

Forum: [Hack Forums](#)

Thread: [HTTPS in MiTM](#)

javierpena - May 12, 2023, 2:16 pm

I was configuring burp yet again on a fresh VM and this got me thinking about HTTPS certs. How exactly do they work? Can I craft my own cert and "incert" (no pun intended ?) into a victim browser, so I can decrypt the data I receive when performing MiTM without the need for SSL strip

Honestly I don't really know much about these things and this is just an idea. Can it be done? How to make my own certificate and decrypt data passed through SSL?

I will appreciate any help including resources to read or if anyone has already done it and can speak from experience

Thanks!

Its1234 - May 13, 2023, 4:56 am

In my opinion, mitm is not that useful because it takes too much effort and it's not worth it in the end. the only thing I can think of that Mitm is good for is when you're on someone else's network and you want to see what websites they always visit

Don't break your head trying to figure out how to do it just focus on something else like DNS poisoning and redirecting and all that

javierpena - May 13, 2023, 4:57 am

(May 13, 2023 04:56 AM)Its1234 Wrote: [\[CITE\]](#) In my opinion, mitm is not that useful because it takes too much effort and it's not worth it in the end. the only thing I can think of that Mitm is good for is when you're on someone else's network and you want to see what websites they always visit

Don't break your head trying to figure out how to do it just focus on something else like DNS poisoning and redirecting and all that

Thanks for your input but I am interested in this specific method

Dread.Reaper - May 13, 2023, 6:00 am

I mean there is always self signed SSL certs....

javierpena - May 13, 2023, 6:04 am

(May 13, 2023 06:00 AM)Dread.Reaper Wrote: [\[CITE\]](#) I mean there is always self signed SSL certs....

why all experts always talk in riddles ?

Dread.Reaper - May 13, 2023, 6:07 am

(May 13, 2023 06:04 AM)javierpena Wrote: [\[CITE\]](#) why all experts always talk in riddles ?

<https://stackoverflow.com/questions/21297139/how-do-you-sign-a-certificate-signing-request-with-your-certification-authority>

You can sign your own SSL certificates for this purpose. (Keeping in mind it can still cause warnings on some browsers that is not a Certificate authority issued one)

javierpena - May 13, 2023, 6:09 am

(May 13, 2023 06:07 AM)Dread.Reaper Wrote: [\[CITE\]](#)

<https://stackoverflow.com/questions/21297139/how-do-you-sign-a-certificate-signing-request-with-your-certification-authority>

You can sign your own SSL certificates for this purpose. (Keeping in mind it can still cause warnings on some browsers that is not a Certificate authority issued one)

Thanks I will check this out ?

Dread.Reaper - May 13, 2023, 6:22 am

(May 13, 2023 06:09 AM)javierpena Wrote: [\[CITE\]](#) Thanks I will check this out ?
?

Also...

(May 13, 2023 06:04 AM)javierpena Wrote: [\[CITE\]](#) why all experts always talk in riddles ?
I could ask why all newbies are trying to do things with stuff they dont understand. ?

You gotta understand how the tech works before you can go messing about with it ?

javierpena - May 13, 2023, 6:24 am

(May 13, 2023 06:22 AM)Dread.Reaper Wrote: [\[CITE\]](#) ?

Also...

I could ask why all newbies are trying to do things with stuff they dont understand. ?

You gotta understand how the tech works before you can go messing about with it ?
I am a wild card more commonly known as a joker ?