

Forum:[Hack Forums](#)

Thread: [Port Scanner By The Alchemist\[PHP\]](#)

The Alchemist16 - January 7, 2013, 10:00 am

Hello Hack Forums,

So, this is an online portscanner coded by me in PHP.

Port Scanners are programs used to check for any open ports in a server. It can be used by website owners to check whether any port in his/her server's is open or not. Or, it may be used by hackers for the same but with a different aim.:D

This port scanner made by me uses multiple(parallel) requests to check whether ports are open on a server or not using TCP scanning.

Since it uses multiple parallel requests, its very fast compared to other portscanners.

Save the file with a .php extension and upload it to your hosting account or your localhost and then, surf the php file.

Its important that your server supports PHP cURL.

Here's the code :

PHP Code

```
<?php
<!DOCTYPE html PUBLIC
"-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Port Scanner</title>

<style type="text/css">

body
{
color: #ffffff;
text-shadow: 2px 2px #000000;
background-color: #282828;
font-family: Arial, Helvetica, sans-serif;
}

pre
{
background-color: #353535;
border: solid 1px #505050;
}

input
{
font-family: Arial, Helvetica, sans-serif;
```

[illegible]

```

if(isset($_POST['target']) && isset($_POST['upper']) && isset($_POST['lower'])
    && isset($_POST['submit']) && is_numeric($_POST['upper']) && is_numeric($_POST['lower'])
    && (filter_var($_POST['target'],FILTER_VALIDATE_IP) || filter_var($_POST['target'],
FILTER_VALIDATE_URL)))
{
    $target = $_POST['target'];
    $flag = 0;
    $lower = $_POST['lower']; //set lower limit
    $upper = $_POST['upper']; //set upper limit
    if($lower <= 0)
    {
        $lower = 1;
    }
    if($upper >= 65536)
    {
        $upper = 65535;
    }
    $numberof = ($upper - $lower) + 1; //number of parallel requests
    $ar = range($lower,$upper); //putting all the ports in an array
    for($i=0 ; $i < $numberof ; $i++)
    {
        $ch[$i] = curl_init($target);
        curl_setopt($ch[$i], CURLOPT_PORT, $ar[$i]);
        curl_setopt($ch[$i], CURLOPT_RETURNTRANSFER, true);
    }
    $mh = curl_multi_init();
    // Thanks to PeopleUnderTheStairs for the idea of using multi cURL
    for($i=0 ; $i < $numberof ; $i++)
    {
        curl_multi_add_handle($mh,$ch[$i]);
    }
    $running = NULL;
    do
    {
        curl_multi_exec($mh,$running);
    }while($running);
    for($i = 0 ; $i < $numberof ; $i++)
    {
        if(!curl_error($ch[$i]))
        {
            $flag = 1;
            echo '<span style="color: #F00;">Port '.$ar[$i].' is open</span><br />';
        }
        curl_multi_remove_handle($mh,$ch[$i]);
        curl_close($ch[$i]);
    }
    curl_multi_close($mh); //All the curl handlers and multi curl handlers are closed
    if($flag == 0)
    {
        echo '<span style="color: #F00;">No open ports found between '.$lower.' and '.$upper.
'</span>';
    }
}

```

?>
</div>
</body>
</html>

Thanks to PeopleUnderTheStairs for giving me the idea of using multi curl handler.

PLEASE GIVE FEEDBACK!!

CarrotMilk - January 7, 2013, 10:28 am

Just to let you know, the isset() function supports multiple parameters so you don't need a bunch of &&s in your conditionals.

The Alchemist16 - January 7, 2013, 10:36 am

^^^ I never knew that.(how could I not know that??? DAMN)

Thanks for notifying. DAMN, how could I miss that out??!!!

CarrotMilk - January 7, 2013, 10:50 am

Don't worry haha, a lot of people don't :')

Novalty - January 7, 2013, 4:27 pm

I just wish that empty() accepted multiple arguments :(

badbrains - January 7, 2013, 4:40 pm

(Jan 7, 2013 05:27 PM)Novalty Wrote: [\[CITE\]](#) I just wish that empty() accepted multiple arguments :(PHP Code

```
<?php
function isEmpty() {
    foreach(func_get_args() as $arg) {
        if(empty($arg)) {
            return true;
        }
    }

    return false;
}

$e = isEmpty('a', 'a', 1);
var_dump($e);
?>
```

The Alchemist16 - January 7, 2013, 8:52 pm

^^^ I've gotta do some research on that function func_get_args()

Will be helpful in the future.

CarrotMilk - January 8, 2013, 7:45 am

PUTS YOU STOLE MY FUNCTION FU.

But instead of empty(), you should use strlen(). It'll return 0 for an empty param (not false), but it'll return 1 for a string '0' or 0 whereas empty() would return true.

badbrains - January 8, 2013, 7:50 am

(Jan 8, 2013 08:45 AM)CarrotMilk Wrote: [\[CITE\]](#) PUTS YOU STOLE MY FUNCTION FU.

But instead of empty(), you should use strlen(). It'll return 0 for an empty param (not false), but it'll return 1 for a string '0' or 0 whereas empty() would return true.

uhh, I never stole it, I've been using that function for a long time now lol.

CarrotMilk - January 8, 2013, 7:52 am

(Jan 8, 2013 08:50 AM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) uhh, I never stole it, I've been using that function for a long time now lol.

<https://hackforums.net/showthread.php?tid=2423972&pid=21919546#pid21919546>

madder than a giraffe on steroids

badbrains - January 8, 2013, 8:02 am

(Jan 8, 2013 08:52 AM)CarrotMilk Wrote: [\[CITE\]](#)

<https://hackforums.net/showthread.php?tid=2423972&pid=21919546#pid21919546>

madder than a giraffe on steroids

>implying i use inline code blocks

yah ur gay boi

neway im goin to school nao

BlackMotion - January 8, 2013, 8:19 am

thanks for source i downloaded it to my archive

Zoidberg - January 8, 2013, 12:49 pm

Great work, I don't even know about this stuff.

Next I'd try making this update realtime with AJAX. IE: scan 1 port, wait for a response, once a response is gotten from the ajax request, write it to the page and move to the next port.

^intentional hr right here, this is not a low quality double post

Oh also if you're using cURL i'd add something in the beginning that will make the script die if cURL is not loaded.

PHP Code

```
<?php
if (!in_array('curl', get_loaded_extensions())) {
    die("<h2>You need to enable php_curl!</h2>");
}
```

badbrains - January 8, 2013, 12:57 pm

(Jan 8, 2013 01:49 PM)Zoidberg Wrote: [\[CITE\]](#) Great work, I don't even know about this stuff.

Next I'd try making this update realtime with AJAX. IE: scan 1 port, wait for a response, once a response is gotten from the ajax request, write it to the page and move to the next port.

^intentional hr right here, this is not a low quality double post

Oh also if you're using cURL i'd add something in the beginning that will make the script die if cURL is not loaded.

PHP Code

```
<?php
if (!in_array('curl', get_loaded_extensions())) {
```

```
die("<h2>You need to enable php_curl!</h2>");
}
```

Why use `in_array()`? Why not this:

PHP Code

```
<?php
if(!extension_loaded('curl')) {
throw new Exception('no curl :(');
}
```

Zoidberg - January 8, 2013, 1:01 pm

(Jan 8, 2013 01:57 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) Why use `in_array()`? Why not this:

PHP Code

```
<?php
if(!extension_loaded('curl')) {
throw new Exception('no curl :(');
}
```

Oh, yeah, forgot about that. Either works I guess.

Vlad1k - January 8, 2013, 3:30 pm

Nice work. Couldn't you use `fopen` too?

Not gonna use it, but its pretty interesting.

badbrains - January 8, 2013, 3:32 pm

(Jan 8, 2013 04:30 PM)Vlad1k Wrote: [\[CITE\]](#) Nice work. Couldn't you use `fopen` too?

Not gonna use it, but its pretty interesting.

Of course you could use `fsockopen`, but it would be much slower than the `cURL` implementation

Vlad1k - January 8, 2013, 3:36 pm

It's just so much easier and cleaner. :3

I would live to have `curl_get_contents()`; ^^

badbrains - January 8, 2013, 3:37 pm

(Jan 8, 2013 04:36 PM)Vlad1k Wrote: [\[CITE\]](#) It's just so much easier and cleaner. :3

I would live to have `curl_get_contents()`; ^^

Sure, it's easier, but `mysql_*` functions are easier too -- Do we use them? There is a time and place to use `fsockopen`, and port scanning is not one of them.

(Jan 8, 2013 04:36 PM)Vlad1k Wrote: [\[CITE\]](#) It's just so much easier and cleaner. :3

I would live to have `curl_get_contents()`; ^^

Oh and:

PHP Code

```
<?php
function curl_get_contents($url, array $opts = array()) {
$defaults = array(
```

```

CURLOPT_FOLLOWLOCATION => true,
CURLOPT_RETURNTRANSFER => true,
CURLOPT_USERAGENT => 'Mozilla Firefox 20.0'
);
$opts = array_merge($defaults, $opts);
$ch = curl_init($url);
curl_setopt_array($ch, $opts);
return curl_exec($ch);
}

```

Vlad1k - January 8, 2013, 3:41 pm

Yeah, I usually make a new function (get_page();), that acts exactly like file_get_contents(), but uses CURL in the function.

I was thinking about learning MySQL, and now its PDO, and its getting even harder. (For meh), that's why CarrotMilk taught me how to store a database remotely in files.

badbrains - January 8, 2013, 3:44 pm

(Jan 8, 2013 04:41 PM)Vlad1k Wrote: [\[CITE\]](#) Yeah, I usually make a new function (get_page();), that acts exactly like file_get_contents(), but uses CURL in the function.

I was thinking about learning MySQL, and now its PDO, and its getting even harder. (For meh), that's why CarrotMilk taught me how to store a database remotely in files.

Sorry, that last function doesn't work properly, this does:

PHP Code

```

<?php
function curl_get_contents($url, array $opts = array()) {
    $defaults = array(
        CURLOPT_FOLLOWLOCATION => true,
        CURLOPT_RETURNTRANSFER => true,
        CURLOPT_USERAGENT => 'Mozilla Firefox 20.0'
    );
    $opts = $opts + $defaults;
    $ch = curl_init($url);
    curl_setopt_array($ch, $opts);

    return curl_exec($ch);
}

echo curl_get_contents('google.ca');
?>

```

CurosMJ - January 9, 2013, 3:52 pm

@Alchemist16, nice work, I am developing an GUI for this thing using Twitter Bootstrap.

It'd be nice if we collaborate on sourceforge.

Just made it. Download : [PortScanner-GUI.zip - 83.3 KB](#)

I can't put it on my hosting coz if i get caught doing such things, they'll probably ban me. It will not look cool until you put it on a real php server.

Hope You guys like this . :D

badbrains - January 9, 2013, 5:56 pm

(Jan 9, 2013 04:52 PM)CurosMJ Wrote: [\[CITE\]](#) @Alchemist16, nice work, I am developing an GUI for this thing using Twitter Bootstrap.

It'd be nice if we collaborate on sourceforge.

Just made it. Download : [PortScanner-GUI.zip - 83.3 KB](#)

I can't put it on my hosting coz if i get caught doing such things, they'll probably ban me.

It will not look cool until you put it on a real php server.

Hope You guys like my work . :D

all you did was put a gui on it using a framework you didn't make LOL

CurosMJ - January 9, 2013, 10:25 pm

(Jan 9, 2013 06:56 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) all you did was put a gui on it using a framework you didn't make LOL

Thank You.?????

?

The Alchemist16 - January 10, 2013, 8:59 pm

Everyone, thanks for the feedbacks and suggestions.

@Zoidberg : I don't know AJAX so, I couldn't make that animation kinda thing... Very soon, I'll learn that too.