2023 － 2024 学年 第 1 学期



### 实 验 报 告

课 程 名 C01218

课 程 号 网络安全防护技术

学 生 姓 名 张炳欣

学 生 姓 号 32201241

专 业 班 级 软件工程2204

所 在 学 院 计算机与计算科学学院 指 导 老 师 沈淳

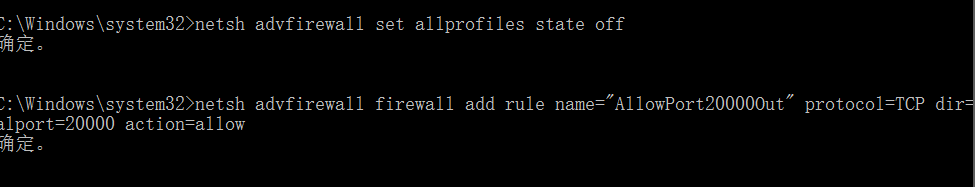
实验报告日期： 2024 年 10 月 22 日

**课程实验报告清单**

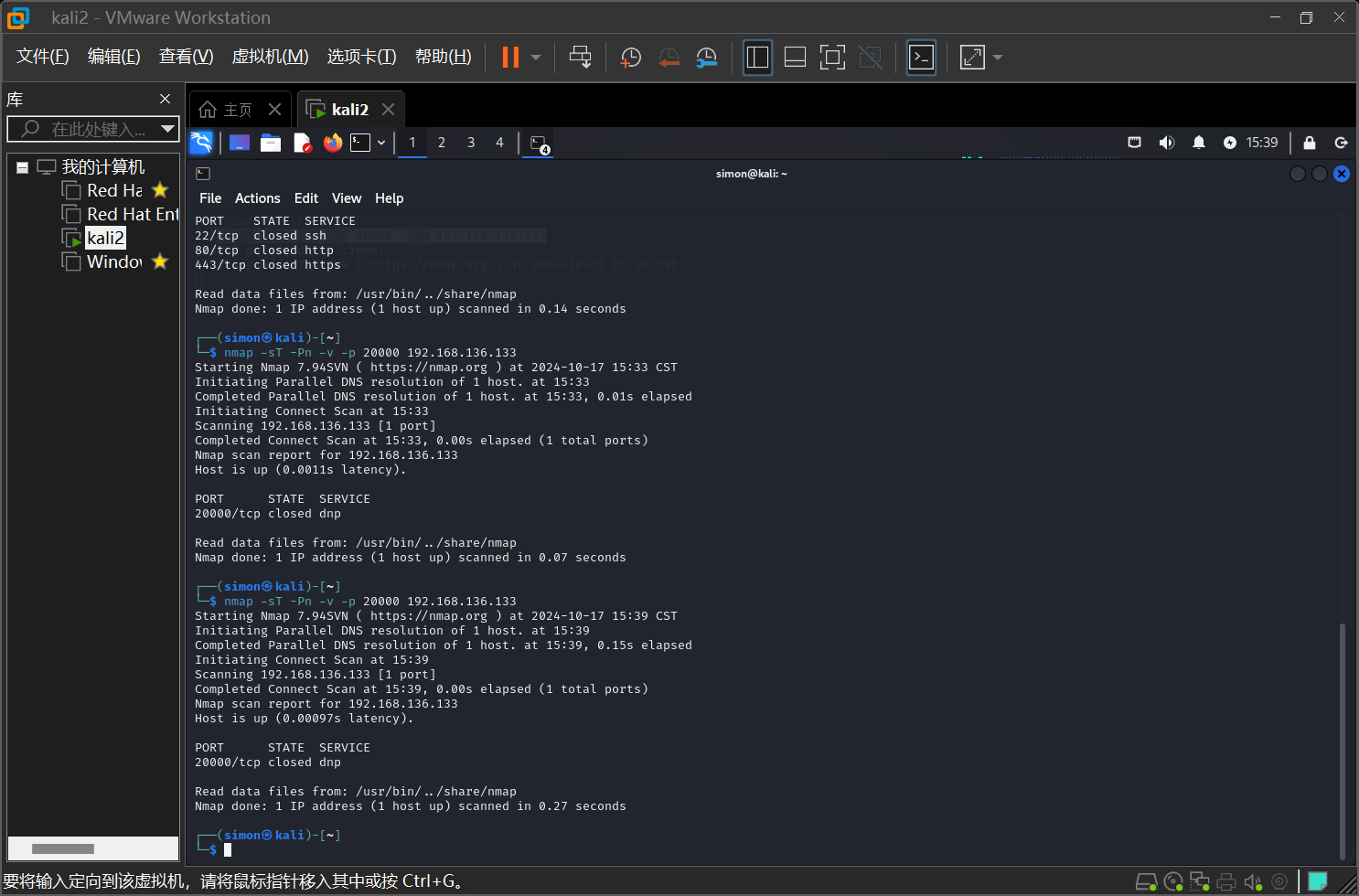
|  |
| --- |
| 目录 |
| 1. 使用nmap进行全连接扫描，要求：将20000端口禁用后指定端口扫描。 |
| 2. 针对某个（可根据自己主机按需要扫描）开启的端口和关闭的端口，使用nmap进行半连接扫描、FIN扫描、UDP扫描，查看扫描结果反馈。 |
| 3. 使用telnet命令对163邮箱服务器的SMTP和POP3服务进行扫描 |
| 4. 开启windows系统的SSH服务，使用nmap对主机进行服务版本信息扫描 |
| 5. 在kali上用metasploit中的http\_version和ssh\_version确定浙大城市学院服务器版本号和ssh服务器版本号 |
| 6. 使用Nessus工具进行漏洞扫描win7系统（把系统的445端口打开再扫描） |
| 7. 使用hydra暴力破解win10的ssh密码 |
| 8. 使用cewl工具对任意网站进行字典生成，要求最小单词长度为6，深入链接层次为2 |
| 9. 使用windows的系统配置扫描 |
| 10. 使用lynis进行linux系统配置扫描 |

完成要求：必须有详细过程。

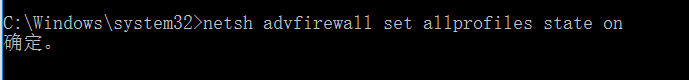
1. 使用nmap进行全连接扫描，要求：将20000端口禁用后指定端口扫描。

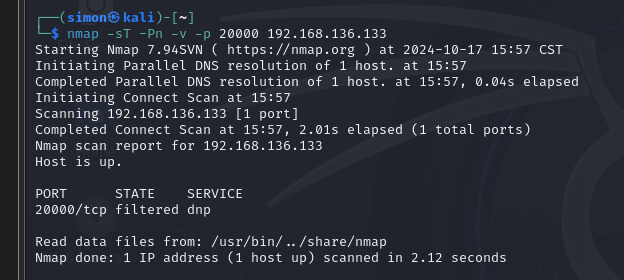
首先把win10防火墙关闭

然后使用kali对其进行全连接 查看20000端口 观察到端口关闭



此时重新打开防火墙 再次进行扫描可以看到其被过滤

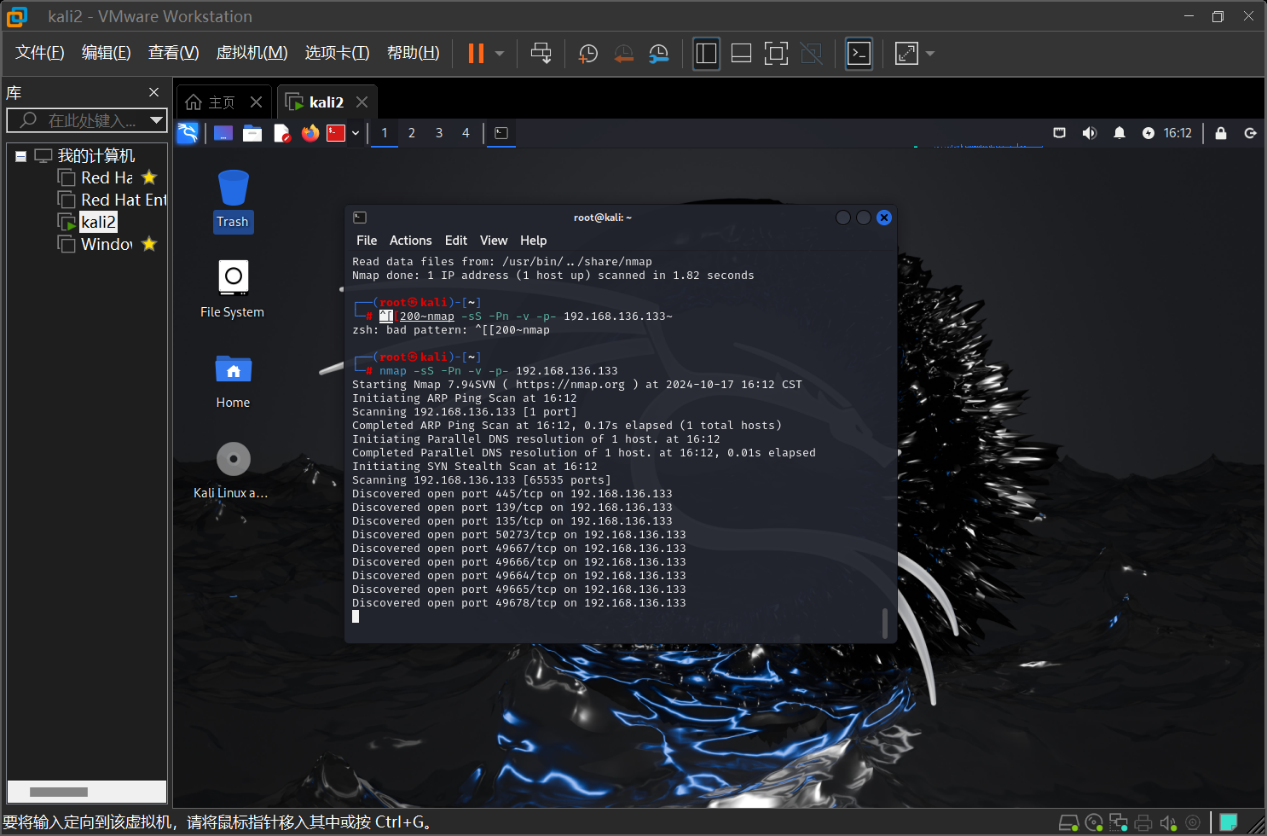


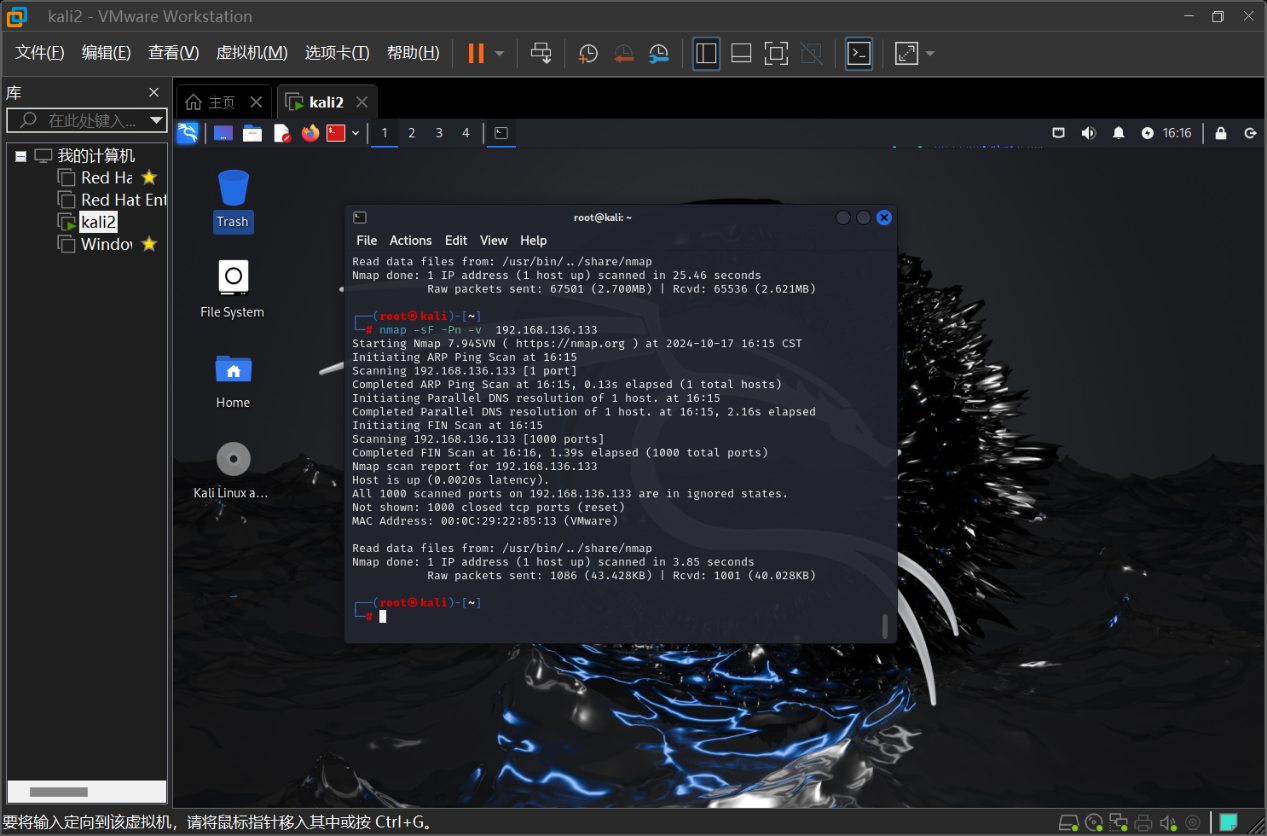


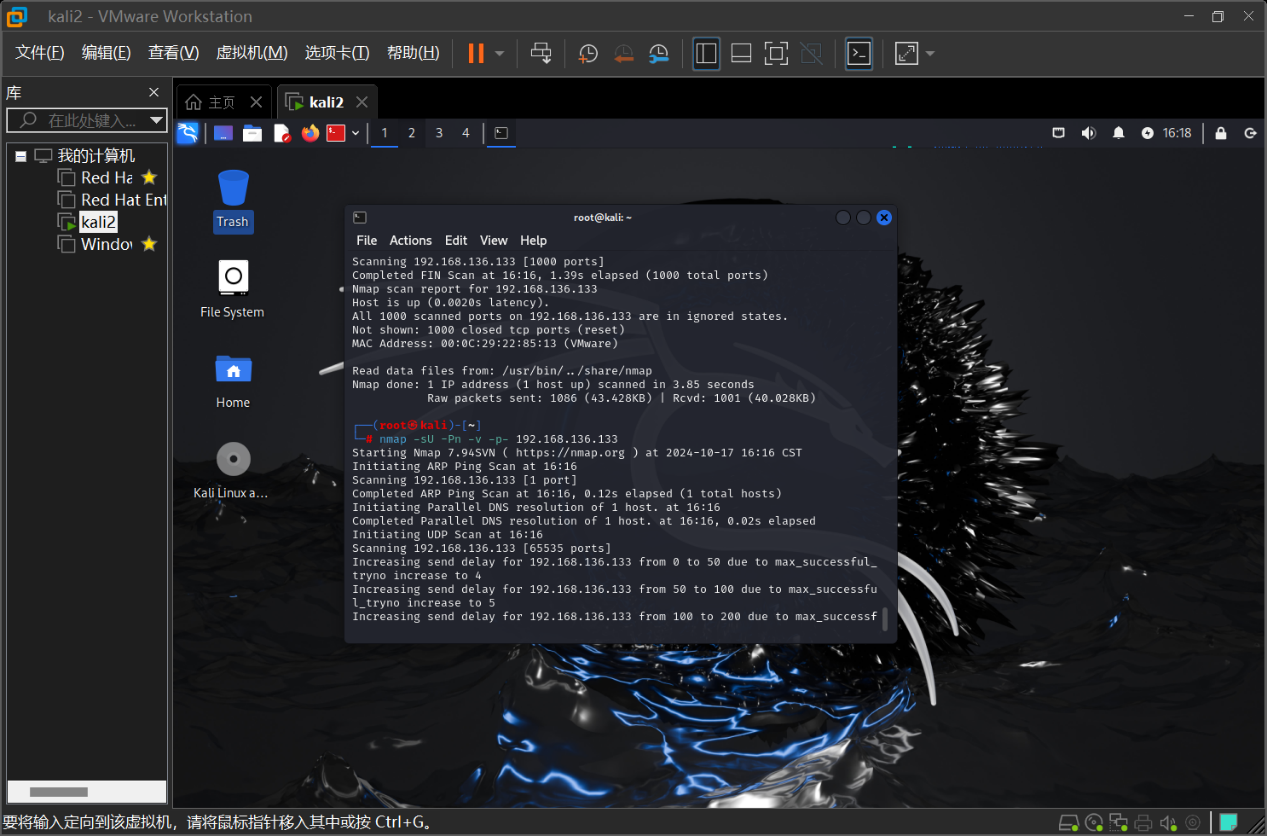
总结：可以通过设置防火墙的规则设置是否能通过的流量 前提是这端口要有服务进行 全连接很容易被过滤

1. 针对某个（可根据自己主机按需要扫描）开启的端口和关闭的端口，使用nmap进行半连接扫描、FIN扫描、UDP扫描，查看扫描结果反馈。

把防火墙关闭后

半连接扫描：

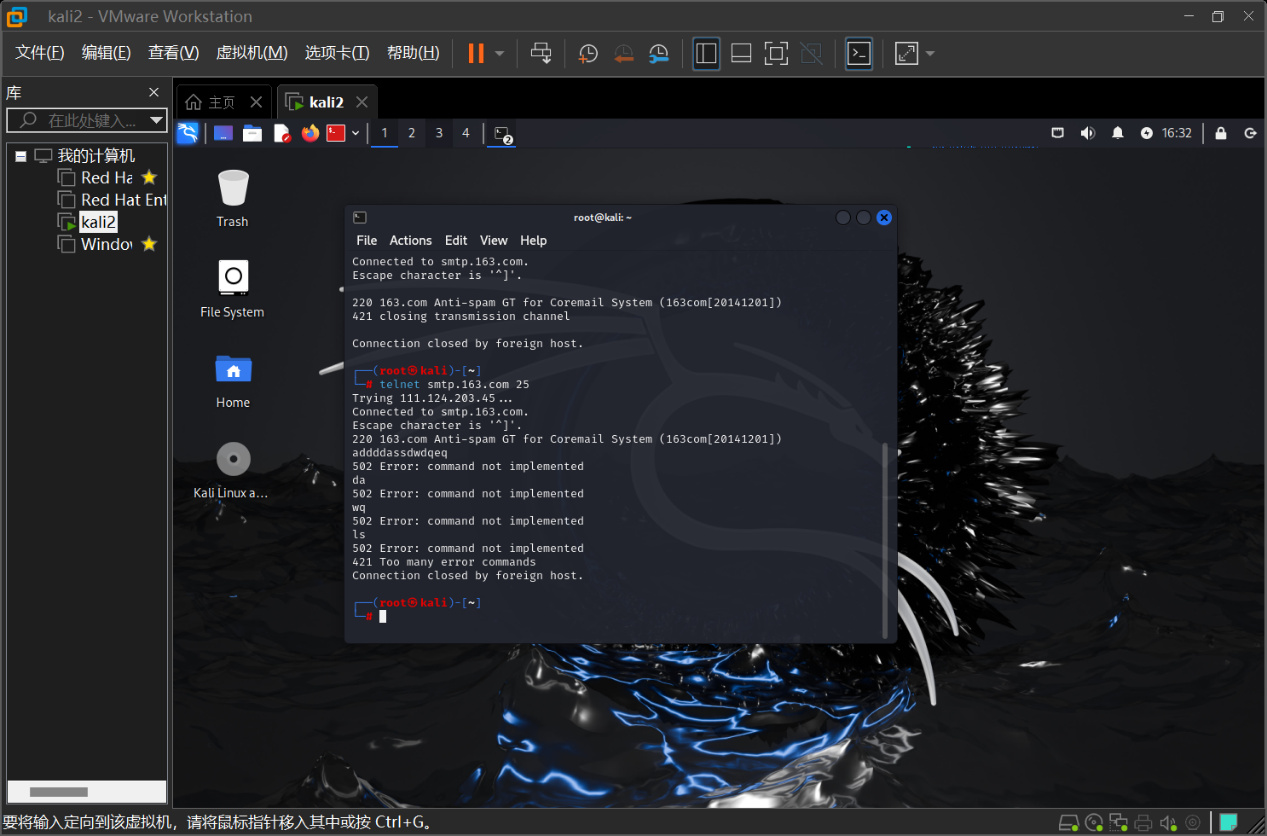
Fin扫描：

Udp扫描：

可以发现三个扫描结果不一样 说明不容的扫描方式不是一定适合同一个系统

1. 使用telnet命令对163邮箱服务器的SMTP和POP3服务进行扫描

首先连接163的smtp 通过百度可知道她的端口是25 进行连接

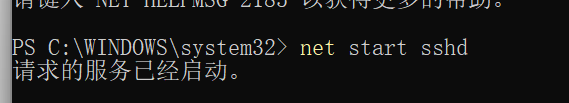


可以看到我们连接上了 但是因为错误命令太多和安全原因被断开连接

Pop3端口百度知道是110端口

可以看到连接成功 后面也是因为安全原因被断开连接

1. 开启windows系统的SSH服务，使用nmap对主机进行服务版本信息扫描

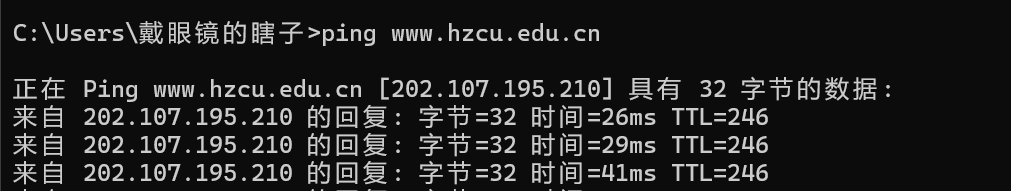


首先开启ssh服务



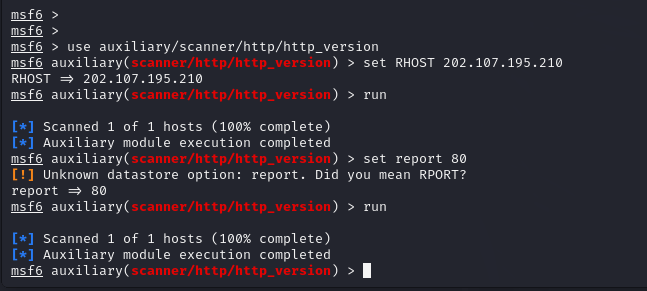
可以看到namp探查到端口22开启了ssh服务

1. 在kali上用metasploit中的http\_version和ssh\_version确定浙大城市学院服务器版本号和ssh服务器版本号

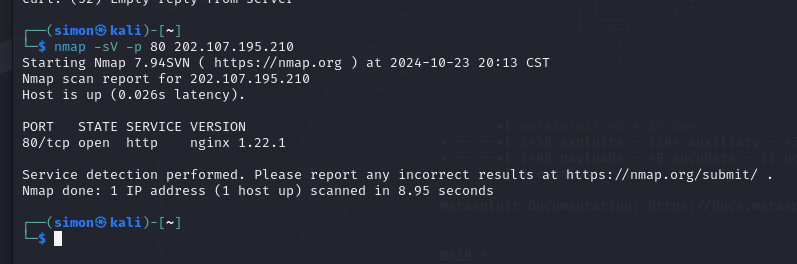


观察到对应的

看http版本



可以看到没有返回 可能是被屏蔽了

换用namp探查 

看得出服务器是nginx 版本1.22.1

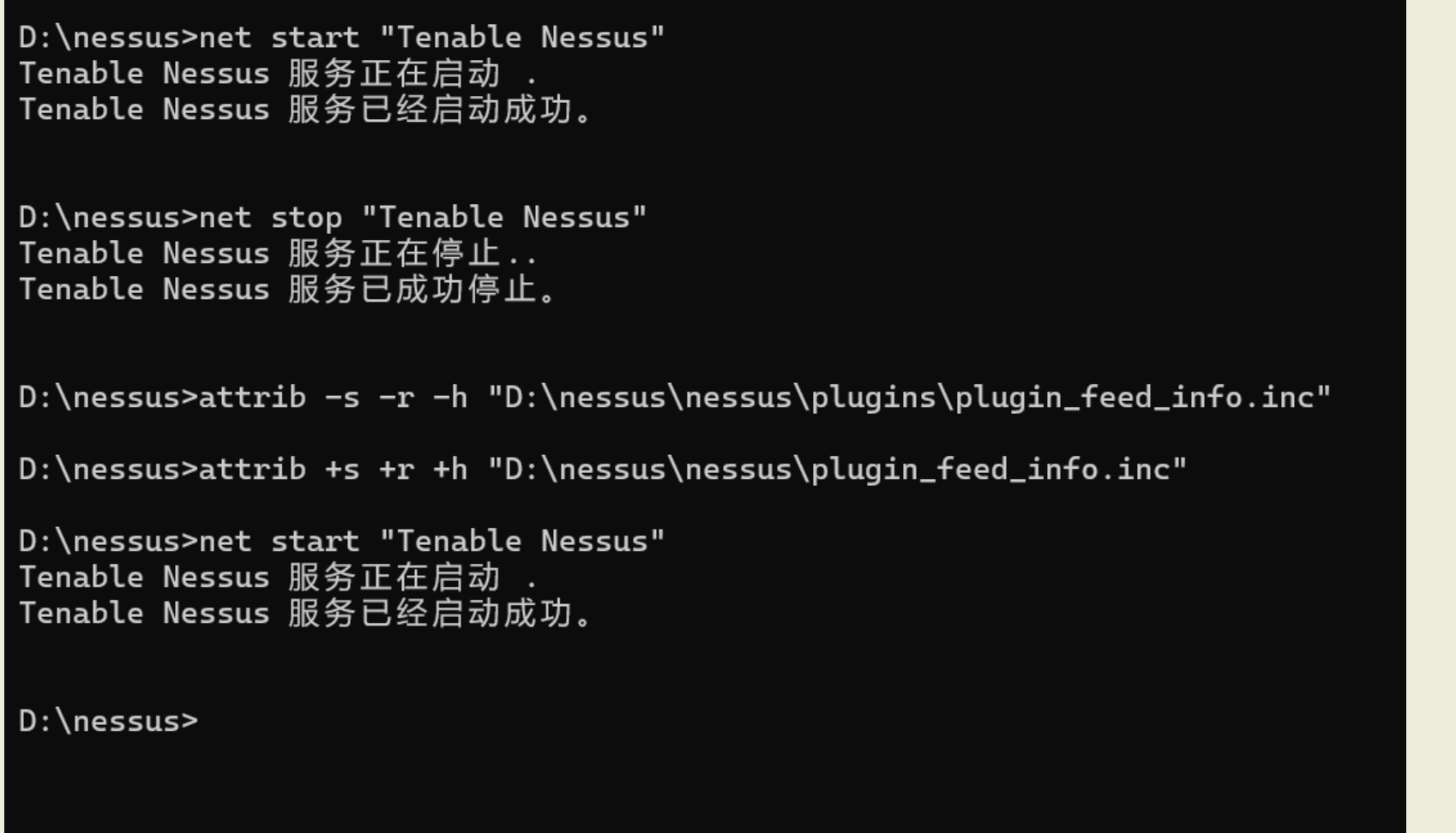
探查ssh版本号

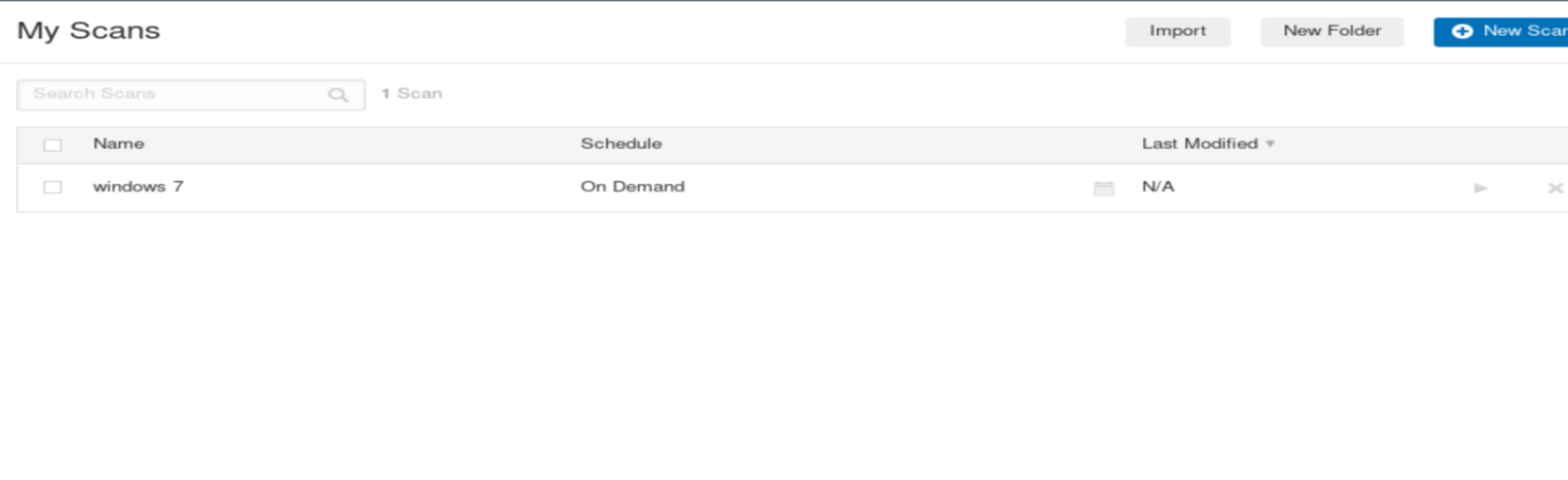


用Metasploit探查发现被拒绝 使用nmap发现也被过滤 最后mascan发现未开放22ssh端口

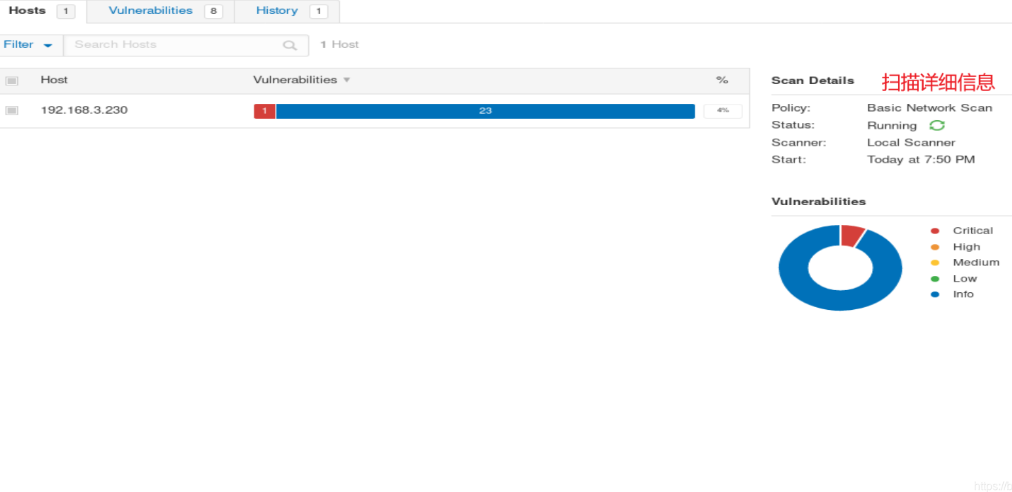
1. 使用Nessus工具进行漏洞扫描win7系统（把系统的445端口打开再扫描）

先开启服务

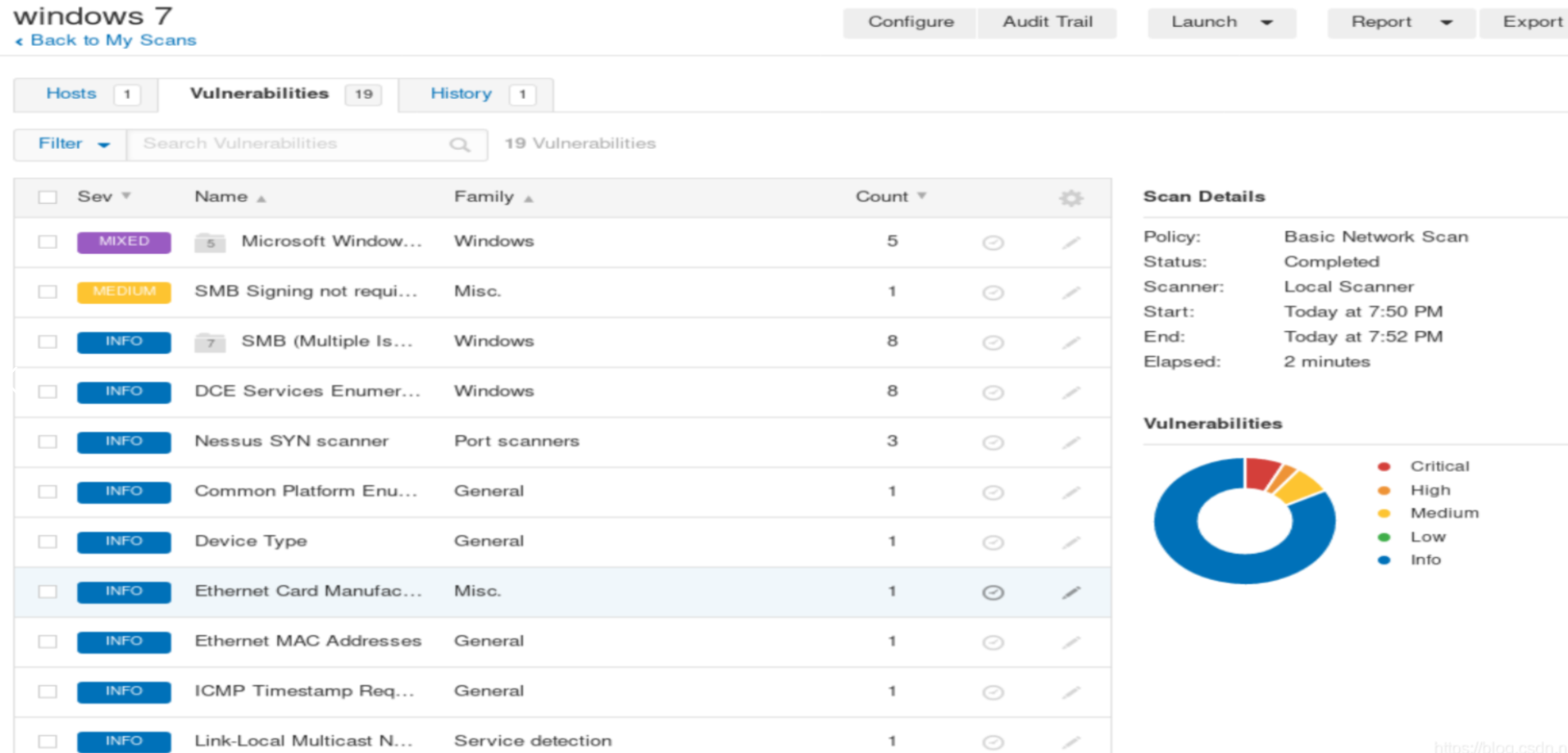


然后新建扫描windows7

对其进行扫描

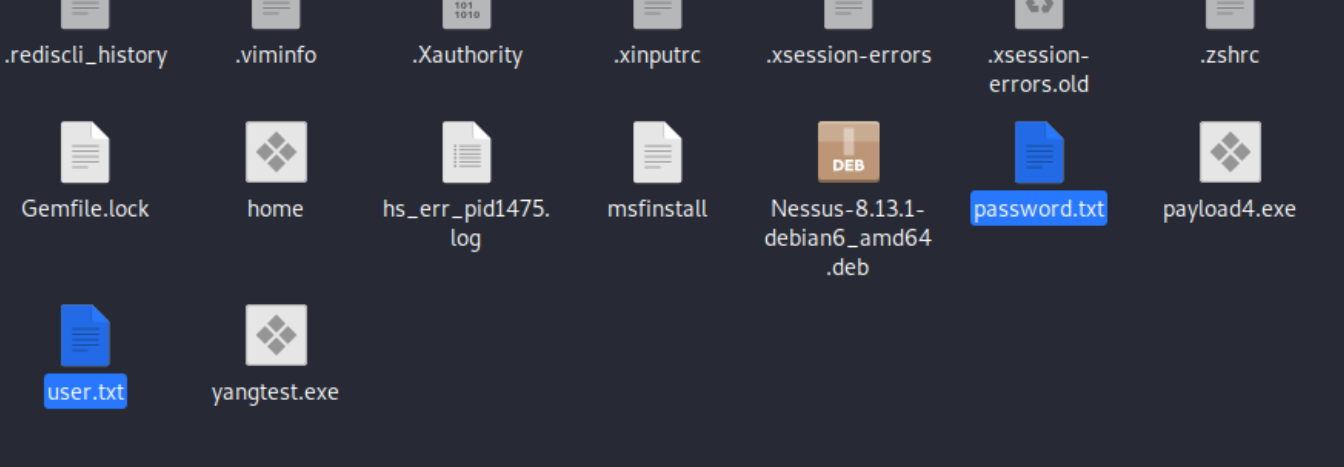


下面是发现的漏洞

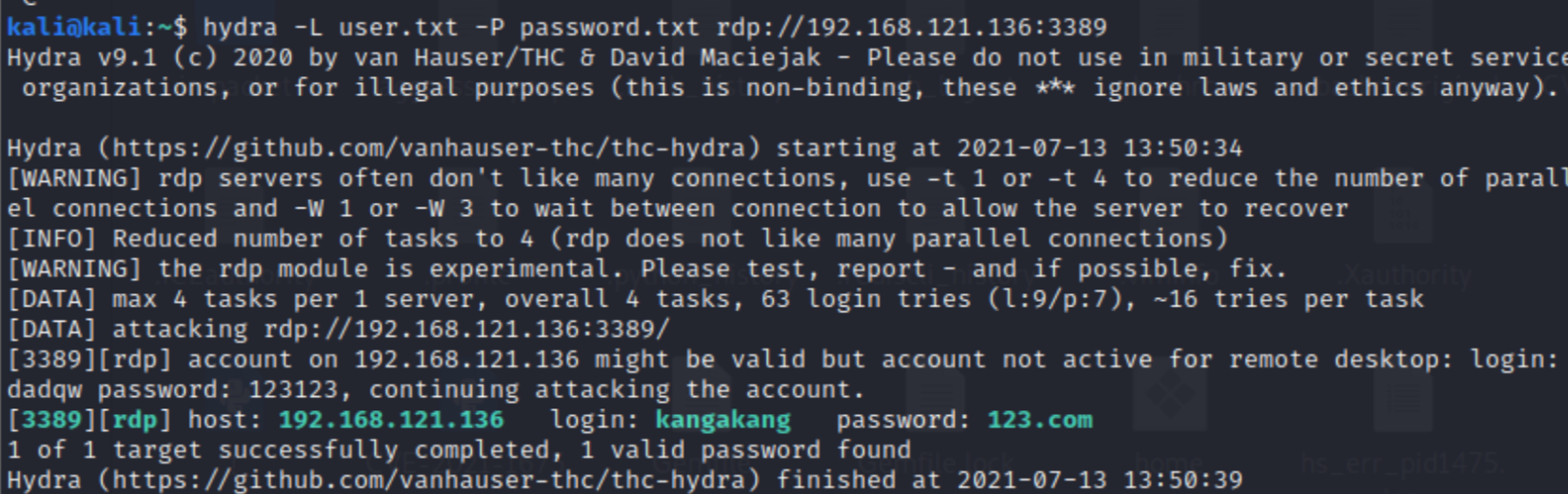


1. 使用hydra暴力破解win10的ssh密码

先设置账户和密码本



采用命令hydra -L user.txt -P password.txt rdp://192.168.121.136:3389执行



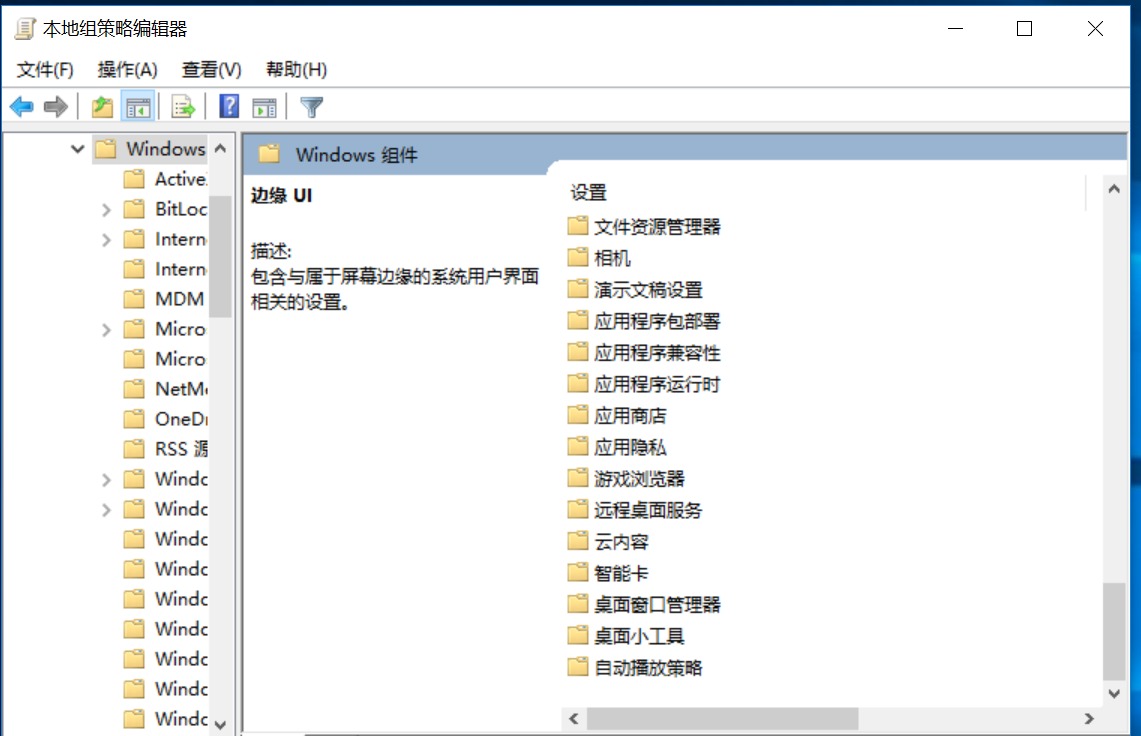
结果显示：192.168.121.136的账号密码为kangakang:[http://123.com](https://link.zhihu.com/?target=http://123.com" \t "https://zhuanlan.zhihu.com/p/_blank)

1. 使用cewl工具对任意网站进行字典生成，要求最小单词长度为6，深入链接层次为2

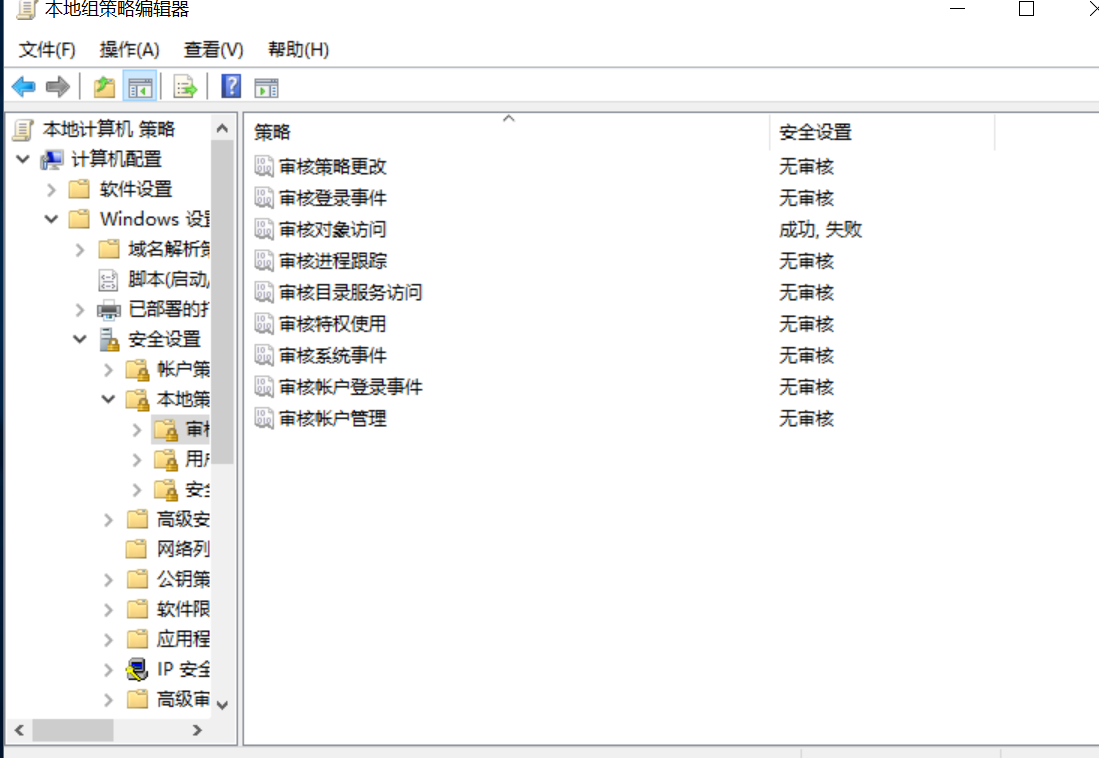
cewl -w output.txt -m 6 -d 2 <https://www.baidu.com>

先尝试学校网站发现被拒绝连接 然后尝试baidu但没登录界面所以没用任何返回 最后尝试ppt中的网站可以得到结果

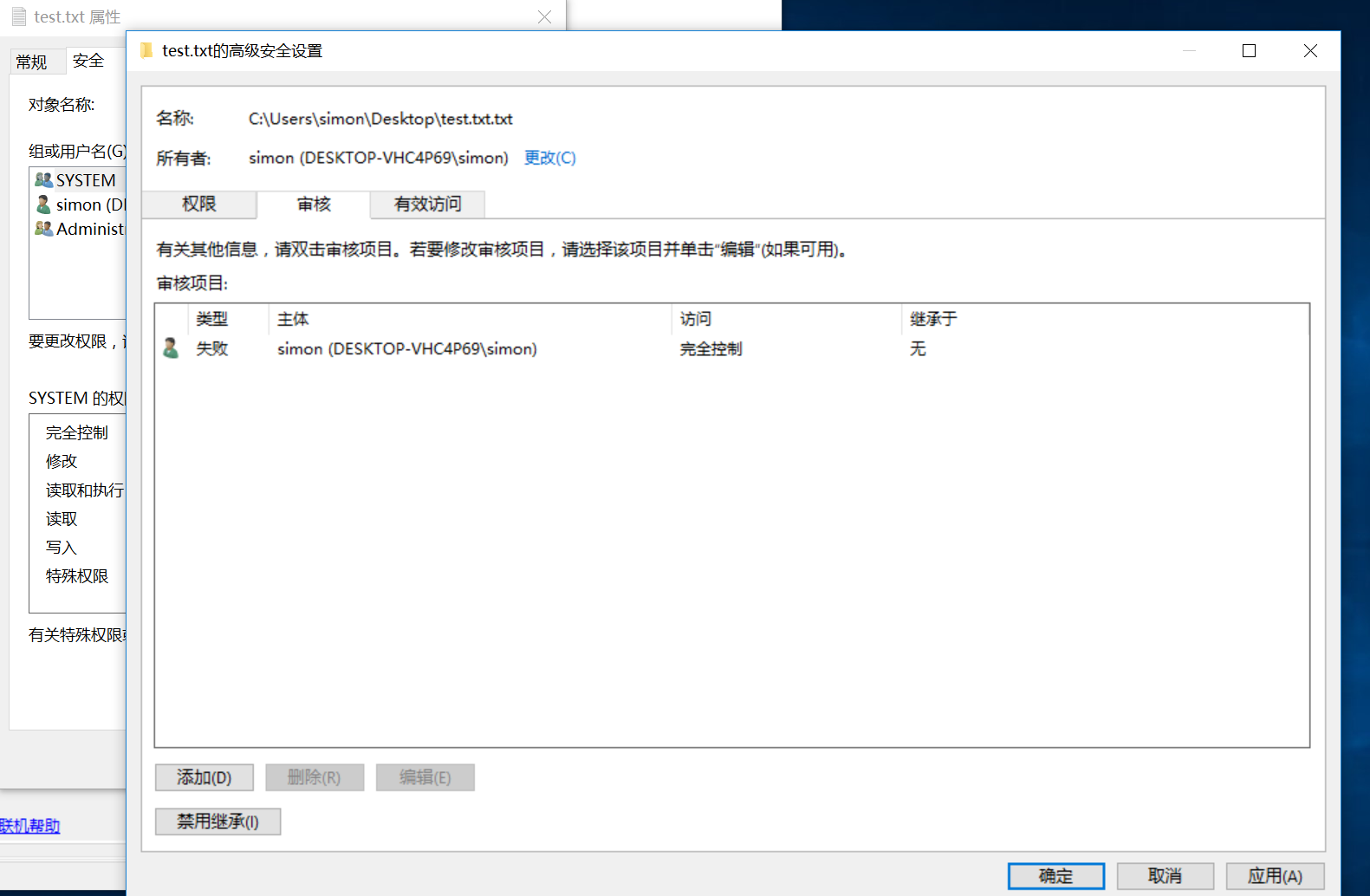
1. 使用windows的系统配置扫描



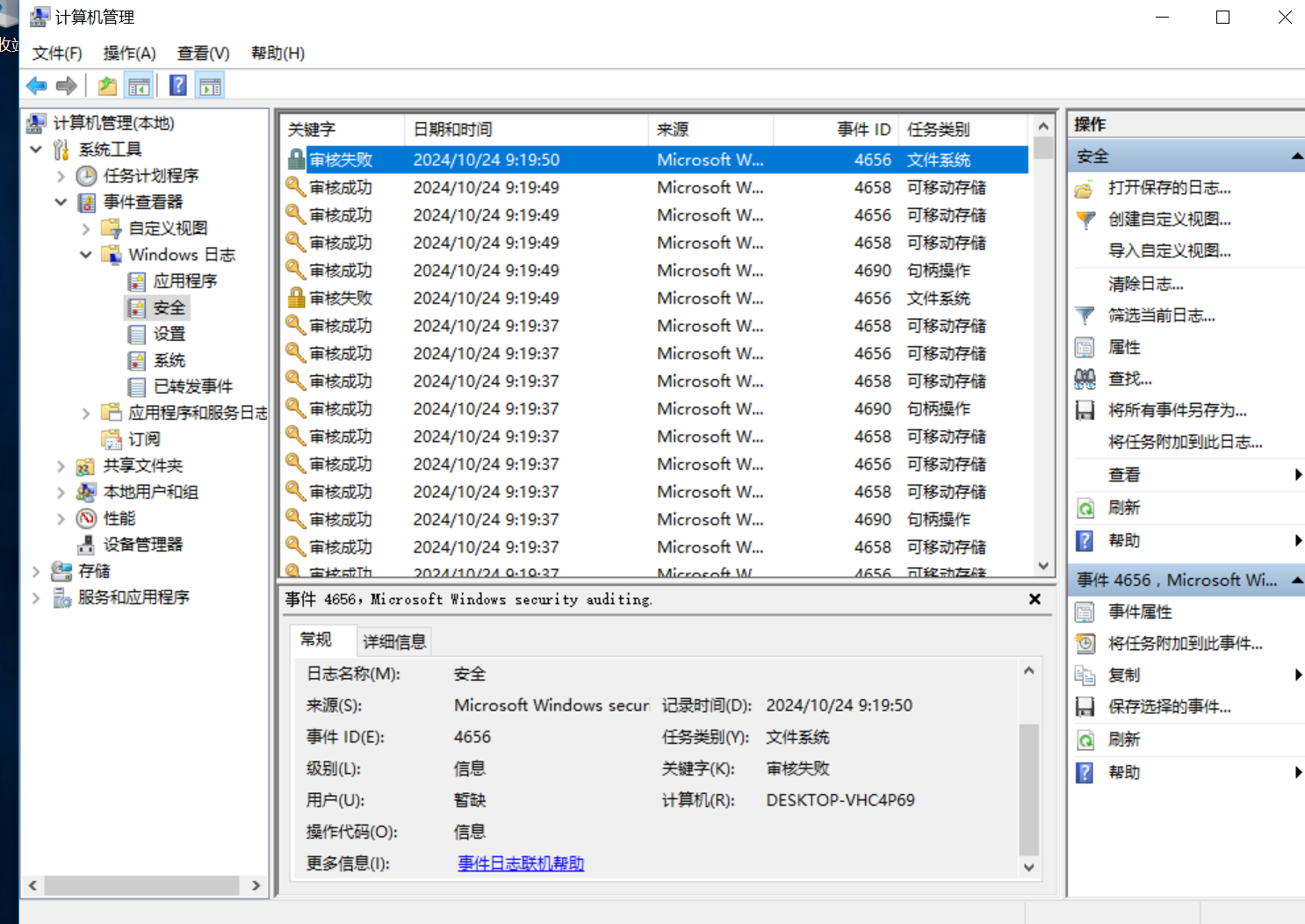
通过gpedit.msc进入 开启策略编辑



进入安全审核 修改审核对象访问

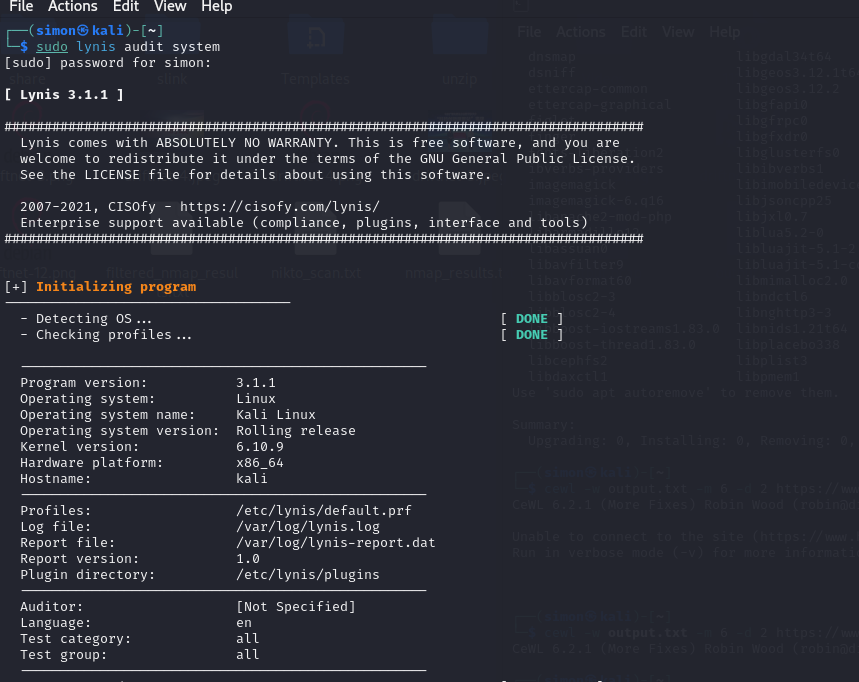


设置文件的审核用户 状态设置为失败

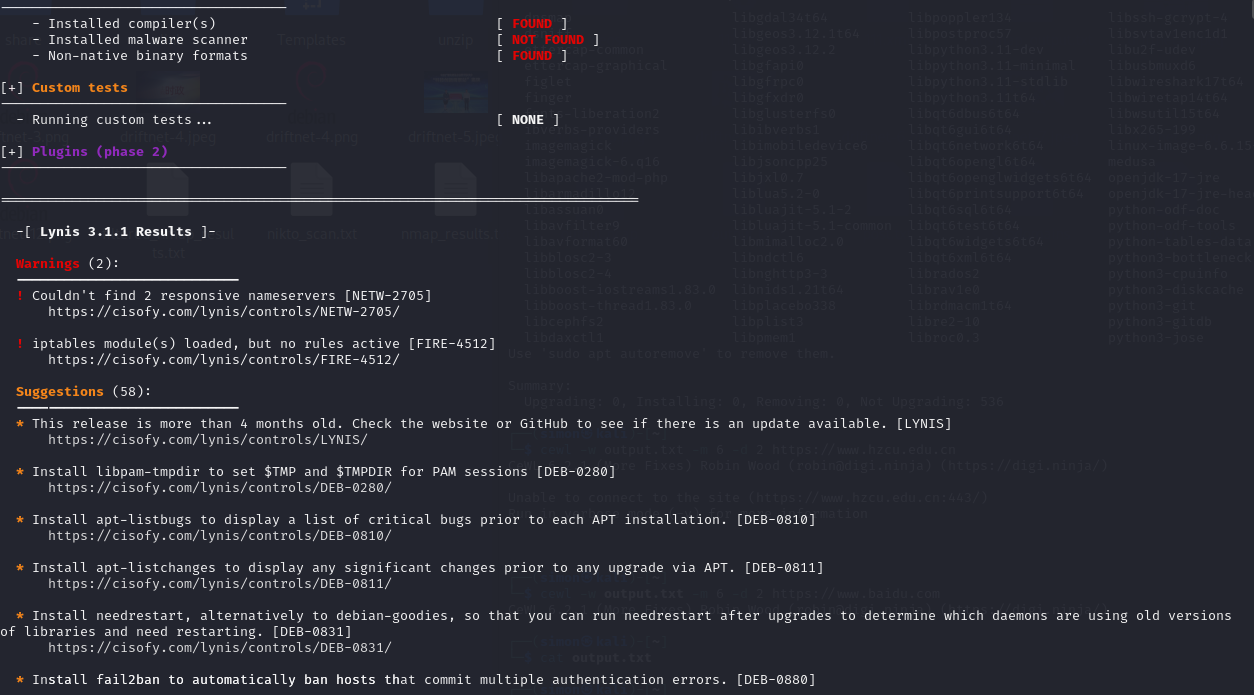
可以在安全日志中看到

安全状态是审核失败

10. 使用lynis进行linux系统配置扫描



首先进行扫描



可以看到我们生成一个简要的结果

然后进入 /var/log/lynis.log

查看详细结果

