**操作系统**

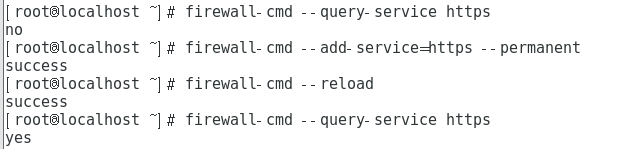
**实验报告**

姓名： 蔡欣彤

日期： 2023.7.6

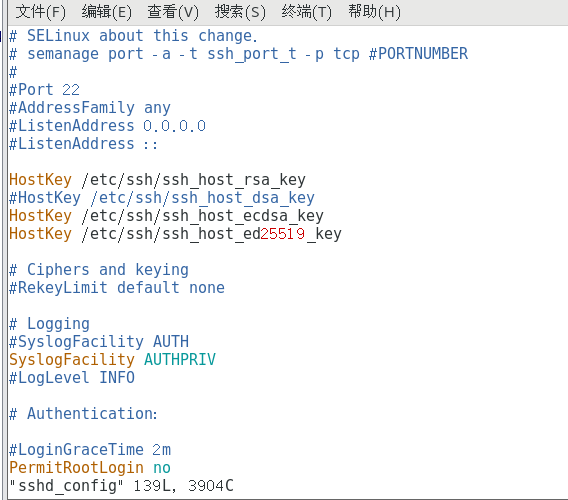
1. **实验题目**

例题1：为Linux防火墙添加HTTPS服务（过程详细截图）



例题2：服务加固SSH（Linux）（过程详细截图）

ssh禁止ROOT用户远程登录



设置root用户的计划任务。每天早上7:50自动开启ssh服务，22:50关闭；每周六的7:30重新启动ssh服务



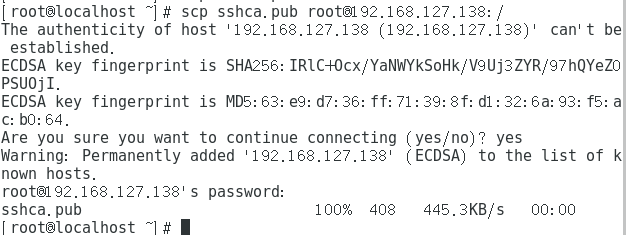
例题3：流量完整性保护（Linux）（过程详细截图）

为了防止密码在登录或者传输信息中被窃取，仅使用证书登录SSH（Linux）

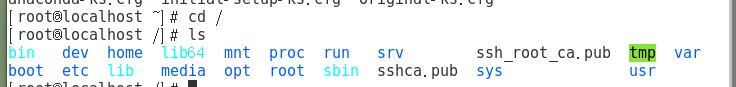
客户端创建密码：

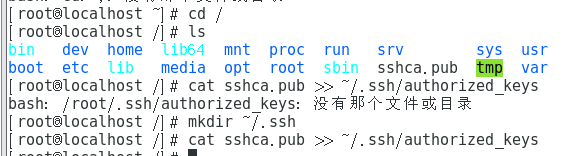


客户端上传到服务器：



服务器：



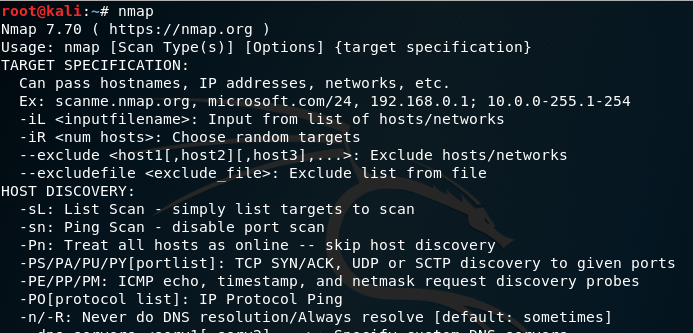


客户端：

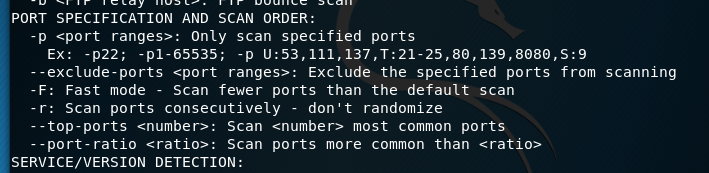


例题4：使用nmap扫描本机的端口，要求扫描全部端口。（过程详细截图）

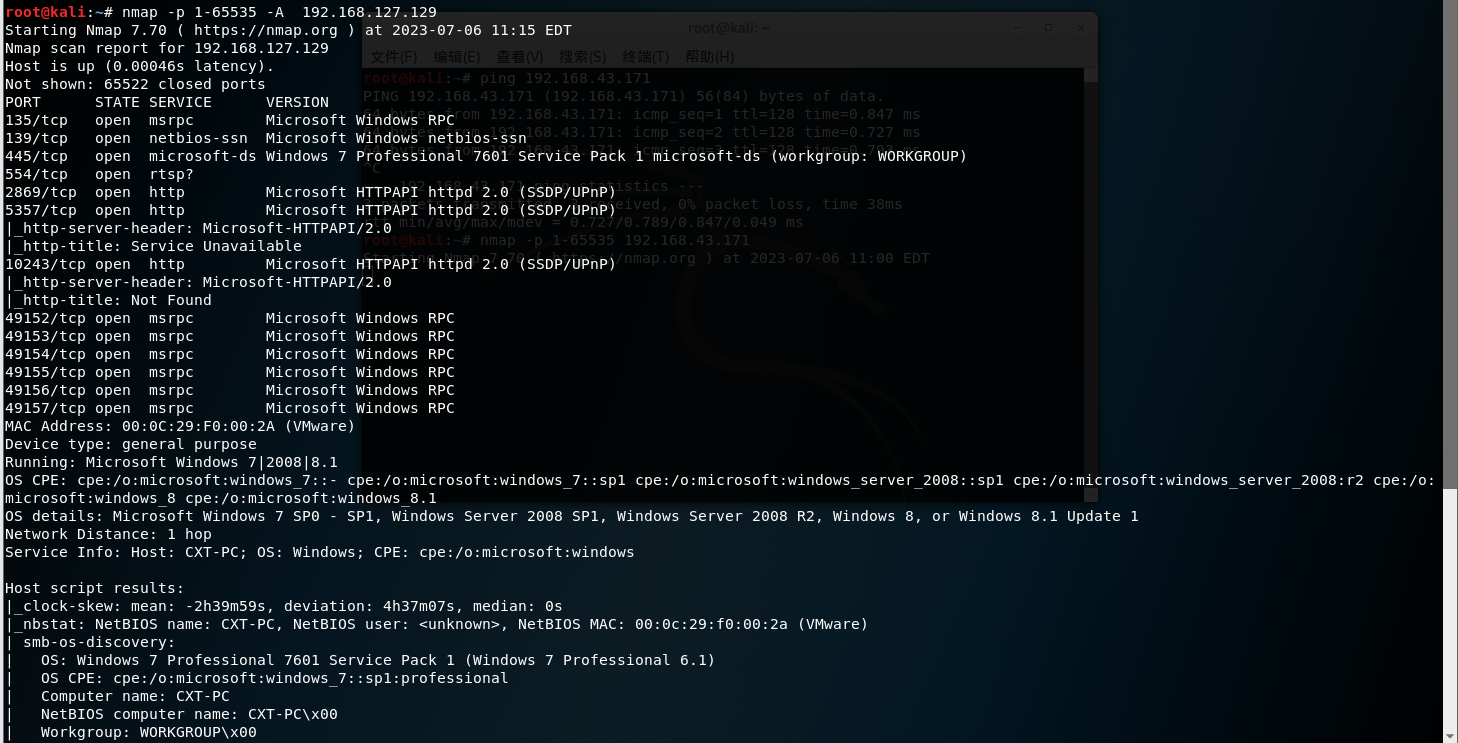
先确认nmap是否存在



查询nmap扫描端口的用法

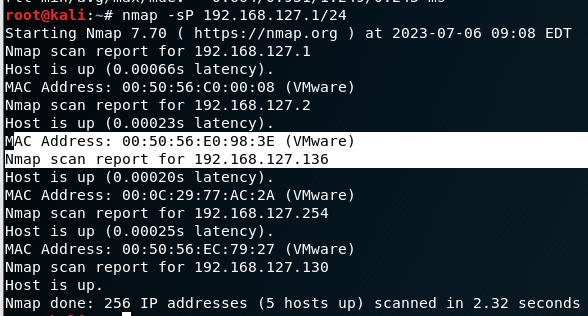


最后输入命令扫描端口1-65535

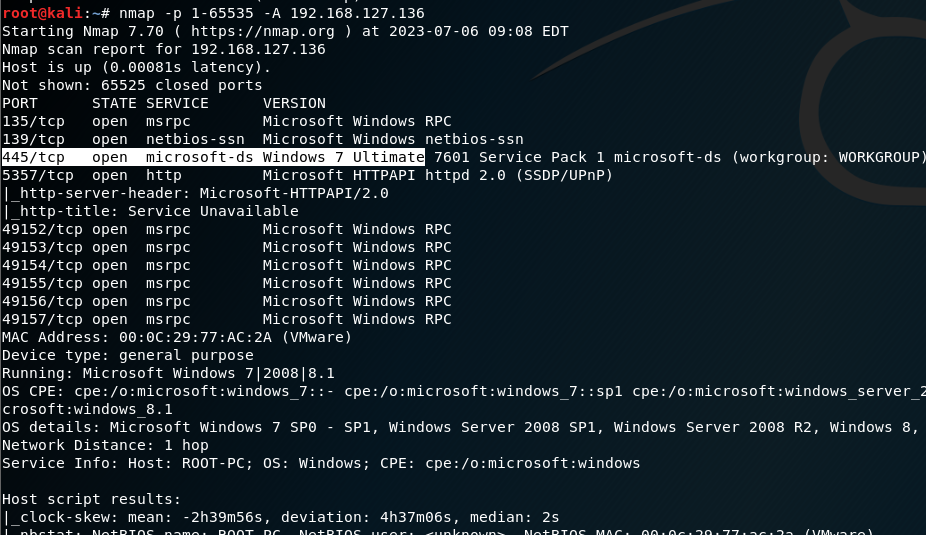


例题5：搭建永恒之蓝的漏洞环境，利用msf工具，复现永痕之蓝漏洞。（过程详细截图）（教程可参考下面网页进行复现：漏洞环境安装<https://blog.csdn.net/m0_62584974/article/details/126322675>

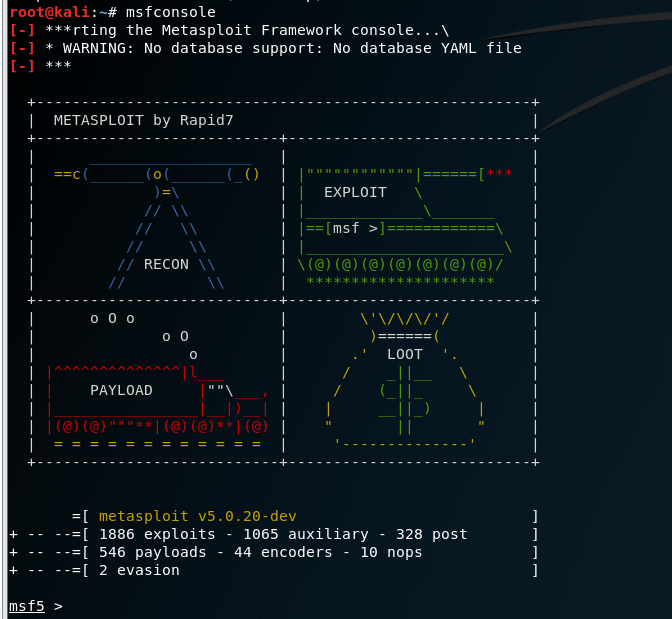
扫描整个192.168.127.0网段



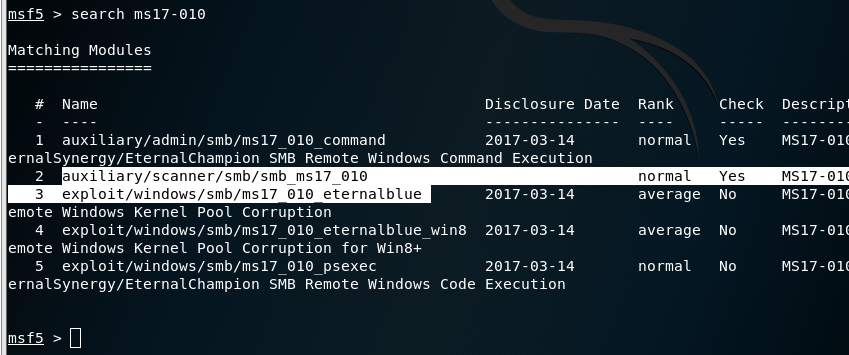
扫描整个端口



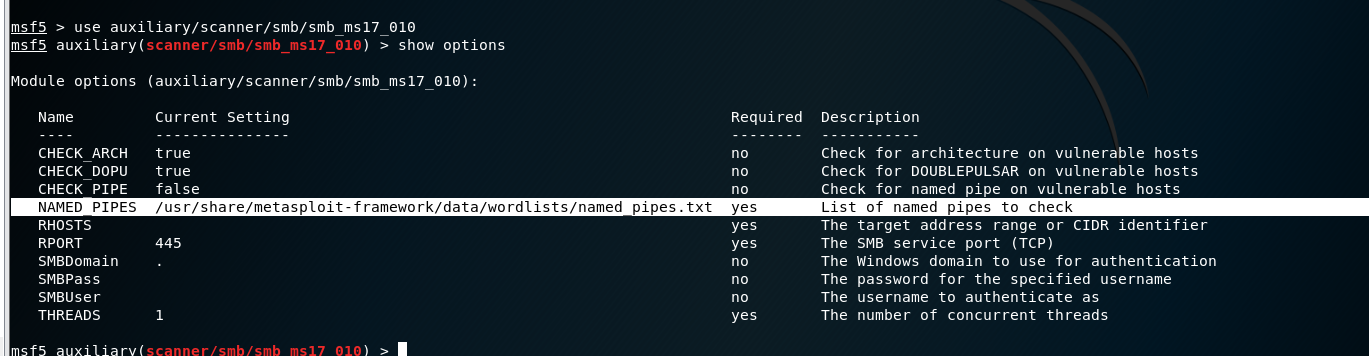
进入MSF控制台



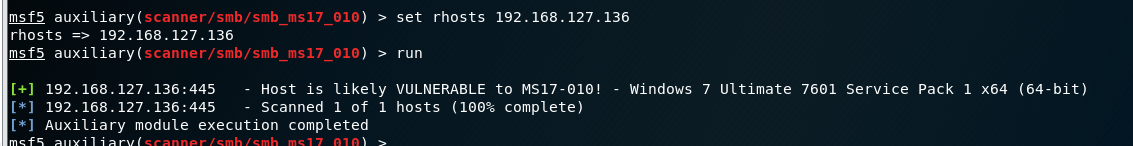
寻找永恒之蓝漏洞利用脚本



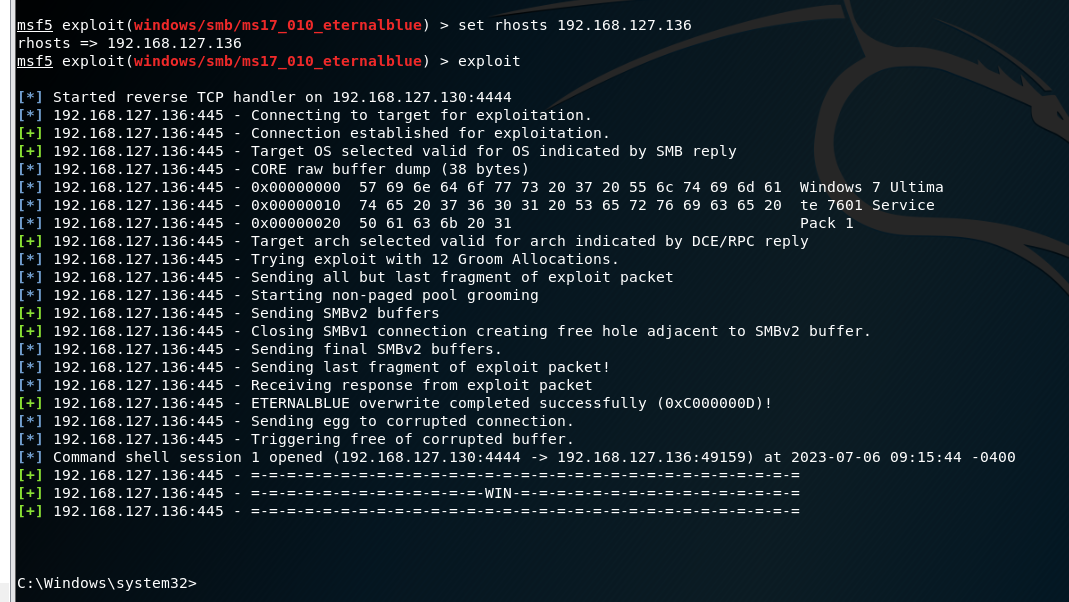
查看该模块所需要的参数配置



设置RHOSTS并执行扫描



填写参数并开始渗透



1. **实验总结**

（在实验中遇到的问题及解决方法、收获是什么）

第三题scp命令不成功，重新安装了一遍centos虚拟机，更改了配置，最后可行了。

学会上网查找答案，比如第二题的星期六；学会看终端的指令help，比如nmap就是看终端的提示做出来的；知道了电脑上win7 professional没有永恒之蓝漏洞，思考了一下原因，好像是安装之初就打了补丁，不得已重装了win7；电脑内存几乎无了。