# 《软件安全技术》综合实验

## 实验三：使用Metasploit工具

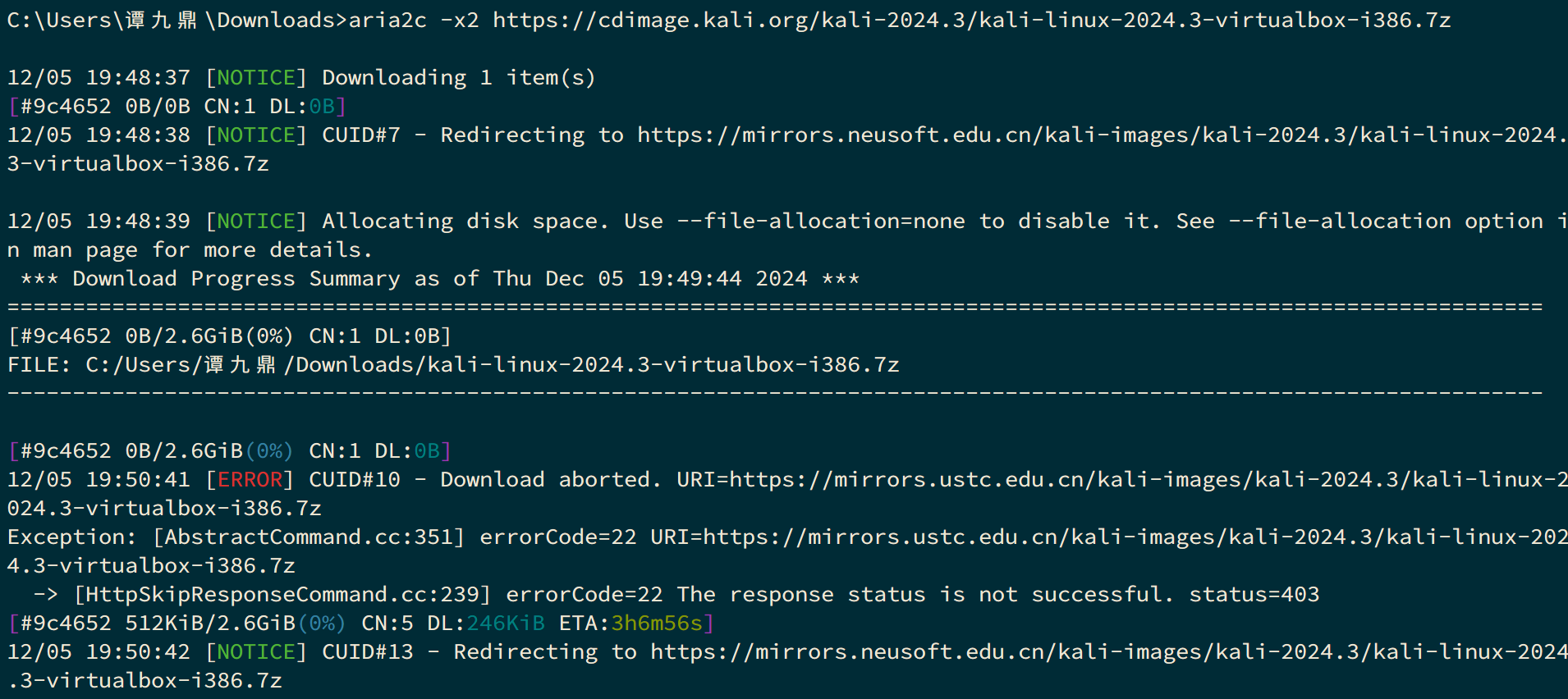
## 作者：谭九鼎

## 学号：522024320137

## 时间：2024年12月

Kali官网，vbox镜像：<https://www.kali.org/get-kali/#kali-virtual-machines>

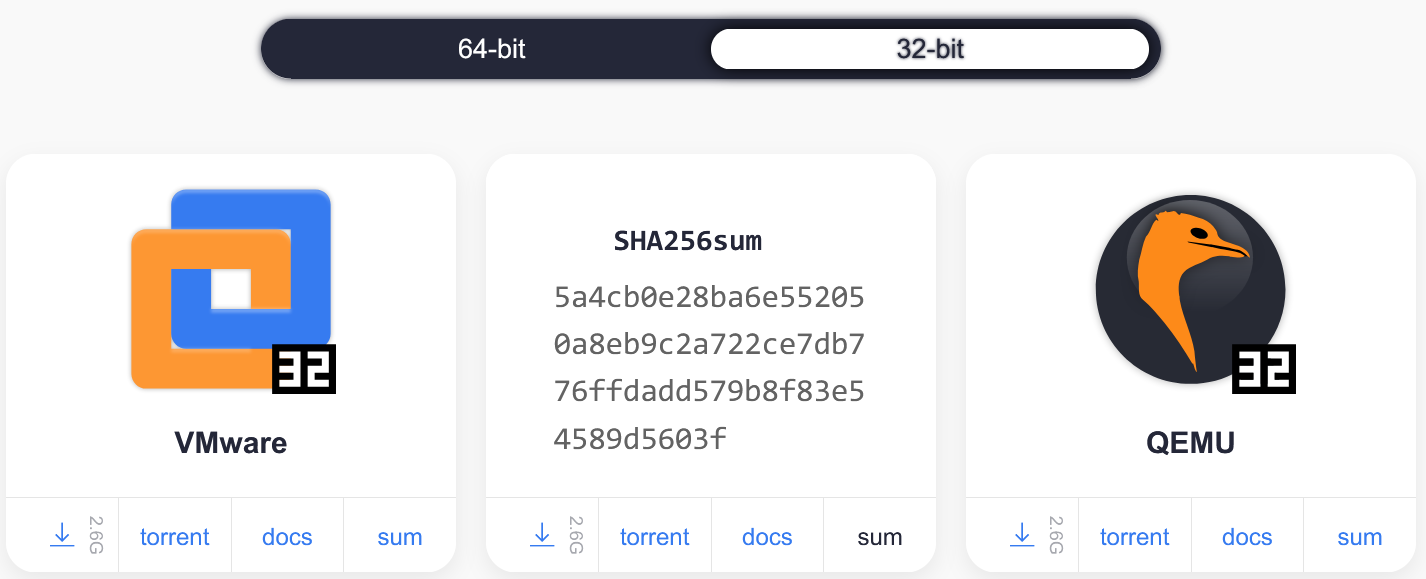
使用aria2c下载：



验证完整性：

使用Powershell命令Get-FileHash计算sha256，对照官网一致。

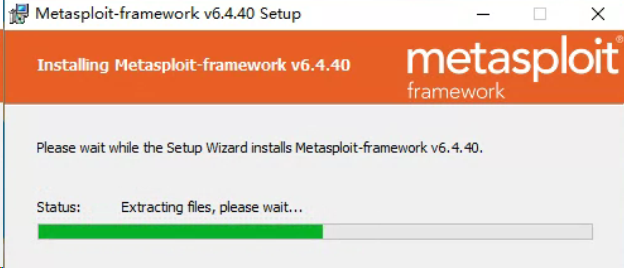




但其实没必要用Kali，直接用Metasploit就好了。

官网：<https://www.metasploit.com/>

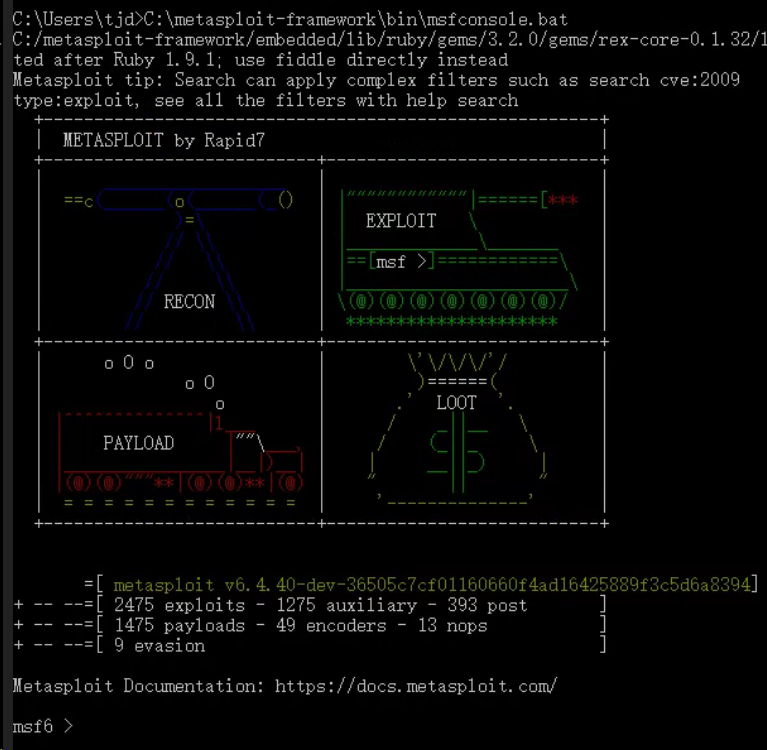
有Windows版。



MS08-067漏洞复现：

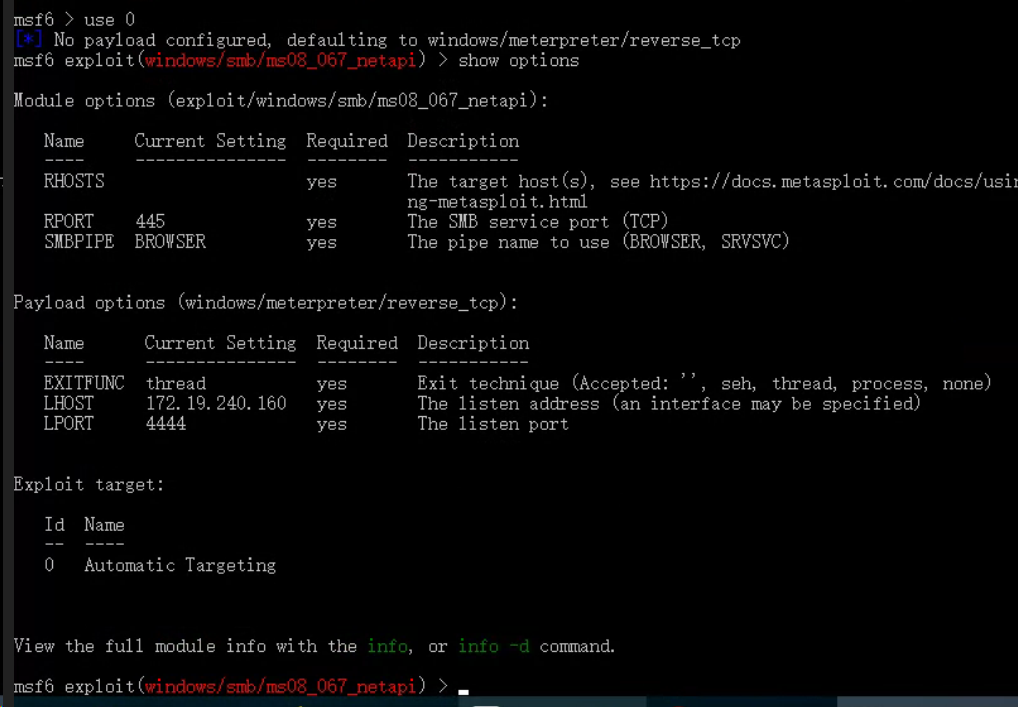
<https://blog.csdn.net/m0_46624929/article/details/142173483>

输入msfconsole 启动msf



search ms08

use 0



Info命令显示一些信息：

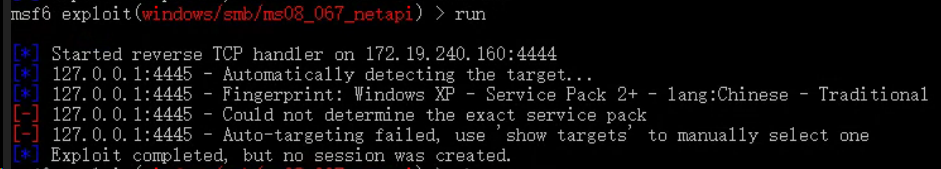


关闭虚拟机xp的防火墙：

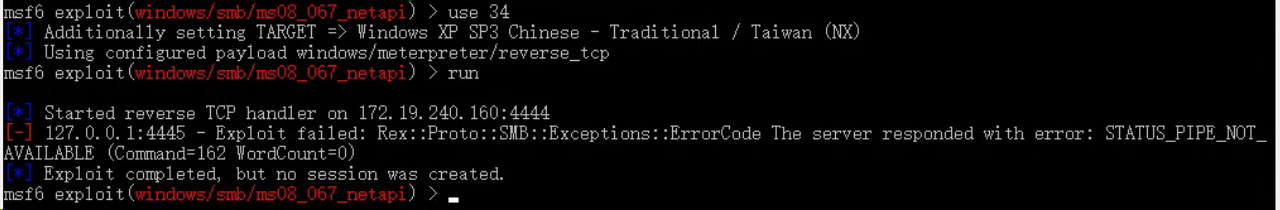


使用set rhost设置目标。

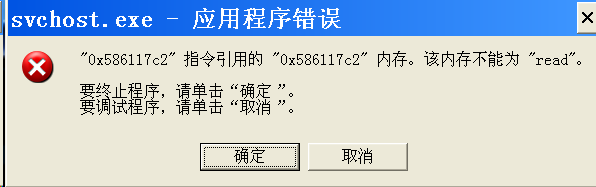
运行run：



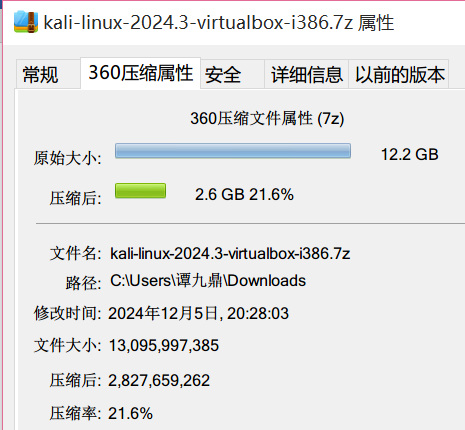
手动选择中文版SP3：



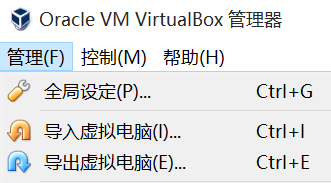
虚拟机报了错，但并没有成功获取到shell。也许是我用的修改版xp补上了漏洞。

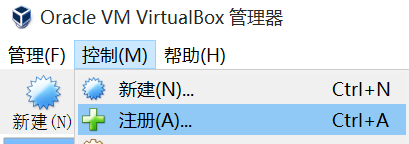


再次尝试。这次使用kali虚拟机，毕竟已经下好了。

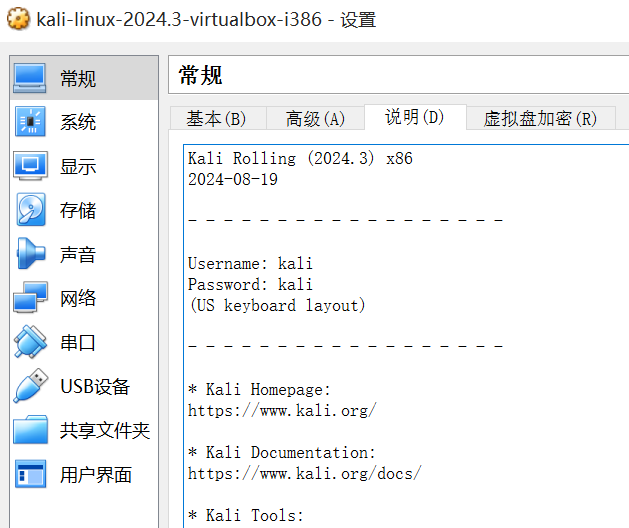


压缩率挺高的。

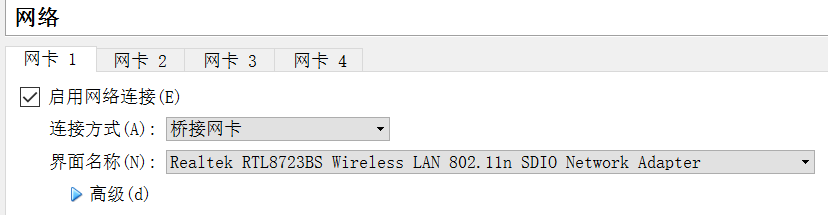




进入vbox，用控制下的注册，不是用导入。



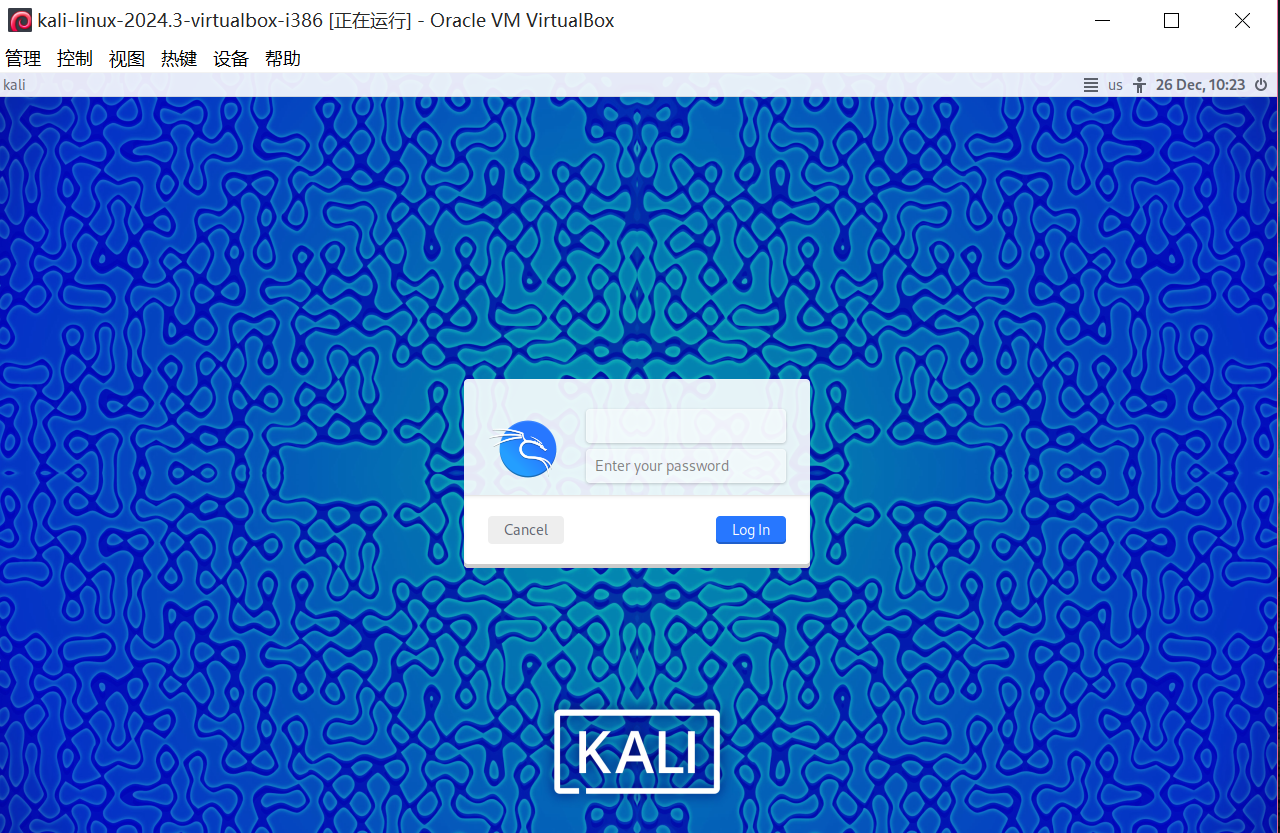
查看说明。里面提到用户名和密码都是kali。



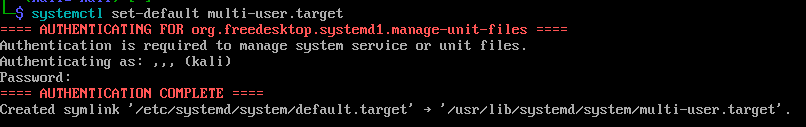
将两个虚拟机的网卡模式都设为桥接



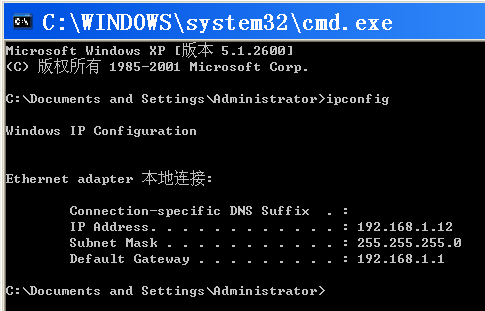


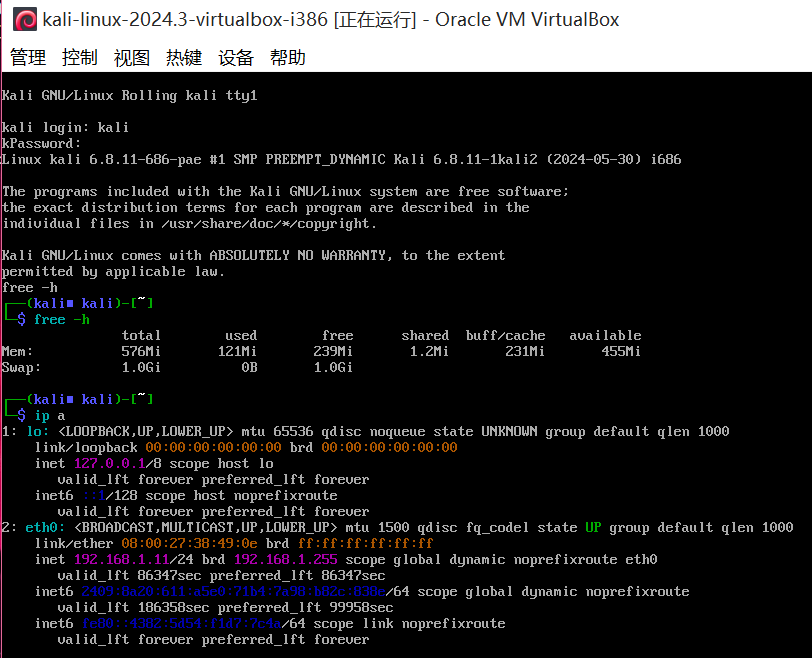


启动虚拟机，进入系统。

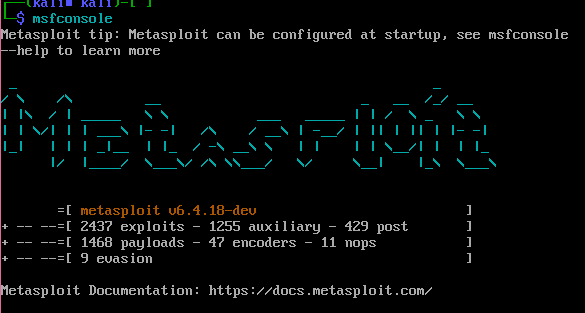


使用systemctl关闭图形化界面，节省资源。





两个虚拟机的IP

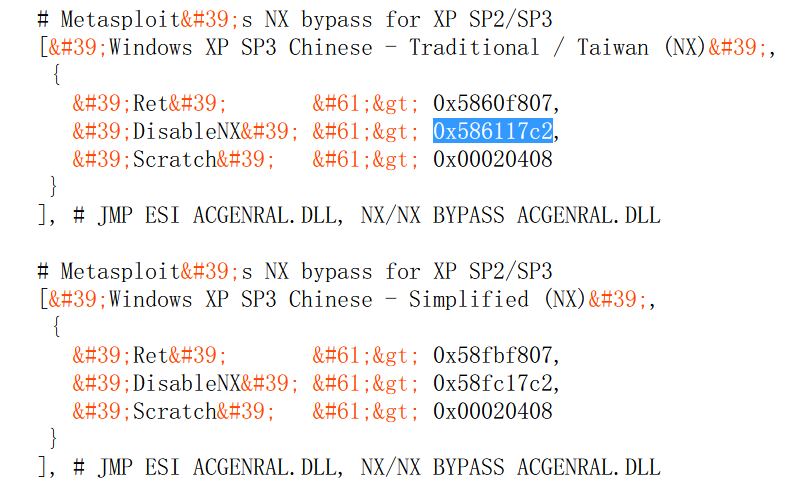


进入msfconsole

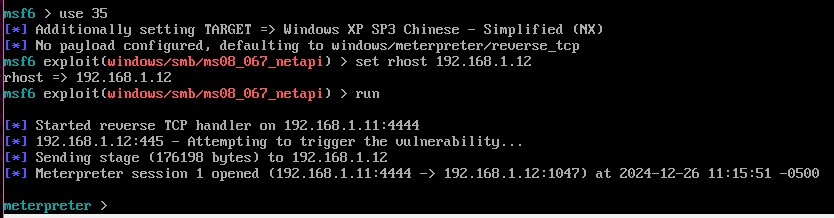
按照先前的步骤，还是报一样的错误。

目前排除了msf的系统和软件问题，两个虚拟机也确定可以互访。其实还是有可能xp的漏洞补上了的，如果要重装xp就太麻烦了。

最后试着搜索了一下报错代码中的指令，因为指令其实对应着汇编，虽然一般来说是没什么效果的。



但还真有发现，那个指令不是乱显示的，而是固定的、有意义的。之前use 0失败，是它猜测为SP2；然后我手动use 34，虽然用了SP3，但语言是繁体中文，我本以为无所谓（也可能是没看到）。但既然报错指令确实对应了use的，底下又有一个简体中文，且指令不同，可以猜测不同语言确实是有影响的。



这回改为use35，成功了。

