[Make a Reverse HTTPS Payload and Send It with CobaltStrike](https://null-byte.wonderhowto.com/how-to/make-reverse-https-payload-and-send-with-cobaltstrike-0165587/)

* BY [**THE\_F1XER**](https://creator.wonderhowto.com/the_fixer/)
* 10/23/2015 6:11 PM

Hello everyone

Today I will show a different way to exploit a windows machine with a reverse https payload..."wait...why https? Isn't tcp good anymore?"

The answer is yes...and no...Actually https has few but very important benefits that tcp hasn't :

**1)**HTTPS hides what is beeing sent over the network, so IDS/IPS systems will not see what's happening (if there is no SSL termination (transparent) ).

**2)**HTTPS will look more normal in firewall logs.

So with that said...let's get started  
First of all we need 2 things present in our system :  
**1)**Metasploit

**2)**Java SE Development Kit (link:)<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

(Download the Linux*x86* tar.gz , extract it and once you do move the folder to the /opt directory)

Once you have that let's install Cobalt Strike Trial (it lasts 21 days) from it's own website <https://www.cobaltstrike.com/download>

Accept the EULA and choose Linux (.tgz)

Now open up terminal and start metasploit and postgresql services with the commands :

***Kali***> *service metasploit start*  
and  
***Kali***>*service postgresql start*

Always within terminal go to the cobaltstrike folder and let's launch it with :  
***Kali***>*./cobaltstrike*  
Now a window will show up ...just press connect

Another window *may* show up about the Metasploit RPC...just click yes.

Now you will see a window that looks pretty much like the Armitage one...but this one is like...the premium version because it has some things more

Now let's make the payload  
Go to Attacks > Packages and the select Windows Executable

Now let's add a Listener

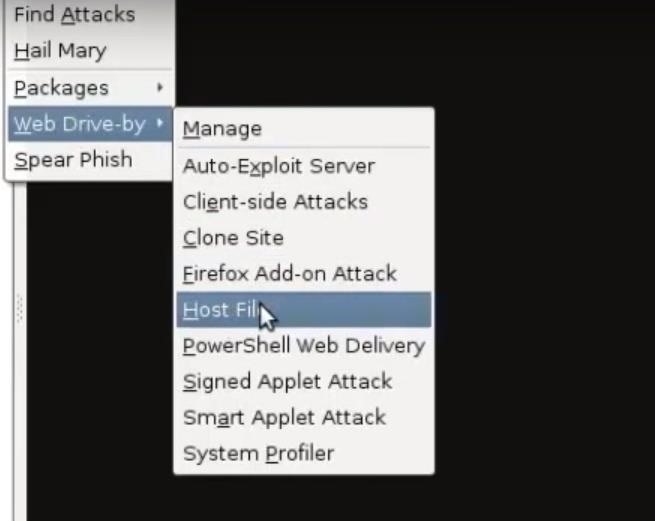
Now select the windows /meterpreter/reverse*https*

Give a name to your payload, put your local ip in the HOST tab and in PORT enter a port number (the https one is 443)...and click Save

Now let's generate the listener and save it wherever you want

"So... now you want to send it to the victim?" You can bet i want and for that I am going to use the the Host File function

Go to Attacks > Web Drive-by and select Host File :

[](https://img.wonderhowto.com/img/original/14/31/63581104745034/0/635811047450341431.jpg)

Now Select your generated payload AND in the URL path change the file.txt in file.exe (this is very important)  
Now click launch and send the URL to the victim and that's it.

Now you will see a screen with red borders...this means that it worked...click on it and click on meterpreter and select what you want to see or do

Thanks for reading (Sorry I couldn't upload some images for some reason... )

ThE-FiXeR