

Forum:[Hack Forums](#)

Thread: [\[TuT\] Slow Brute SSH - A Python SSH Cracker, that works! \[TuT\]](#)

Hooded Robin - March 19, 2012, 5:09 pm

OK, so today I will provide you with a quick introduction to a really awesome SSH cracker which is based on Python, called Slow Brute SSH. It is a Linux only script which works to perform targeted dictionary attacks against a specific user instance. It has the ability to execute commands upon success and has an amazing success detection rate. I ran into problems using NCRACK myself and was looking for something better for this protocol. I tested 4-5 of the better known SSH cracking tools out there and this was the one that received my top rating, mainly due to its simplistic design and easy usability. Many of the other tools I reviewed required different version of LibSSH to be installed, particularly non-standard versions. This leads to tricky installations with tons of pre-requisites in order to get things working. This tool works well right out of the box as it should. It also presents successful findings in a super easy to read format. Here goes the quick overview...

DOWNLOAD: <http://packetstormsecurity.org/files/98803/Slow-SSH-Bruteforcer.html>

Download and extract the tool to your Linux desktop (tar -zxvf downloadname). That's it! It is now installed and ready to go, just jump into the folder and enter the usual `./slowbrute.py -help` to see the list of command options:

You can see the command syntax is fairly easy to use and pick up on. You can essentially just point and shoot and the tool does all the work, easy setup. If you want to use TOR network for added anonymity just turn on TOR prior to launching and then make sure you use the `-T` or `--tor` option to route through the standard TOR port and out to target. If SSH is running on a non-standard port (22) then you can use the `-d` argument to specify the port to attack on instead of the default, if not provided will assume standard port 22 is the target. Not a lot to this one folks, simple and works well...

Here is a quick video to show you how it works in action against live target which NCRACK was unable to successfully register successful login against, hence this tutorial and tool highlight ?
[Video: http://www.youtube.com/watch?v=_-DPvYBtiYQ]

Until next time, Enjoy!

?

A++++ - March 20, 2012, 8:37 am

I have to say that it's a pretty nice tutorial. And for that program you don't even need BT5. Thanks for making the video and sharing.

Anyway I'm wondering that it's posted hours ago and still that's the first post. People don't see the possibilities. ?

Hooded Robin - March 20, 2012, 9:05 am

I am used to it, i usually only get like 1 post for every 100 or so views. Typical HF, glad you enjoyed it and can see the actual potential here.

ocean_smith - *March 10, 2013, 9:11 am*

i love this thanks a lot kisss

i hope it work