

Forum:[Hack Forums](#)

Thread: [Redirecting to another website](#)

Zork - September 11, 2018, 7:27 pm

Hello fellow HF Users,

I am beginning to fiddle around with kali linux and learning constantly new things and today I stumbled upon dns spoofing. But from my noobish understanding the victim is redirected to a fake website which is hosted locally on the attack machine. So a question arose in my mind what instead of redirecting to a locally hosted site you could redirect the user to an external website. For example the user wanted to go facebook.com and instead of that redirected to mystupidwebsite.com. Is it possible to do this kind of thing or would be some kind of tool that can do this? I would really love someone that could explain this to me.

Thanks

?

Edit: Another idea I was thinking what if you redirected the user from facebook.com to ---> hosted locally website on attack machine ---> using javascript redirect the user to the ---> mystupidwebsite.com would that workout too?

CyberStrike - September 11, 2018, 8:50 pm

Well you can point a malicious dns service to where ever you want. Javascript injection happens with ISP's so you can do the same thing also.

Edit: I don't want confusion here so I will clarify that I am assuming it's another machine and you are on their network or you are running a rogue AP, on the internet this is an advanced well funded attacker who does this these aka government.

Infamia - September 13, 2018, 11:48 am

Surely you can just point your router's DNS server to your locally-running DNS server which forwards any irrelevant requests to 1.1.1.1 or 8.8.8.8 or some other DNS server; and returns them, else you return the DNS resolution for your own website:

The process would look like this:

Assume node D hosts DNS server via port 53

1) node A requests facebook.com

1a) node A -> router

1b) router -> query "facebook.com" to node D

1c) node D -> "facebook.com" not in the `shady website` database -> return correct IP

2) node B requests pornhub.com

2a) node B -> router

2b) router -> query "pornhub.com" to node D

2c) node D -> "pornhub.com" not in the `shady website` database -> return correct IP

3) node C requests facefuck.com

3a) node C -> router

3b) router -> query "facefuck.com" to node D

4c) node D -> "facefuck.com" in `shady website` database

4d) node D -> query "fbi.gov" to 1.1.1.1 (ext. DNS server) -> router

