sensepost / reGeorg   Public

Notifications   Fork 820   Star 3k

<> Code   Issues 16   Pull requests 4   Actions   Projects   Wiki   Security   Insigh

master   Go to file   <> Code

- LICENSE.html
- LICENSE.txt
- README.md
- reGeorgSocksProxy.py
- tunnel.ashx
- tunnel.aspx
- tunnel.js
- tunnel.jsp
- tunnel.nosocket.php
- tunnel.php
- tunnel.tomcat.5.jsp

README   License   License

About

The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.

- Readme
- Unknown, Unknown licenses found
- Activity
- Custom properties
- 3k stars
- 121 watching
- 820 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 4

joda32 Willem Mouton

reGeorg

```
  _____  _____  __|__   |__  _____  _____ _
 |     | |  ___||  ___|   ||   ___|/    \|
 |  \  | |  ___||   | |   ||   ___||      ||
 |__|\__\|_____||_____|  __||_____|\_____/|_
                     |_____|
           ... every office needs a to(
```

willem@sensepost.com / @_w_m__

sam@sensepost.com / @trowalts

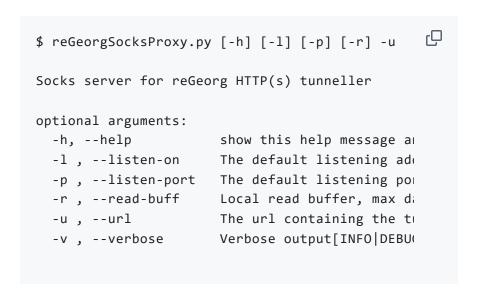etienne@sensepost.com / @kamp_staaldraad

Version

1.0

Dependencies

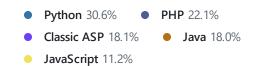reGeorg requires Python 2.7 and the following modules:

- urllib3 - HTTP library with thread-safe connection pooling, file post, and more.

Usage

```
$ reGeorgSocksProxy.py [-h] [-l] [-p] [-r] -u

Socks server for reGeorg HTTP(s) tunneller

optional arguments:
  -h, --help          show this help message ar
  -l , --listen-on    The default listening add
  -p , --listen-port  The default listening por
  -r , --read-buff    Local read buffer, max da
  -u , --url          The url containing the tu
  -v , --verbose      Verbose output[INFO|DEBU(
```

Etienne Stalmans — **staaldraad**

Junaid Loonat — **JunaidLoonat**

vulp1n3

Languages

- Python 30.6%
- PHP 22.1%
- Classic ASP 18.1%
- Java 18.0%
- JavaScript 11.2%

- **Step 1.** Upload tunnel.(aspx|ashx|jsp|php) to a webserver (How you do that is up to you)

- **Step 2.** Configure you tools to use a socks proxy, use the ip address and port you specified when you started the reGeorgSocksProxy.py

** Note, if you tools, such as NMap doesn't support socks proxies, use [proxychains](see wiki) (see wiki)

- **Step 3.** Hack the planet :)

Example

```
$ python reGeorgSocksProxy.py -p 8080 -u http://
```

License

MIT