

Forum:[Hack Forums](#)

Thread: [Scan IP Ranges](#)

GRumPz. - *October 12, 2016, 4:37 pm*

Hello Everyone!

I am trying to teach myself python and I am not sure which direction to go in when it comes to actually creating something that scans IP ranges with a specific port. Can someone help me out or provide a module that would do this?

I would greatly appreciate it!

FinnTheHuman - *October 12, 2016, 6:01 pm*

You would want to look into sockets.

If you are trying to scan what ports are open, make a function that tries to establish a connection, and run it in a for loop.

supadopecat - *October 13, 2016, 1:08 am*

cool thanks for the question and thanks for the comment. i can now explore the sockets mod.

GRumPz. - *October 14, 2016, 4:06 pm*

FinnTheHuman, thanks man greatly appreciated. I will post my source once I get this ironed out. :)

Xtopherus - *October 30, 2016, 9:45 am*

You could do this much more efficiently in bash but if you're a solely a python programmer than yes you will want to look into sockets, send and receive and parsing the return. You could technically just make a front end and use nmap for the sweeping, thus implementing service scanning etc

Note that if you try using a connection type of scan like -sT in nmap you WILL be noticed on log files all over the place, a more discrete but not idiot proof is the SYN scanner.