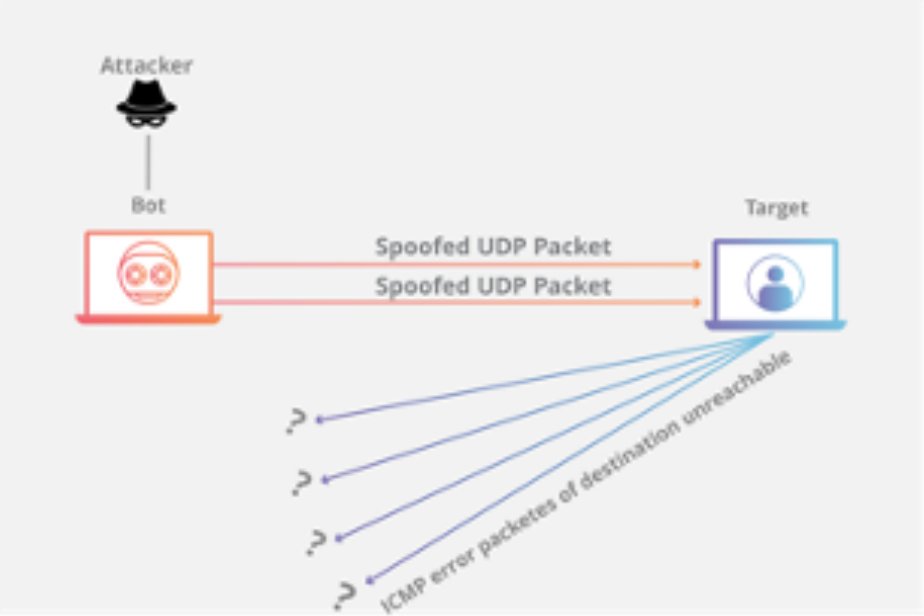
UDP flood

- Grande volume de pacotes UDP enviado para um sistema-alvo
  - compromete capacidade de o sistema processar/responder
- Etapas de um sistema para responder a um pacote UDP enviado para uma porta específica
  - Servidor verifica se existe um programa/serviço atendendo aquela porta
  - Se nenhum programa/serviço atende a porta, o servidor envia um pacote ICMP (destination unreachable)

UDP flood

› Ataque UDP flood explora o ”custo” de tratamento dessas mensagens

› Endereços de origem serão em geral forjados (IP spoofing)



Mitigação de UDP Flood

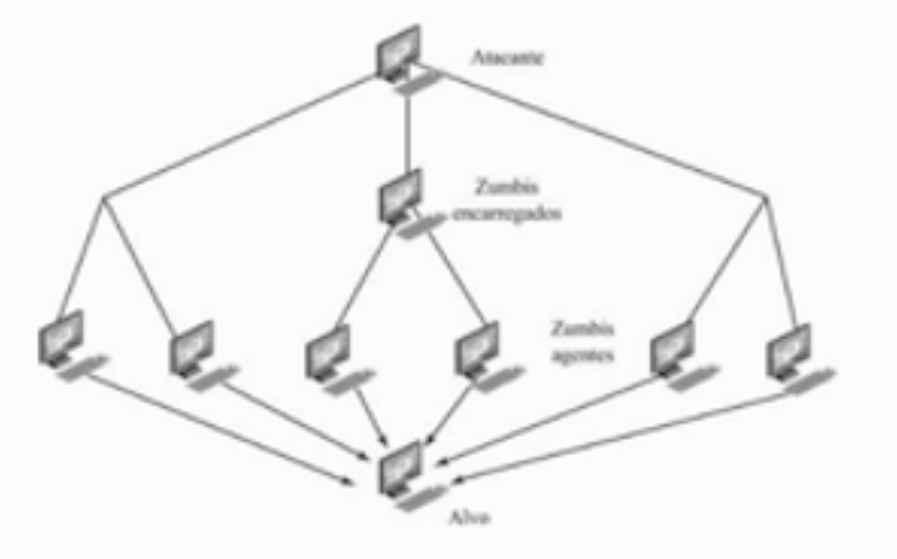
- Limitação da taxa de pacotes UDP recebidos
  - Pode levar a perdas legítimas
- Contratação de serviços "cloud anycast"
  - Filtra na borda (exemplo: não-DNS)
  - Amortece entre vários servidores

Ataques DDoS

› Ataques Distribuídos de Negação de Serviço

› Fazem uso de ”redes de atacantes” para aumentar o volume de sobrecarga do ataque

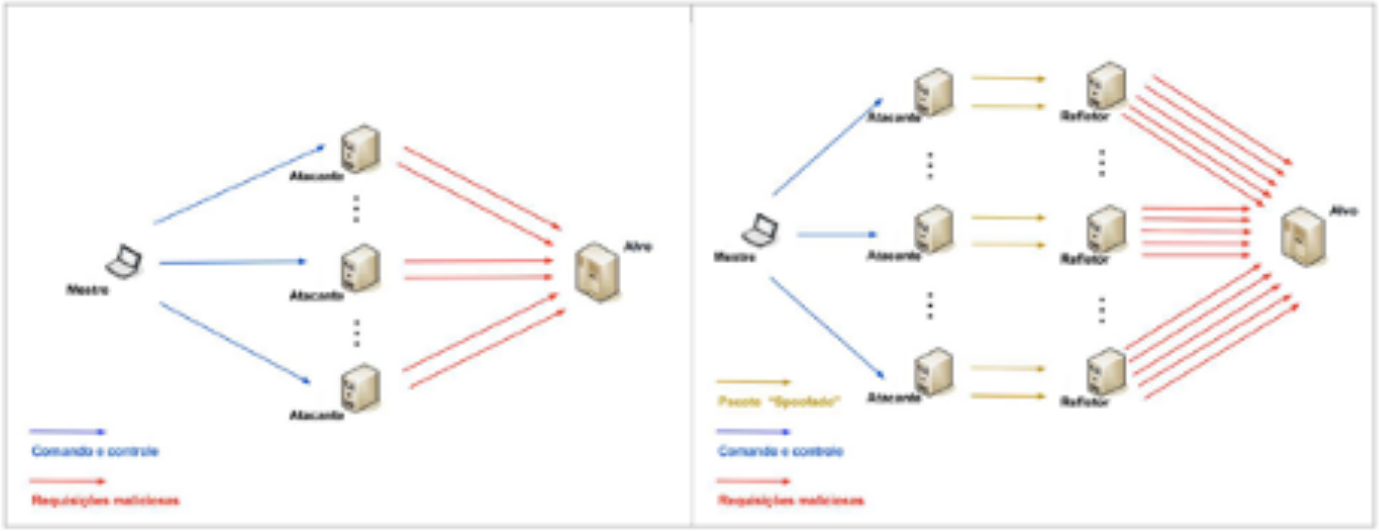
– Geralmente, atacantes são robôs ou zumbis



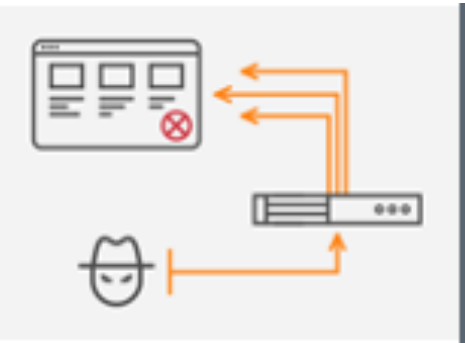
Ataques refletores e amplificadores

› Reflexão: envio para um servidor de pacote forjado com endereço do alvo
  – A resposta do servidor é enviada para o alvo
  – Precisa ser UDP – sem conexão

› Amplificação: resposta é maior que a consulta (bytes)



Exemplo de amplificação (DNS)



```
10:40:39.811543 IP 146.164.250.148.2051 > 146.164.10.2.53: 35188+
ANY? google.com. (28)
0x0000:  4500 0038 91ed 0000 4011 bee8 92a4 fa94  E..8....@.......
0x0010:  92a4 0a02 0803 0035 0024 2f63 8974 0100  .......5.$/c.t..
0x0020:  0001 0000 0000 0000 0667 6f6f 676c 6503  .........google.
0x0030:  636f 6d00 00ff 0001                      com.....
```

```
10:40:39.812316 IP 146.164.10.2.53 > 146.164.250.148.2051: 35188
15/4/4 A 173.194.42.135, A 173.194.42.136, A 173.194.42.137, A
173.194.42.142, A 173.194.42.128, A 173.194.42.129, A 173.194.42.130,
A 173.194.42.131, A 173.194.42.132, A 173.194.42.133, A
173.194.42.134, NSns1.google.com., NS ns2.google.com.,
NS ns4.google.com., NS ns3.google.com. (396)
0x0000:  4500 01a8 82e5 0000 3f11 cd80 92a4 0a02  E.......?.......
0x0010:  92a4 fa94 0035 0803 0194 f3f2 8974 8180  .....5.......t..
0x0020:  0001 000f 0004 0004 0667 6f6f 676c 6503  .........google.
0x0030:  636f 6d00 00ff 0001 c00c 0001 0001 0000  com.............
0x0040:  0105 0004 adc2 2a87 c00c 0001 0001 0000  ......*.........
0x0050:  0105 0004 adc2 2a88 c00c 0001 0001 0000  ......*.........
0x0060:  0105 0004 adc2 2a89 c00c 0001 0001 0000  ......*.........
0x0070:  0105 0004 adc2 2a8e c00c 0001 0001 0000  ......*.........
0x0080:  0105 0004 adc2 2a80 c00c 0001 0001 0000  ......*.........
0x0090:  0105 0004 adc2 2a81 c00c 0001 0001 0000  ......*.........
0x00a0:  0105 0004 adc2 2a82 c00c 0001 0001 0000  ......*.........
0x00b0:  0105 0004 adc2 2a83 c00c 0001 0001 0000  ......*.........
0x00c0:  0105 0004 adc2 2a84 c00c 0001 0001 0000  ......*.........
0x00d0:  0105 0004 adc2 2a85 c00c 0001 0001 0000  ......*.........
0x00e0:  0105 0004 adc2 2a86 c00c 0002 0001 0005  ......*.........
0x00f0:  3160 0006 036e 7331 c00c c00c 0002 0001  1`...ns1........
0x0100:  0005 3160 0006 036e 7332 c00c c00c 0002  ..1`...ns2......
0x0110:  0001 0005 3160 0006 036e 7334 c00c c00c  ....1`...ns4....
0x0120:  0002 0001 0005 3160 0006 036e 7333 c00c  ......1`...ns3..
0x0130:  c00c 0002 0001 0005 3160 0002 c0ea c00c  ........1`......
0x0140:  0002 0001 0005 3160 0002 c0fc c00c 0002  ......1`........
0x0150:  0001 0005 3160 0002 c0d8 c00c 0002 0001  ....1`..........
0x0160:  0005 3160 0002 c10e c0d8 0001 0001 0005  ..1`............
0x0170:  30aa 0004 d8ef 200a c0ea 0001 0001 0005  0.............. .
0x0180:  30aa 0004 d8ef 220a c10e 0001 0001 0005  0.....".........
0x0190:  30aa 0004 d8ef 240a c0fc 0001 0001 0005  0.....$.........
0x01a0:  30aa 0004 d8ef 260a                      0.....&.
```

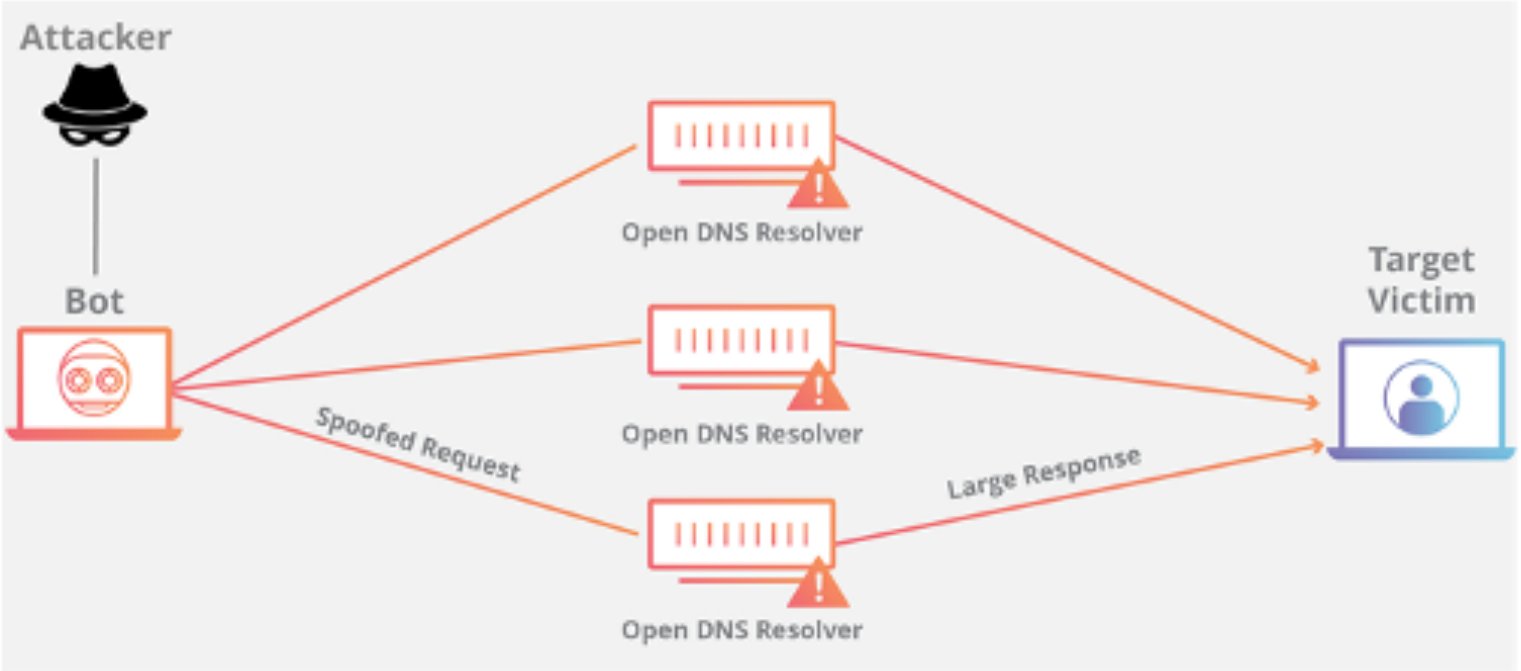
Fatores de Amplificação

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange

Protocol	Bandwidth Amplification Factor	Vulnerable Command
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7,6]	56 to 70	—
TFTP [23,6]	60	—
Memcached [25]	10,000 to 51,000	—

Ataque de amplificação DNS

› Ataques baseados em reflexão
  – Explora DNS resolvers abertos



Passos de um ataque de amplificação DNS

- O invasor usa um endpoint comprometido para enviar pacotes UDP com endereços IP falsificados para um recursor DNS.
- O endereço falsificado nos pacotes aponta para o endereço IP real da vítima.
- Cada um dos pacotes UDP faz uma solicitação a um resolvedor de DNS, geralmente passando um argumento como "ANY" para receber a maior resposta possível.
- Depois de receber as solicitações, o resolvedor de DNS, que está tentando ser útil ao responder, envia uma grande resposta ao endereço IP falsificado.
- O endereço IP do alvo recebe a resposta e a infra-estrutura de rede circundante fica sobrecarregada com o dilúvio de tráfego, resultando em uma negação de serviço.

Mitigação de ataques DNS-refl-amp

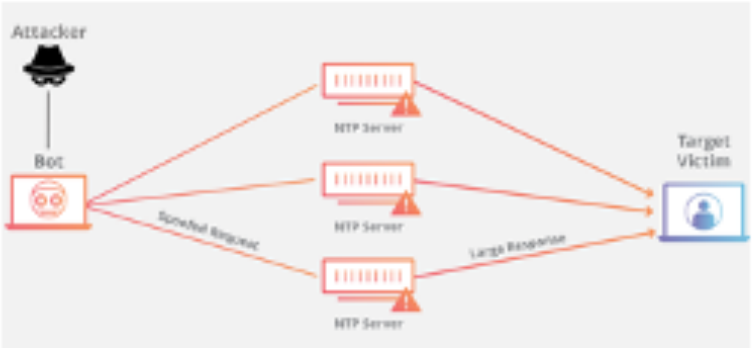
- Redução do número de DNS resolvers
- Verificação de pacotes forjados
  - Filtragem de pacotes
- Anycast na nuvem
  - Distribuição/espalhamento das requisições

NTP amplification

- Ataque DDoS volumétrico baseado em reflexão/amplificação
- Explora o protocolo NTP (network time protocol)
  - Usado para sincronização de hosts
- Explora o comando monlist
  - retorna os últimos 600 IPs que consultaram o servidor
  - incremento de mais de 200 o tamanho da consulta
- Passos do ataque: similar ao DNS

Passos do ataque

- O invasor usa uma botnet para enviar pacotes UDP com endereços IP falsificados para um servidor NTP que tenha seu comando monlist ativado. O endereço IP falsificado em cada pacote aponta para o endereço IP real da vítima.
- Cada pacote UDP faz uma solicitação ao servidor NTP usando seu comando monlist, resultando em uma grande resposta.
- O servidor responde então ao endereço falsificado com os dados resultantes.
- O endereço IP do alvo recebe a resposta e a infra-estrutura de rede circundante fica sobrecarregada com o dilúvio de tráfego, resultando em uma negação de serviço.

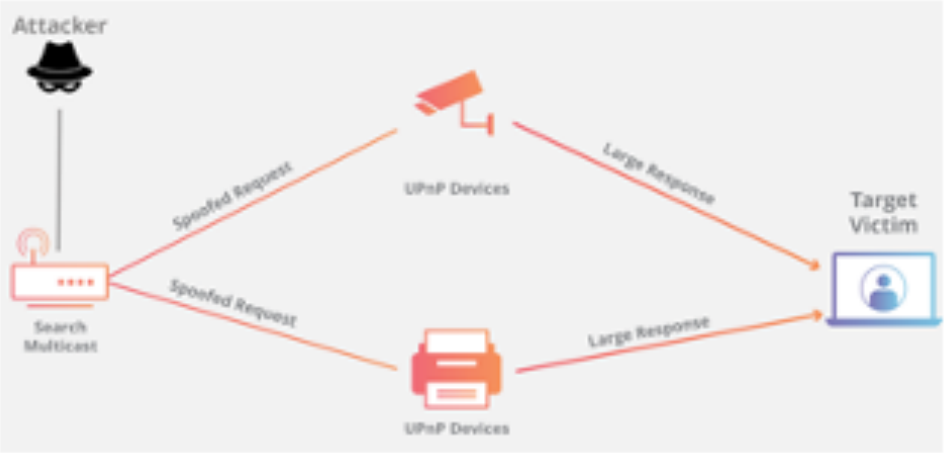


Mitigação de ataques NTP-refl-amp

- Desabilitar monlist - redução do número de NTP servers que respondem ao comando (versão 4.2.7+)
- Verificação de pacotes forjados
  - Filtragem de pacotes
- Anycast na nuvem
  - Distribuição/espalhamento das requisições

Ataque SSDP

- Explora protocolos Universal Plug and Play (UPnP)
  - UPnP é usado para que dispositivos divulguem sua existência para uma rede
  - Um dos pacotes que o dispositivo envia é uma ”descrição” ou ”lista de serviços”
- Baseia-se em amplificação



Passos do Ataque SSDP

- Primeiro, o invasor realiza uma varredura em busca de dispositivos plug-and-play que possam ser utilizados como fatores de amplificação.
- Conforme o atacante descobre dispositivos em rede, eles criam uma lista de todos os dispositivos que respondem.
- O invasor cria um pacote UDP com o endereço IP falsificado da vítima visada.
- O invasor usa uma botnet para enviar um pacote de descoberta falsificado para cada dispositivo plug-and-play com uma solicitação para o máximo de dados possível definindo determinados sinalizadores, especificamente ssdp: rootdevice ou ssdp: all.
- Como resultado, cada dispositivo enviará uma resposta à vítima visada com uma quantidade de dados até cerca de 30 vezes maior que a solicitação do invasor.
- O alvo recebe então um grande volume de tráfego de todos os dispositivos e fica sobrecarregado, resultando potencialmente em negação de serviço ao tráfego legítimo.

Mitigação

› Avaliar se seus dispositivos são vulneráveis ao ataque

› Filtrar tráfego UDP de entrada para porta 1900

› Monitoramento de tráfego para a porta 1900

› Uso de Anycast na nuvem

Ataque DDoS memcached

- Explora o memcached para obter amplificação
  - Sistema de cache distribuído
  - Usado na web para armazenar páginas e acelerar o acesso
- O memcached tem a opção de usar UDP
- Fator de amplificação enorme: mais de 50mil !

Etapas do ataque DDoS memcached

- Um invasor implanta uma grande carga de dados em um servidor de memcached exposto.
- Em seguida, o invasor falsifica uma solicitação HTTP GET com o endereço IP da vítima visada.
- O servidor de memcached vulnerável que recebe a solicitação, que está tentando responder, envia uma grande resposta ao destino.
- O servidor de destino ou sua infraestrutura circundante não consegue processar a grande quantidade de dados do servidor de memcached, resultando em sobrecarga e negação de serviço para solicitações legítimas.

Mitigação do ataque DDoS memcached

› Desabilitar UDP dos servidores memcached

› Implantar firewall nos servidores memcached

› Prevenir IP spoofing

› Desenvolver software com menos respostar UDP

› Uso de Anycast na nuvem

Comentário sobre Anycast

› Forma de atribuir ao mesmo IP várias máquinas

› De forma simplificada, uma consulta ou busca por IP irá te levar para do datacenter mais próximo
  – O que esses mitigadores de ataques DDoS fazem é se basear na ”força” para amortecer a sobrecarga

Comentário sore projeto de protocolos

- UDP é um protocolo sem conexão que pode ser a base de muitos protocolos de aplicação
  - no entanto, protocolos pouco pensados podem ser a base para ataques dos mais diversos tipos
    - UDP permite spoofing
    - UDP permite amplificação

Ataques DDoS em camada de aplicação

- Tem como alvo protocolos de aplicação
  - o ”topo” da pilha ISO/OSI (L7)
  - exemplo: requisições HTTP GET ou HTTP POST
- Esgota recursos do serviço alvo, além de recursos de rede
- Assimetria (ilimitada) entre os recursos necessários para ”solicitar” e para ”responder”

Mitigação de ataques L7

- Dificuldade de detecção
  - geralmente botnet – tráfego aparentemente legítimo
  - necessidade de estratégia adaptativa / análise comportamental
- Ferramentas
  - Web Application Firewall
  - Testes para dificultar ação de bots – ex.: captcha, login,...
  - Filtro de pacotes com base em dados de reputação de Ips
  - Uso de redes anycast e terceiros

Teste de Desempenho e Ataques Transacionais

```
<servers>
  <server host="[redacted].com.br" port="80" type="tcp"></server>
</servers>

<load duration="30" unit="minute">
  <arrivalphase phase="1" duration="30" unit="minute">
    <users arrivalrate="1000" unit="minute"></users>
  </arrivalphase>
</load>

<options>
</options>

<sessions>
  <session name="frete_[redacted]" probability="60" type="ts_http">
  </session>

  <session name="basket_[redacted]" probability="19.2" type="ts_http">
  </session>

  <session name="login_[redacted]" probability="9.6" type="ts_http">
  </session>

  <session name="pagamento_[redacted]" probability="8" type="ts_http">
  </session>

  <session name="confirmacao_pagamento_[redacted]" probability="3.2" type="ts_http">
  </session>
```

```
▼ object {5}
  ▼ GET https://www.google.com.br/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8 [56428] {5}
      label : https://www.google.com.br/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8
      url   : https://www.google.com.br/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8
      method : GET
      timestamp : 1452832456420
    ▶ headers [6]
  ▶ GET https://www.google.com.br/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8 [56434] {5}
  ▶ GET http://www.google.com/ [56435] {5}
  ▶ GET https://www.google.com.br/complete/search?sclient=psy-ab&site=&source=hp&q=&oq=&gs_l=&pk=1&bav=on.2,or.r_cp.
  ▼ POST https://plus.google.com/u/0/_/n/gcosuc [56448] {6}
      label : https://plus.google.com/u/0/_/n/gcosuc
      url   : https://plus.google.com/u/0/_/n/gcosuc
      method : POST
    ▼ body {1}
        ntok : APfa8byVhVYgHmOPpu4ftWoSk5vY8yTsgIr8wlc86EK8yTyx4-rRBQk1hmcKquiDY6rZP_ERq4s9L7p4n163dC9nkbC4WkAuYYg==
      timestamp : 1452832458134
    ▶ headers [8]
```

```
+------------------+------------------+------------+----------------+------------------+
| IP               | Provider/Region  | Status     | Attacking for  | Network Traffic  |
+------------------+------------------+------------+----------------+------------------+
| 162.242.209.131  | rackspace/iad    | attacking  | 707            | 56.06 Mbps       |
| 166.78.156.213   | rackspace/dfw    | attacking  | 707            | 78.98 Mbps       |
| 119.9.88.66      | rackspace/hkg    | attacking  | 707            | 64.86 Mbps       |
| 119.9.54.214     | rackspace/syd    | attacking  | 707            | 84.58 Mbps       |
+------------------+------------------+------------+----------------+------------------+
Total network traffic: 284.48 Mbps
* Press Control + C to stop the status panel
```

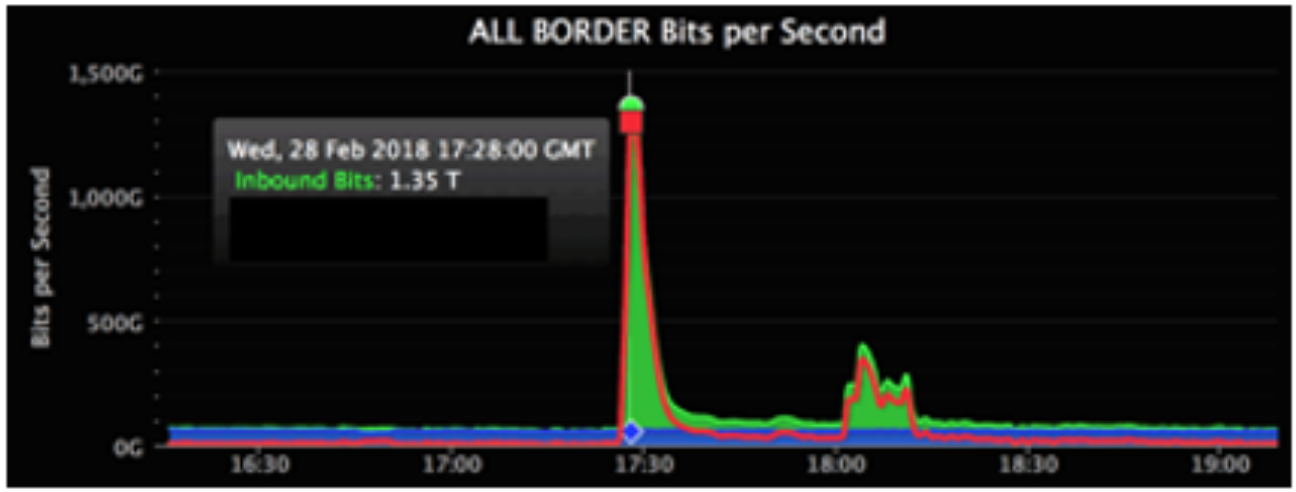
Ataques DDoS notórios – GitHub 2018

› Fevereiro de 2018 – maior ataque em volume

› Ataque DDoS memcached

› Pico de tráfego: 1,35 Tbps

› Mitigação iniciou em 10 min: total 20 min off



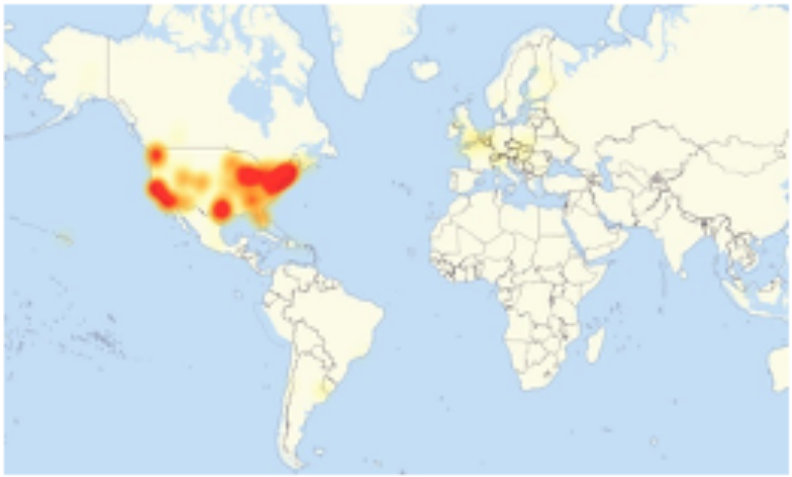
Ataques DDoS notórios – Mirai/Dyn 2016

› Outubro de 2018 – botnet de dispositivos IoT

› Sobrecarga do provedor DYN de DNS

› Número de dispositivos: 100 mil

› Indisponibilidade de grandes serviços



Ataques DDoS notórios – GitHub 2015

- Maior ataque até então
- Evidências de participação da China
  - motivação política – software em desenvolvimetno para contornar monitoramento chinês
- Infecção por código Javascript
  - browsers haviam visitado site do Baidu
  - browsers infectados realizavam http requests para páginas-alvo no GitHub

Ataques DDoS notórios – Spamhaus 2013

- Maior até então: 300 Gbps
- Spamhaus: sistema anti-spam
- Motivação: a Spamhaus blacklisted várias faixas de IP da Cyberbunker
- Algumas prisões associadas ao ataque

Ataques DDoS notórios – Estônia 2007

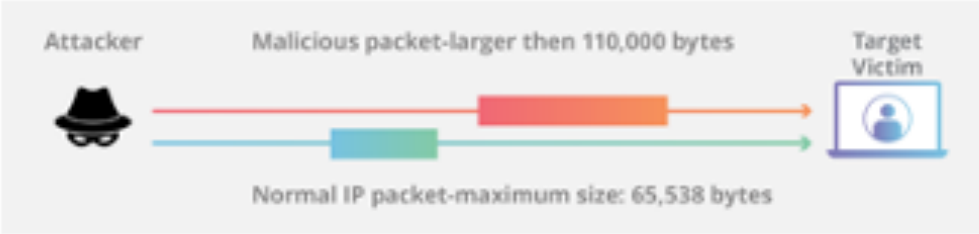
- Em abril de 2007, a Estônia foi atingido por um ataque DDoS em massa, direcionado a serviços governamentais, instituições financeiras e meios de comunicação.
  - Efeito esmagador: o governo da Estônia foi um dos primeiros a adotar o governo on-line
- Considerado por muitos como o primeiro ato de guerra cibernética
  - Resposta a um conflito político com a Rússia sobre a realocação do "Soldado de Bronze de Tallinn",
  - O governo russo é suspeito de envolvimento e um cidadão estoniano da Rússia foi preso como resultado
  - O governo russo não deixou que as autoridades estonianas fizessem mais investigações na Rússia.

Ataques DDoS notórios – Mafiaboy 2000

- Em 2000, um hacker de 15 anos conhecido como "Mafiaboy" derrubou vários sites importantes, como CNN, Dell, E-Trade, eBay e Yahoo, que na época era o mecanismo de busca mais popular do mundo.
  - Conseqüências devastadoras, incluindo a criação de caos no mercado de ações.
- Mafiaboy - um estudante de ensino médio chamado Michael Calce - coordenou o ataque invadindo as redes de várias universidades e usando seus servidores para conduzir o ataque DDoS.
  - As conseqüências desse ataque levaram diretamente à criação de muitas das leis atuais sobre cibercrime.

Ataques históricos – Ping of the Death

› Pacote ICMP Ping muito maior que o máximo previsto
  – muitas implementações não eram preparadas para tratar tais pacotes
  – sistema travava etc.

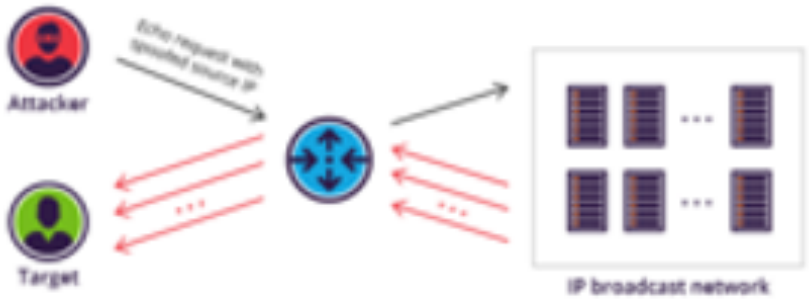


› Mitigação: filtrar pacotes mal-formados

› Curiosidade: um ping da morte foi descoberto para uma implementação Windows do IPv6 em 2013

Ataques históricos – Ataque Smurf

- Explorava vulnerabilidade no protocolo ICMP
  - funcionalidade de broadcast
  - Possivelmente, primeiro ataque amplificado
- Etapas:
  - O malware Smurf é usado para gerar uma solicitação *Echo* falsa contendo um IP de origem falsificado, que é, na verdade, o endereço do servidor de destino.
  - A solicitação é enviada para uma rede de distribuição de IPs intermediária.
  - A solicitação é transmitida na rede para todos os *hosts* da mesma. Neste caso os IP's serão trocados (técnica spoofing) pelo endereço IP da vitima(Servidor) escolhida pelo *hacker;
  - Cada host envia uma resposta ICMP para o endereço de origem falsificado.
  - Com respostas ICMP suficientes encaminhadas, o servidor de destino é derrubado.



Ataques históricos - Slowloris

› Estratégia oposta a do DDoS volumétrico
  – envia poucos pacotes com grande intervalo, mantendo abertas as conexões
  – Difícil detecção: furtivo (poucos pacotes) e aparentemente, tráfego legítimo
  – Desenvolvido por Robert "RSnake" Hansen

Em resumo

- Tipos de Ataque
  - Camada de Aplicação: explora protocolos de aplicação
  - Ataques a Protocolos: exploram vulnerabilidades em protocolos
  - Ataques volumétricos: buscam sobrecarregar com volume
- Recursos
  - Botnet: aumenta o número de "atacantes"
  - Reflexão: aumenta o potencial volumétrico
- Mitigação
  - Eliminação de vulnerabilidades
  - Buraco Negro
  - Limitação de taxa de serviço
  - WAF (Web Application Firewall)
  - Difusão em Rede Anycast