

Forum:[Hack Forums](#)

Thread: [SSL strip not working on sites like facebook, twitter etc.](#)

shvm0396 - October 6, 2016, 8:36 am

Hi there, I am trying to execute MITM attack using SSL strip.. But its not working on sites like facebook, twitter, gmail.. Is there any fix or substitute to sniff passwords from these sites over a WIFI network..

I am using Kali Linux OS and arpspoof and sslstrip for this attack. please help.

pomwtin - October 6, 2016, 10:36 am

Ye, those sites are using HSTS. You can bypass this by using sslstripv2+dns2proxy if target is navigating to webpage by browser, or cacheraser if target is navigating to webpage via url.

Also, give it 30 min and lookup what this HSTS is... it will be more clearer what I am speaking of then, how it works and how to get past it

shvm0396 - October 6, 2016, 11:21 pm

okay .. thanks for help.. I will check this out .. I was surprised to see that most banking sites do not use HSTS .. they can be stripped simply through sslstrip..

Have you tried bettercap to bypass HSTS ?

pomwtin - October 7, 2016, 12:27 am

(Oct 6, 2016 11:21 PM)shvm0396 Wrote: [\[CITE\]](#) okay .. thanks for help.. I will check this out .. I was surprised to see that most banking sites do not use HSTS .. they can be stripped simply through sslstrip..

Have you tried bettercap to bypass HSTS ?

Usually bank sites forces ssl or do not work at all without encryption, at least this is what I noticed till now... Of course it will depend from bank to bank, but it would be a bit foolish not to force https...

I believe bettercap uses method with sslstrip v2+ dns2proxy

shvm0396 - October 12, 2016, 10:09 pm

okay i'm gonna try bettercap then.. and will let you know the results.

bo0m - October 13, 2016, 12:43 am

try mimf framework

Reptile-Ermac - October 13, 2016, 3:12 am

(Oct 12, 2016 10:09 PM)shvm0396 Wrote: [\[CITE\]](#) okay i'm gonna try bettercap then.. and will let you know the results.

its ettercap mate ! there are many apps to do that . Use zAnti or SSLStrip to strip https to http. Then use packet capture to finish the rest of the work bro ?

pomwtin - October 13, 2016, 3:49 am

(Oct 13, 2016 03:12 AM)Reptile-Ermac Wrote: [\[CITE\]](#) its ettercap mate

No, bettercap is in general better

azag - *October 14, 2016, 3:48 am*

it'll not work unless you make the phone , pc or whatever accept your certificate .. or just dns spoof the targeted websites you wanna sniff