

Forum:[Hack Forums](#)

Thread: [Tutorial | How To Test Your RAT | Sandboxie/Anubis | 2 methods](#)

Phoeni? - February 17, 2013, 3:13 am

So recently I saw a h3ll lot of guys making thread asking for a test install in order to check the working for their RAT,

I would like to show you how you can test you RAT on yourself Using "Sandboxie" and Anubis.

NOTE: I am assuming that you already know how to set-up a RAT that includes Port-Forwarding etc

Method 1: (Sandboxie):

Introducing Sandboxie

[img]http://www.freakitude.com/images/2007/sandboxie-logo.png[/img]

Sandboxie runs your programs in an isolated space which prevents them from making permanent changes to other programs and data in your computer.

[img]http://www.sandboxie.com/img/FrontPage/FrontPageAnimation.gif[/img]

[img]http://www.sandboxie.com/img/FrontPage/FrontPageLegend.png[/img]

The red arrows indicate changes flowing from a running program into your computer. The box labeled Hard disk (no sandbox) shows changes by a program running normally. The box labeled Hard disk (with sandbox) shows changes by a program running under Sandboxie. The animation illustrates that Sandboxie is able to intercept the changes and isolate them within a sandbox, depicted as a yellow rectangle. It also illustrates that grouping the changes together makes it easy to delete all of them at once.

Step 1.

Download Sandboxie from [HERE](#)

Spoiler ([Click to View](#))

Step 2.

While creating a stub from you RAT client use 127.0.0.1 (this is your computer's personal IP) Instead of your No-Ip Host.

NOTE:IF your Router support NAT LOOPBACK then you can use No-Ip

Spoiler ([Click to View](#))

Step3.

Edit the required settings then build the stub,

Step 4.

Right click on your Stub.
Click "Run Sandboxed".

Step 5.

You will know if your server is working without harming your machine.

Spoiler ([Click to View](#))

When you don't show up when you test it on yourself then you're probably using your external address when testing, (Eg, your WAN IP, or your No-ip DNS) and most likely your router/gateway/modem doesn't have NAT loopback support. Nothing to worry about, just when you test within your network use internal addresses, (eg, if your testing on the computer that is running the client use 127.0.0.1, if you're testing within your network on a different computer use the address of the computer hosting the client).

Then you are Good to go, again make the Stub from you rat client, this time using your "No-Ip" Host, and get them slaves ?

Method 2: (Anubis):

Note: This method will also work if your router doesn't support NAT loopback.

Important : DO NOT UPLOAD CRYPTED SERVERS ON ANUBIS, Because it distributes samples, and most of the times crypted server doesn't work

[b]Step 1.:

Make a stub using No-Ip host from your RAT client.

Step 2.

Visit this site <http://anubis.iseclab.org/>

Step 3.

Follow the steps given in the picture below

Step 4. Wait for Anubis to complete the Analysis.

Step 5. If you get a random/unknown slave on your RAT client, then your rat is working just Fine. Congratulations.

Tip: Now when you Crypt your rat for spreading, add "Startup" function only from the Crypter.

Regards,

note :This Tutorial is for Educational Purposes only, use the information at your own risk! I am not responsible if you use this knowledge for unethical purposes.

Revcode - February 17, 2013, 3:22 am

Nice and very helpful tutorial. Great job!

Phoeni? - February 17, 2013, 3:24 am

(Feb 17, 2013 04:22 AM)jebemtihljeb Wrote: [\[CITE\]](#) Nice and very helpful tutorial. Great job! thanks :)

I hope this helps people who are desperate to test their RAT

Snoopy - February 17, 2013, 3:50 am

I tried this and still fail to show up in my client, any help?

Phoeni? - February 17, 2013, 3:55 am

(Feb 17, 2013 04:50 AM)tahir. Wrote: [\[CITE\]](#) I tried this and still fail to show up in my client, any help? yes sure, what error are you getting while running your server under sandboxie ?

1CE™ - February 17, 2013, 3:56 am

good tutorial dear..you look, when i check my ports, all of my ports including 80 is always closed..when i did your tutorial, i get myself as slave..so does this mean if i infect others, i will get them as my slaves even though canyouseeme.org shows that my ports are closed?

Phoeni? - February 17, 2013, 3:59 am

(Feb 17, 2013 04:56 AM)1CE.CODER Wrote: [\[CITE\]](#) good tutorial dear..you look, when i check my ports, all of my ports including 80 is always closed..when i did your tutorial, i get myself as slave..so does this mean if i infect others, i will get them as my slaves even though canyouseeme.org shows that my ports are closed?

If you can't see your Ports Opened on "canyouseeme.org" you won't be able to get slaves mate,

Quote: NOTE: I am assuming that you already know how to set-up a RAT that includes Port-Forwarding etc
?

Snoopy - February 17, 2013, 4:01 am

(Feb 17, 2013 04:55 AM)Phoeni? Wrote: [\[CITE\]](#) yes sure, what error are you getting while running your server under sandboxie ?

I run the server in Sandbox and I get the error message that is supposed to show up, then the AVG detection shows up but I don't remove the threat yet. And then the Sandbox recover file thing shows up.

1CE™ - February 17, 2013, 4:02 am

(Feb 17, 2013 04:59 AM)Phoeni? Wrote: [\[CITE\]](#) If you can't see your Ports Opened on "canyouseeme.org" you won't be able to get slaves mate,

?yup i know all that..the weird thing is when i did your tutorial, i checked my port on canyouseeme and it says closed..but i still get myself as slave..weird huh?

the most weird thing is port 80 must always be open to have access http(internet), but my port 80 is always closed, yet now i am using internet and replying to your quote...)

Phoeni? - February 17, 2013, 4:05 am

Quote: I run the server in Sandbox and I get the error message that is supposed to show up, then the AVG detection shows up but I don't remove the threat yet. And then the Sandbox recover file thing shows up.

Try disabling you AV

and if it still doesn't work try running sandboxie as an Administrator

(Feb 17, 2013 05:02 AM)1CE.CODER Wrote: [\[CITE\]](#) yup i know all that..the weird thing is when i did

your tutorial, i checked my port on canyouseme and it says closed..but i still get myself as slave..weird huh?

the most weird thing is port 80 must always be open to have access http(internet), but my port 80 is always closed, yet now i am using internet and replying with your quote..:)

Yes, the firewall/AV of your PC may be blocking the ports,
or it may be closed because you may be using 2 routers,

Snoopy - February 17, 2013, 4:15 am

(Feb 17, 2013 05:05 AM)Phoeni? Wrote: [\[CITE\]](#) Try disabling you AV
and if it still doesn't work try running sandboxie as an Administrator

Yes, the firewall/AV of your PC may be blocking the ports,
or it may be closed because you may be using 2 routers,
OK, I ran it with UAC and AVG disabled and I appeared in my client but I got this.

I think that means it didn't run on Sandbox?

#Skyline - February 17, 2013, 4:17 am

Ok what if your router doesn't support NAT loopback. What happens then?

Phoeni? - February 17, 2013, 4:21 am

(Feb 17, 2013 05:17 AM)#Skyline Wrote: [\[CITE\]](#) Ok what if your router doesn't support NAT loopback. What happens then?

If a router supports NAT loopback then running the server with sandboxy on your machine with No-Ip would work

but if the router doesn't support that 127.0.0.1 will always work ?

(Feb 17, 2013 05:15 AM)tahir. Wrote: [\[CITE\]](#) OK, I ran it with UAC and AVG disabled and I appeared in my client but I got this.

I think that means it didn't run on Sandbox?Ya I think it wasn't running on sandboxy

1CE™ - February 17, 2013, 4:23 am

(Feb 17, 2013 05:05 AM)Phoeni? Wrote: [\[CITE\]](#) Try disabling you AV
and if it still doesn't work try running sandboxie as an Administrator

Yes, the firewall/AV of your PC may be blocking the ports,
or it may be closed because you may be using 2 routers,
okay..final question, if let say i use 82 as port, when i tested on sandbox and it works on myself, so if i infect others by changing 127.0.0.1 to no-ip, will i get some slaves for sure?

Phoeni? - February 17, 2013, 4:25 am

(Feb 17, 2013 05:23 AM)1CE.CODER Wrote: [\[CITE\]](#) okay..final question, if let say i use 82 as port, when i tested on sandbox and it works on myself, so if i infect others by changing 127.0.0.1 to no-ip, will i get some slaves for sure?127.0.0.1 is internal IP of any PC,

but to have external connections one must have specific ports opened
if you can't see ports open in canyouseeme.org you won't be able to get connections from your slaves.

Snoopy - February 17, 2013, 4:25 am

(Feb 17, 2013 05:21 AM)Phoeni? Wrote: [\[CITE\]](#) If a router supports NAT loopback then running the server with sandboxy on your machine with No-Ip would work but if the router doesn't support that 127.0.0.1 will always work ?

Ya I think it wasn't running on sandboxy
So my server will only work if executed with administrator privileges?

Phoeni? - February 17, 2013, 4:27 am

(Feb 17, 2013 05:25 AM)tahir. Wrote: [\[CITE\]](#) So my server will only work if executed with administrator privileges?

No, on your slaves PC they won't require to run the RAT as administrator,

aspirin - February 17, 2013, 10:50 am

Nice man.

Will surely help the newbies out.

5 star :)

Phoeni? - February 17, 2013, 10:51 am

(Feb 17, 2013 11:50 AM)aspirin Wrote: [\[CITE\]](#) Nice man.

Will surely help the newbies out.

5 star :)

Thanks man :)

I hope they all profit from this thread ?

Tutelary - February 17, 2013, 11:18 am

Nice tutorial, especially about the NAT Loopback. Not a lot of people put that in, and it needs to be known. Thanks.

sapmi - February 27, 2013, 2:27 pm

Word of advice guys. I did this behind the Bshades VPN (all ports opened VPN), put local host in my server settings (127.0.0.1) and it didn't work. However, I disconnected from the VPN, and it worked! This is obvious because you're testing on your own network, using 127.0.0.1. But I panicked for 30 mins thinking it all went wrong.

So moral of story, don't test this behind a vpn. I know it's obvious for veterans, but us noobies have to learn the hard way sometimes. I've learned shitloads so far! :)

Hedex - February 27, 2013, 2:33 pm

Hopefully, this should cut down the threads as long as it stays alive. Well done for making the effort.

Phoeni? - February 28, 2013, 2:21 am

(Feb 27, 2013 03:33 PM)UKF Wrote: [\[CITE\]](#) Hopefully, this should cut down the threads as long as it stays alive. Well done for making the effort.

Thanks for the Feedback, Hope folks follow this tut before making those test install threads. ?

PhilippKing93 - March 8, 2013, 7:06 am

i also have a problem setting up my rat with no-ip, any help?
thanks in advance

machbe - May 10, 2013, 11:06 am

I managed to successfully test my rat, after going through your dark comet tutorial. Thanks

ivegotabigone - May 12, 2013, 5:00 pm

This was extremely helpful. Thanks.

Now I know my server works.

tambov - May 13, 2013, 2:54 am

thanks, it was really helpful.

Tried it and worked perfectly. :)

Phoeni? - May 15, 2013, 11:02 pm

(May 13, 2013 02:54 AM)tambov Wrote: [\[CITE\]](#) thanks, it was really helpful.

Tried it and worked perfectly. :)

(Mar 8, 2013 08:06 AM)PhilippKing93 Wrote: [\[CITE\]](#) i also have a problem setting up my rat with no-ip, any help?

thanks in advance

(May 10, 2013 11:06 AM)machbe Wrote: [\[CITE\]](#) I managed to successfully test my rat, after going through your dark comet tutorial. Thanks

(May 12, 2013 05:00 PM)ivegotabigone Wrote: [\[CITE\]](#) This was extremely helpful. Thanks.

Now I know my server works.

Thanks for the feedback, I am glad you could benefit from this tutorial

Also I updated a thread with a second method to test your Rat ?

Jacywashere13 - May 15, 2013, 11:16 pm

Nice tutorial, thanks for sharing :)

Phoeni? - May 18, 2013, 1:34 am

(May 15, 2013 11:16 PM)Jacywashere13 Wrote: [\[CITE\]](#) Nice tutorial, thanks for sharing :)

Your welcome ?

Thanks for the feedback

carb0ns - May 18, 2013, 2:16 am

Bro very helpful tutorial. Great job!

bigwilly - October 22, 2013, 1:38 am

One of the most precise TUTORIALS i have seen around here about Test .Thank you

gregluffy - November 13, 2013, 4:58 am

nice tutorial .when i test my server on anubis nothing happend.i have open 82 port and the default ip from neighbour's router.can i rat people on diffrens networks if my server is on local 127.0.0.1?i use lan ip not wan

BITDurg1 - November 15, 2013, 9:53 am

Thanks for the help!

35 characters

:)

youdealinwitavillain - January 31, 2014, 1:43 pm

thanks this worked! very good tutorial

Your Offline - January 31, 2014, 1:45 pm

Good tutorial and I can vouch that this works well to test out if files are infected.

HypnoPast - May 3, 2014, 12:24 pm

I tested this and it still doesn't work?

I get the error I created but cannot see myself in my DC list?

Any suggestions?

turkcoder - August 7, 2014, 12:54 pm

thanks :)

I hope this helps people who are desperate to test their RAT

CANNACH - August 8, 2014, 6:52 am

Thanks for this share bro, it's a good tuto

Nikem.D ? - August 8, 2014, 8:59 am

nice tutorial buddy . it will help lots of people who dont know how to test their RAT and seeks help .
thanks a lot ans keep it up .

epicz - June 26, 2015, 7:59 am

sorry, but i don't really get this "Step 5. If you get a random/unknown slave on your RAT client, then your rat is working just Fine. Congratulations." - can someone explain? how do you get a random slave when uploading for scanning?

jobi - July 28, 2015, 11:15 pm

My port is setup, client settings and module set up..

However when i try to create a stub and run the stub through sandboxie, i never show up in the user list but if i refresh my socket/ports i get a new connection with the status of "Established" still it doesnt show up in the user list though.

For Anubis, when i upload the stub i get a Fatal Submission Error?

Much help would be apreciated? Thanks in advance!

Acquire Zion - July 30, 2015, 10:15 am

When testing on Sandboxie why should I get enter 127 IP over the DNS?

Shadow4222 - July 30, 2015, 10:55 am

HAHHAAHAHAHAH ARE U JOKING? TESTING RAT ON SANDBOXIE? ITS NOT POSSIBLE, DUMBASS, I TRIED AND I DIDNT APPEAR ON RAT

The Unusual Hunter - July 30, 2015, 12:42 pm

Well i ratted myself doing this help me with my own rat.

Nvm it is fine now

Decipher™ - July 30, 2015, 3:45 pm

Great TuT Should help Out alot of People!

itsMeCherry - August 15, 2015, 5:50 am

Thanks alot for this tutorial mate.

richgod - December 24, 2015, 10:40 am

(Feb 17, 2013 04:50 AM)tahir. Wrote: [\[CITE\]](#) I tried this and still fail to show up in my client, any help? Same with me, if anyone can help me i don't know what's the issue because my port is clearly working as when i test it using canyouseeme.org

Supreme.tm - December 24, 2015, 12:35 pm

(Jul 30, 2015 10:55 AM)Shad0w_ Wrote: [\[CITE\]](#) HAHHAHAHAHAHAH ARE U JOKING? TESTING RAT ON SANDBOXIE? ITS NOT POSSIBLE, DUMBASS, I TRIED AND I DIDNT APPEAR ON RAT Are you dumb? If it doesn't work than your RAT doesn't work.

sNize - December 24, 2015, 1:21 pm

is there a way to test the crypted rat with the DNS i wanna use?

MikeTheGamer - December 24, 2015, 10:53 pm

What's funny is:

- 1.This thread is old as FUCK
- 2.A SHIT TON of people still want test slaves