

Forum:[Hack Forums](#)

Thread: [\[Help\] Opening a localhost tcp port to get access from another pc?](#)

HolGORE - November 2, 2014, 2:11 am

Hey,

first of all, im a noob and im trying to learn pentesting atm.

it's a test server and on it a webserver is installed, which is only accessable by the localhost tcp port 12345.

i have to get access to it and find a flag file.

i already tried it with netcat, but maybe wrong? (.182 ist the vm ip)

```
ncat --sh-exec "ncat 192.168.1.182 12345" -l 8000 --keep-open
```

im not sure whether this is the wrong way, or what i have to do after it to get access?

hope someone can help me thank you.

greetz

alowenthal - November 2, 2014, 10:47 am

(Nov 2, 2014 03:11 AM)HolGORE Wrote: [\[CITE\]](#) ncat --sh-exec "ncat 192.168.1.182 12345" -l 8000 --keep-open

That simply redirects port 8000 to 12345 on your local machine.

HolGORE - November 2, 2014, 11:16 pm

ah ok so i just misunderstood this command.

could you tell me how i can get access to this webserver?

c00perzz - November 4, 2014, 8:15 am

(Nov 3, 2014 12:16 AM)HolGORE Wrote: [\[CITE\]](#) ah ok so i just misunderstood this command.

could you tell me how i can get access to this webserver?

What do you mean by "get access to this webserver"?

You need to hack it?

You need to find which webserver is running and find possible vulnerabilities.

You may want to exploit any web application it may run

You may want to scan the machine of OS level vulnerabilities.

Your post is too general. We need more info in order to help

p.s: somebody move this to the right section