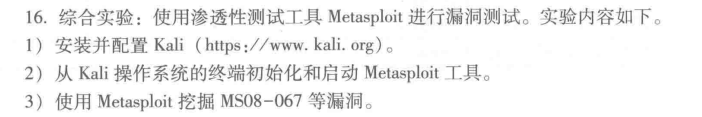
## 题目：

P239 16



## 实验介绍：

MS08-067是一个由微软在2008年发布的安全漏洞编号，该漏洞存在于Windows操作系统的服务中。它是一个远程执行代码漏洞，允许攻击者通过特制的网络请求远程执行恶意代码，而无需身份验证。攻击者可以利用这个漏洞来获取系统的控制权，并在受影响的系统上执行恶意操作。

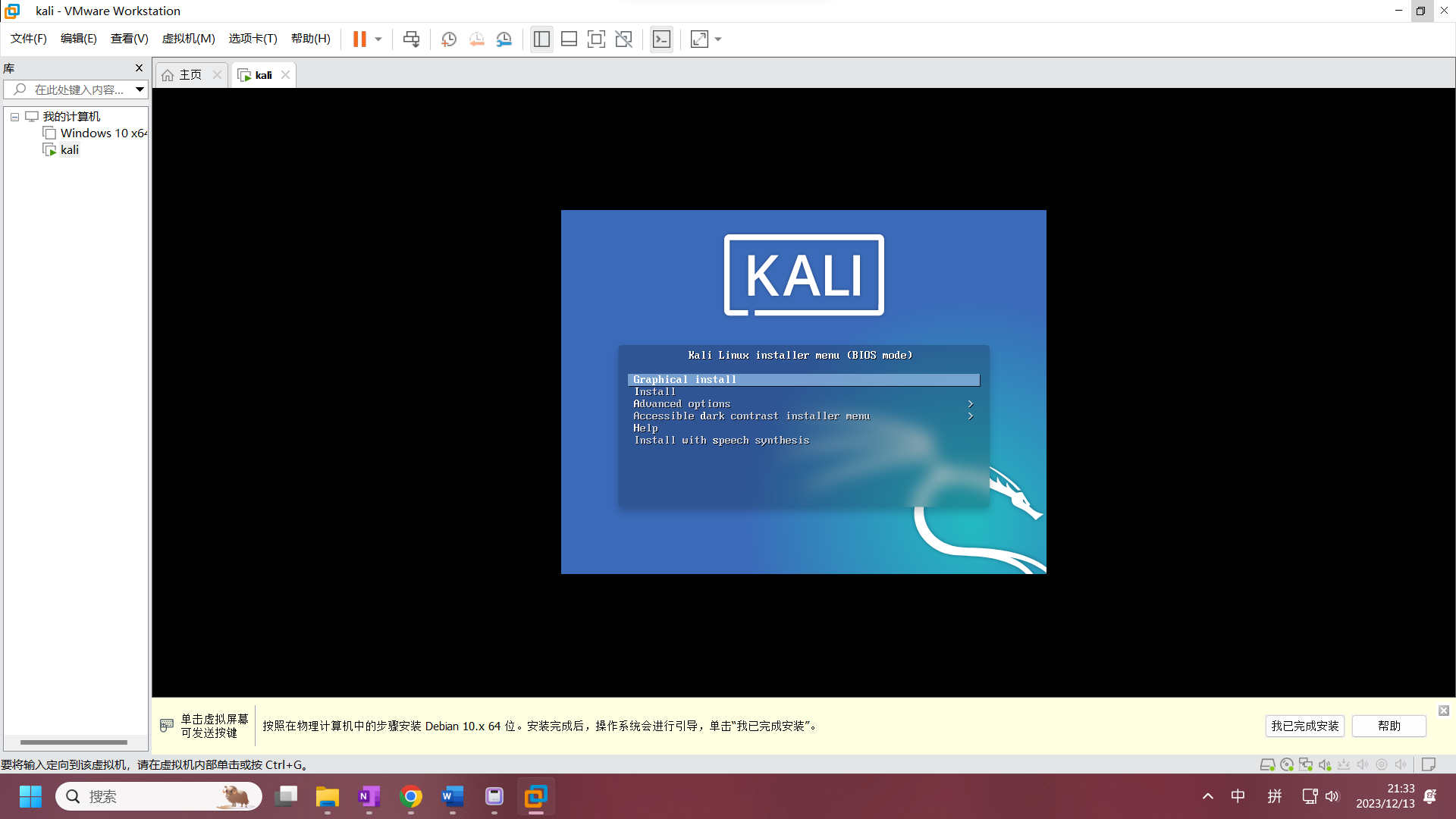
本实验还另外挖掘了ms10-046，通过这个漏洞攻击者可以通过发送特制的网络请求利用这个漏洞，从而导致远程执行恶意代码。

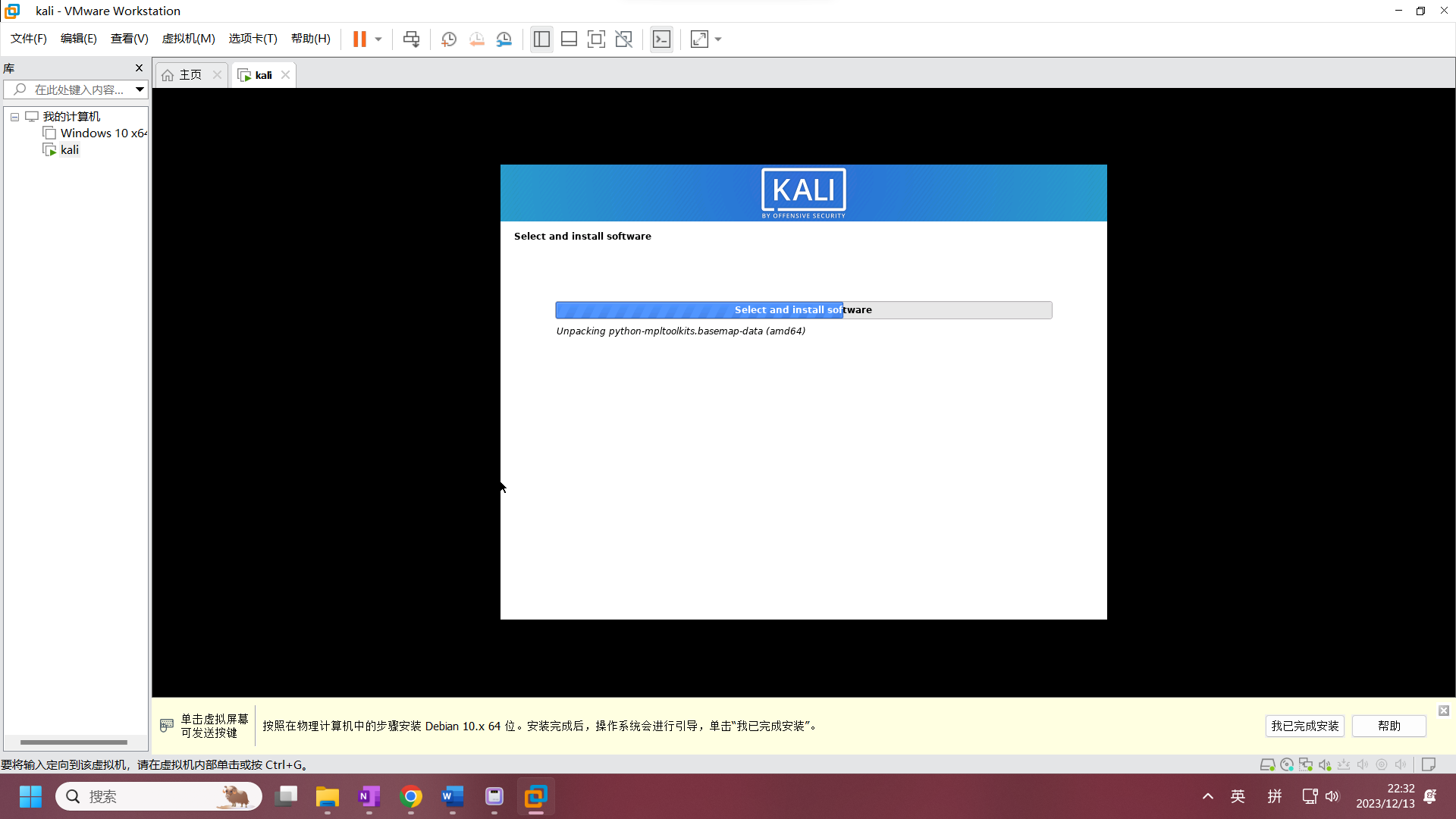
Metasploit是一个知名的安全渗透测试框架，其中包含了许多漏洞利用模块，包括针对MS08-067漏洞的利用模块。使用Metasploit的相关模块，渗透测试人员可以尝试利用这个漏洞，尝试对运行受影响Windows XP系统的目标进行攻击。

## 软件安装：

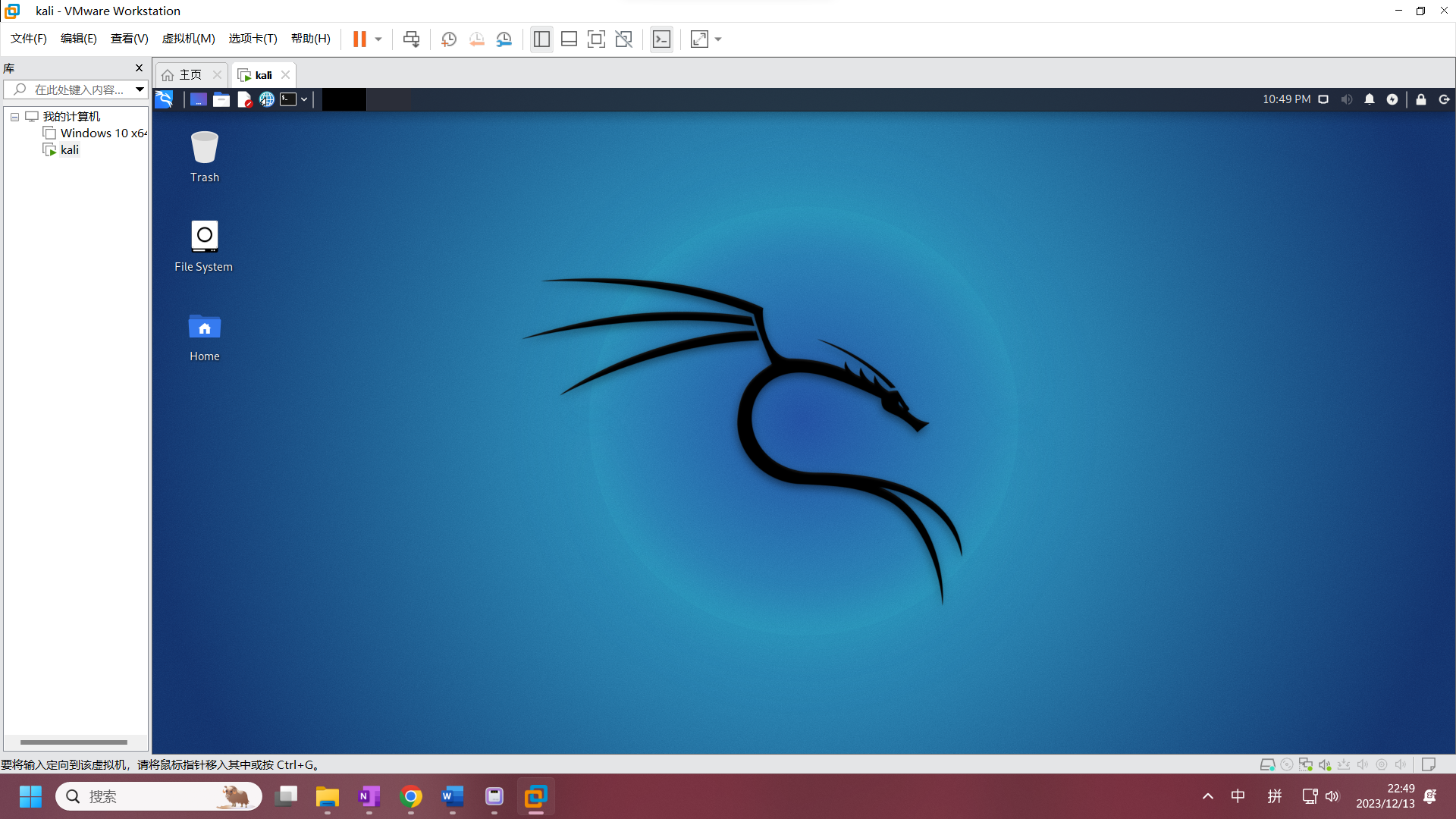
在VMware上安装kali，选择的版本为2021.2



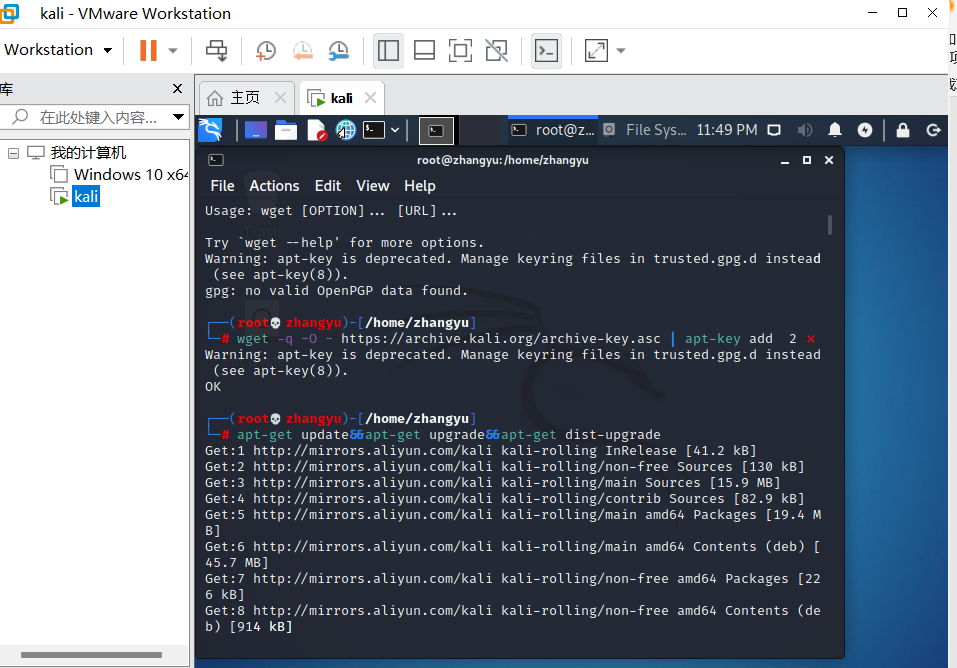




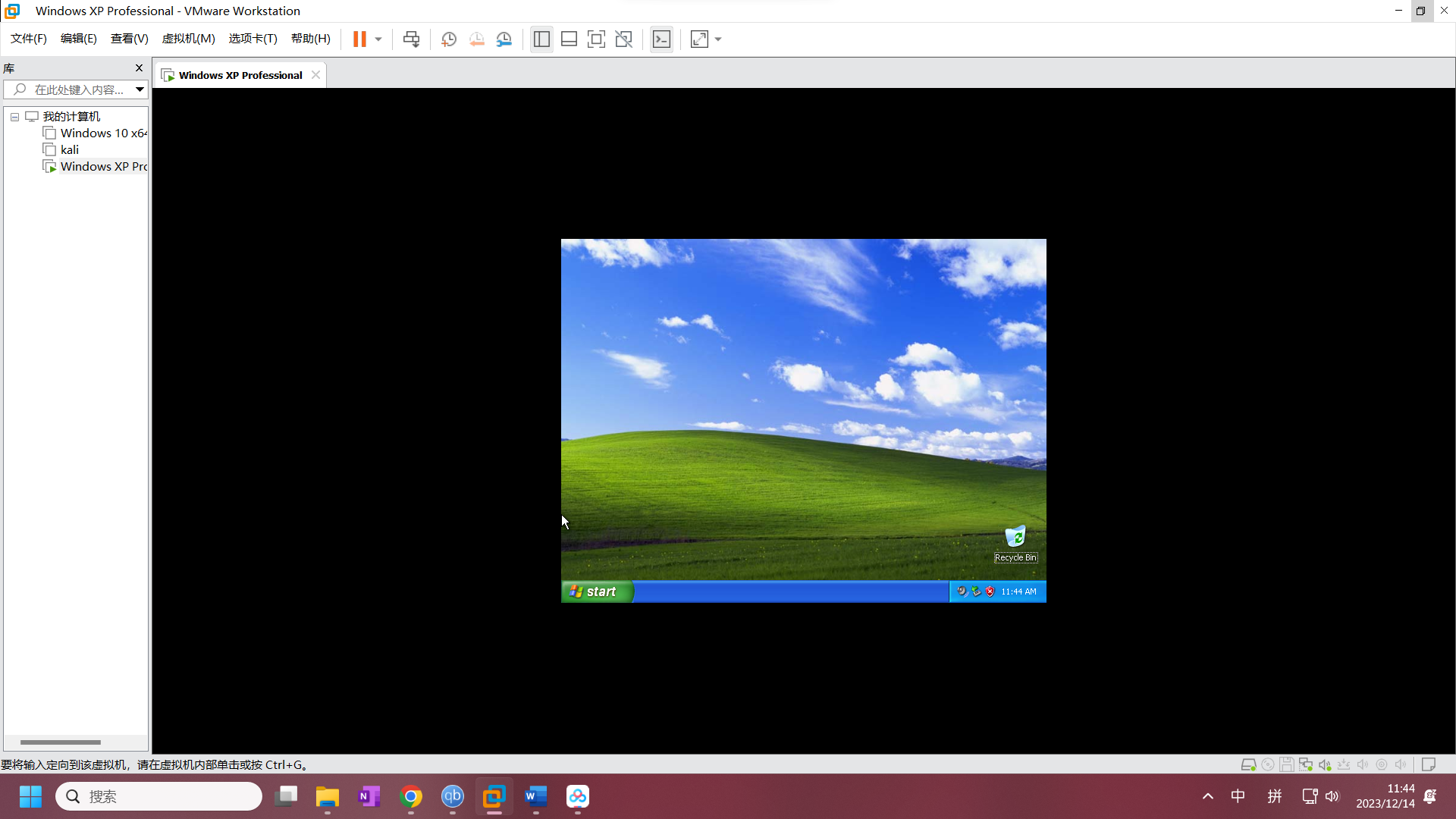
安装完成：



配置：

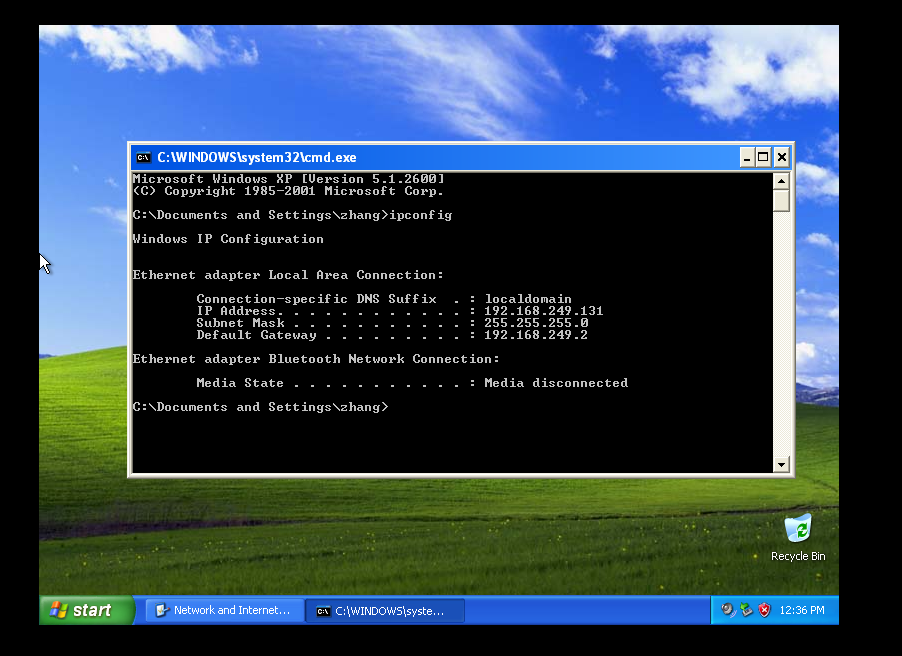


安装靶机，系统为windows xp：

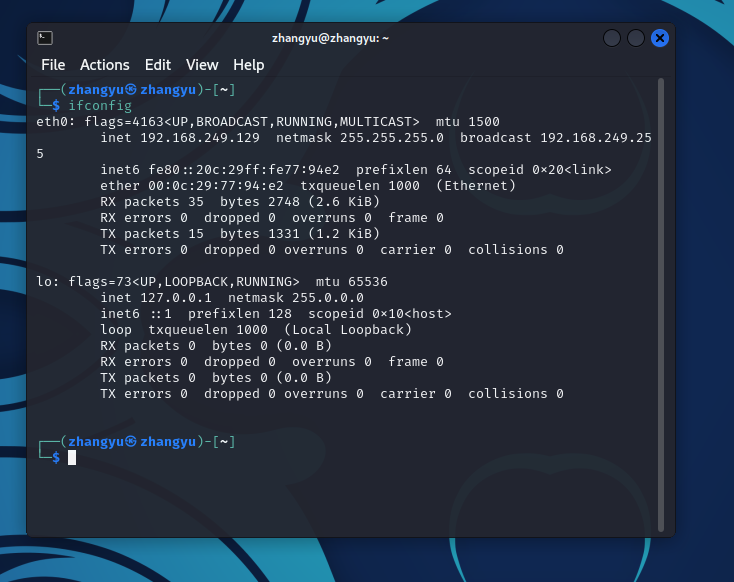


## 挖掘ms08-067

先验证两台机器互相ping得通：



Windows ip 192.168.249.131

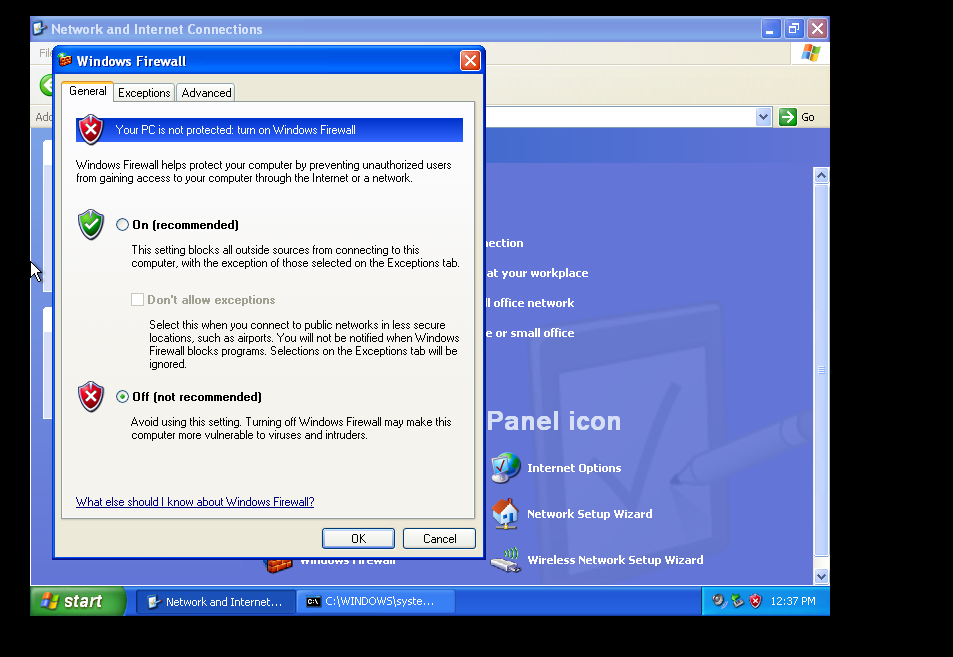


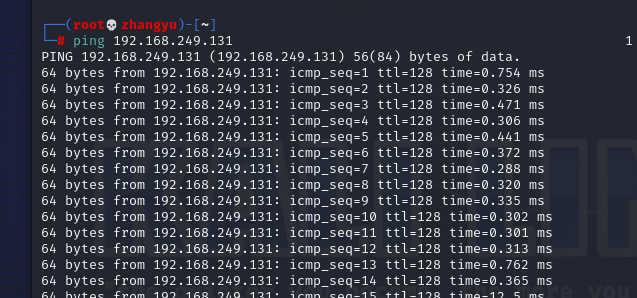
Kali ip 192.168.249.129



在ping靶机的时候出现了一些小问题，一开始是ping不通的。

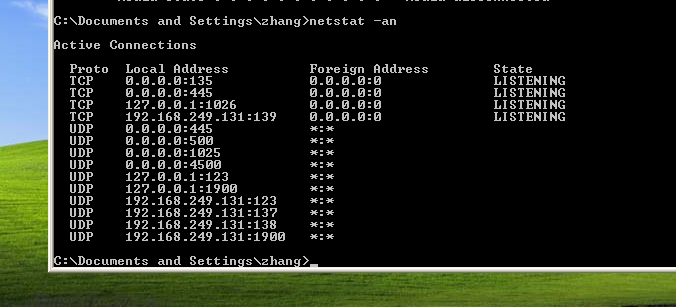
解决方法：

在控制面板windows防火墙里面选择关闭就可以了，看来是防火墙一开始把icmp给截胡了

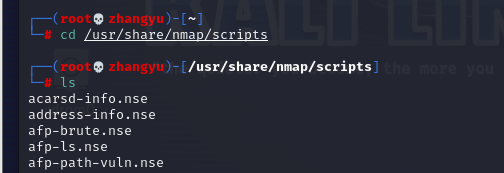


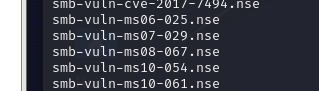
终于是ping通了

查看靶机开放了哪些端口，可以看到445端口是开着的



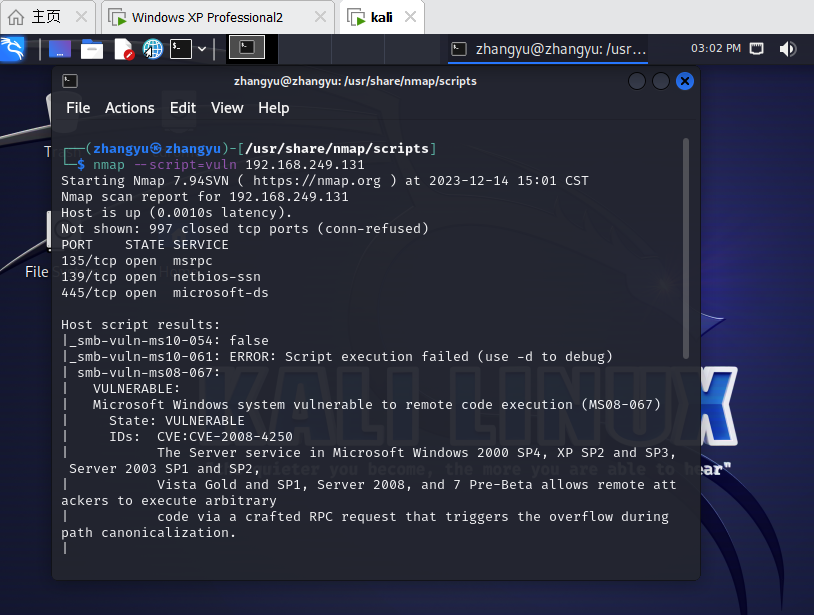
用kali的nmap工具看是否存在ms08-067漏洞



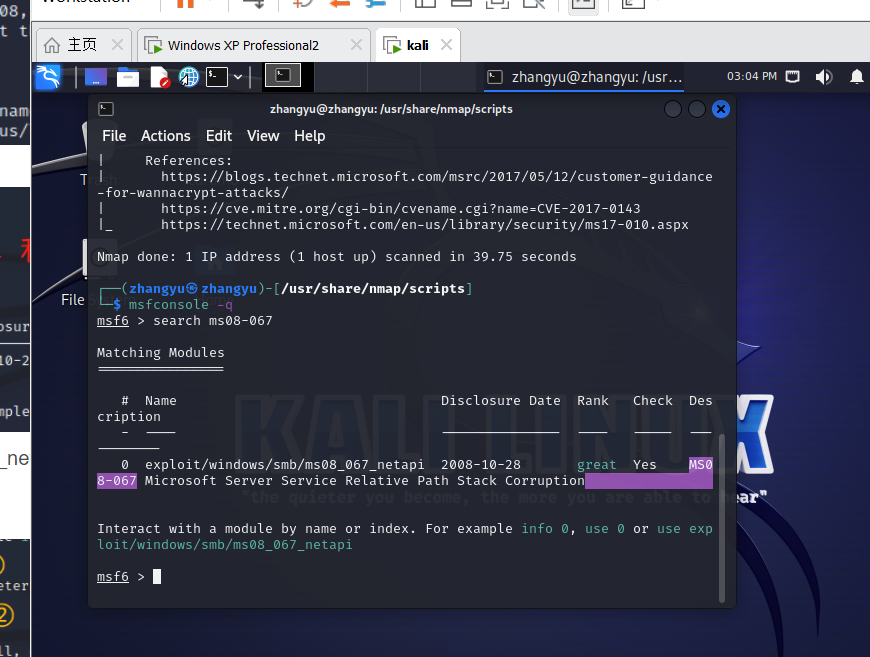


找到了

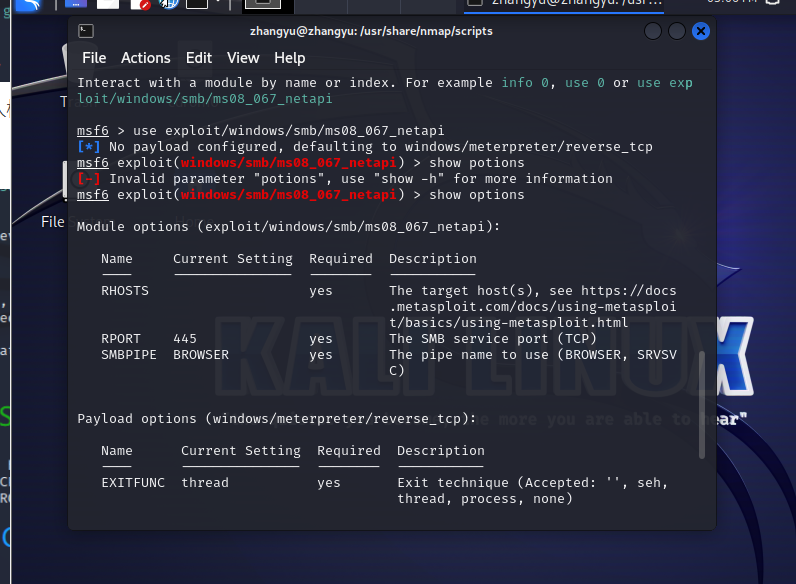
对靶机进行漏洞扫描

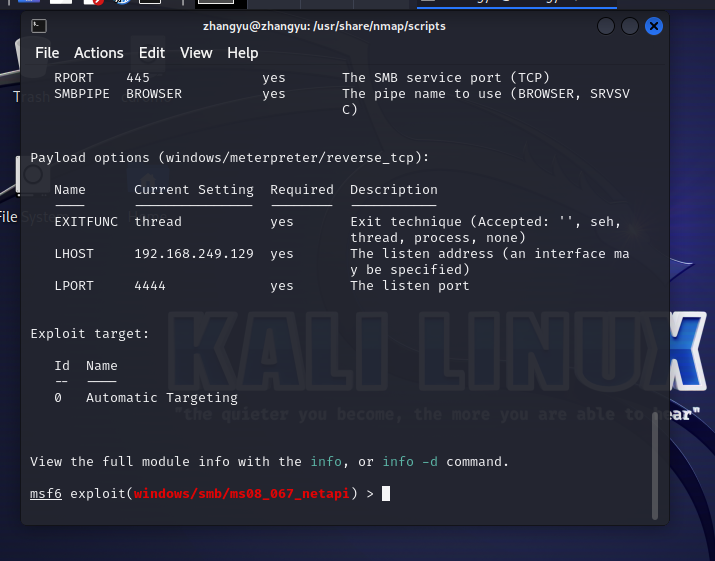


启动metasploit，用search查看可利用的模块

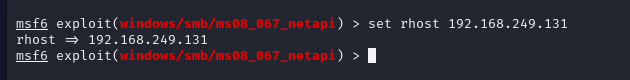


进入模块并且查看下使用说明

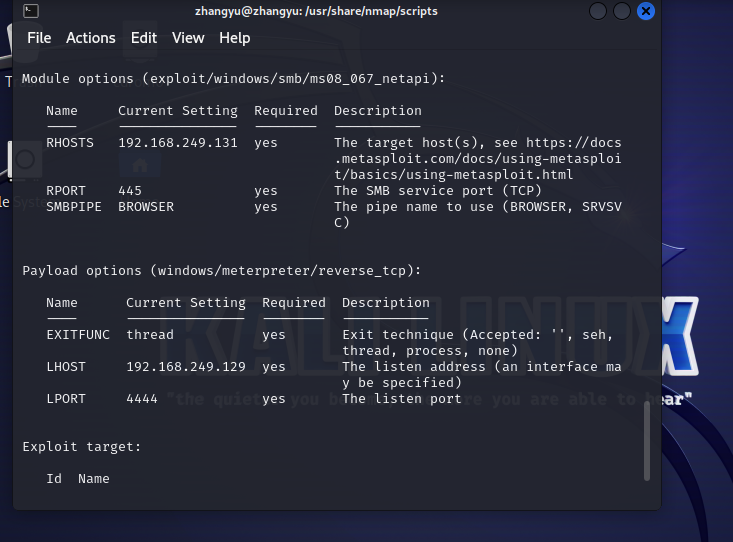




但是靶机的ip没设置好，设置一下

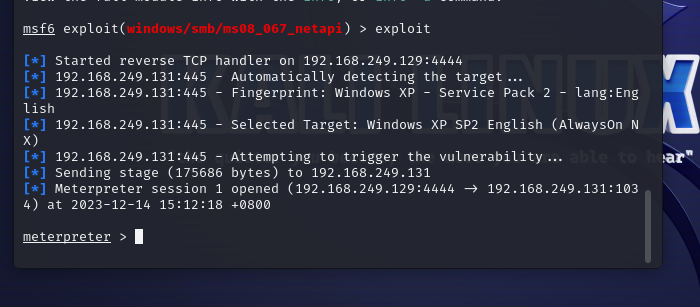


检查下：



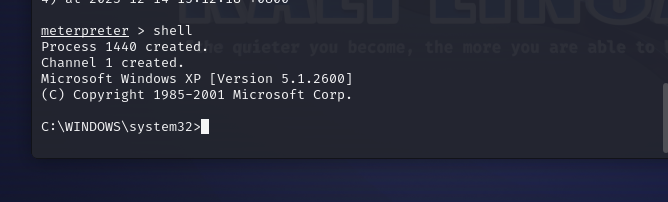
可以看到全都设置好准备就绪了

开始攻击：



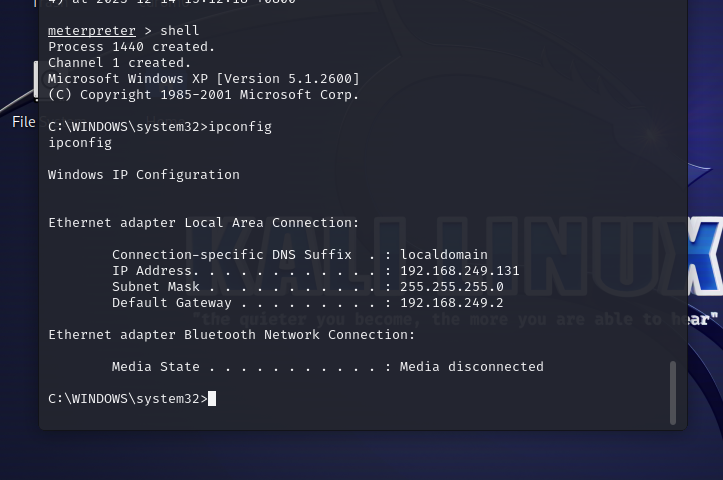
可以看到成功将大量的数据给发了过去，造成了缓冲区溢出

在msf中远程打开靶机命令行：



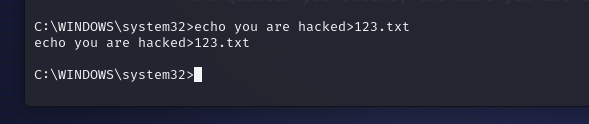
还真能打开！

检查一下是不是远程的靶机：

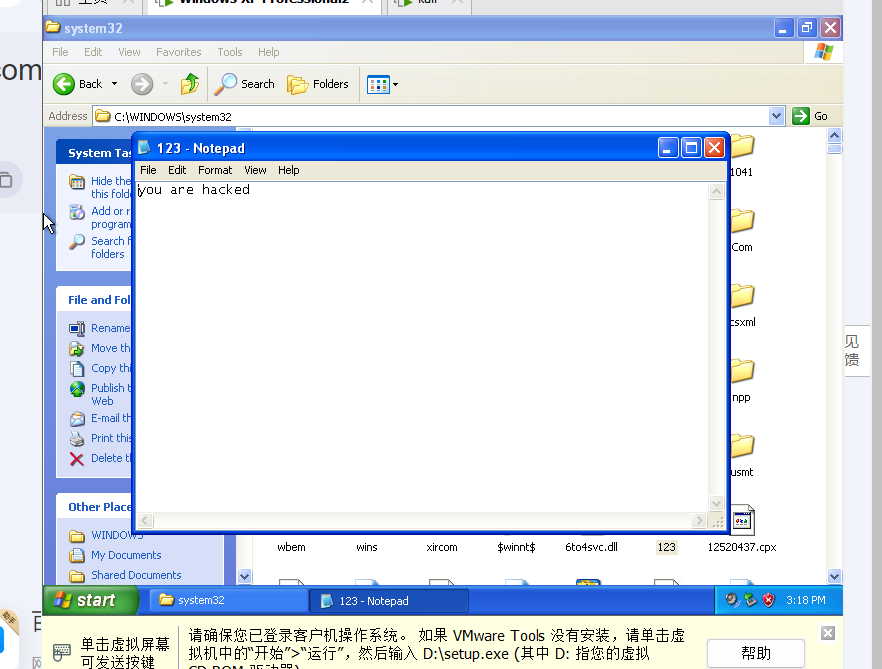


从ip地址可以看到确实是靶机

下面就可以通过命令行为所欲为了



看看靶机对应位置：

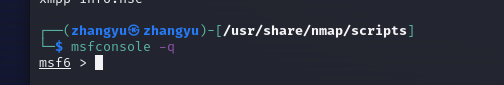


可以看到在kali虚拟机的msf中我已经成功可以操作windows xp靶机了，渗透成功！

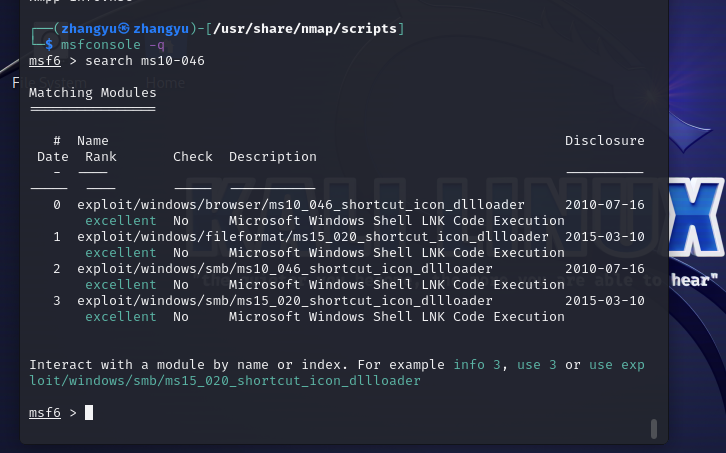
## ms10\_046

其实ms08-067和其他此类的挖掘过程都是差不多的

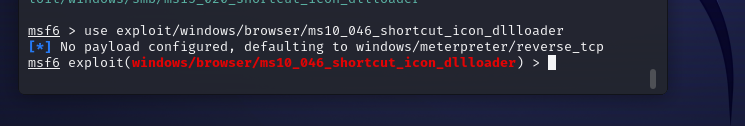
进入msfconsole



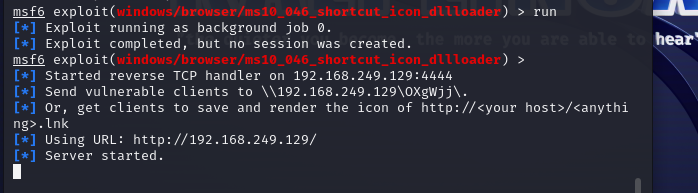
寻找漏洞相关模块



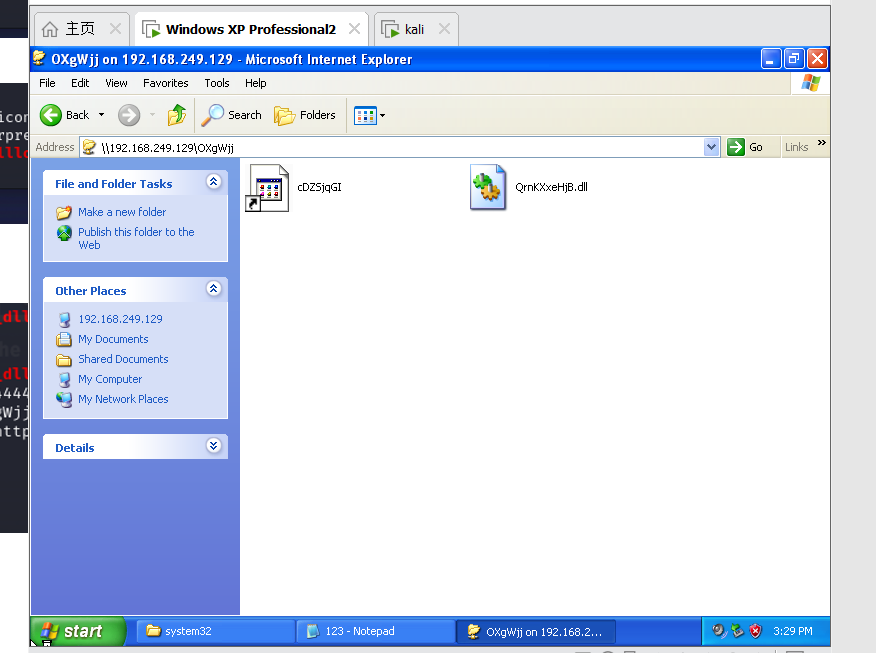
使用第一个模块



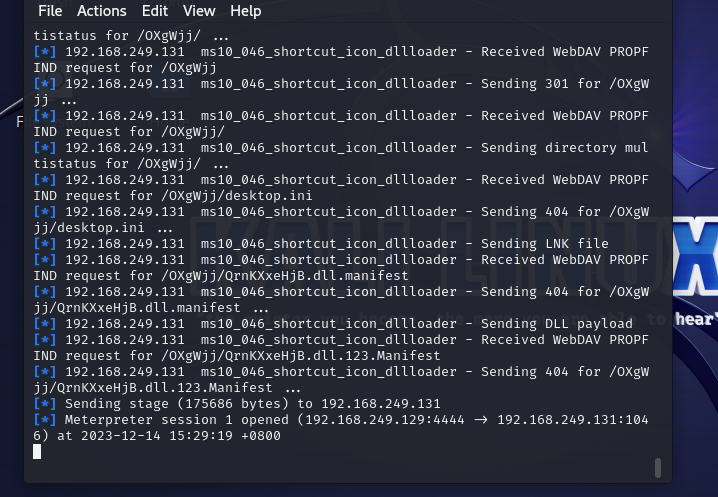
运行



打开靶机访问url：



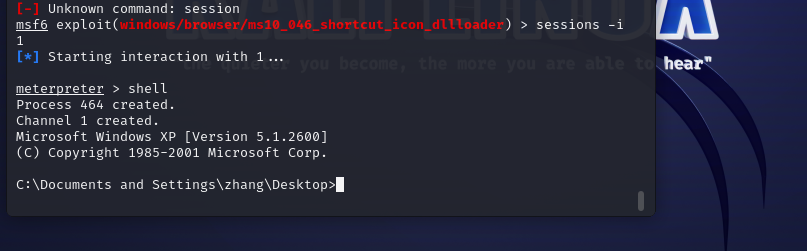
回到msf，控制台显示渗透完成



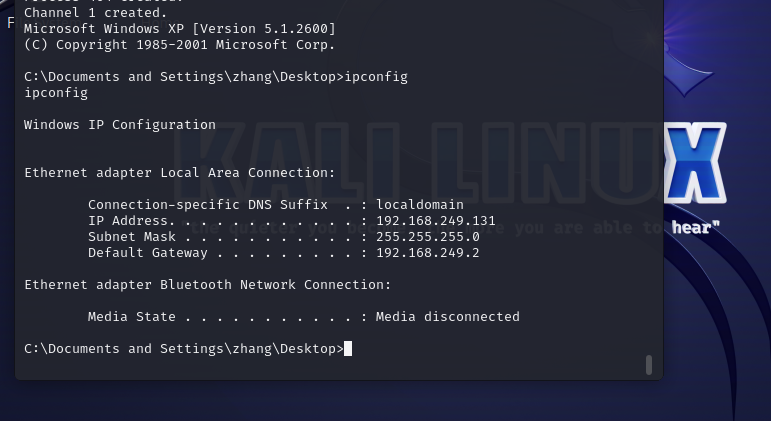
Sessions查看会话



打开这id为1的会话并进入靶机的shell：



确认下是否为靶机：



下面还可以进行类似写文件等操作，这里不多演示了。