

Forum:[Hack Forums](#)

Thread: [Virtual Hosts](#)

tzoun - March 12, 2015, 6:31 am

Hello!

I want to find how many sites a web server is hosting. I tried 2 of them that possibly are on the same server and the only thing that changed in their IP was the last part (xxx.xxx.xxx.aaa) does this means that are on the same server?

If I write a script that changes only the last part of the IP and searches for all the rest combinations will I find every possible site that host on this server?

Hooded Robin - March 12, 2015, 7:08 am

Check DNS results to find out what you want. You can use online service like YougetSignal.com to do this for you as well, but this will handle resolving all sites on the same IP (A, AAAA, MX, PTR, etc). That said it is possible for a server to host more than one IP, so may require checking against each IP you find but again DNS is your friend here. Lastly it is entirely possible that this client/target/customer has rights to the entire IP block range, meaning they could very well own all IP's on the netblock, hence you seemingly finding them on the .0-255 C block. Usually a simple whois can identify netblock ownerships. Enumeration and recon are what you need to do to verify what is in scope for target and what is not, you can find lots of tutorials if you do a bit of searching here on HF and on the Google...best of luck to you

tzoun - March 17, 2015, 7:27 am

Thank you very much Hooded Robin, really helpful. :)