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 11 月 13 日

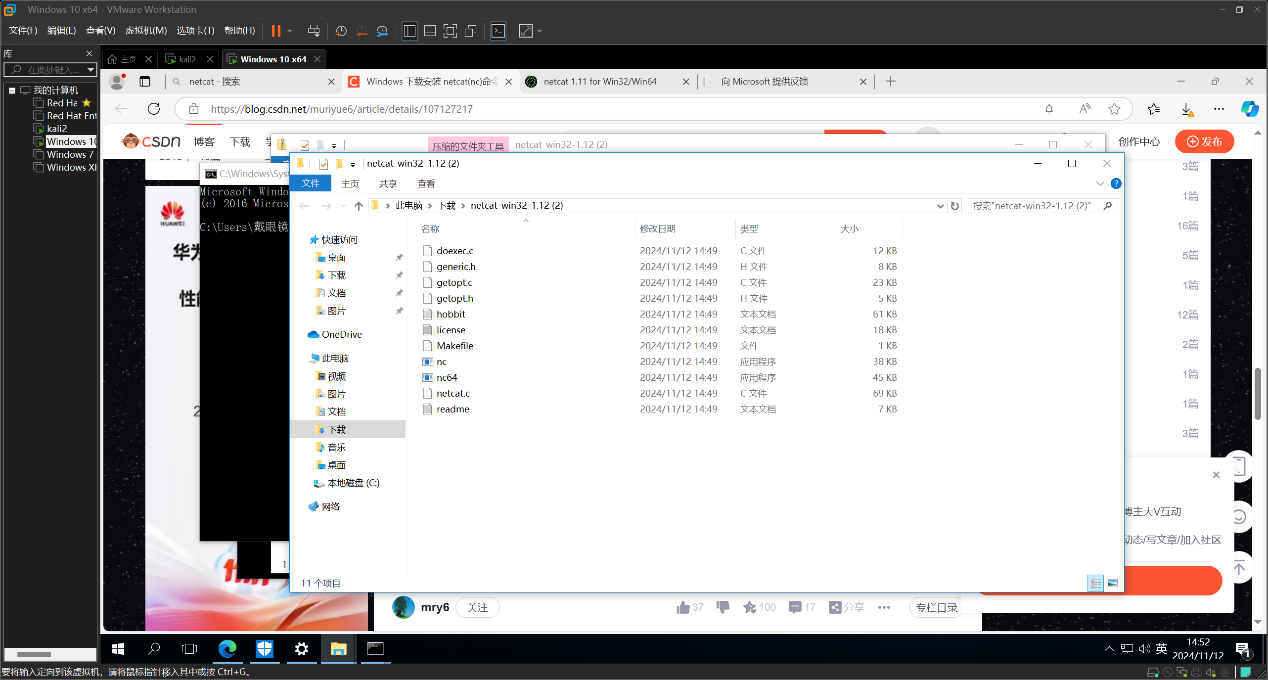
**课程实验报告清单**

|  |
| --- |
| 目录 |
| 1. 使用netcat完成主动连接和反向连接 |
| 2. 在win系统上，通过修改注册表方式增加一项开机启动项，并重启验证是否生效。 |
| 3. 在kali系统上，通过修改.profile文件增加一项开机启动项 |
| 4. 使用Meterpreter创建网络后门，并修改注册表和创建管理员账户 |
| 5. 通过wevtutil工具清除win系统的系统日志， |
| 6. 用vim查看log日志，并用logtamper修改wtmp日志 |

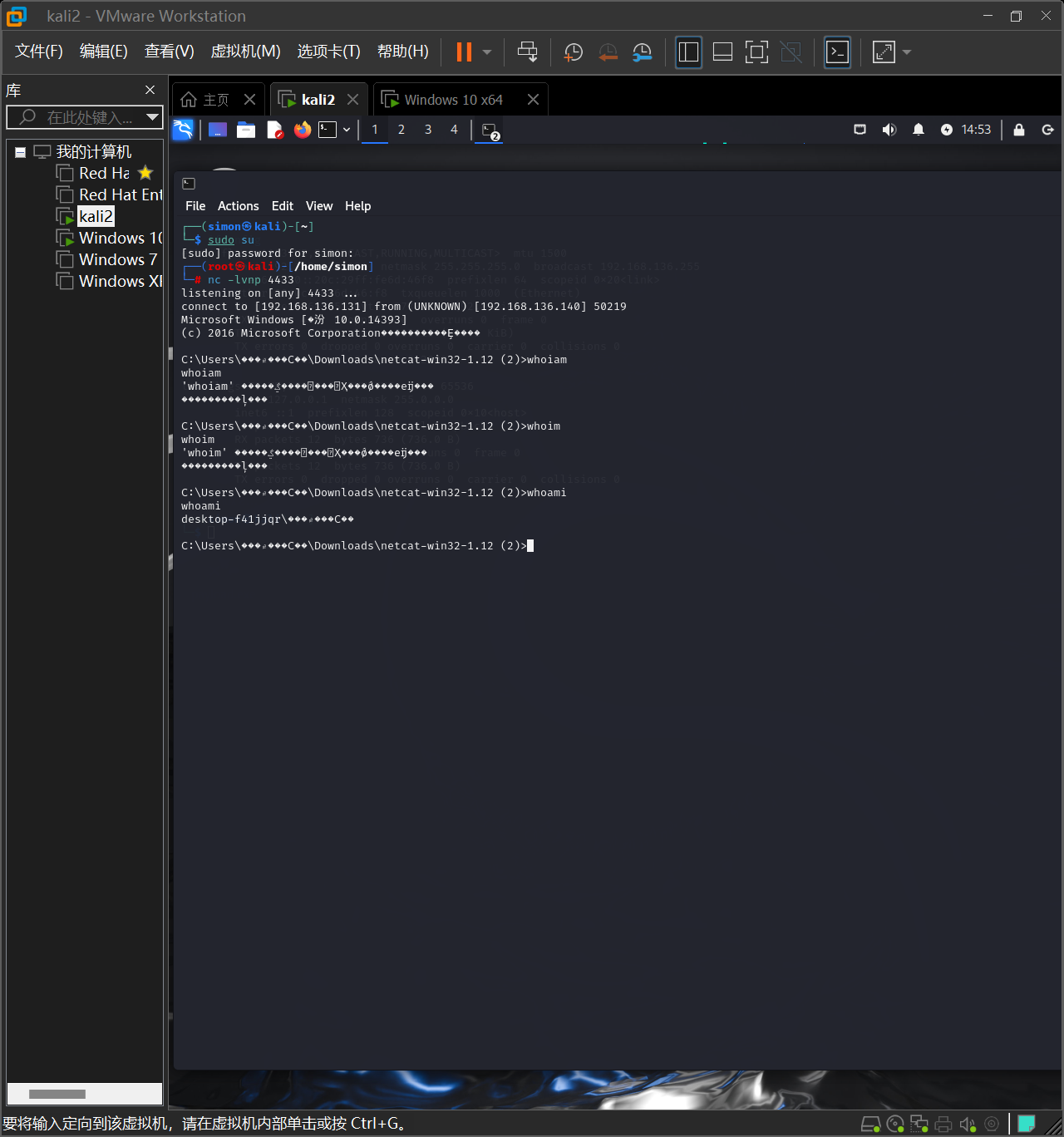
完成要求：必须有详细过程。

1. 使用netcat完成主动连接和反向连接

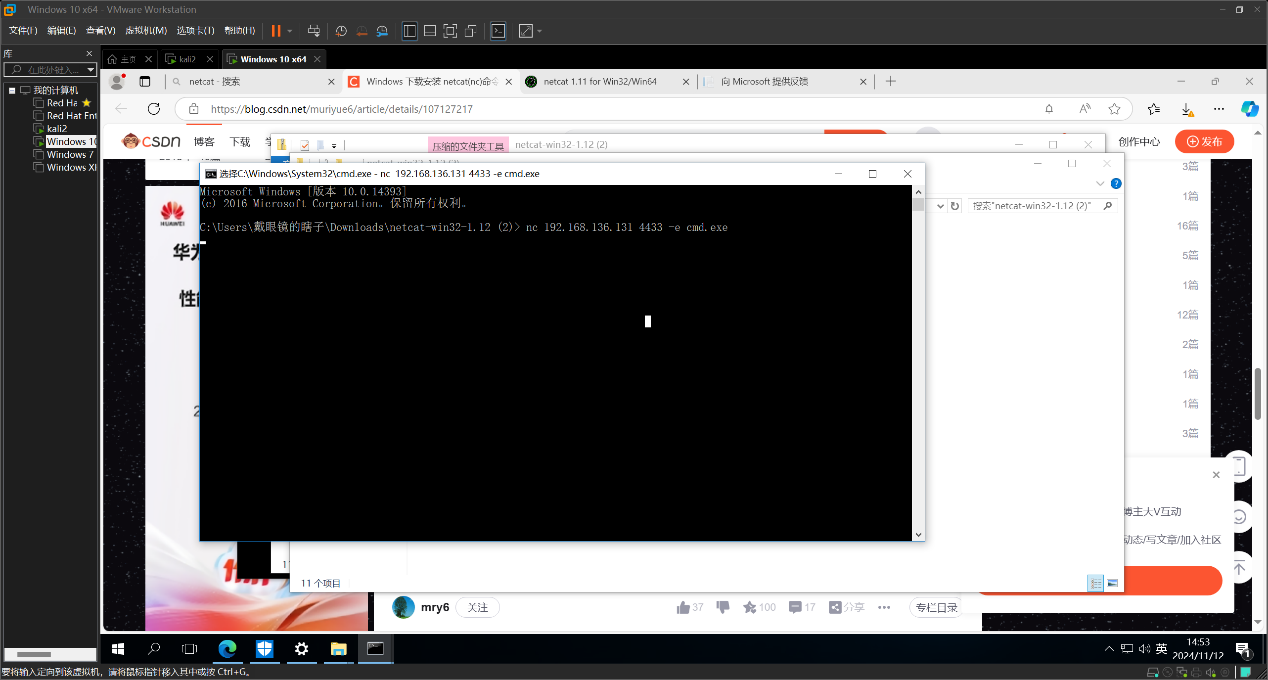
在win10下载netcat



在kali检测4433端口

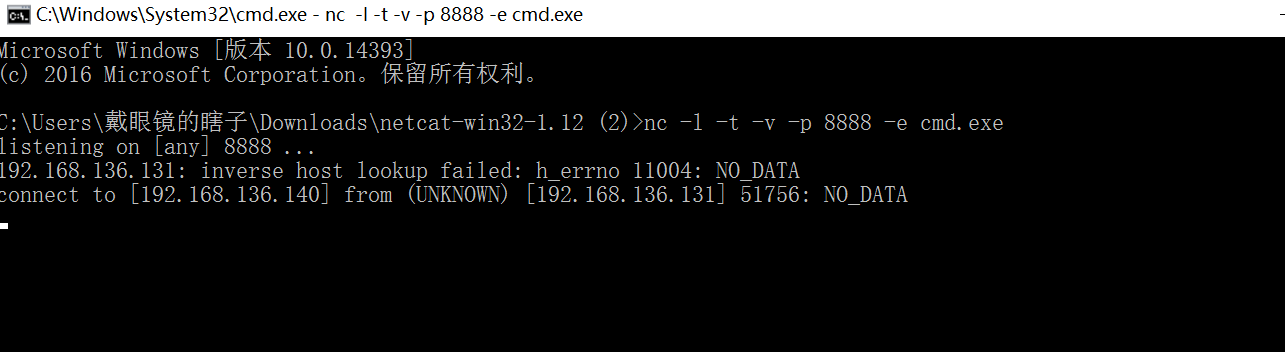


在win连接 之后再kali连接成功

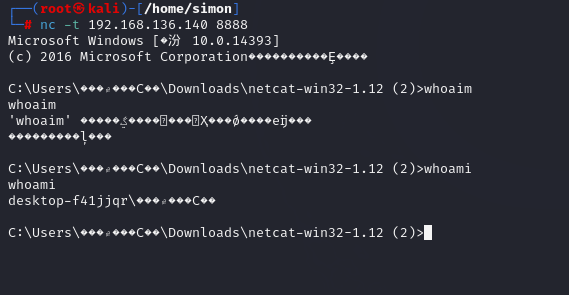


正向连接：

Win10开启端口

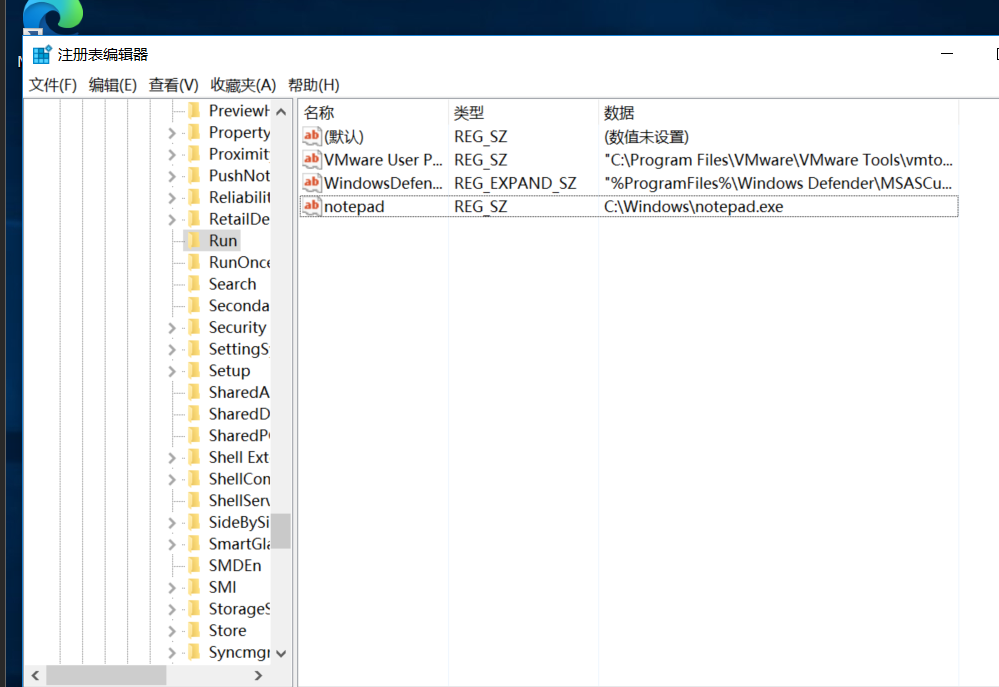


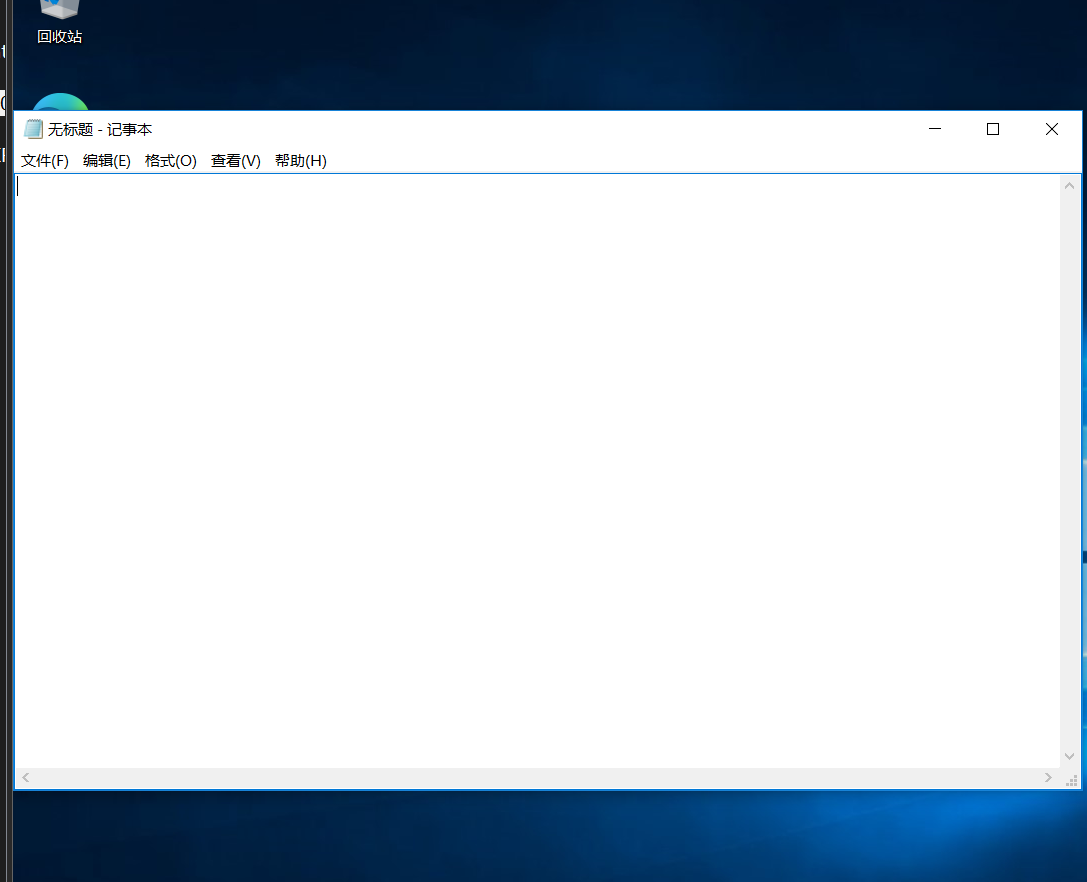
Kali直接连接就好



1. 在win系统上，通过修改注册表方式增加一项开机启动项，并重启验证是否生效。

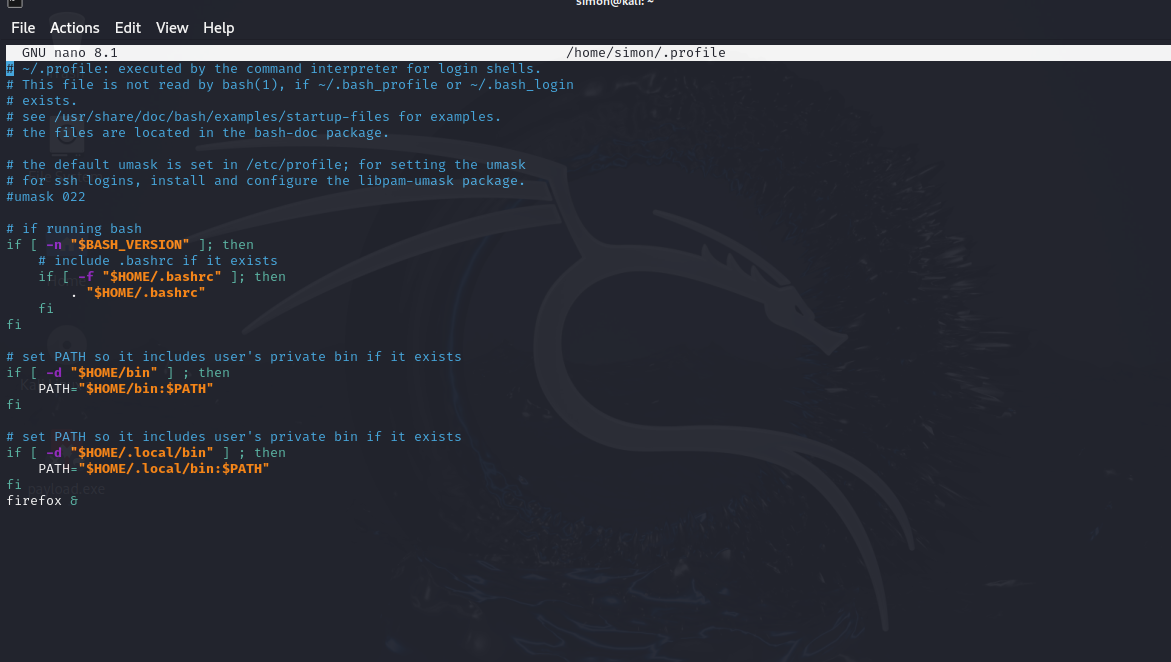
先进入特定路径



开机后可以看到自动打开 但响应很慢

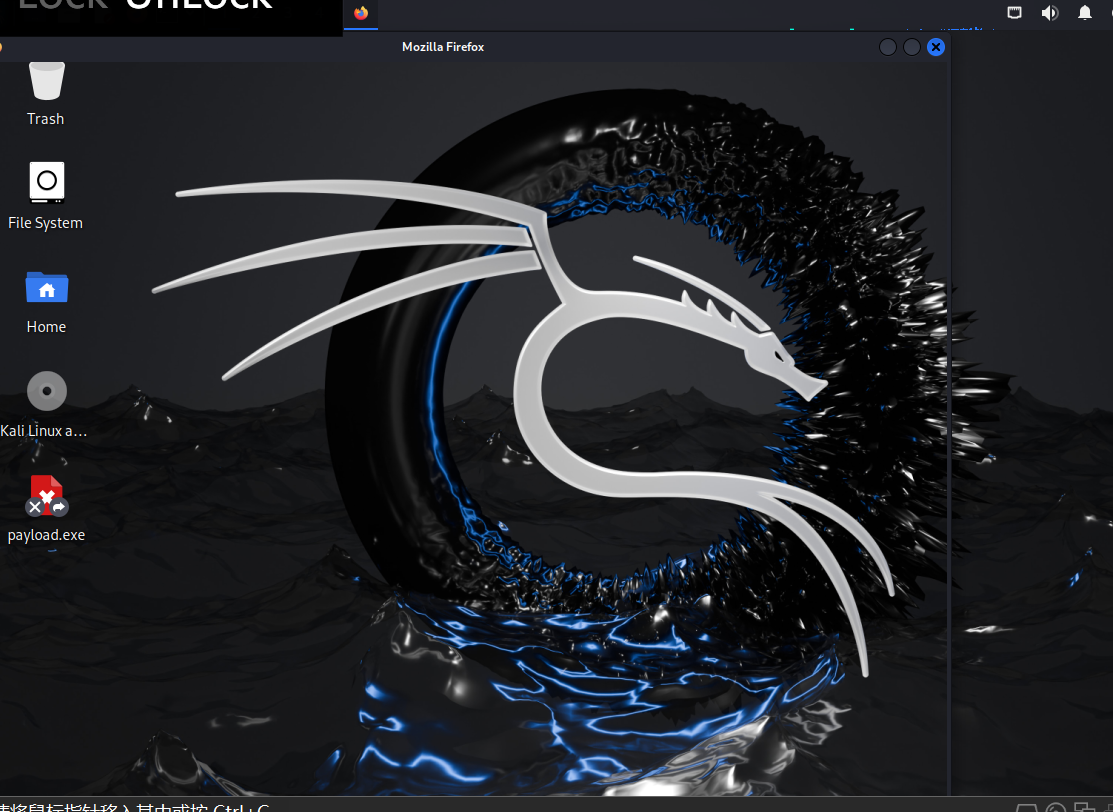
1. 在kali系统上，通过修改.profile文件增加一项开机启动项

进入修改 添加浏览器



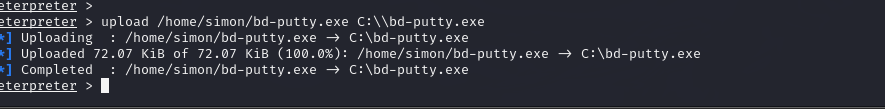
重启查看

看得到启动了浏览器 但是反应很慢 依旧在加载



1. 使用Meterpreter创建网络后门，并修改注册表和创建管理员账户

在上节课基础上连接到win7之后

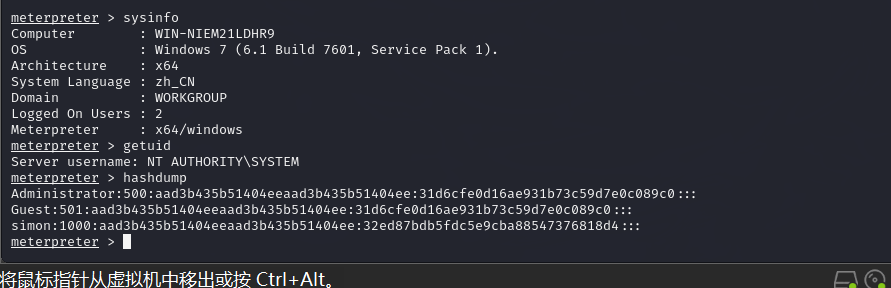


上传恶意代码到靶机

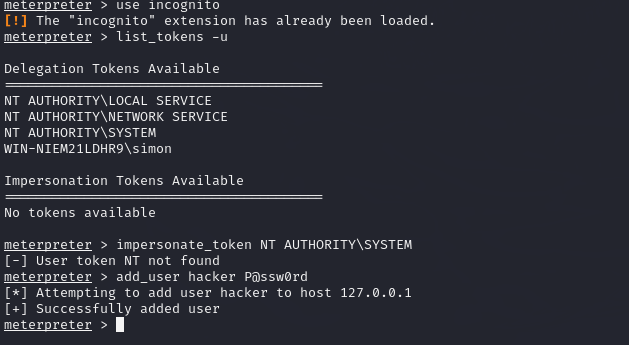
就是已经上传了后门

接下来可以通过修改注册表来设置长久后门\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*



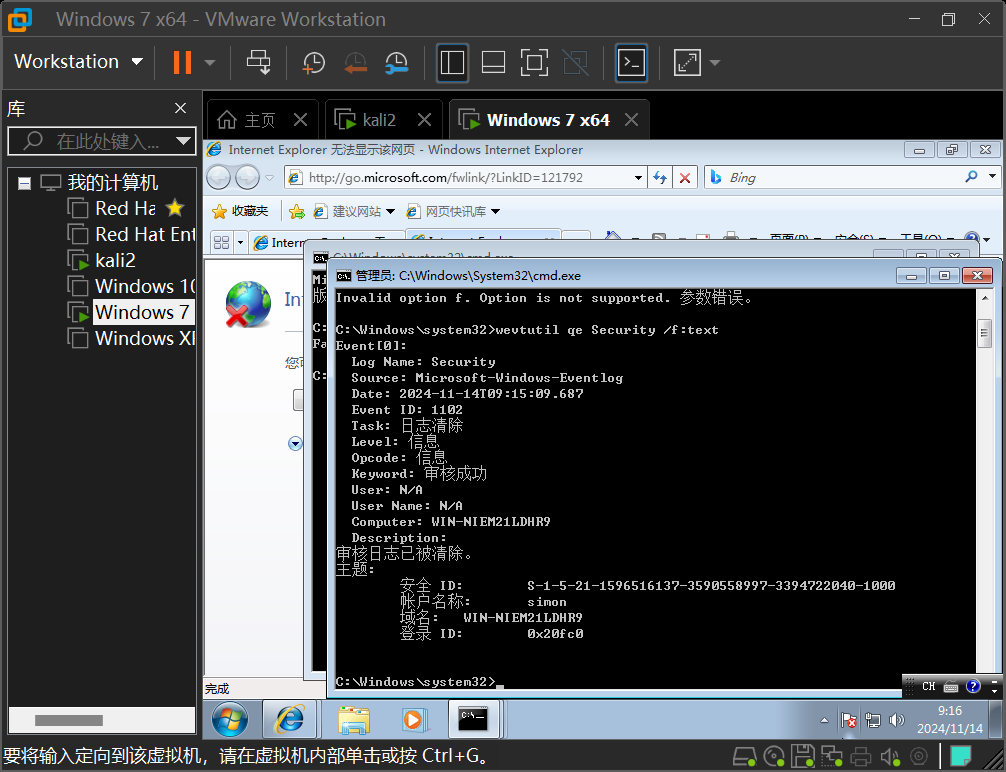
查看哈希密码

添加用户



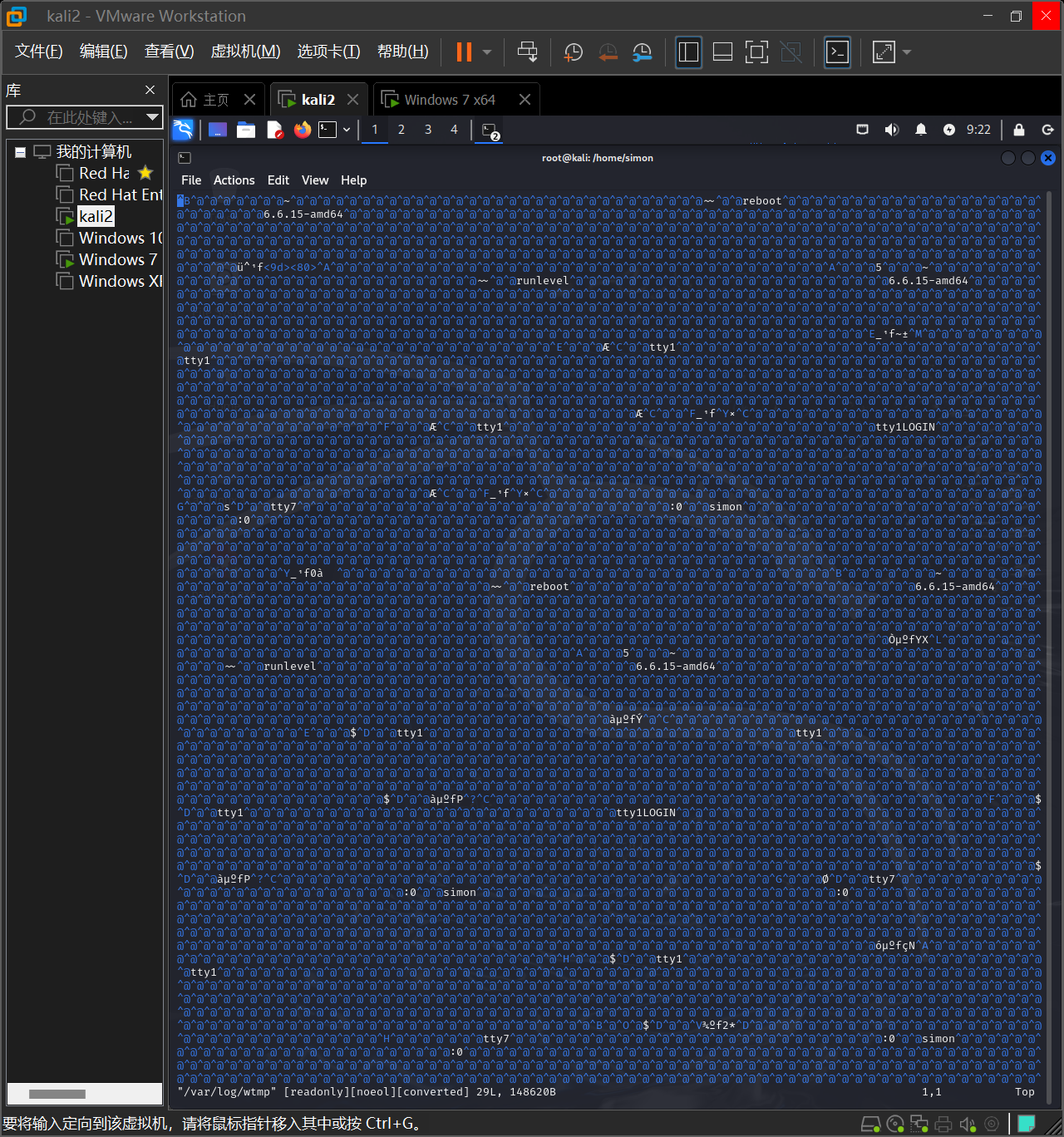
1. 通过wevtutil工具清除win系统的系统日志，

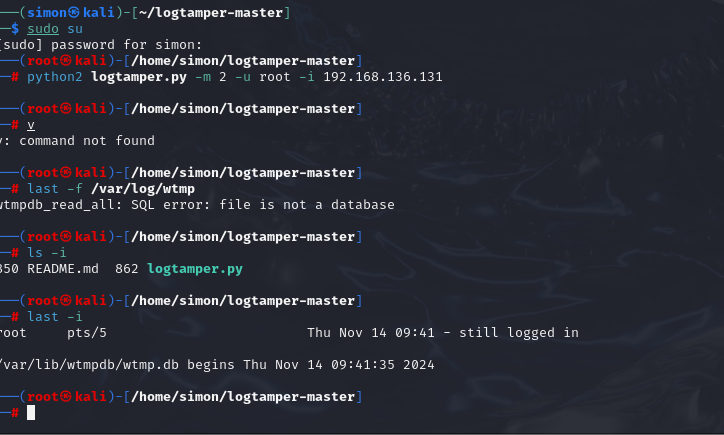
管理员登录cmd

直接运行命令就好

1. 用vim查看log日志，并用logtamper修改wtmp日志

使用vim /var/log/wtmp之后





看得日志