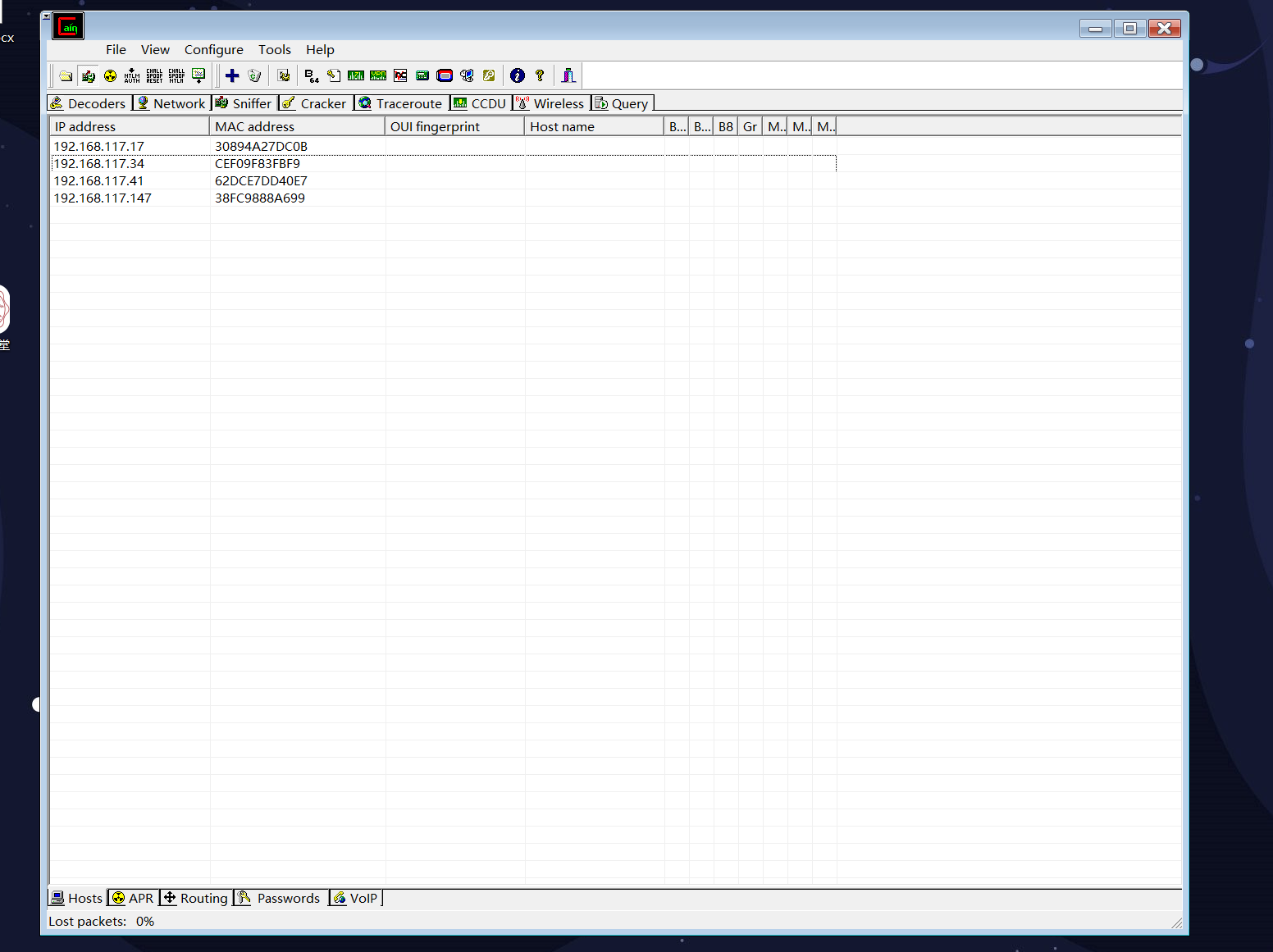
ARP攻击实验

为了实验方便，电脑均使用同一手机热点（一局域网）

首先把电脑互相ping（不然被攻击方无法使用服务器）

攻击方查询网络，寻找目标



进行完ARP欺骗操作以后等待

服务器方

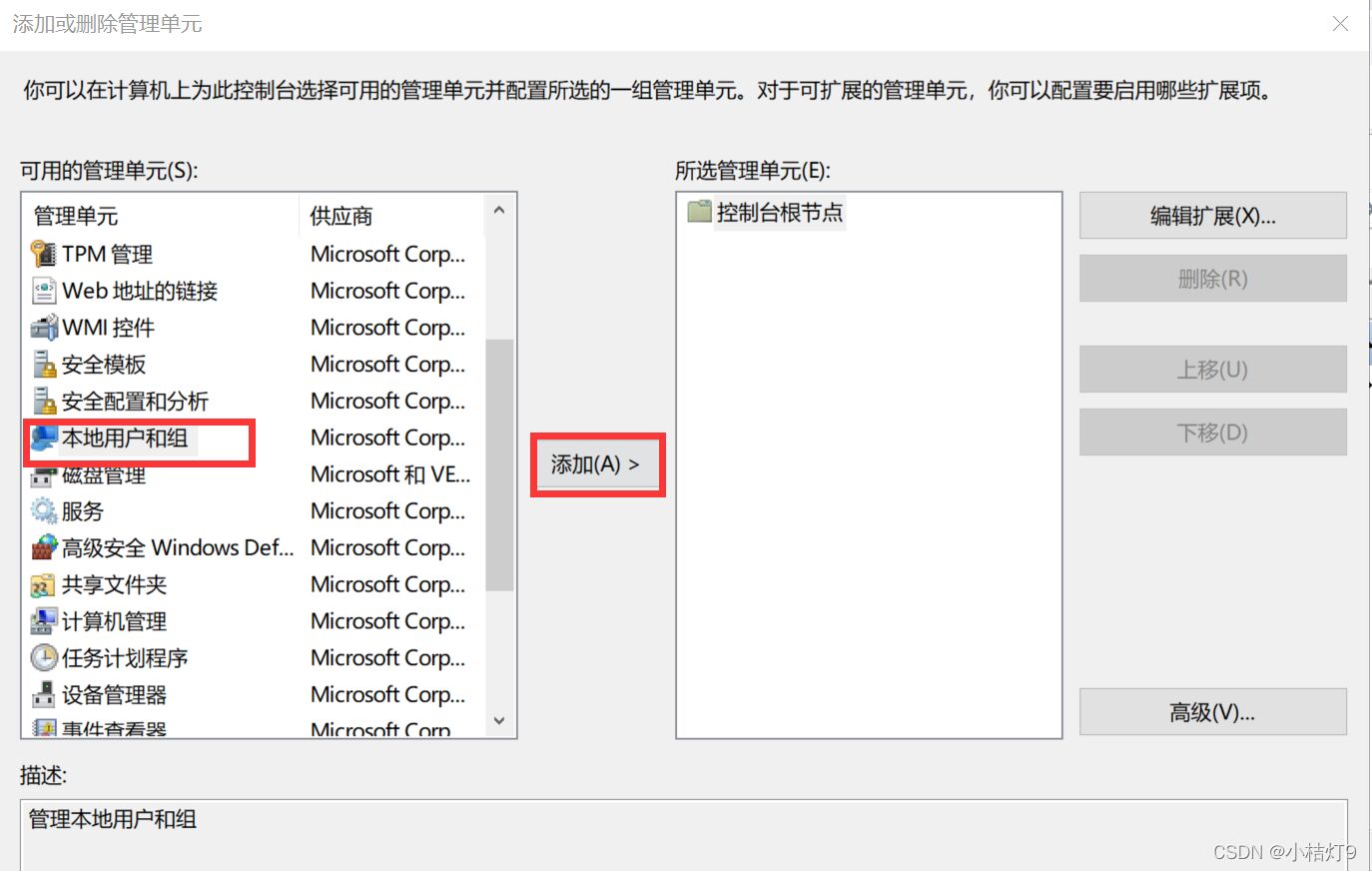
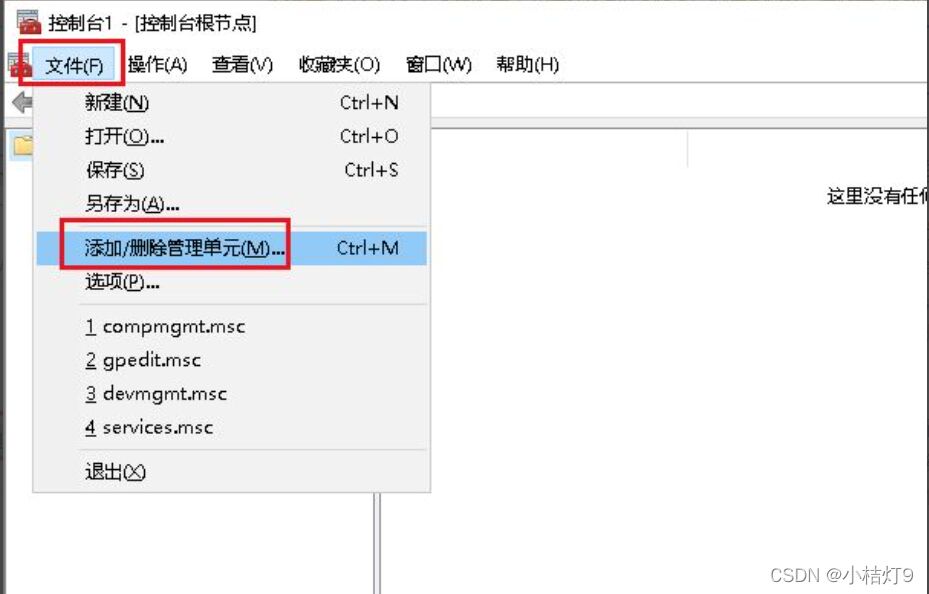
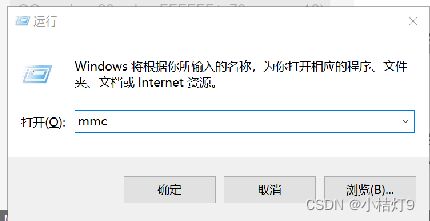
配置时遇到许多问题，在下面一一列举

搭建站点

创建用户时

家庭版win10或者win11没有本地用户和组

可以尝试通过运行mmc命令来添加本地用户和组。具体步骤为：开始->运行->输入“mmc”回车，打开“控制台”->点击“文件”->"添加/删除管理单元"->点击“添加”按钮->在“添加独立单元”对话框中选择“本地用户和组”，并点击“完成”->关闭“添加独立单元”对话框，在“添加/删除管理单元”对话框点“确定”。



需要注意的是，如果通过运行mmc命令仍无法添加本地用户和组，可以考虑参考

<https://blog.csdn.net/weixin_45062683/article/details/123699316?utm_source=app&app_version=5.1.1&code=app_1562916241&uLinkId=usr1mkqgl919blen>

或者用以下命令直接添加

net user,查询计算机下所有的用户名;  
net user 用户名 密码 /add,新增一个账户;  
net user 用户名 /delete,删除用户;  
net user 用户名 新密码,修改用户密码  
以上命令在管理员终端使用

创建成功以后

被攻击方尝试访问，显示ftp文件夹错误

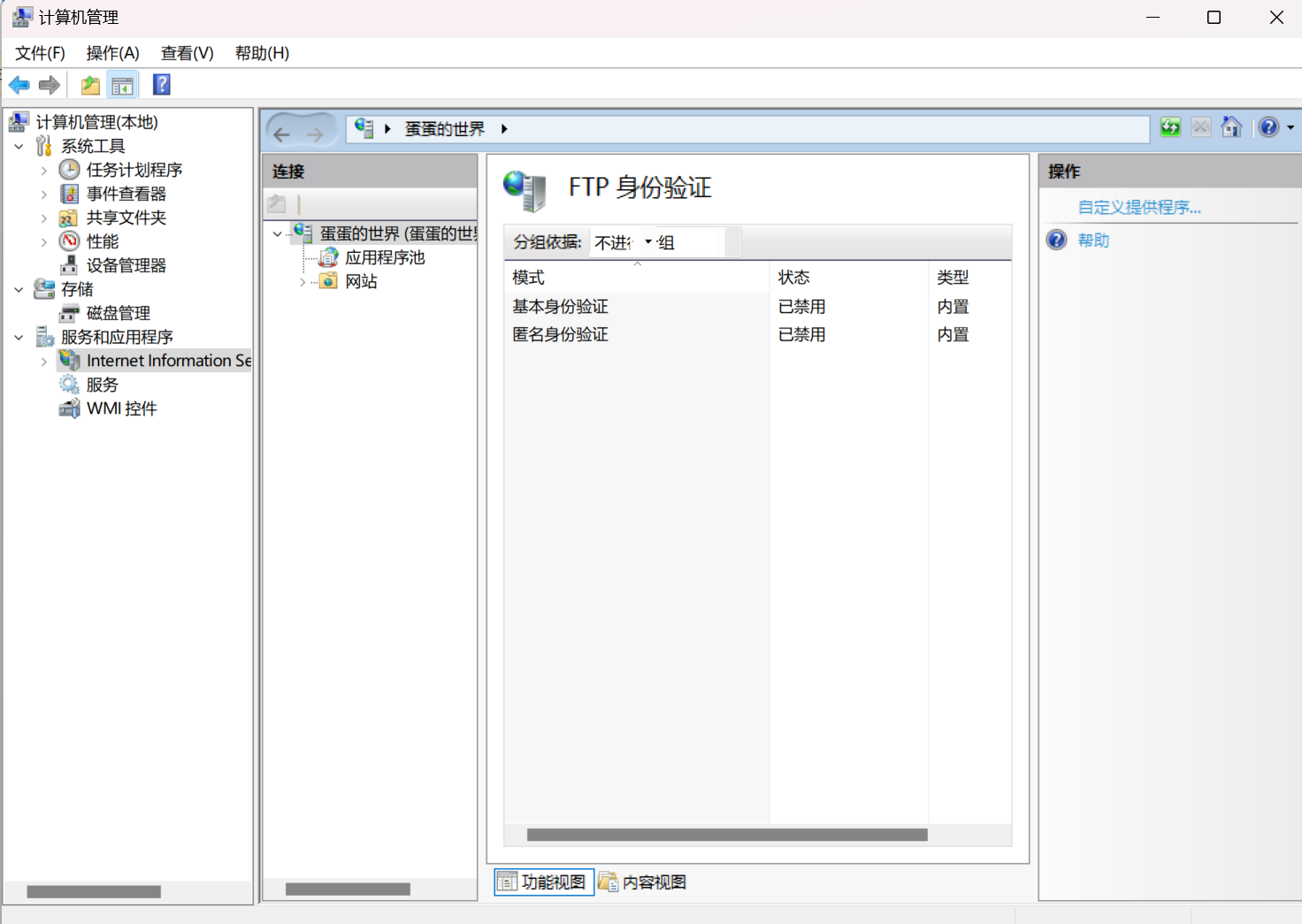
ftp用指定的用户名和密码无法登录到该ftp服务器

经过查询，需要进行检查

因为系统默认是大部分权限是禁止的，需要你去查询

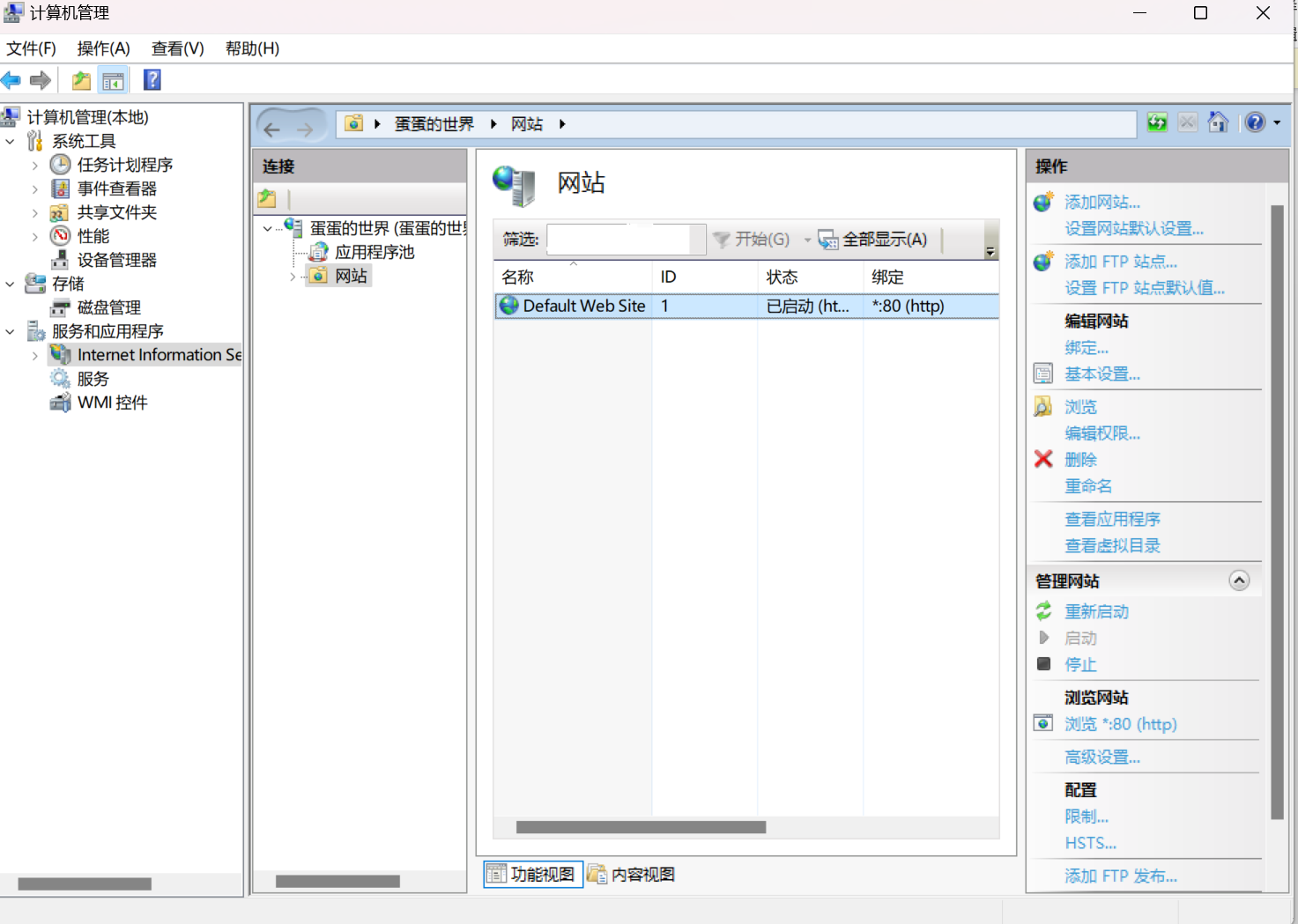
在计算机管理的ftp身份验证

默认基本身份验证是禁用，选择启用



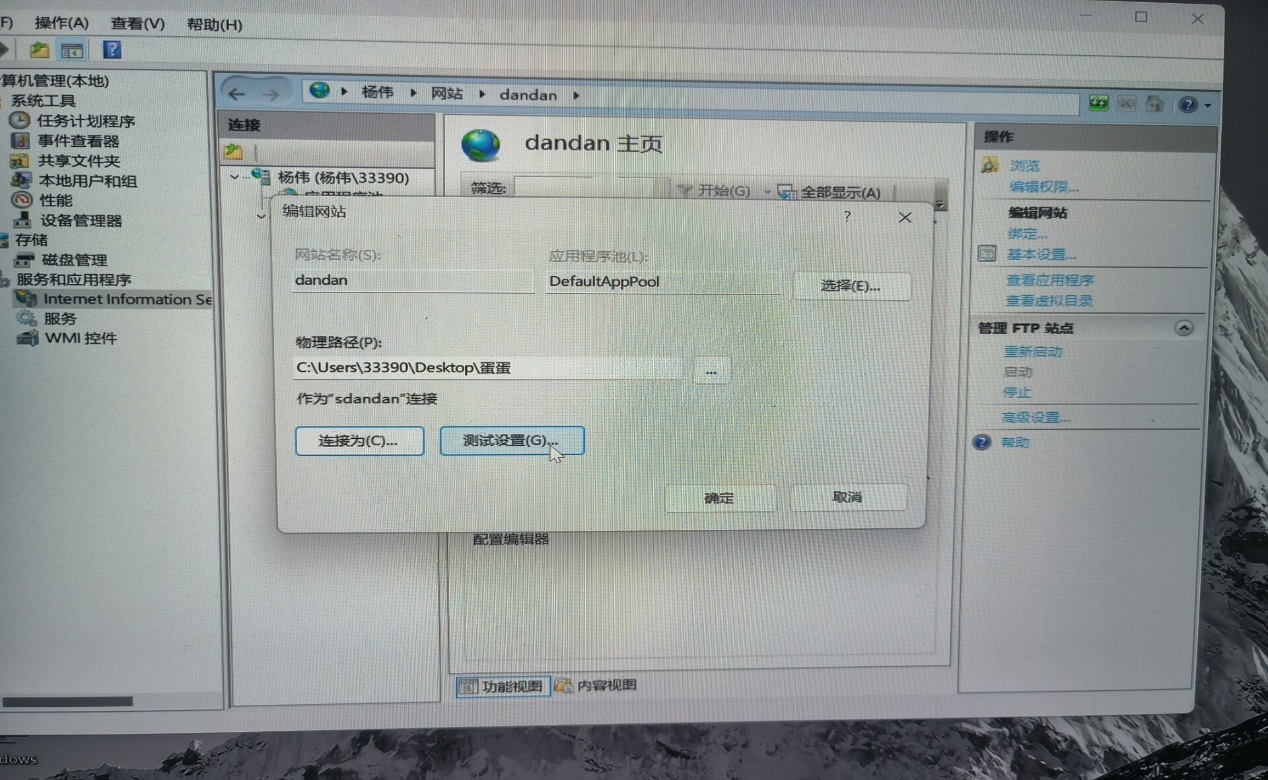
此时进行检查

打开建立的网站



点击网站，右侧的基本设置

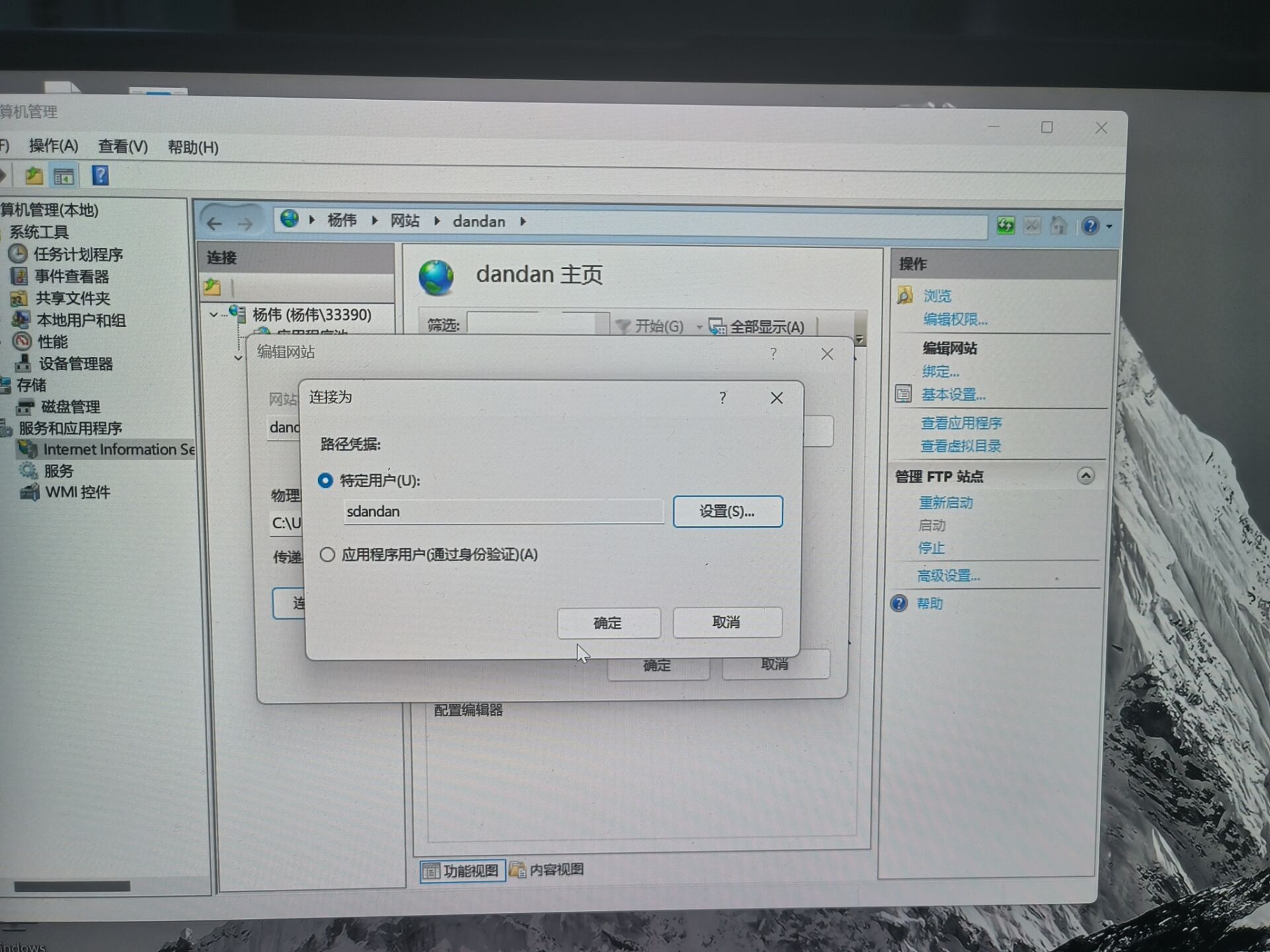
点击测试设置





一般可能出现第二个问题

返回，点击连接为…，点击特定用户，输入之前创建的用户信息

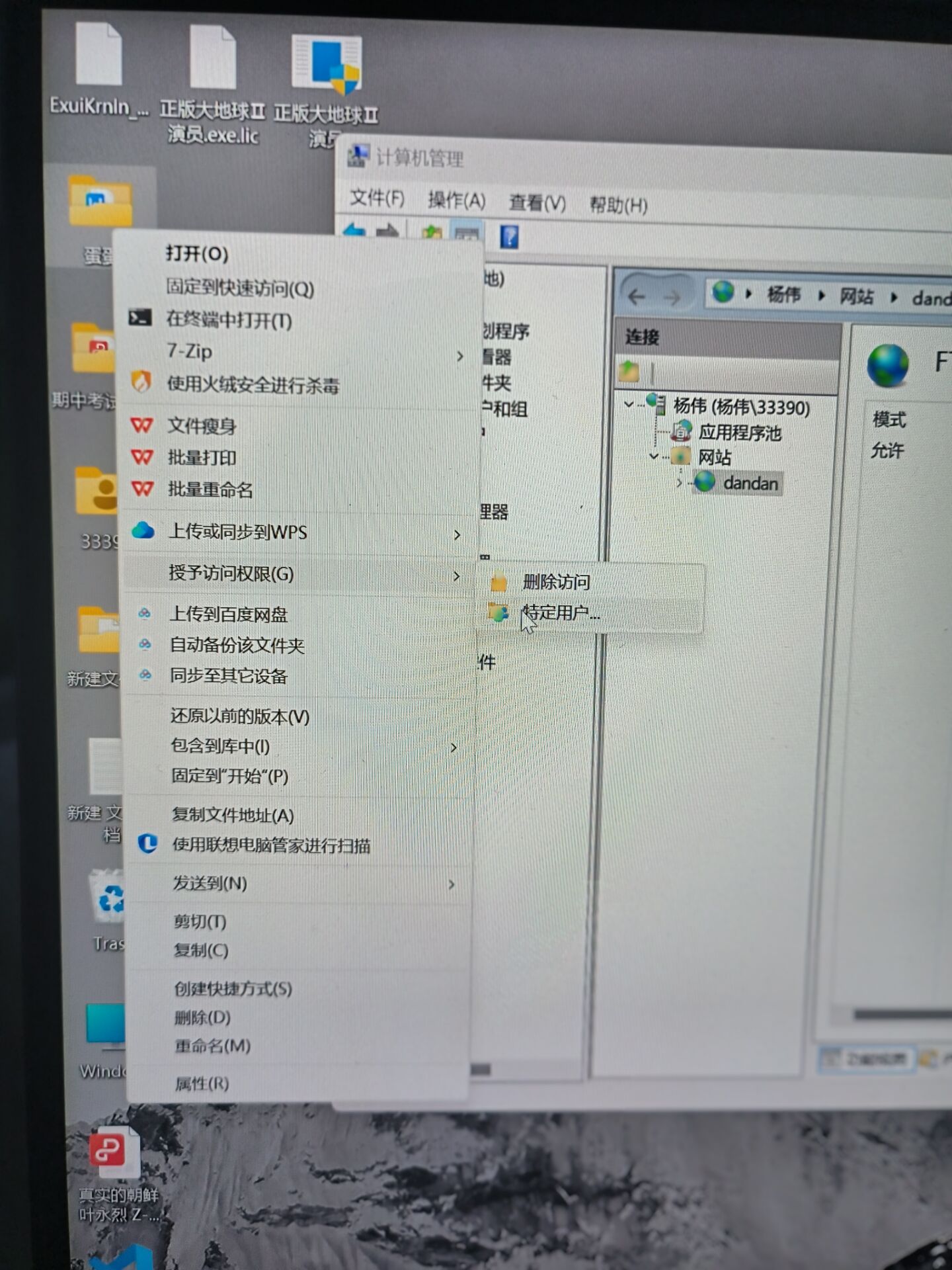


此时再次测试，有可能直接成功，也有可能继续错误，不能展开以证明使用权

此时与你网站设定的物理地址有关

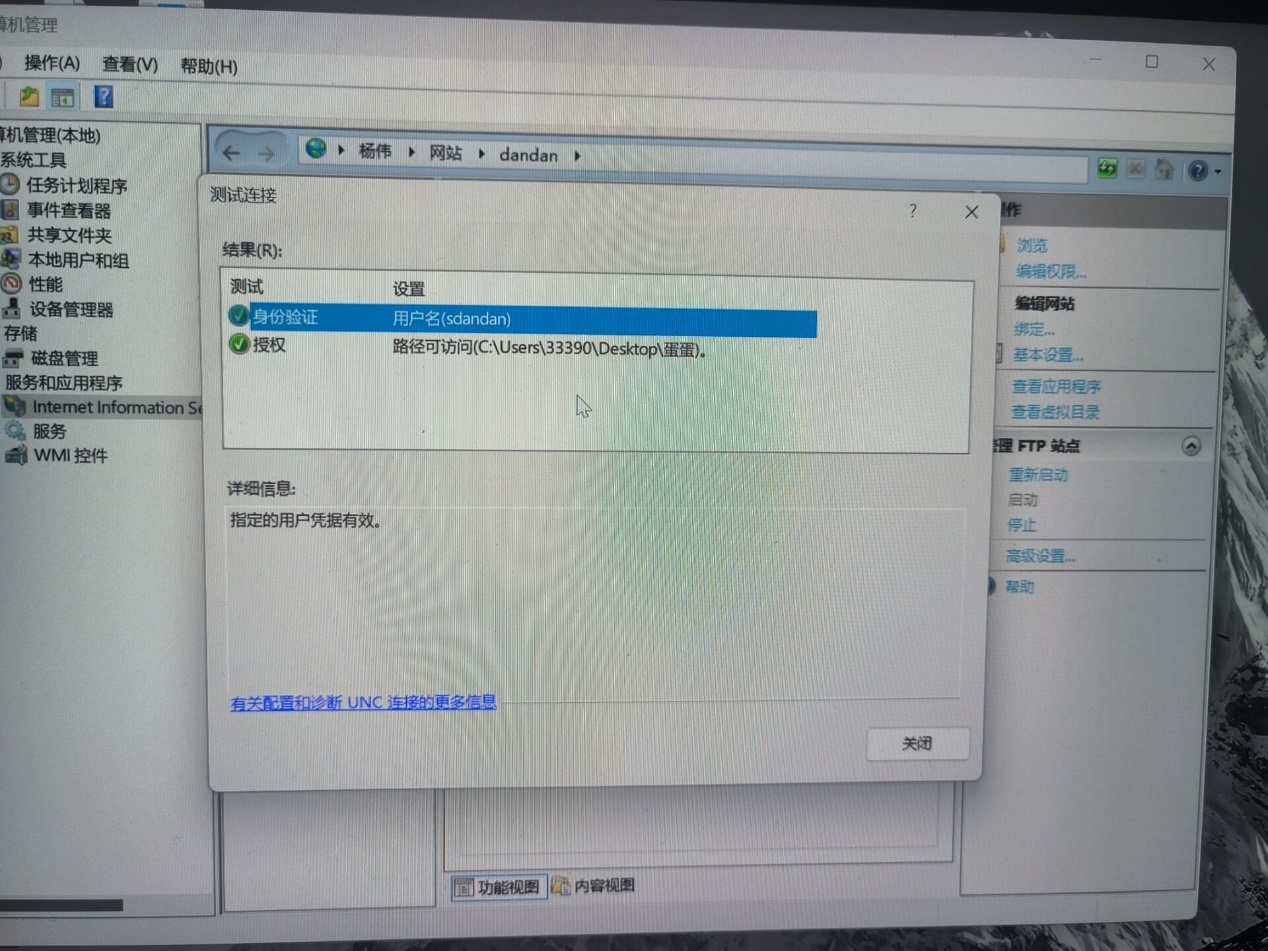
我们组选择的是一个文件夹

找到这个文件夹，如下操作



选择自己创建的用户共享这个文件（提供使用权）

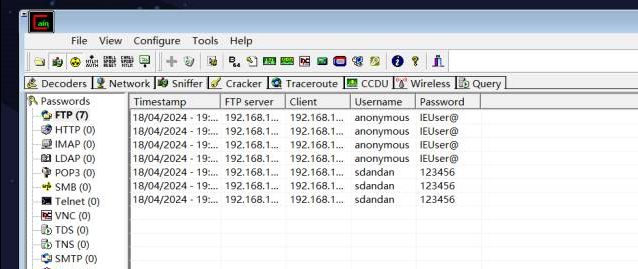
再次测试



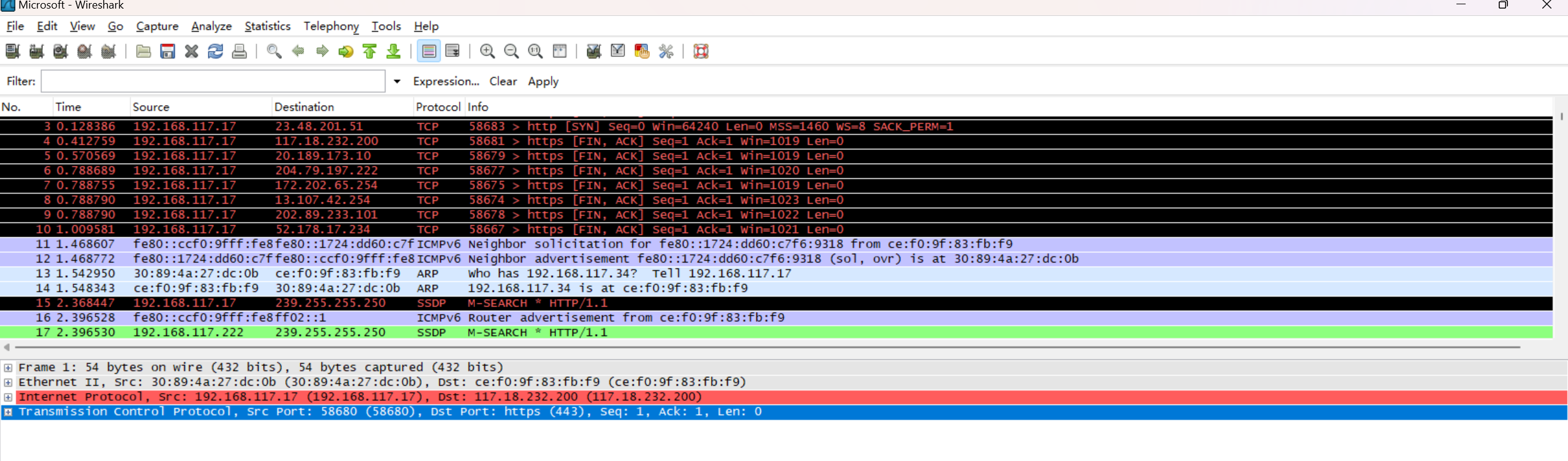
此时被攻击方可以顺利访问该文件

在输入时

攻击方获得账户和密码



此时被攻击方抓包为



实验结束