EarthWorm

Archived: 2026-04-05 18:39:13 UTC

关于 EW 的介绍

下图是一张示意图:

该工具能够以“正向”、“反向”、“多级级联”等方式打通一条网络隧道，直达网络深处，用蚯蚓独有的手段突破网络限制，给防火墙松土。

工具包中提供了多种可执行文件，以适用不同的操作系统，Linux、Windows、MacOS、Arm-Linux 均被包括其内，更多平台的支持还在维护中，敬请期待。

使用方法：

以下所有样例，如无特殊说明代理端口均为1080，服务均为SOCKSv5代理服务.

该工具共有 6 种命令格式（ssocksd、rcsocks、rssocks、lcx_slave、lcx_listen、lcx_tran）。

- **1. 正向 SOCKS v5 服务器**

```
$ ./ew -s ssocksd -l 1080
```

- **2. 反弹 SOCKS v5 服务器**

  这个操作具体分两步：

  a) 先在一台具有公网 ip 的主机A上运行以下命令：

```
$ ./ew -s rcsocks -l 1080 -e 8888
```

  b) 在目标主机B上启动 SOCKS v5 服务 并反弹到公网主机的 8888端口

```
$ ./ew -s rssocks -d 1.1.1.1 -e 8888
```

  成功。

- **3. 多级级联**

  工具中自带的三条端口转发指令，

它们的参数格式分别为：

```
 $ ./ew -s lcx_listen -l  1080   -e 8888
$ ./ew -s lcx_tran   -l  1080   -f 2.2.2.3 -g 9999
$ ./ew -s lcx_slave  -d 1.1.1.1 -e 8888    -f 2.2.2.3  -g  9999
```

通过这些端口转发指令可以将处于网络深层的基于TCP的服务转发至根前,比如 SOCKS v5。

首先提供两个“二级级联”本地SOCKS测试样例：

a) lcx_tran 的用法

```
 $ ./ew -s ssocksd  -l 9999
$ ./ew -s lcx_tran -l 1080 -f 127.0.0.1 -g 9999
```

b) lcx_listen、lcx_slave 的用法

```
 $ ./ew -s lcx_listen -l 1080 -e 8888
$ ./ew -s ssocksd    -l 9999
$ ./ew -s lcx_slave  -d 127.0.0.1 -e 8888 -f 127.0.0.1 -g 9999
```

再提供一个“三级级联”的本地SOCKS测试用例以供参考

```
 $ ./ew -s rcsocks -l 1080 -e 8888
$ ./ew -s lcx_slave -d 127.0.0.1 -e 8888 -f 127.0.0.1 -g 9999
$ ./ew -s lcx_listen -l 9999 -e 7777
$ ./ew -s rssocks -d 127.0.0.1 -e 7777
```

数据流向: SOCKS v5 -> 1080 -> 8888 -> 9999 -> 7777 -> rssocks

补充说明：

1.为了减少网络资源的消耗，程序中添加了超时机制，默认时间为10000毫秒（10秒），用户可以通过追加 -t 参数来调整这个值，单位为毫秒。在多级级联功能中，超时机制将以隧道中最短的时间为默认值。

2.多级级联的三种状态可以转发任意以TCP为基础的通讯服务，包括远程桌面／ssh服务 等。

3. ew_for_arm_32 在android手机、小米路由器和树莓派 上测试无误。

4.该工具借用了 ssocks 和 lcx.exe 的操作逻辑，并进行更多的功能强化，才最终成型。吃水不忘挖井人，下面附上一篇介绍 sSocks 的帖子链接。 http://www.freebuf.com/articles/system/12182.html

5.工具本身并无好坏，希望大家以遵守相关法律为前提来使用该工具，对于恶意使用该工具造成的损失，和开发者无关。

联系作者：

-->

rootkiter@rootkiter.com

如果您在使用中有什么好想法，或遇到什么BUG，都可以主动联系我。我会尽最大所能让这个工具更加完美。

鸣谢：

感谢各位同事和朋友的支持，没有你们的帮助就不会有这样一款工具。愿你们越来越 v5，越来越 87。

想知道都有谁提供过帮助？使用 -a 参数就能看到他们。
