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

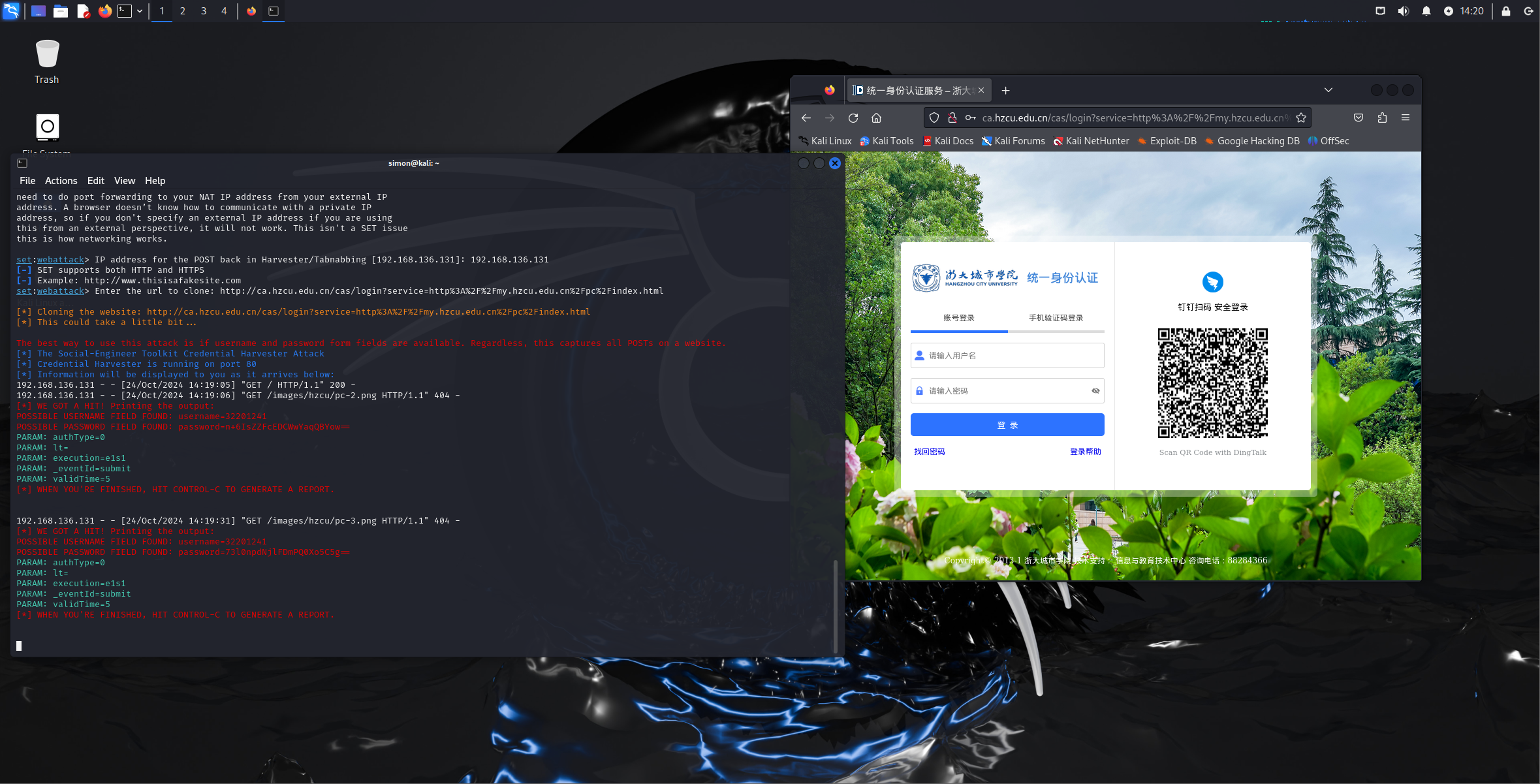
实验报告日期： 2024 年 10 月 24 日

**课程实验报告清单**

|  |
| --- |
| 目录 |
| 1. 使用SET工具制作钓鱼网站，并在后台捕捉用户名和密码。 |
| 2. 使用John the ripper破解linux的口令信息 |
| 3. 使用hashcat破解基于NTLM hash生成的windows用户密码 |
| 4. 使用RainbowCrack进行彩虹表破解下面提供的加密内容，彩虹表生成可以提供下面参数（小写字母和数字，4位，sha1算法）  （062c648aaf68174757c50ab1aeebb61e059c1d1b） |
| 5. 使用Ettercap实现DNS欺骗 |
| 6. 使用BP实现Web欺骗，网页修改成功并发送到浏览器显示出来 |

完成要求：必须有详细过程。

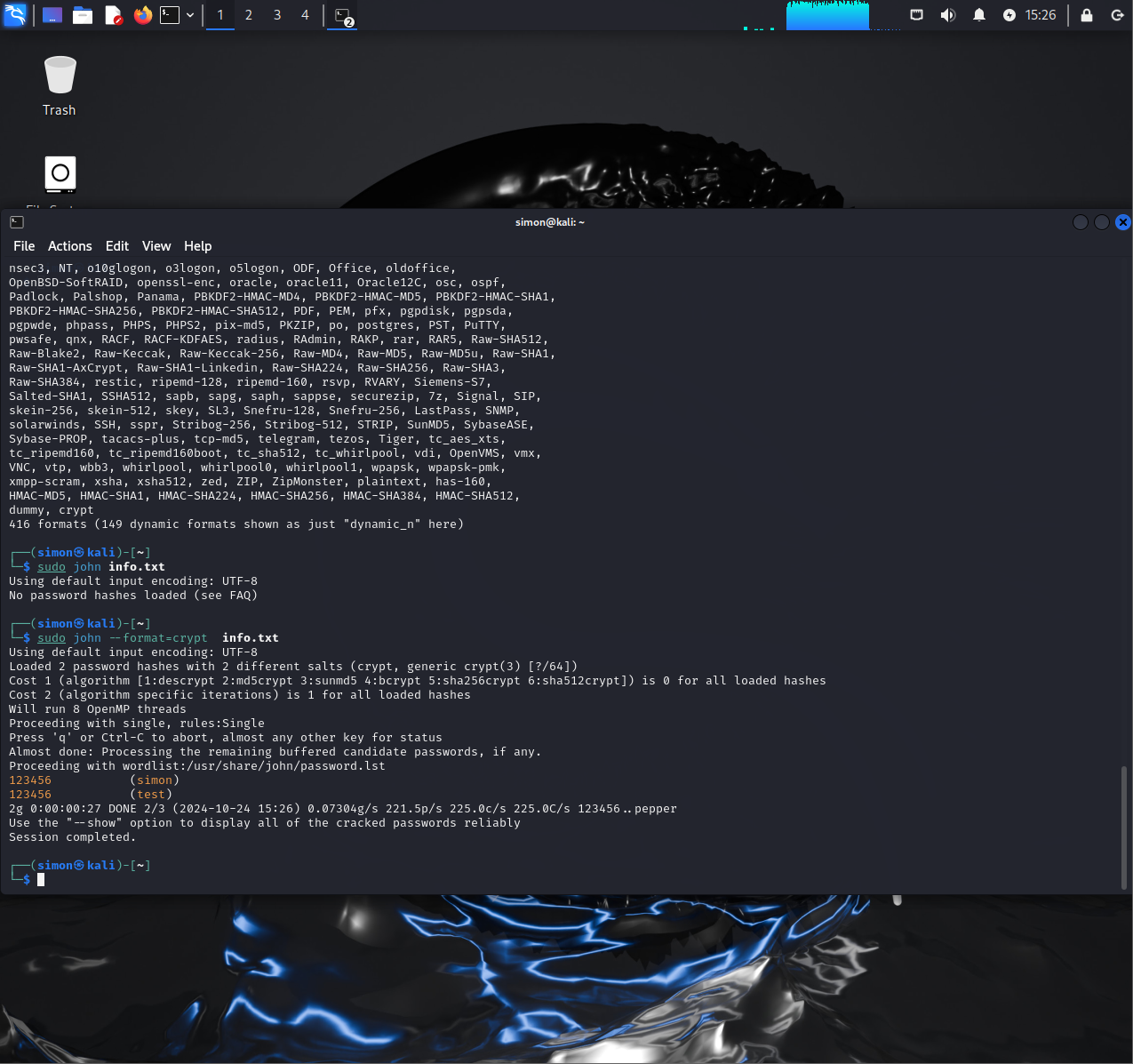
1. 使用SET工具制作钓鱼网站，并在后台捕捉用户名和密码。



设置的目标ip是kali 用kali尝试发现成功

换ip尝试本机

1. 使用John the ripper破解linux的口令信息



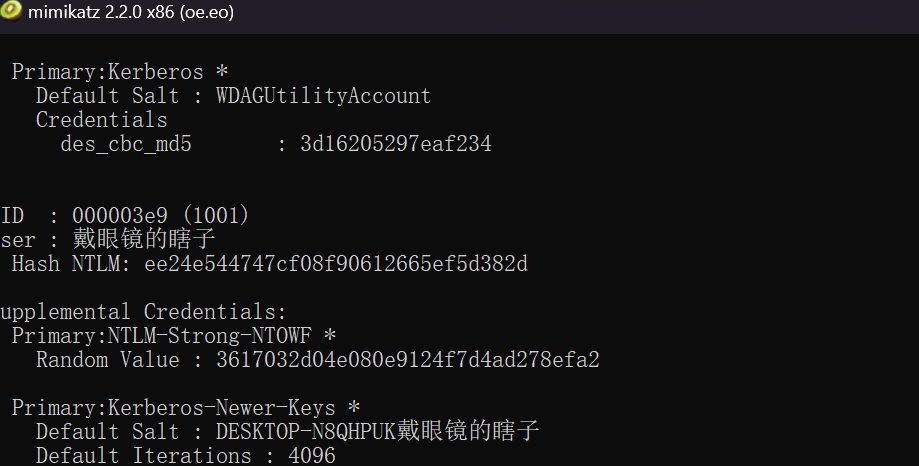
把用户的信息shadow导入到info里面 查看后发现密码被加密

询问ai知道这种加密方式是crypt

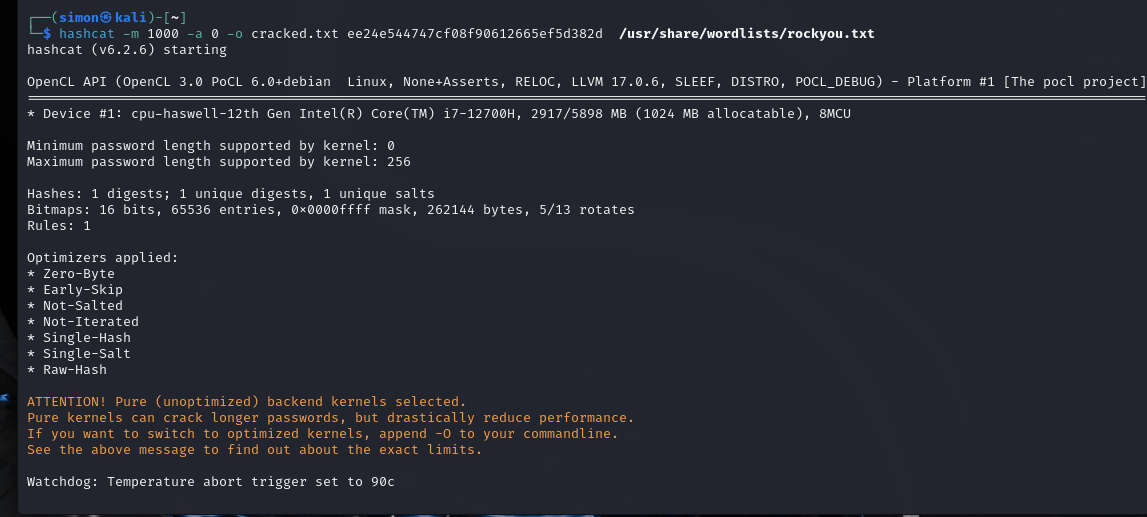
然后用john来解密

1. 使用hashcat破解基于NTLM hash生成的windows用户密码

先用mimikaze得到windows的密码的ntlm



然后进入kali使用hashcat对这个进行破译

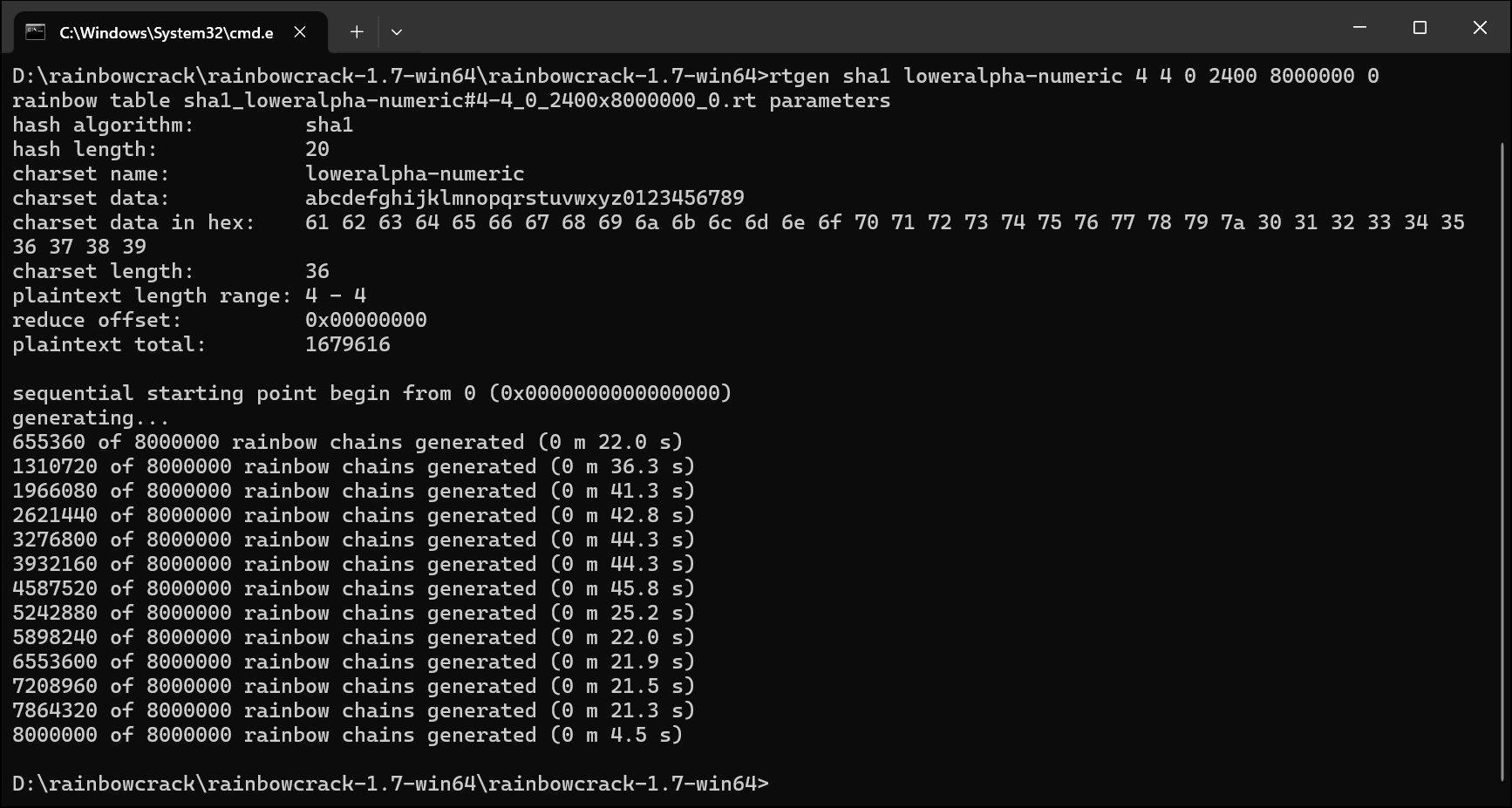


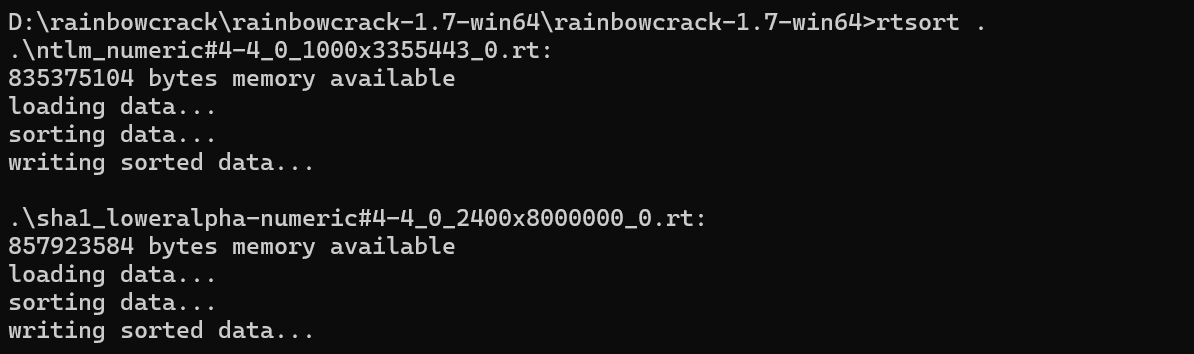
但我的密码本太小这里无法破译出来 更换更大密码本即可

4. 使用RainbowCrack进行彩虹表破解下面提供的加密内容，彩虹表生成可以提供下面参数（小写字母和数字，4位，sha1算法）

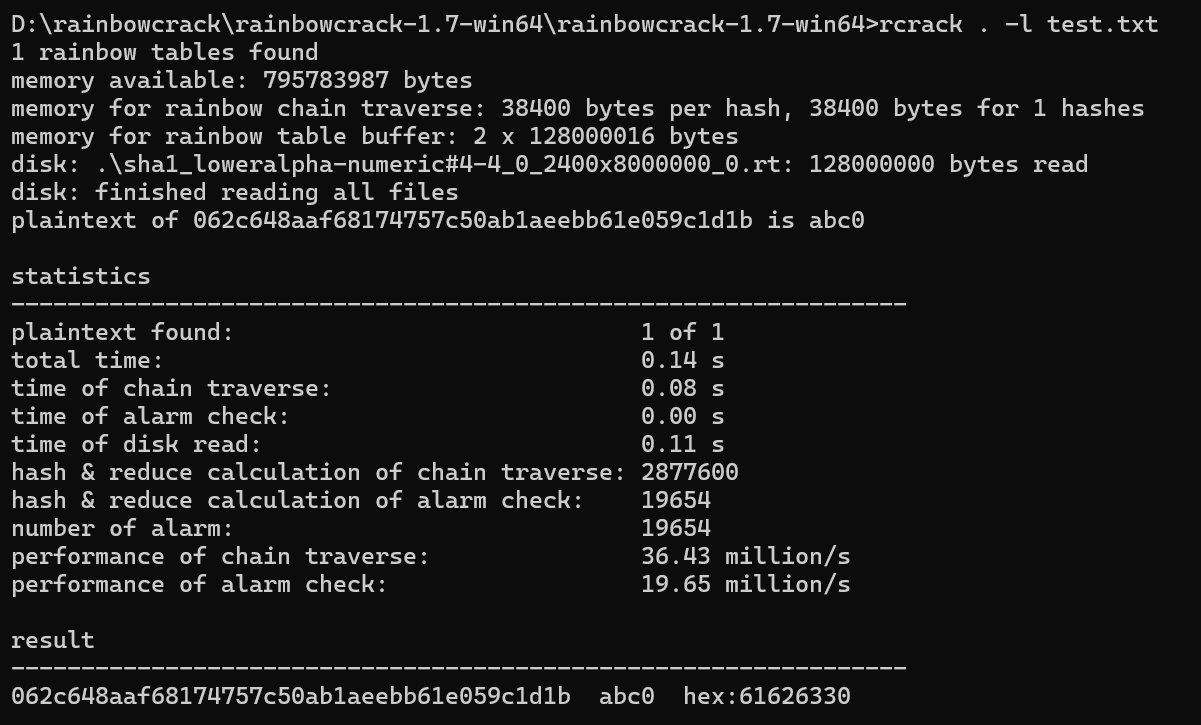
（062c648aaf68174757c50ab1aeebb61e059c1d1b）

先生成彩虹表

排序

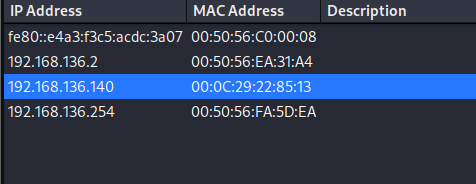


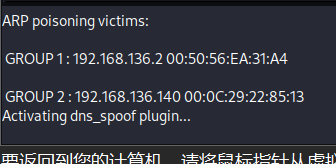
破译



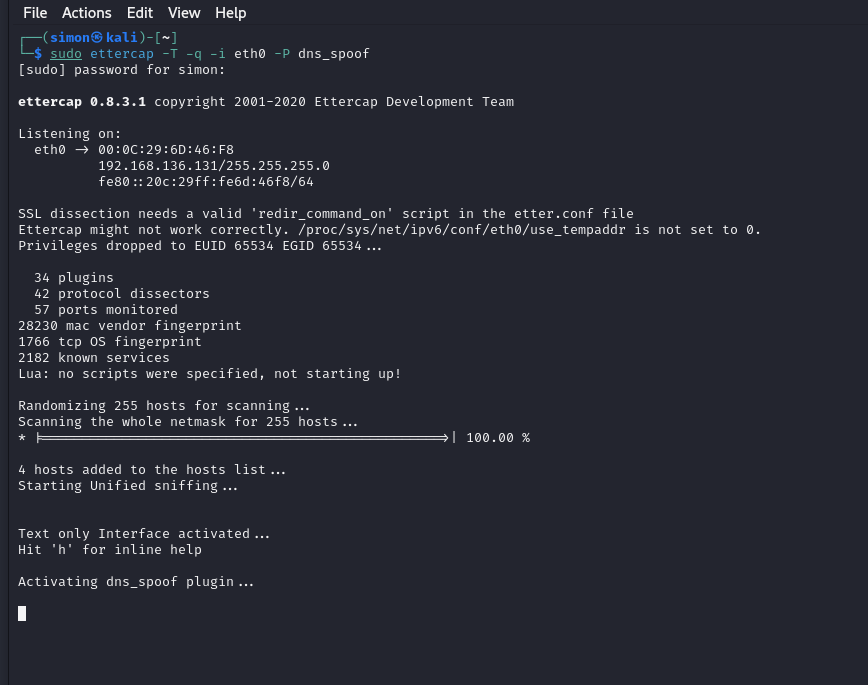
5. 使用Ettercap实现DNS欺骗

先嗅探到靶机

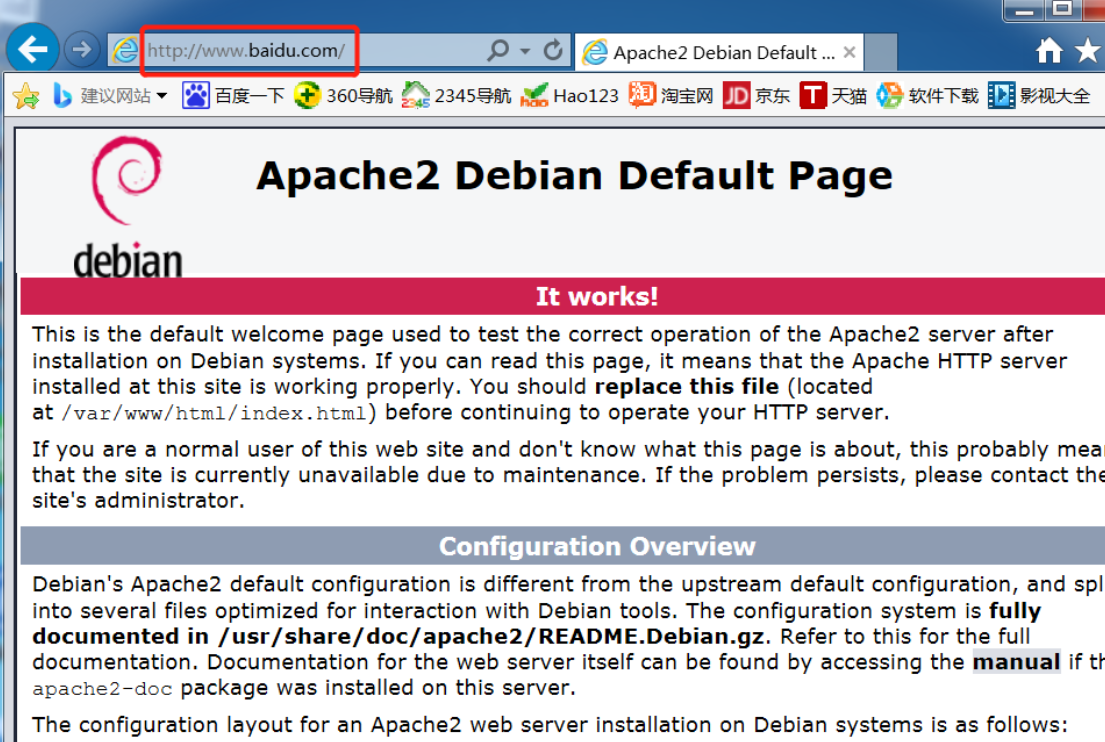




开启dns攻击



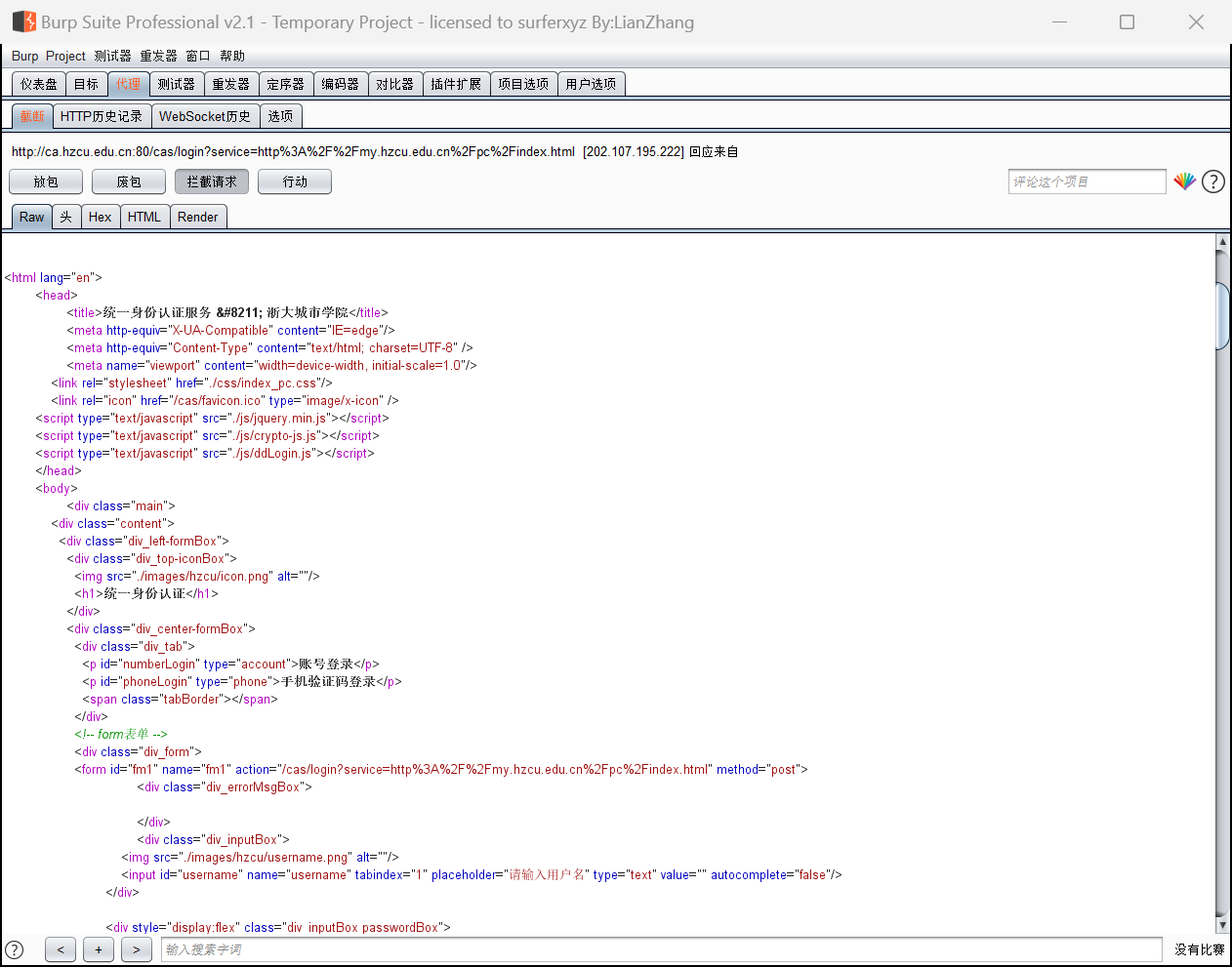
开始攻击



随便打开网站发现劫持成功

6. 使用BP实现Web欺骗，网页修改成功并发送到浏览器显示出来

抓取学校登录系统回显



修改其中title的内容为我的学号



可以看到修改成功