

Forum:[Hack Forums](#)

Thread: [Is it still possible to SSL Strip for the purpose of DNS Spoofing an official website](#)

Godofdeathftw - May 28, 2019, 1:29 pm

I've spent the day using some different tools (MITMf, Ettercap and dnsspoof) to DNS Spoof websites such as Facebook, Gmail, etc. Grabbing the entered credentials on a duplicate website works totally fine when I just make up my own random website domain, but when I try to redirect the official facebook to my unofficial domain, I always get the error "Your connection is not private", and the webpage never loads. I hoped that this could be fixed by using an SSL Strip (--hsts using MITMf), but that didn't change anything.

```
(python mitmf.py -i eth0 --spoof --arp --dns --target 192.xxx.xx.xxx --gateway 192.xxx.xx.x --hsts)
```

Are newer browsers totally protected from any kind of SSL Strip that would work for DNS Spoofing?

Is there any way that I can spoof a official domain such as Facebook or Gmail? If not, are there any other methods you can recommend I look into for stealing data on a local network?

P.S. I'm doing this just for fun, to give my brother a scare, because it's cool, and to maybe become a White Hat Hacker in the future.

Mad76e. - May 29, 2019, 3:04 pm

(May 28, 2019 01:29 PM)Godofdeathftw Wrote: [\[CITE\]](#) I've spent the day using some different tools (MITMf, Ettercap and dnsspoof) to DNS Spoof websites such as Facebook, Gmail, etc. Grabbing the entered credentials on a duplicate website works totally fine when I just make up my own random website domain, but when I try to redirect the official facebook to my unofficial domain, I always get the error "Your connection is not private", and the webpage never loads. I hoped that this could be fixed by using an SSL Strip (--hsts using MITMf), but that didn't change anything.

```
(python mitmf.py -i eth0 --spoof --arp --dns --target 192.xxx.xx.xxx --gateway 192.xxx.xx.x --hsts)
```

Are newer browsers totally protected from any kind of SSL Strip that would work for DNS Spoofing?

Is there any way that I can spoof a official domain such as Facebook or Gmail? If not, are there any other methods you can recommend I look into for stealing data on a local network?

P.S. I'm doing this just for fun, to give my brother a scare, because it's cool, and to maybe become a White Hat Hacker in the future.

Hmm.. I do believe this falls under another subforum, i will try to move it for you

Godofdeathftw - May 30, 2019, 12:15 pm

(May 29, 2019 03:04 PM)YadaYadaVad Wrote: [\[CITE\]](#) Hmm.. I do believe this falls under another subforum, i will try to move it for you

OH, good to know. Which subform would you recommend I post it under?

Mad76e. - May 30, 2019, 12:26 pm

(May 30, 2019 12:15 PM)Godofdeathftw Wrote: [\[CITE\]](#) OH, good to know. Which subform would you recommend I post it under?

I asked it to be moved to Beginner hacking Subforum, you dont need to do anything, it will be

moved there eventually

Godofdeathftw - May 31, 2019, 5:06 pm

(May 30, 2019 12:26 PM)YadaYadaVad Wrote: [\[CITE\]](#) I asked it to be moved to Beginner hacking Subforum, you dont need to do anything, it will be moved there eventually

Thanks man, I appreciate it!