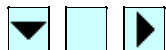


GTER15 – Exemplos de Aplicações do GNU/Linux Netfilter Iptables



[Back to Home](#)

[Home](#)

Apresentação

- :: [Objetivos Estratégia](#)
- :: [Dados do Autor](#)

Visão Geral

- :: [Scripts com o Iptables](#)
- :: [Malformed Packets](#)

ARP Poisoning

- :: [ARP Poisoning default gateway](#)
- :: [ARP Poisoning Iptables](#)

Denial of Service

- :: [TCP SYN FLOOD: características](#)
- :: [Syn Flood: Resultados](#)
- :: [Syn Flood: reações mais comuns](#)
- :: [Syn Flood: reação viável atualmente](#)
- :: [Syn Flood Netfilter](#)
- :: [Denial of Service \(DoS\): outros tipos](#)

© 2003 by Antonio Batista
<antonio@CintraBatista.net>

Onde buscar este documento na Internet

<http://www.CintraBatista.net/docs/sent/gter/>

(a partir de 2ª feira, 14/04/2003)

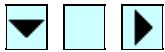
Palestra apresentada na Reunião do [GTS](#), ocorrida em conjunto com a 15ª Reunião do [GTER](#).

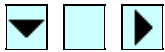
DATA: Quarta-feira, 09/abril/2003, às 11:00

LOCAL:

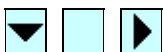
Centro de Convenções Frei Caneca
Rua Frei Caneca, 569, 4º andar
São Paulo - SP

Área de conteúdo atualizada em Wednesday, 2003–April–09 03:52:37 GMT–3 (São Paulo, Brazil, South America)

<h2>Objetivos Estratégia</h2>	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<p>Objetivos</p> <ul style="list-style-type: none"> • Disponibilizar conteúdo para servir de referências futuras • Apresentar soluções criativas com o uso de Netfilter Iptables • Explicar o possível dentro da limitação de tempo: 50 minutos <p>Estratégia</p> <p>Devido à limitação de tempo, optou-se por enriquecer/diversificar o conteúdo, conseqüentemente sacrificando-se as explicações mais detalhadas, embora procurando limitar um pouco o conteúdo para não haver um desequilíbrio exagerado.</p>
<p>Área de conteúdo atualizada em Wednesday, 2003–April–09 04:37:39 GMT–3 (São Paulo, Brazil, South America)</p>	

<h2>Dados do Autor</h2>	
 <p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<p>Back to Home</p> <p>Antonio Augusto de Cintra Batista <antonio@CintraBatista.net></p> <p>Engenheiro Eletrônico</p> <p>Security Officer – Diveo</p> <p>Proprietário – IPtrip – Fabricação de Roteadores de Borda (BGP, OSPF)</p> <p>Fundador em 1987 – SodalyS – Fabricação desde 1991 de aparelhos para o tratamento da hiperhidrose (excesso de suor).</p>
<p>Área de conteúdo atualizada em Wednesday, 2003–April–09 07:12:05 GMT–3 (São Paulo, Brazil, South America)</p>	

Scripts com Iptables



[Back to Home](#)

[Home](#)

Apresentação

:: [Objetivos](#)

[Estratégia](#)

:: [Dados do](#)

[Autor](#)

Visão Geral

:: [Scripts com](#)

[o Iptables](#)

:: [Malformed](#)

[Packets](#)

ARP

Poisoning

:: [ARP](#)

[Poisoning](#)

[default](#)

[gateway](#)

:: [ARP](#)

[Poisoning](#)

[Iptables](#)

Denial of

Service

:: [TCP SYN](#)

[FLOOD:](#)

[características](#)

:: [Syn Flood:](#)

[Resultados](#)

:: [Syn Flood:](#)

[reações mais](#)

[comuns](#)

:: [Syn Flood:](#)

[reação viável](#)

[atualmente](#)

:: [Syn Flood](#)

[Netfilter](#)

:: [Denial of](#)

[Service \(DoS\):](#)

[outros tipos](#)

Exemplo de um script com recursos diversos

```
#!/bin/bash
#
# (C) by Antonio Batista
# Licensed as a free software under GNU GPL version 2
#
# Iptables programs directory
PRGDIR="/usr/local/iptables/bin"
# Iptables data directory
DATDIR="/usr/local/iptables/data"
# Load appropriate modules.
# modprobe ip_tables
# modprobe ip_conntrack
# modprobe ip_conntrack_ftp
# to protect against arp poisoning
GW="10.1.1.1"
MAC="00:02:4B:CB:11:00"
/usr/sbin/arp -s $GW $MAC 2>/dev/null
# These lines are here in case rules are already in place and the script
# is ever rerun on the fly.
# We want to remove all rules and pre-existing user defined chains and
# zero the counters before we implement new rules.
iptables -F
iptables -X
iptables -Z
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
## =====
# RULES
# A custom chain to log and drop.
# We must remember that the LOG target is a
# "non-terminating target", i.e., a match on this rule does
# not stop the rules traversal, and the next target (DROP)
# results evaluated as well.
iptables -N dropcounter
iptables -A dropcounter -j RETURN
iptables -N logdrop
iptables -A logdrop -m limit --limit 10/s --limit-burst 4 -j LOG \
--log-prefix "[SYN FLOOD] "
iptables -A logdrop -j dropcounter
iptables -A logdrop -j DROP
```

GTER15: Exemplos de Aplicações do GNU/Linux Netfilter Iptables

```
iptables -N logmalform
iptables -A logmalform -m limit --limit 10/s --limit-burst 4 -j LOG \
  --log-prefix "[MALFORMED] "
iptables -A logmalform -j DROP

iptables -N malf-group
#$PRGDIR/malf-group.sh
iptables -A malf-group -p tcp --tcp-flags SYN,FIN SYN,FIN -j logmalform
iptables -A malf-group -p tcp --tcp-flags SYN,RST SYN,RST -j logmalform
iptables -A malf-group -p tcp --tcp-flags FIN,RST FIN,RST -j logmalform
iptables -A malf-group -j RETURN

#####
# INPUT chain groups
#####
iptables -N in-best-group
#$PRGDIR/in-best-group.sh
iptables -A in-best-group -j RETURN

# iptables -N in-pre-ids-group
# $PRGDIR/in-pre-ids-group.sh
# iptables -A in-pre-ids-group -j RETURN

iptables -N in-malf-group
#$PRGDIR/in-malf-group.sh
iptables -A in-malf-group -j malf-group
iptables -A in-malf-group -j RETURN

iptables -N in-bad-group
#$PRGDIR/in-bad-group.sh
iptables -A in-bad-group -j RETURN

iptables -N in-good-group
#$PRGDIR/in-good-group.sh
iptables -A in-good-group -j RETURN

iptables -N in-deny-group
#$PRGDIR/in-deny-group.sh
iptables -A in-deny-group -j RETURN

iptables -N in-accept-group
#$PRGDIR/in-accept-group.sh
iptables -A in-accept-group -j RETURN

iptables -N in-dsg-group
#$PRGDIR/in-dsg-group.sh
iptables -A in-dsg-group -j RETURN

iptables -N in-customer-group
#$PRGDIR/in-customer-group.sh
iptables -A in-customer-group -j RETURN

# iptables -N in-ids-group
# $PRGDIR/in-ids-group.sh
# iptables -A in-ids-group -j RETURN

iptables -N in-fw-group
#$PRGDIR/in-fw-group.sh
iptables -A in-fw-group -j RETURN
```

```

#####
# FORWARD chain groups
#####
# iptables -N fwd-best-group
# $PRGDIR/fwd-best-group.sh
# iptables -A fwd-best-group -j RETURN

# iptables -N fwd-malf-group
#$PRGDIR/fwd-malf-group.sh
# iptables -A fwd-malf-group -j malf-group
# iptables -A fwd-malf-group -j RETURN

# iptables -N fwd-bad-group
# $PRGDIR/fwd-bad-group.sh
# iptables -A fwd-bad-group -j RETURN

# iptables -N fwd-good-group
# $PRGDIR/fwd-good-group.sh
# iptables -A fwd-good-group -j RETURN

# iptables -N fwd-deny-group
#$PRGDIR/fwd-deny-group.sh
# iptables -A fwd-deny-group -j RETURN

# iptables -N fwd-accept-group
#$PRGDIR/fwd-accept-group.sh
# iptables -A fwd-accept-group -j RETURN

# iptables -N fwd-dsg-group
#$PRGDIR/fwd-accept-group.sh
# iptables -A fwd-dsg-group -j RETURN

# iptables -N fwd-customer-group
# $PRGDIR/fwd-customer-group.sh
# iptables -A fwd-customer-group -j RETURN

# iptables -N fwd-fw-group
#$PRGDIR/fwd-fw-group.sh
# iptables -A fwd-fw-group -j RETURN

#####
# OUTPUT chain groups
#####
iptables -N out-malf-group
$PRGDIR/out-malf-group.sh
iptables -A out-malf-group -j malf-group
iptables -A out-malf-group -j RETURN

iptables -N out-good-group
$PRGDIR/out-good-group.sh
iptables -A out-good-group -j RETURN

iptables -N out-fw-group
$PRGDIR/out-fw-group.sh
iptables -A out-fw-group -j RETURN

## SYN-FLOOD

```

GTER15: Exemplos de Aplicações do GNU/Linux Netfilter Iptables

```
#
iptables -N syn-flood
iptables -A syn-flood -m limit --limit 50/s --limit-burst 4 -j RETURN
iptables -A syn-flood -j logdrop

#####
# INPUT
#####
# The conventional chains
iptables -A INPUT -i lo -j ACCEPT
# Best Group
iptables -A INPUT -j in-best-group
# Pre-IDS Group
# iptables -A INPUT -j in-pre-ids-group
# Malformed
iptables -A INPUT -j in-malf-group
# Bad VIP
iptables -A INPUT -j in-bad-group
# Good VIP
iptables -A INPUT -j in-good-group
# Deny Group
iptables -A INPUT -j in-deny-group
# Accept Group
iptables -A INPUT -j in-accept-group
# Deny Services Group
iptables -A INPUT -j in-dsg-group
# Customer Group
iptables -A INPUT -j in-customer-group
# Syn Flood
iptables -A INPUT -p tcp --syn -j syn-flood
# Firewall
iptables -A INPUT -j in-fw-group
# DEFAULT DROP
iptables -A INPUT -m limit --limit 10/s --limit-burst 4 -j LOG \
  --log-prefix "[INPUT FW] "
iptables -A INPUT -j DROP
# IDS Group
# iptables -A INPUT -j in-ids-group
# iptables -A INPUT -j DROP

#####
# FORWARD
#####
# Best VIP
# iptables -A FORWARD -j fwd-best-group
# Malformed
# iptables -A FORWARD -j fwd-malf-group
# Bad VIP
# iptables -A FORWARD -j fwd-bad-group
# Good VIP
# iptables -A FORWARD -j fwd-good-group
# Deny Group
# iptables -A FORWARD -j fwd-deny-group
# Accept Group
# iptables -A FORWARD -j fwd-accept-group
# Deny Services Group
# iptables -A FORWARD -j fwd-dsg-group
# Customer VIP
# iptables -A FORWARD -j fwd-customer-group
```

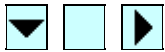
GTER15: Exemplos de Aplicações do GNU/Linux Netfilter Iptables

```
# Syn Flood
# iptables -A FORWARD -p tcp --syn -j syn-flood
# Firewall
# iptables -A FORWARD -j fwd-fw-group
# DEFAULT ACCEPT
# iptables -A FORWARD -m limit --limit 10/s --limit-burst 4 -j LOG \
# --log-prefix "[FORWARD FW] "
# iptables -A FORWARD -j ACCEPT

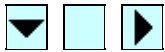
#####
# OUTPUT
#####
iptables -A OUTPUT -o lo -j ACCEPT
# Malformed
iptables -A OUTPUT -j out-malf-group
# Good VIP
iptables -A OUTPUT -j out-good-group
# Deny Group
# Accept Group
# Deny Services Group
# SynFlood
iptables -A OUTPUT -p tcp --syn -j syn-flood
# Firewall
iptables -A OUTPUT -j out-fw-group
# DEFAULT ACCEPT
iptables -A OUTPUT -j ACCEPT

# THE END
# =====
```

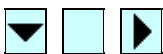
Área de conteúdo atualizada em Wednesday, 2003–April–09 10:35:50 GMT–3 (São Paulo, Brazil, South America)

<h1>Pacotes fora do padrão</h1>	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos :: Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<h2>Exemplo de regras</h2> <pre>iptables -N logmalform iptables -A logmalform -m limit --limit 10/s --limit-burst 4 -j LOG \ --log-prefix "[MALFORMED] " iptables -A logmalform -j DROP iptables -N malf-group #\$PRGDIR/malf-group.sh iptables -A malf-group -p tcp --tcp-flags SYN,FIN SYN,FIN -j logmalform iptables -A malf-group -p tcp --tcp-flags SYN,RST SYN,RST -j logmalform iptables -A malf-group -p tcp --tcp-flags FIN,RST FIN,RST -j logmalform iptables -A malf-group -j RETURN</pre>

Área de conteúdo atualizada em Wednesday, 2003–April–09 10:39:20 GMT–3 (São Paulo, Brazil, South America)

ARP Poisoning default gateway	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<h2 style="text-align: center;">Entradas estáticas na tabela ARP</h2> <pre>GW="10.1.1.1" MAC="00:02:4B:CB:11:00" /usr/sbin/arp -s \$GW \$MAC 2>/dev/null</pre> <p>Pode-se fazer o mesmo com outros gateways ou máquinas mais críticas</p> <p>Consultando a tabela ARP:</p> <pre>arp -na</pre>
<p>Área de conteúdo atualizada em Wednesday, 2003-April-09 02:22:17 GMT-3 (São Paulo, Brazil, South America)</p>	

ARP Poisoning Iptables



[Back to Home](#)

[Home](#)

Apresentação

:: [Objetivos](#)

[Estratégia](#)

:: [Dados do](#)

[Autor](#)

Visão Geral

:: [Scripts com](#)

[o Iptables](#)

:: [Malformed](#)

[Packets](#)

ARP

Poisoning

:: [ARP](#)

[Poisoning](#)

[default](#)

[gateway](#)

:: [ARP](#)

[Poisoning](#)

[Iptables](#)

Denial of

Service

:: [TCP SYN](#)

[FLOOD:](#)

[características](#)

:: [Syn Flood:](#)

[Resultados](#)

:: [Syn Flood:](#)

[reações mais](#)

[comuns](#)

:: [Syn Flood:](#)

[reação viável](#)

[atualmente](#)

:: [Syn Flood](#)

[Netfilter](#)

:: [Denial of](#)

[Service \(DoS\):](#)

[outros tipos](#)

EXEMPLO de "programação" de firewall camada 2, ou roteador:

```
# ARP Poisoning
iptables -A FORWARD -j arp-fw-group
# Best VIP
iptables -A FORWARD -j fwd-best-group
# Malformed
iptables -A FORWARD -j fwd-malf-group
# Bad VIP
iptables -A FORWARD -j fwd-bad-group
# Good VIP
iptables -A FORWARD -j fwd-good-group
# Deny Group
iptables -A FORWARD -j fwd-deny-group
# Accept Group
iptables -A FORWARD -j fwd-accept-group
# Deny Services Group
iptables -A FORWARD -j fwd-dsg-group
# Customer VIP
iptables -A FORWARD -j fwd-customer-group
# Syn Flood
iptables -A FORWARD -p tcp --syn -j syn-flood
# Firewall
iptables -A FORWARD -j fwd-fw-group
# DEFAULT DROP
iptables -A FORWARD -m limit --limit 10/s --limit-burst 4 -j LOG \
--log-prefix "[FORWARD FW] "
iptables -A FORWARD -j DROP
```

Chain arp-fw-group em detalhes:

```
iptables -N arp-fw-group
iptables -A arp-fw-group -p all -m mac --mac-source ! 00:11:22:33:44:55 \
-s 10.1.2.3 -j DROP
iptables -A arp-fw-group -p all -s 10.1.2.3 -j RETURN
iptables -A arp-fw-group -p all -m mac --mac-source ! 66:77:88:99:AA:BB \
-s 10.1.2.4 -j DROP
iptables -A arp-fw-group -p all -s 10.1.2.4 -j RETURN
iptables -A arp-fw-group -p all -s 10.1.2.0/23 -j DROP
# Bloqueia todo o restante por default
iptables -A arp-fw-group -p all -j DROP
```

A ferramenta está aí... para colocar em produção de forma escalável, pode-se criar uma política e implantá-la tecnicamente fazendo scripts que consultam a tabela do **arpwatch**:

- /var/lib/arpwatch/eth0.dat

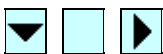
- /var/lib/arpwatch/eth1.dat

Pode-se utilizar esta chain arp-fw-group – que criamos – nas seguintes chains pré-definidas:

- PREROUTING, para pacotes que acabaram de entrar nas tabelas **nat** ou **mangle**.
- INPUT, para pacotes que acabaram de entrar nas tabelas **filter** ou **mangle**.
- FORWARD, no caso de firewall camada 2 (firewall em bridge), ou firewall operando como roteador. Tabelas: **filter** ou **mangle**.

Área de conteúdo atualizada em Wednesday, 2003–April–09 03:34:07 GMT–3 (São Paulo, Brazil, South America)

TCP SYN FLOOD: características



[Back to Home](#)

[Home](#)

Apresentação

:: [Objetivos Estratégia](#)

:: [Dados do Autor](#)

Visão Geral

:: [Scripts com o Iptables](#)

:: [Malformed Packets](#)

ARP Poisoning

:: [ARP Poisoning default gateway](#)

:: [ARP Poisoning Iptables](#)

Denial of Service

:: [TCP SYN FLOOD: características](#)

:: [Syn Flood: Resultados](#)

:: [Syn Flood: reações mais comuns](#)

:: [Syn Flood: reação viável atualmente](#)

:: [Syn Flood Netfilter](#)

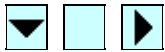
:: [Denial of Service \(DoS\): outros tipos](#)

Características típicas:

- 30 a 100 K pacotes/segundo (um portscan gera em torno de 0.5 a 1.0 K pacotes/segundo).
- Pacotes tipicamente de 40 bytes.
- Endereço de origem falsificado sem repetição (para dificultar identificação da origem).
- A quase totalidade das Operadoras não têm processos bem definidos para identificar a interface mais externa de sua rede por onde entra o DoS.
- Endereço de destino bem determinado.
- Um laptop PIII 600 MHz é capaz de gerar 17 K pacotes/segundo com falsificação randômica do endereço IP de origem.
- Quase 100% dos ataques DoS são originados do Exterior, e acontecem durante o nosso horário comercial (o intuito é causar mais impacto, à noite ou final-de-semana um cliente de um ISP costuma nem perceber que foi atacado).
- O que a Imprensa costuma divulgar como DDoS pode não passar de DoS proveniente de uma única máquina.

- **Sintoma 1:** ataque SYN flood à porta de http de um cliente brasileiro? **Causa provável:** alguém no Exterior está **muito** nervoso porque recebeu um SPAM anunciando o tal website, e o ISP não respondeu ou não tomou atitude. Vide newsgroup de SPAM, spews.org e spamhaus.org.
- **Sintoma 2:** o ataque passou a se estender para outros servidores "inocentes"? **Causa provável:** o SPAM é muito insistente e o tal carinha que o recebeu está **hiper** nervoso. **Solução:** a mais barata pode ser cancelar o contrato com o seu cliente que hospeda o site do spammer?

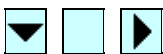
Área de conteúdo atualizada em Wednesday, 2003–April–09 10:52:00 GMT–3 (São Paulo, Brazil, South America)

<h2>Syn Flood: Resultados</h2>	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<ul style="list-style-type: none"> • 2 a 3 K pacotes/segundo já são suficientes para causar DoS em todos os firewalls conhecidos (nem precisa dos 30 a 100 K pkts/s). • Firewall está em DoS => toda a estrutura de rede abaixo dele está em DoS, e não somente o endereço IP destinatário do ataque. • O recurso que os firewalls e equipamentos de rede costumam chamar de <i>Syn Flood Defender</i> não passa de um portscan defender, e ainda faz com que estes equipamentos entrem em DoS mais rapidamente. Portscan é tipicamente originado por IP de origem verdadeiro (não "spoofado"). • Após alguns segundos sob TCP Syn Flood, todos os firewalls conhecidos precisam de um boot manual porque não conseguem retornar sozinhos à sua condição normal, após cessado o ataque. • Se colocarmos o OpenBSD, FreeBSD e Linux configurados em bridge (2 interfaces ethernet em série com o tráfego IP), os 2 primeiros atingem 100% de CPU no início de um DoS do tipo Syn Flood. O Linux mantém o consumo médio em torno de 15%.

- Mesmo tendo baixo consumo de CPU durante o ataque, os recursos internos do Linux se tornam escassos e ocorre significativa degradação (mas não indisponibilidade). Há tempo para uma detecção e uma reação.

Área de conteúdo atualizada em Wednesday, 2003–April–09 10:48:36 GMT–3 (São Paulo, Brazil, South America)

Syn Flood: reações mais comuns



[Back to Home](#)

[Home](#)

Apresentação

:: [Objetivos](#)

[Estratégia](#)

:: [Dados do](#)

[Autor](#)

Visão Geral

:: [Scripts com o](#)

[Iptables](#)

:: [Malformed](#)

[Packets](#)

ARP Poisoning

:: [ARP](#)

[Poisoning](#)

[default gateway](#)

:: [ARP](#)

[Poisoning](#)

[Iptables](#)

Denial of Service

:: [TCP SYN](#)

[FLOOD:](#)

[características](#)

:: [Syn Flood:](#)

[Resultados](#)

:: [Syn Flood:](#)

[reações mais](#)

[comuns](#)

:: [Syn Flood:](#)

[reação viável](#)

[atualmente](#)

:: [Syn Flood](#)

[Netfilter](#)

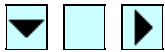
:: [Denial of](#)

[Service \(DoS\):](#)

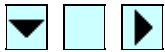
[outros tipos](#)

- Identificação do endereço IP atacado.
- Bloqueio rápido deste IP atacado (garantir a disponibilidade do restante da rede).
- Identificação da interface de rede intra-AS mais externa, e AS adjacente.
- Solicitar que o AS adjacente identifique a sua interface de rede intra-AS mais externa, e assim sucessivamente até chegar na origem. Esta abordagem é hoje muito teórica e não funciona na prática com a grande maioria dos AS's.
- **Alternativa viável que sobrou:** identificar e bloquear o endereço IP atacado, o mais rapidamente possível.
- **Uma alternativa esperada para futuro (breve?):** ICMP traceback
<http://www.ietf.org/internet-drafts/draft-ietf-itrace-04.txt>
 Meu sentimento a respeito: falta algoritmo de garantia de autenticidade da origem destes pacotes (e não é por falta de tecnologia para isto).

Área de conteúdo atualizada em Wednesday, 2003-April-09 10:58:07 GMT-3 (São Paulo, Brazil, South America)

Syn Flood: reação viável atualmente	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<h2>Requer a solução de um PROBLEMA PRINCIPAL</h2> <ul style="list-style-type: none"> • Detecção automática e rápida do endereço IP atacado.
<p>Área de conteúdo atualizada em Wednesday, 2003–April–09 06:24:07 GMT–3 (São Paulo, Brazil, South America)</p>	

<h1>Syn Flood Netfilter</h1>	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<h2 style="text-align: center;">Regras de iptables</h2> <ul style="list-style-type: none"> • Chains criadas para a detecção: <pre>## SYN-FLOOD # iptables -N syn-flood iptables -A syn-flood -m limit --limit 500/s --limit-burst 4 -j RETURN iptables -A syn-flood -j logdrop iptables -N logdrop iptables -A logdrop -m limit --limit 10/s --limit-burst 4 -j LOG \ --log-prefix "[SYN FLOOD] " iptables -A logdrop -j DROP</pre> <ul style="list-style-type: none"> • Exemplo de como elas podem ser chamadas: <pre># Customer chain iptables -A FORWARD -j fwd-customer-group # Syn Flood iptables -A FORWARD -p tcp --syn -j syn-flood # Firewall chain iptables -A FORWARD -j fwd-fw-group # DEFAULT DROP iptables -A FORWARD -m limit --limit 10/s --limit-burst 4 -j LOG \ --log-prefix "[FORWARD FW] " iptables -A FORWARD -j DROP</pre>
<p>Área de conteúdo atualizada em Wednesday, 2003–April–09 10:59:59 GMT–3 (São Paulo, Brazil, South America)</p>	

Denial of Service (DoS): outros tipos	
	Back to Home
<p>Home</p> <p>Apresentação :: Objetivos Estratégia :: Dados do Autor</p> <p>Visão Geral :: Scripts com o Iptables :: Malformed Packets</p> <p>ARP Poisoning :: ARP Poisoning default gateway :: ARP Poisoning Iptables</p> <p>Denial of Service :: TCP SYN FLOOD: características :: Syn Flood: Resultados :: Syn Flood: reações mais comuns :: Syn Flood: reação viável atualmente :: Syn Flood Netfilter :: Denial of Service (DoS): outros tipos</p>	<ul style="list-style-type: none"> • Seja o protocolo ICMP, UDP, OSPF, IP-in-IP, SCTP, ... • A abordagem é análoga, com pequenas adaptações (configurações) para atender necessidades particulares.
<p>Área de conteúdo atualizada em Wednesday, 2003–April–09 06:55:13 GMT–3 (São Paulo, Brazil, South America)</p>	