

Forum:[Hack Forums](#)

Thread: [Basic SlowLoris Guide](#)

Osiris - May 20, 2019, 7:23 am

NOTE: Yes, I meant to post this in the tutorial section. But from what I understand, HF has banned a lot of discussions related to Blackhat activity so it was damn near impossible for me to really go into depth and explain how it works so I suggest you simply google it yourself. There are also different codes floating around out there but I recommend the one here in this thread.

EDUCATIONAL PURPOSES ONLY

Hello, this is my first post here after 5-6 years. I used to be part of the Reviewers back in the day and I heard the site kind of fell off but I am going to give it another chance. Anyway, I am not sure if this has been posted yet but I'd like to share a fun little Perl script that you guys might find useful. Fact of the matter is I am sure you've heard of it but I haven't seen it on here yet! I am quite sure many people know about this, but there's probably some who don't. We'll see.

First, a little brief background about the code.

Basically, this is what is known as the Slo*loris attack. It is a very unique attack in the sense that it is the name given to a Perl HTTP client that can be used if need be as a DOS stress testing tool against most, but not all Apache-based HTTP servers. There is however, an unimaginable amount of general packets.

Slo*loris operates by repeatedly starting up a large amount of valid HTTP packet requests to the server, while in turn using the TCP traffic to keep the connections open. By doing this, it consumes large amounts of resources from the target server.

and keeping these connections open using a minimal amount of TCP traffic, in order to consume server resources. Once server resources are exhausted, the server will no longer be able to respond to legitimate traffic.

Slooris is the name of a perl-based HTTP client that can be used as a tool to test your own home's web speed, your business website speed, and experimental stress testing to ensure your site is at peak performance. It is quite the marvel, and it's an oldie too. It operates by repeatedly initiating several hundred completely valid HTTP requests to the server, and in turn keeping the same connections open using a minimal amount of TCP traffic, in order to consume as much server resources as possible. Once server resources are exhausted, the server will no longer be able to respond to legitimate traffic.

How Is It Done?

Disclaimer: Anything you read, do not do. This is strictly for educational purposes only. If you decide to do anything said by me, I am not responsible at all for your actions.

The Sloloris is a very simple DOS attack. The idea of any DOS/DDoS attack, is simply that you try to overload a target by giving it as much bandwidth as possible, causing it to break. It is a layer 7 attack. Slooris is different from typical denials of service in that Slooris traffic utilizes legitimate HTTP traffic, and does not rely on using special "bad" HTTP requests that exploit bugs in specific HTTP servers. Because of this, existing IPS and IDS solutions that rely on signatures to detect attacks will generally not recognize Slooris. This means that Slooris is capable of being effective even when

standard enterprise-grade IPS and IDS systems are in place.

EDUCATIONAL AND TESTING PURPOSES ONLY

I am going to keep this section very brief because this is a touchy subject, however, if you'd like some more information in regards to this attack or any others, do let me know. It is fairly easy to setup, but I can help with this as well.

Programs Needed For Windows

Windows 7-10:

Perl

sl*wloris . pl <--- code. no spaces between period

[Directions]

Combine the Perl program in one folder, along with the sl*wloris.pl script

Ensure the directory is set correctly, it is fairly common sense at this point

Enter the destination information

For example:

>>>> # cd /thePathToYourSl*wloris.plFile

3)# ./sl*wloris.pl

4)# perl sl*wloris.pl -dns (Stress Site URL or IP) -options <<<<<

Needed programs for Linux:

Ubuntu 14.04.1

Linux kernel 3.13.0-33-generic

Apache 2.4.7-1ubuntu4.9

nginx 1.4.6-1ubuntu3.4

slowhttptest 1.6-1

The code used for Linux: slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u (hostthere) -x 24 -p 3

Easy stuff. Enjoy guys.

ShinyThings - May 20, 2019, 7:27 am

Talk about a trip down memory lane to 2009

Osiris - May 20, 2019, 7:35 am

(May 20, 2019 07:27 AM)ShinyThings Wrote: [\[CITE\]](#) Talk about a trip down memory lane to 2009

You can tell I haven't been on here in a long time, lmao.

ShinyThings - May 20, 2019, 7:36 am

(May 20, 2019 07:35 AM)Osiris Wrote: [\[CITE\]](#) You can tell I haven't been on here in a long time, lmao.

I remember using Slowloris when everyone else was using loic haha most of these methods won't even take down a small site these days

Osiris - May 20, 2019, 7:38 am

(May 20, 2019 07:36 AM)ShinyThings Wrote: [\[CITE\]](#) I remember using Slowloris when everyone else was using loic haha most of these methods won't even take down a small site these days

Indeed, it will take down your regular old home connection though quite easily. It depends really. It's certainly nothing crazy strong but it's a nice little code for beginners and it's kind of fun to mess with.

bluriy - May 20, 2019, 7:41 am

(May 20, 2019 07:23 AM)Osiris Wrote: [\[CITE\]](#) NOTE: Yes, I meant to post this in the tutorial section. But from what I understand, HF has banned a lot of discussions related to Blackhat activity so it was damn near impossible for me to really go into depth and explain how it works so I suggest you simply google it yourself. There are also different codes floating around out there but I recommend the one here in this thread.

EDUCATIONAL PURPOSES ONLY

Hello, this is my first post here after 5-6 years. I used to be part of the Reviewers back in the day and I heard the site kind of fell off but I am going to give it another chance. Anyway, I am not sure if this has been posted yet but I'd like to share a fun little Perl script that you guys might find useful. Fact of the matter is I am sure you've heard of it but I haven't seen it on here yet! I am quite sure many people know about this, but there's probably some who don't. We'll see.

First, a little brief background about the code.

Basically, this is what is known as the Slo*loris attack. It is a very unique attack in the sense that it is the name given to a Perl HTTP client that can be used if need be as a DOS stress testing tool against most, but not all Apache-based HTTP servers. There is however, an unimaginable amount of general packets.

Slo*loris operates by repeatedly starting up a large amount of valid HTTP packet requests to the server, while in turn using the TCP traffic to keep the connections open. By doing this, it consumes large amounts of resources from the target server.

and keeping these connections open using a minimal amount of TCP traffic, in order to consume server resources. Once server resources are exhausted, the server will no longer be able to respond to legitimate traffic.

Slooris is the name of a perl-based HTTP client that can be used as a tool to test your own home's web speed, your business website speed, and experimental stress testing to ensure your site is at peak performance. It is quite the marvel, and it's an oldie too. It operates by repeatedly initiating several hundred completely valid HTTP requests to the server, and in turn keeping the same connections open using a minimal amount of TCP traffic, in order to consume as much server resources as possible. Once server resources are exhausted, the server will no longer be able to respond to legitimate traffic.

How Is It Done?

Disclaimer: Anything you read, do not do. This is strictly for educational purposes only. If you decide to do anything said by me, I am not responsible at all for your actions.

The Sloloris is a very simple DOS attack. The idea of any DOS/DDoS attack, is simply that you try to overload a target by giving it as much bandwidth as possible, causing it to break. It is a layer 7 attack. Slooris is different from typical denials of service in that Slooris traffic utilizes legitimate HTTP traffic, and does not rely on using special "bad" HTTP requests that exploit bugs in specific HTTP servers. Because of this, existing IPS and IDS solutions that rely on signatures to detect attacks will generally not recognize Slooris. This means that Slooris is capable of being effective even when standard enterprise-grade IPS and IDS systems are in place.

EDUCATIONAL AND TESTING PURPOSES ONLY

I am going to keep this section very brief because this is a touchy subject, however, if you'd like some more information in regards to this attack or any others, do let me know. It is fairly easy to

setup, but I can help with this as well.

Programs Needed For Windows

Windows 7-10:

Perl

sl*wloris . pl <--- code. no spaces between period

[Directions]

Combine the Perl program in one folder, along with the sl*wloris.pl script

Ensure the directory is set correctly, it is fairly common sense at this point

Enter the destination information

For example:

>>>> # cd /thePathToYourSl*wloris.plFile

3)# ./sl*wloris.pl

4)# perl sl*wloris.pl -dns (Stress Site URL or IP) -options <<<<<

Needed programs for Linux:

Ubuntu 14.04.1

Linux kernel 3.13.0-33-generic

Apache 2.4.7-1ubuntu4.9

nginx 1.4.6-1ubuntu3.4

slowhttptest 1.6-1

The code used for Linux: slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u (hosthere) -x 24 -p 3

Easy stuff. Enjoy guys.

soo good bro thx

(May 20, 2019 07:36 AM)ShinyThings Wrote: [\[CITE\]](#) I remember using Slowloris when everyone else was using loic haha most of these methods won't even take down a small site these days this is really useful

Osiris - May 21, 2019, 8:23 pm

Bump for anyone who's interested in this skid guide still at this time and age.

Remember, it honestly works wonders on home connections. And quite honestly, some websites on a rare occasion!

serviceagent - June 10, 2019, 12:21 pm

LOL. you could just yes kali linux it provides you everything better and slowloris..