

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Performing a Slowloris DoS attack \[STEP BY STEP EASY TO FOLLOW\]](#)

Morbsy - June 9, 2011, 9:10 pm

HOW TO SUCCESSFULLY PERFORM A SLOWLORIS DOS ATTACK

Hi all, lately I've been having a lot of random people adding me on MSN asking me how to DoS a website with their own internet connection, I'm all for helping these people but it gets tiring explaining things and team viewing all the time so I thought I would make a step by step tutorial that even newbies will find easy to follow.

I'm not going to go into detail on how it works so if you want a detailed explanation you can visit the "official" page below:

<http://hackers.org/slowloris/>

Step 1

Ok so the first thing you want to do is check to see if your target website is vulnerable to a Slowloris DoS attack.

The following are confirmed as vulnerable: Apache 1.x

Apache 2.x

GoAhead WebServer

Apache is a very popular webserver and these versions are still extremely easy to come by.

You can check which version a site is running by visiting the link below:

<http://uptime.netcraft.com/>

(There are many other ways to do this, but for beginners this is a simple page you can bookmark)

So just type in the URL of your target in the search box at the top of the page

You will then be brought to this page;

[attachment=103]

as you can see in the picture, it lists the webserver as Apache/2.2.3 (FH) - This means it is vulnerable :]

So now you know your target is vulnerable, now what?

Step 2

I'm going to assume your using a windows based machine, if your already using a linux then you will have no problems doing any of these next steps.

You will need to download VMWare Workstation and Backtrack 4.

(Doesnt have to be Backtrack, but it is useful for other tasks so you might aswell get it)

If you watch this tutorial it will show you how to set it all up

(Both programs can be obtained through popular torrent sites)

This video was not made by me

[Video: <http://www.youtube.com/watch?v=ICwTdOgszA8>]

Step 3

Assuming you have followed the instructions up until now you should have a Linux system or Backtrack opened in front of you.

If you forgot the login info for backtrack already it is;

User: root

Pass: toor

then type: startx

Once its done loading you will need to open Konsole and type the following;

```
ifconfig eth0 up
```

```
dhclient eth0
```

This will enable your networking.

Then also type in the following to install the appropriate modules;

There will be some prompts you will need to press yes or no.. `perl -MCPAN -e 'install IO::Socket::INET'`

```
perl -MCPAN -e 'install IO::Socket::SSL'
```

Now you should have an operating system that can access the internet. Try opening the Firefox browser just to test. If it doesn't work for you PM me and I will help you set up.

Step 4

Go back to windows and visit the below URL:

<http://hackers.org/slowloris/slowloris.pl>

This is the Slowloris script, make sure you copy the entire script - the best way to do this is CTRL+A then copy.

Go back into Backtrack and open up "Kate - Advanced Text Editor"

By click on the "Start" icon > Utilities > Kate

If you still cant find it I have included a picture below;

[attachment=104]

Once you have opened Kate, click on "New Session"

Then just right click and paste, like you would any other text program.

Now click File>Save As> slowloris.pl

Just save it in /root/ for easy access, should be automatically set to root anyway.

Now you should have a perl file called "Slowloris.pl" on the "desktop"

Step 5

Now you finally get to initiate your attack.

Open up Konsole again and type the following;

```
perl slowloris.pl -dns [WEBSITE URL HERE] -port 80 -timeout 500 -num 600 -tcpto 5
```

Let me elaborate..

"perl slowloris.pl" is simply telling it to open that file, "-dns [website]" is the website you want to attack, "-port 80" is the port to attack, 80 is best for websites "-timeout 500" is how long your threads

will sleep for.

You can change timeout if you want but I find these setting work best. All other settings should not be changed for this particular attack.

Step 6

Now wait it out, give it some time to build. It can take up to 5 minutes some times but once its down it will stay down until you stop the attack.

You can stop the attack by CTRL+C

Here are some other commands that may also be of use to you, they have been copied direct from the script itself;

Code HTTPReady Bypass

HTTPReady only follows certain rules so with a switch Slowloris can bypass HTTPReady by sending the attack as a POST verses a GET or HEAD request with the -httpready switch.

HTTPReady Bypass Example

```
perl slowloris.pl -dns www.example.com -port 80 -timeout 2000 -num 500 -tcpto 5 -httpready
```

Stealth Host DoS

If you know the server has multiple webserver running on it in virtual hosts, you can send the attack to a seperate virtual host using the -shost variable. This way the logs that are created will go to a different virtual host log file, but only if they are kept separately.

Stealth Host DoS Example:

```
perl slowloris.pl -dns www.example.com -port 80 -timeout 30 -num 500 -tcpto 1 -shost  
www.virtualhost.com
```

HTTPS DoS

Slowloris does support SSL/TLS on an experimental basis with the -https switch. The usefulness of this particular option has not been thoroughly tested, and in fact has not proved to be particularly effective in the very few tests I performed during the early phases of development. Your mileage may vary.

HTTPS DoS Example:

```
perl slowloris.pl -dns www.example.com -port 443 -timeout 30 -num 500 -https
```

HTTP Cache

Slowloris does support cache avoidance on an experimental basis with the -cache switch. Some caching servers may look at the request path part of the header, but by sending different requests each time you can abuse more resources. The usefulness of this particular option has not been thoroughly tested. Your mileage may vary.

HTTP Cache Example:

perl slowloris.pl -dns www.example.com -port 80 -timeout 30 -num 500 -cache
CONCLUSION - -

I hope this Tutorial was helpful for you and if you have an questions please feel free to PM me.
Also if I've left anything out please let me know :)

Bibliography;

www.hackers.org
www.uptime.netcraft.com

This guide was written and compiled by myself and you will not find it anywhere else.
I give credit to ha.ckers.org and netcraft.com

Thanks for reading!

-Morbsy

NotAk-47 - June 9, 2011, 9:21 pm

Thanks, do you have a msn i could contact you at i actually had a few questions about it. p.s repped for the good tutorial :)

Morbsy - June 9, 2011, 9:23 pm

(Jun 9, 2011 09:21 PM)Inferior Wrote: [\[CITE\]](#) Thanks, do you have a msn i could contact you at i actually had a few questions about it. p.s repped for the good tutorial :)
MSN is in my signature :)

Cheers

gladiator17 - June 9, 2011, 9:31 pm

is it possibl 2 hack user accounts in mobile chat sites???? plzz m very eager 2 knw abt it.

Mr.Cube - June 9, 2011, 9:47 pm

wow great effort on the guide very understandable good work:D

NotAk-47 - June 9, 2011, 9:51 pm

Added your msn, please add me back (wreckedrs@live.com) Thanks!

Morbsy - June 9, 2011, 11:57 pm

(Jun 9, 2011 09:47 PM)chives Wrote: [\[CITE\]](#) wow great effort on the guide very understandable good work:D

Thanks, took me a few hours. But should save time in the long run.

cY?eRteRR?Ri?t - June 10, 2011, 12:01 am

Very nice tut bro great job :}

conan_1 - June 10, 2011, 12:33 am

Great Job Mate ;) well done !

-iLikeRainbows. - July 6, 2011, 12:01 pm

Great Guide, Will certainly help people :)

Forever Young - July 6, 2011, 12:40 pm

Nice tut, but it much easier to use QSlowloris which is Windows based and works the same...

PenGuin :O - July 6, 2011, 12:47 pm

Do you still need to use a VPN / Proxy to not getting caught?

kevin_n - July 6, 2011, 12:51 pm

thanks alot buddy.im gonna check it out.in addition i'll add u to ask my question.
best regards

thethatguy - July 6, 2011, 1:05 pm

(Jul 6, 2011 12:47 PM)PenGuin :O Wrote: [\[CITE\]](#) Do you still need to use a VPN / Proxy to not getting caught?

Your are posting packets to the server there is no way that they can prove that DOS was your goal. Every time you click something on a site you send and receive packets. I have attacked more Apache servers than I have written my name never heard a word.

I once had a server offline 43 hours not sure if the cpu defragmented the temporary file load or if they restarted it.

SIM-429621 - July 6, 2011, 1:22 pm

I just tried it on apache 2.2.9 and after 13638 packets sent the website is still online.

thethatguy - July 6, 2011, 1:33 pm

(Jul 6, 2011 01:22 PM)Passenger Wrote: [\[CITE\]](#) I just tried it on apache 2.2.9 and after 13638 packets sent the website is still online.

So why did you stop ? How many childs ?

SIM-429621 - July 6, 2011, 1:51 pm

(Jul 6, 2011 01:33 PM)thethatguy Wrote: [\[CITE\]](#) So why did you stop ? How many childs ?

I stopped because I have been waiting for about 10 mins and in the thread it's stated that the victim should be down in about 5mins, this server is nothing special, it just seems that it doesn't work with 2.2.9 at least.

BTW: wtf are childs?

PenGuin :O - July 6, 2011, 1:57 pm

(Jul 6, 2011 01:05 PM)thethatguy Wrote: [\[CITE\]](#) Your are posting packets to the server there is no way that they can prove that DOS was your goal. Every time you click something on a site you send and receive packets. I have attacked more Apache servers than I have written my name never heard a word.

I once had a server offline 43 hours not sure if the cpu defragmented the temporary file load or if they restarted it.

But youre doing so much requests in a short time.

Its obvious that your goal is to take down that site, isnt it? :/

thethatguy - July 6, 2011, 2:05 pm

(Jul 6, 2011 01:57 PM)PenGuin :O Wrote: [\[CITE\]](#) But youre doing so much requests in a short time.

Its obvious that your goal is to take down that site, isnt it? :/

No you had your verbatim gaming mouse on by accident which hits 50 times a millisecond and your friend messed around on your pc and what's dos.

Anyway I found this will let you know if it goes down and after how long.

Frequenceh - July 6, 2011, 2:10 pm

(Jul 6, 2011 01:51 PM)Passenger Wrote: [\[CITE\]](#) I stopped because I have been waiting for about 10 mins and in the thread it's stated that the slave should be down in about 5mins, this server is nothing special, it just seems that it doesn't work with 2.2.9 at least.

BTW: wtf are childs?

Something you like to touch.

thethatguy - July 6, 2011, 2:29 pm

(Jul 6, 2011 02:05 PM)thethatguy Wrote: [\[CITE\]](#) No you had your verbatim gaming mouse on by accident which hits 50 times a millisecond and your friend messed around on your pc and what's dos.

Anyway I found this will let you know if it goes down and after how long.

[>> Down <<](#)

The message is . Please enter a message longer than 25 characters.

xarisis - July 7, 2011, 4:20 am

I totally appreciate your work and I was glad to see that there are still some smart people here but why the hell are you providing (script) kids with machine guns?

They will pull the trigger everywhere without thinking of the consequences! Seriously. We don't need any more cyber kids messing around and if they actually hit a site they will propably get arrested as they won't be able to cover their tracks. Anyway, what I wanted to say is good job composing this tutorial.

AliKasra - July 7, 2011, 8:46 am

hey man very nice thank you so much ;)

AliKasra - July 7, 2011, 8:46 am

hey man very nice thank you so much ;)

iqbal678 - July 7, 2011, 11:03 am

Nice tutorial thanx bro.. will help me a lot...

unknown2 - July 28, 2011, 6:38 am

Followed all the steps the terminal stuck on "Building sockets" for a long time,what to do?

No??????? - July 28, 2011, 6:54 am

This is a great tutorial, I will definitely be trying this later on.

razor1911 - July 28, 2011, 7:22 am

There is a lot easier way to do this but props to OP for the effort.

Anonymous.7654 - July 29, 2011, 8:24 am

Thanks so much for the Guide,i always use Slowloris and Linux.

tarung1793 - August 15, 2011, 12:52 pm

Thank you for this guide It is really helpfull....

ThankYouAndGoodbye - August 15, 2011, 2:17 pm

Am i the only person that thinks this is in the wrong section?

Useful but in the wrong section

Happy Hacking

s0lar

Morbsy - September 30, 2011, 2:33 am

(Aug 15, 2011 02:17 PM)sol@ris Wrote: [CITE](#) Am i the only person that thinks this is in the wrong section?

Useful but in the wrong section

Happy Hacking

s0lar

You are correct, however people will look in this forum for such topics.

Cheers

darkmaster121 - September 30, 2011, 8:22 am

very detailed tutorial, thanks for writing it. Must have taken a while ?

noober1001 - October 12, 2011, 11:58 pm

Great guide bro.

Thank you so much for this.

anonymau5e - November 20, 2012, 8:05 pm

For some reason it works, but it's only sending 0 packets!?