

Forum:[Hack Forums](#)

Thread: [What to add to my one liner?](#)

javierpena - April 9, 2023, 4:25 am

So I am scanning IP's for open 80 port to find some easy (custom coded forgotten websites, old wordpress, etc.) targets in the wild so I can train myself with Kali and its tools.

Code for i in {4..253}; do curl x.x.x.\$i -v; done

This is what I use at the moment, which is not bad, but now I want to improve on it. Obviously it currently prints a lot of these:

Code >

* Recv failure: Connection reset by peer

* Closing connection 0

curl: (56) Recv failure: Connection reset by peer

* Trying x.x.x.x :80...

* Connected to x.x.x.x (x.x.x.x) port 80 (#0)

> GET / HTTP/1.1

> Host: x.x.x.x

> User-Agent: curl/7.87.0

> Accept: */*

>

My problem is I cannot " | grep <html> " because it will not show me IP on the "grep" line. So what can I do to get rid of the noise and make it show only the good stuff? Please don't suggest any ready-to-go software I want to make my own and learn to bash or whatever.

Thanks!

Edit: I want to make it x.x.0.0/16 but I need to find a way to remove the unwanted results, this is why I am running it on basically /24 atm

Ducky - April 13, 2023, 7:42 pm

Depends how fancy you want to be! If you don't want to write your own software, take a look at nmap (single target scans) or masscan (huge scans) :D