






Sign in


 **rapid7 / metasploit-framework** Public


 Notifications


 Fork 14k


 Star 34.1k


 Code


 Issues 410

 Pull requests 44

 Discussions

 Actions

 Projects 1

 Wiki


Reverse shell with portmap.io #11337

Closed

4 tasks

Parshuram2 opened this issue on Jan 31, 2019 · 3 comments

New issue



Parshuram2 commented on Jan 31, 2019 • edited

Steps to reproduce

How'd you do it?

- ...I have a general question.
- ... Is it possible to get a reverse shell with Portmap.io? NOT creating a PAYLOAD.
I am using
windows/dcerpc/ms03_026_dcom
so will it give me a shell back if i set LHOST as my portmap.io url and LPORT as my local port or is it just not possible. I have tried multiple times ..but so far failed. So, I am guessing it has to do with the reverse connection which is somehow not coming through. Or am I making a mistake in setting parameters for e.g I tried to set my portmap.io URL as SRVHOST as well..but I guess the connection just doesn't come back to my machine which is a VIRTUALbox KALI LINUX.

This section should also tell us any relevant information about the environment; for example, if an exploit that used to work is failing, tell us the victim operating system and service versions.

Expected behavior

Assignees

No one assigned

Labels

question

Projects

None yet




Milestone

No milestone

Development

No branches or pull requests

3 participants



What should happen? reverse shell should connect

Current behavior

What happens instead? reverse shell does not connect

You might also want to check the last ~1k lines of

```
/opt/metasploit/apps/pro/engine/config/logs/framework.log  
g or  
~/.msf4/logs/framework.log for relevant stack traces
```

System stuff

Metasploit version

Get this with the `version` command in msfconsole (or `git log -1 --pretty=oneline` for a source install).

I installed Metasploit with:

- ☐ Kali package via apt
- ☐ Omnibus installer (nightly)
- ☐ Commercial/Community installer (from <http://www.rapid7.com/products/metasploit/download.jsp>)
- ☐ Source install (please specify ruby version)

OS

What OS are you running Metasploit on?

Virtual box Kali Linux



wvu commented on Jan 31, 2019

Contributor



Please provide actual details. This is likely a networking misconfiguration.



bcoles added the **question** label on Feb 1, 2019

 **bcoles** commented on Feb 1, 2019

Contributor



Portmap.io is a port forwarding service (similar to ngrok).

You'll want to tell the payload to connect back to the publicly accessible host name / IP address. This can be achieved with: `set ReverseListenerBindAddress`.

These references may be of use:

- <https://www.corelan.be/index.php/2014/01/04/metasploit-meterpreter-and-nat/>
- <https://onehostcloud.hosting/connecting-metasploit-behind-nat-network/>

 **wwu** commented on Feb 1, 2019 • edited

Contributor



Set `LHOST` and `LPORT` to your public IP and public port. Set `ReverseListenerBindAddress` and `ReverseListenerBindPort` to your local IP and local port.

If you don't set `ReverseListenerBindAddress`, and it can't bind to `LHOST`, it'll fall back on `0.0.0.0`. Make sure everything is routing correctly, and make sure your payload can egress to your handler.

That's all. Please take support to IRC or e-mail in the future. GitHub is primarily for code contributions, bug reports, and feature requests. Thanks!



wwu closed this as completed on Feb 1, 2019

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)

