

Forum:[Hack Forums](#)

Thread: [Mitm](#)

yuuta - December 27, 2023, 8:59 am

I'm studying sniffing and mitm but I have some questions, is it not possible to decrypt HTTPS traffic? I've been reading about this and he talks about techniques like sslstrip and sslstrip2 but from what I've seen both are obsolete, if for example you try to do this in a Chrome browser with Facebook traffic for example it doesn't work because of the hsts preload, I can't find it other efficient techniques for this, is currently the only solution just phishing or are there other methods? Note: I'm using bettercap

DramaKing - December 27, 2023, 4:21 pm

(Dec 27, 2023 09:59 AM)yuuta Wrote: [\[CITE\]](#) I'm studying sniffing and mitm but I have some questions, is it not possible to decrypt HTTPS traffic? I've been reading about this and he talks about techniques like sslstrip and sslstrip2 but from what I've seen both are obsolete, if for example you try to do this in a Chrome browser with Facebook traffic for example it doesn't work because of the hsts preload, I can't find it other efficient techniques for this, is currently the only solution just phishing or are there other methods? Note: I'm using bettercap

SSLstrip is not going to work against Facebook. hstshijack might, however, if you can poison DNS and redirect from the Facebook site so that HSTS doesn't apply. You can also actually decrypt TLS by supplying the keys to Wireshark.

yuuta - December 27, 2023, 8:12 pm

(Dec 27, 2023 05:21 PM)DramaKing Wrote: [\[CITE\]](#) SSLstrip is not going to work against Facebook. hstshijack might, however, if you can poison DNS and redirect from the Facebook site so that HSTS doesn't apply. You can also actually decrypt TLS by supplying the keys to Wireshark.

The last part is interesting, do you know of any posts about it? If yes I would appreciate it

DramaKing - December 27, 2023, 9:10 pm

(Dec 27, 2023 09:12 PM)yuuta Wrote: [\[CITE\]](#) The last part is interesting, do you know of any posts about it? If yes I would appreciate it

I should tell you that I tend to be a bit snide when skids ask for the impossible. The Wireshark docs will explain how to decrypt TLS segments, but Diffie-Hellman key exchange gives nothing for a MitM to extract session keys.

<https://wiki.wireshark.org/TLS>

yuuta - December 29, 2023, 3:54 am

(Dec 27, 2023 10:10 PM)DramaKing Wrote: [\[CITE\]](#) I should tell you that I tend to be a bit snide when skids ask for the impossible. The Wireshark docs will explain how to decrypt TLS segments, but Diffie-Hellman key exchange gives nothing for a MitM to extract session keys.

I don't know what you define as a scoundrel but thanks for the information, I'm really studying information security and hacking, maybe one day I'll be recognized, I apologize if I was rude and thanks for the information again