

Forum:[Hack Forums](#)

Thread: [Shell Uploaded - Can't back connect?](#)

SIM-1241186 - April 26, 2013, 12:20 pm

So after some quick SQLi, I've got my shell uploaded. I'd like to begin rooting the server, but I can't get netcat to establish a connection with my shell.

I successfully listen on my port:

however when I connect through my shell nothing happens. It's worked in the past, can't seem to figure out what's wrong now.

Any ideas?

Thanks. ?

Processor - April 26, 2013, 12:31 pm

May I ask what shell you are using?

vmkbot - April 26, 2013, 12:34 pm

did you port forward the port 1604, you need to have the port open before it can be addressed.

SIM-1241186 - April 26, 2013, 12:34 pm

(Apr 26, 2013 12:34 PM)vmkbot Wrote: [\[CITE\]](#) did you port forward the port 1604?

Of course. I've had it forwarded for quite a while, and I just re-checked It's still forwarded.

(Apr 26, 2013 12:31 PM)Processor Wrote: [\[CITE\]](#) May I ask what shell you are using?

I'm using Dhanush. But I've tried uploading other shells and connecting with those, still getting the same result.

I've also tried re-downloading netcat.

vmkbot - April 26, 2013, 12:39 pm

presuming that it's forwarded for the correct address, have you checked your firewall?

SIM-1241186 - April 26, 2013, 12:40 pm

(Apr 26, 2013 12:39 PM)vmkbot Wrote: [\[CITE\]](#) presuming that it's forwarded for the correct address, have you checked your firewall?

It is. And yes, I've checked my firewall. I've even tried disabling it and trying again. Still the same result. ?

vmkbot - April 26, 2013, 12:44 pm

have you tried other ports? my guess is that the server's security may be blocking outgoing connections

SIM-1241186 - April 26, 2013, 12:46 pm

(Apr 26, 2013 12:44 PM)vmkbot Wrote: [\[CITE\]](#) have you tried other ports? my guess is that the server's security may be blocking outgoing connections

Yes I've tried other ports. And that shouldn't be the case, because I've successfully connected to it in the past. This problem has occurred with every other site I have shelled as well.

Pendragon - April 26, 2013, 12:52 pm

What language is the backconnect coded in? Have you checked to see if it's installed on the sever? Also try using ports < 1000.

SIM-1241186 - April 26, 2013, 12:56 pm

(Apr 26, 2013 12:52 PM)Pendragon Wrote: [\[CITE\]](#) What language is the backconnect coded in? Have you checked to see if it's installed on the sever? Also try using ports < 1000.

There's options for Perl, Python, and PHP. I've tried all of them. Yes, I've checked to see if it's installed on the server, and they are.

PHP Code

```
<?php
```

Where is Perl?: perl: /usr/bin/perl.1355319536 /usr/bin/perl /usr/local/bin/perl /usr/share/man/man1/perl.1.gz

Where is Python?: python: /usr/bin/python2.6-config /usr/bin/python2.6 /usr/bin/python /usr/lib/python2.6 /usr/lib64/python2.6 /usr/include/python2.6 /usr/share/man/man1/python.1.gz

What difference would a port lower than 1000 make..?

Cathal - April 26, 2013, 12:58 pm

(Apr 26, 2013 12:56 PM)hackforumspang Wrote: [\[CITE\]](#) There's options for Perl, Python, and PHP. I've tried all of them. Yes, I've checked to see if it's installed on the server, and they are.

PHP Code

```
<?php
```

Where is Perl?: perl: /usr/bin/perl.1355319536 /usr/bin/perl /usr/local/bin/perl /usr/share/man/man1/perl.1.gz

Where is Python?: python: /usr/bin/python2.6-config /usr/bin/python2.6 /usr/bin/python /usr/lib/python2.6 /usr/lib64/python2.6 /usr/include/python2.6 /usr/share/man/man1/python.1.gz

What difference would a port lower than 1000 make..?

It wouldn't. Is safe mode enabled? List all disabled functions please.

SIM-1241186 - April 26, 2013, 1:09 pm

(Apr 26, 2013 12:58 PM)MrCathal09 Wrote: [\[CITE\]](#) It wouldn't. Is safe mode enabled? List all disabled functions please.

PHP Code

```
<?php
```

Disable functions : None Safe Mode : OFF

Pendragon - April 26, 2013, 1:18 pm

(Apr 26, 2013 12:58 PM)MrCathal09 Wrote: [\[CITE\]](#) It wouldn't. Is safe mode enabled? List all disabled functions please.

Says who? Many boxes disable ports > 1000 because they are not privileged ports. This is why you need to be root when binding a port < 1000.

I have no problem with people correcting me, just make sure you're actually correcting me.

Cathal - April 26, 2013, 1:24 pm

(Apr 26, 2013 01:18 PM)Pendragon Wrote: [\[CITE\]](#) Says who? Many boxes disable ports > 1000 because they are not privileged ports. This is why you need to be root when binding a port < 1000.

I have no problem with people correcting me, just make sure you're actually correcting me.
Fair enough, here's your correction. Fix the inequality. And sorry, I genuinely didn't know that. Still learnin.

Pendragon - April 26, 2013, 1:34 pm

(Apr 26, 2013 01:24 PM)MrCathal09 Wrote: [\[CITE\]](#) Fair enough, here's your correction. Fix the inequality. And sorry, I genuinely didn't know that. Still learnin.

The "inequalities" I used are exactly what I meant to say. And if you didn't know that what I said to begin with was true, then why did you automatically deny it instead of perhaps Googling it first to do some "learnin"?

SIM-1241186 - April 26, 2013, 1:35 pm

(Apr 26, 2013 01:34 PM)Pendragon Wrote: [\[CITE\]](#) The "inequalities" I used are exactly what I meant to say. And if you didn't know that what I said to begin with was true, then why did you automatically deny it instead of perhaps Googling it first to do some "learnin"?

Thank you for both of the replies.

Don't fight.

-I've tried lower ports, still no avail.

Cathal - April 26, 2013, 1:43 pm

(Apr 26, 2013 01:34 PM)Pendragon Wrote: [\[CITE\]](#) The "inequalities" I used are exactly what I meant to say. And if you didn't know that what I said to begin with was true, then why did you automatically deny it instead of perhaps Googling it first to do some "learnin"?

Why the fuck would I Google something I thought I was right about? I accepted I was wrong, not much else I can do. So build a bridge and get the fuck over it.

SIM-1241186 - April 26, 2013, 3:52 pm

Still unsolved.

If anyone else has any input, it would be greatly appreciated.

I've ran a test using:

```
nc -vv -l -p 1604
```

Then entering 127.0.0.1:1604 in my browsers address bar, and I get an established connection. So my port definitely is open. Not sure why I can't connect :\

Cathal - April 26, 2013, 4:01 pm

Well all you're proving is that the problem isn't client side.. I have the exact same problem with a lot of my shells as well, never did find a fix.

SIM-1241186 - April 26, 2013, 4:54 pm

(Apr 26, 2013 04:01 PM)MrCathal09 Wrote: [\[CITE\]](#) Well all you're proving is that the problem isn't client side.. I have the exact same problem with a lot of my shells as well, never did find a fix.

Damn. Well I guess you're right. It really doesn't seem like the problems on my end, they must of did something because I remember using the exact site in the past and having no problems.

Fml.

Vivek_s - April 26, 2013, 10:08 pm

Connection from localhost dont need port open. If you want to check your client side problem, try on other sites which are working fine.

For this site, why dont you try shell made other than in php like cgi shell ?

Phizo - April 27, 2013, 1:32 am

Firewalls tend to block outgoing connections to arbitrary ports, consequently preventing the socket being created.

Have you tried using a port from a legitimate service such as MySQL (3306)? This is the problem that I encounter the most.

SIM-1241186 - April 27, 2013, 3:18 am

(Apr 27, 2013 01:32 AM)Phizo Wrote: [\[CITE\]](#) Firewalls tend to block outgoing connections to arbitrary ports, consequently preventing the socket being created.

Have you tried using a port from a legitimate service such as MySQL (3306)? This is the problem that I encounter the most.

Just gave it a try. Still the same problem. I'm starting to think that it's just server side, and I have bad luck ?

Processor - April 28, 2013, 1:13 am

(Apr 27, 2013 03:18 AM)hackforumspang Wrote: [\[CITE\]](#) Just gave it a try. Still the same problem. I'm starting to think that it's just server side, and I have bad luck ?

Your probably right.. Because I have never had this happen after going through all the solutions.

Xpired - April 29, 2013, 12:24 pm

try open ur port or u can use weeveely

-- -- -- -- --

SIM-1241186 - April 29, 2013, 1:16 pm

(Apr 29, 2013 12:24 PM)Xpired™ Wrote: [\[CITE\]](#) try open ur port or u can use weeveely

-- -- -- -- --

Port is definitely open..I'm not that dumb.

Will look into Weeveely though, thanks for the suggestion.

edit: Weeveely works pretty good. Although I wasn't able to root, because I keep getting 'permission denied' when attempting to use gcc. But thanks for suggesting it, as I now have it for the future.