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

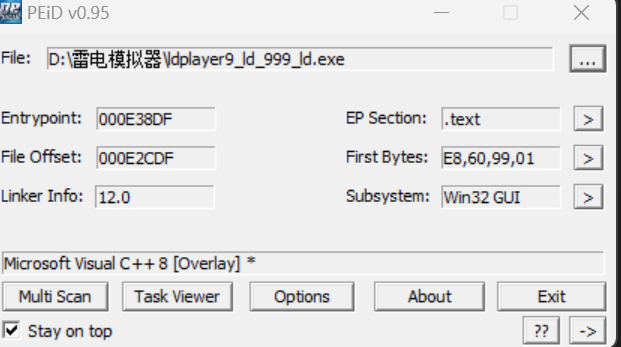
实验报告日期： 2024 年 11 月 7 日

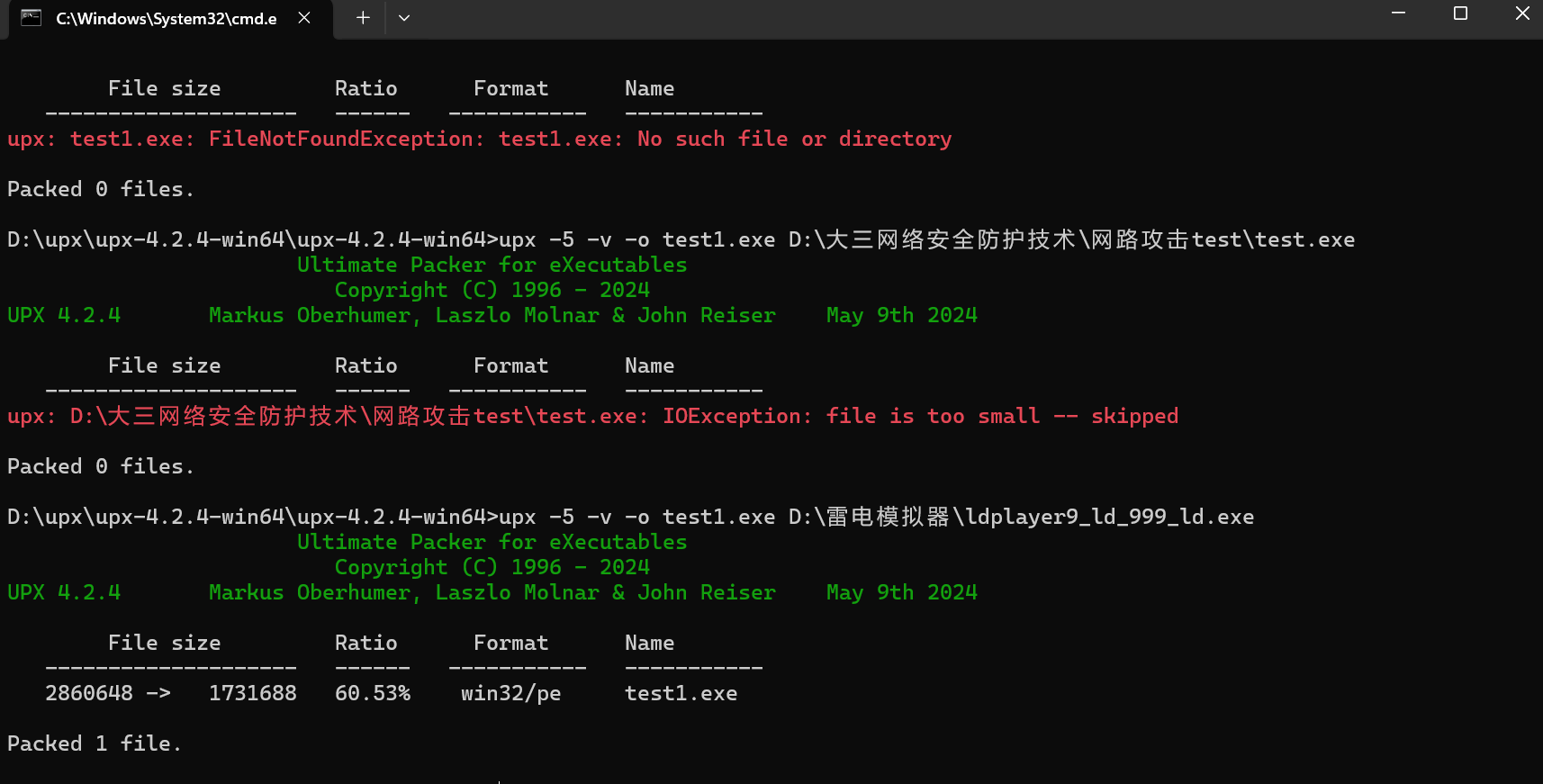
**课程实验报告清单**

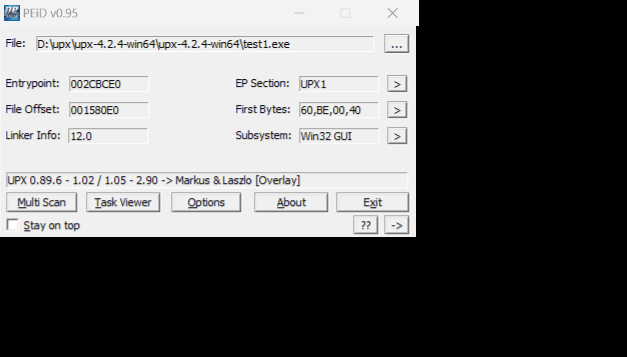
|  |
| --- |
| 目录 |
| 1. 使用upx加壳成test.exe，并用PEId查验，然后再将test.exe脱壳，用PEID查看是否和原始文件一致。 |
| 2. 使用msfvenom工具生成多态代码，应用exploit模块进行反向连接远程主机 |
| 3. 利用Windows SMB漏洞进行攻击，获得shell，并且在后渗透阶段截图验证 |
| 4. 安装LOIC，并使用LOIC进行TCP、UDP协议的Dos攻击 |
| 5. 应用MS12-020漏洞对服务器进行逻辑攻击 |

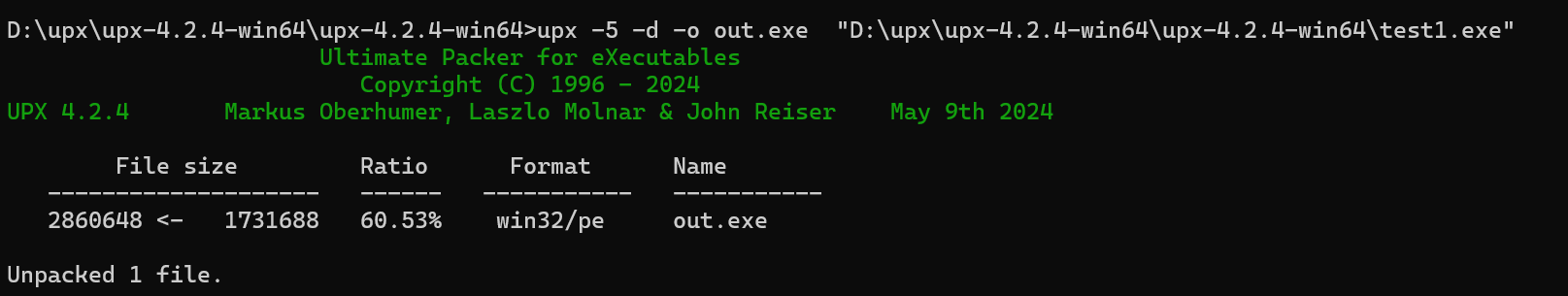
完成要求：必须有详细过程。

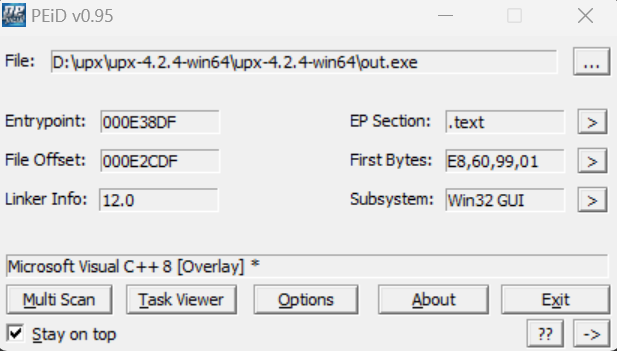
1. 使用upx加壳成test.exe，并用PEId查验，然后再将test.exe脱壳，用PEID查看是否和原始文件一致



。

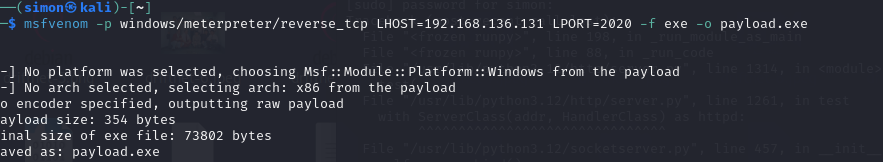




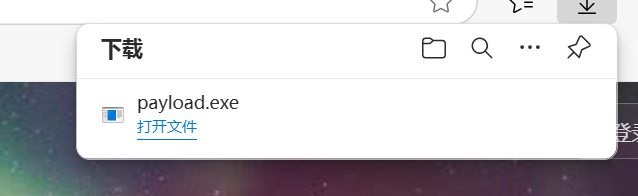


1. 使用msfvenom工具生成多态代码，应用exploit模块进行反向连接远程主机

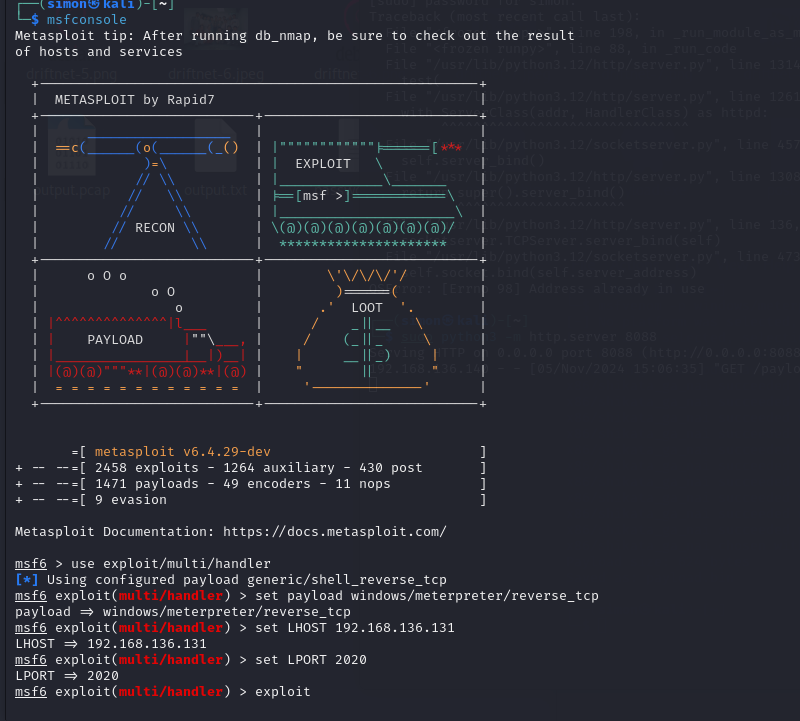
生成payload

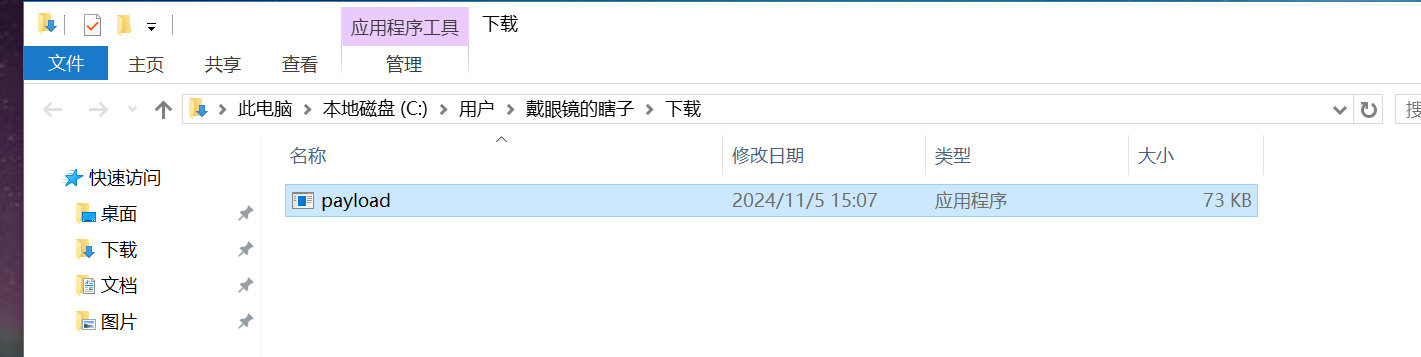


靶机下载payload

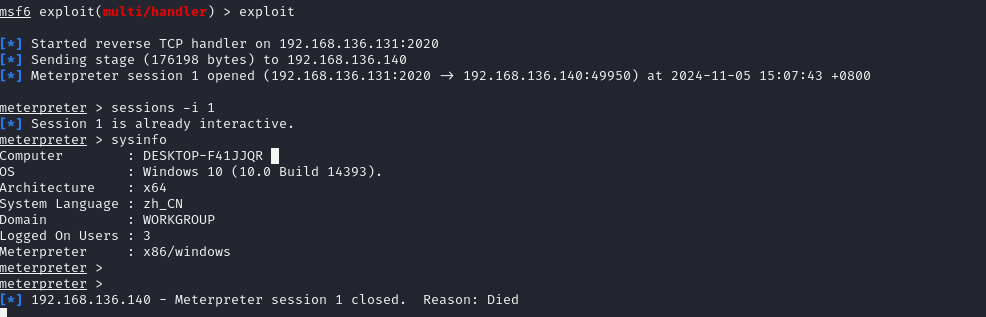


攻击机开启监听端口

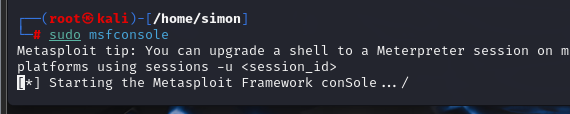


靶机运行payload

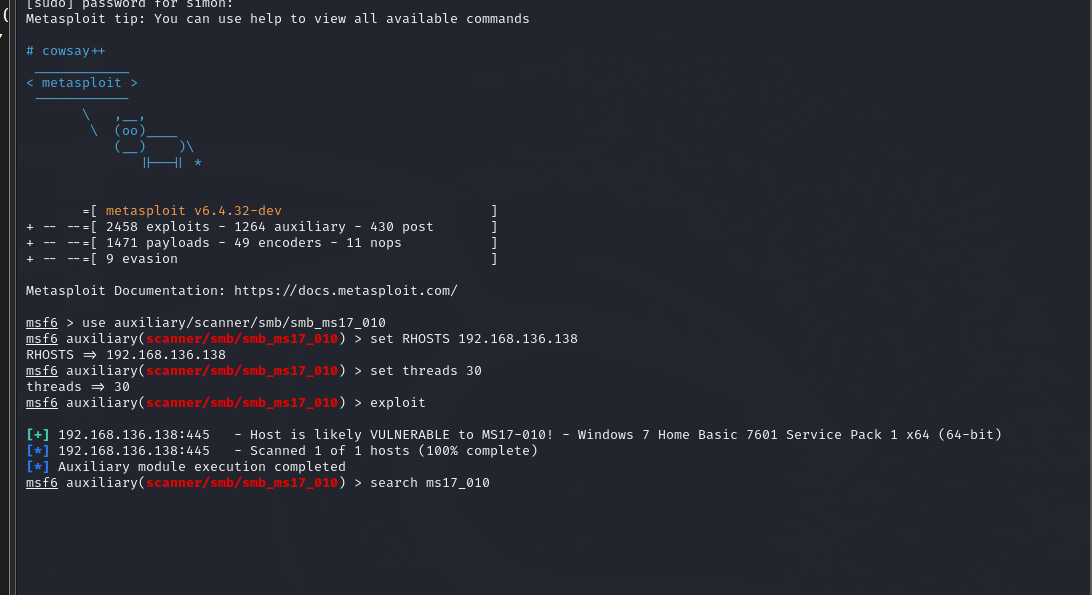
监听到 入侵成功

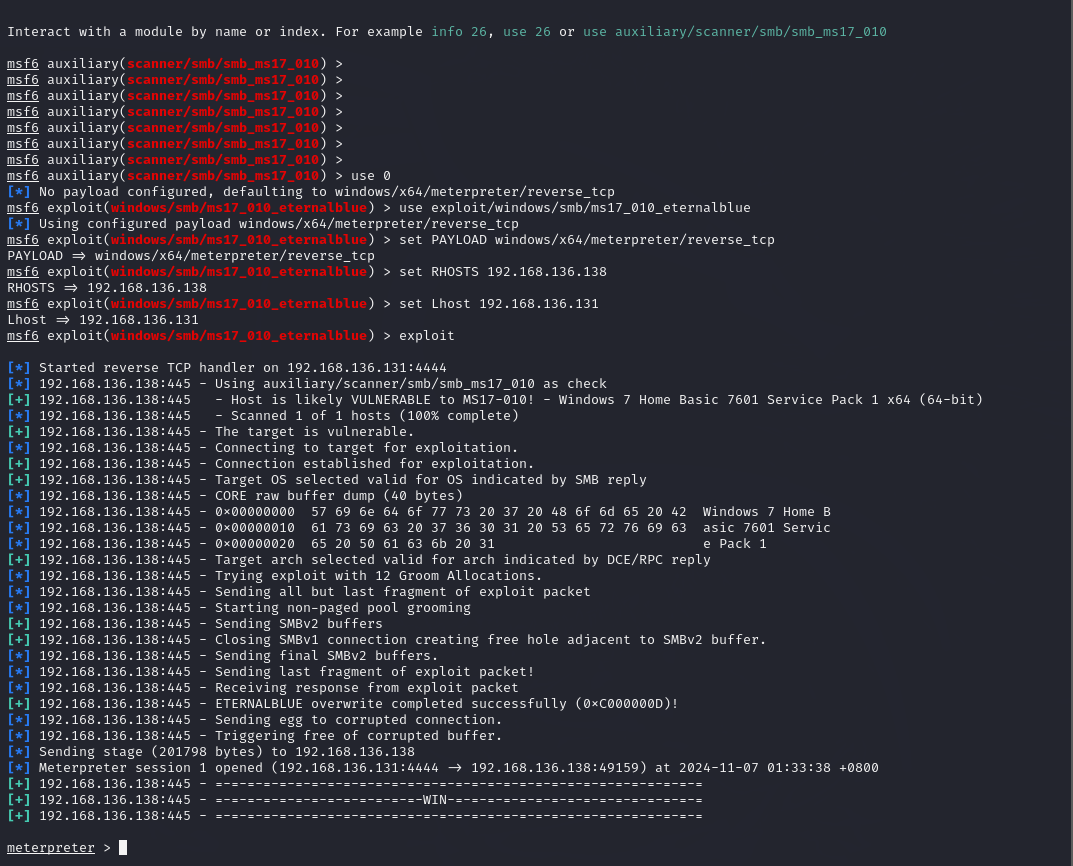


1. 利用Windows SMB漏洞进行攻击，获得shell，并且在后渗透阶段截图验证

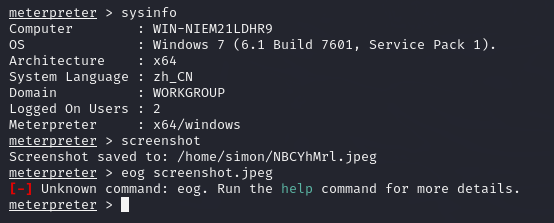


启动metasploit

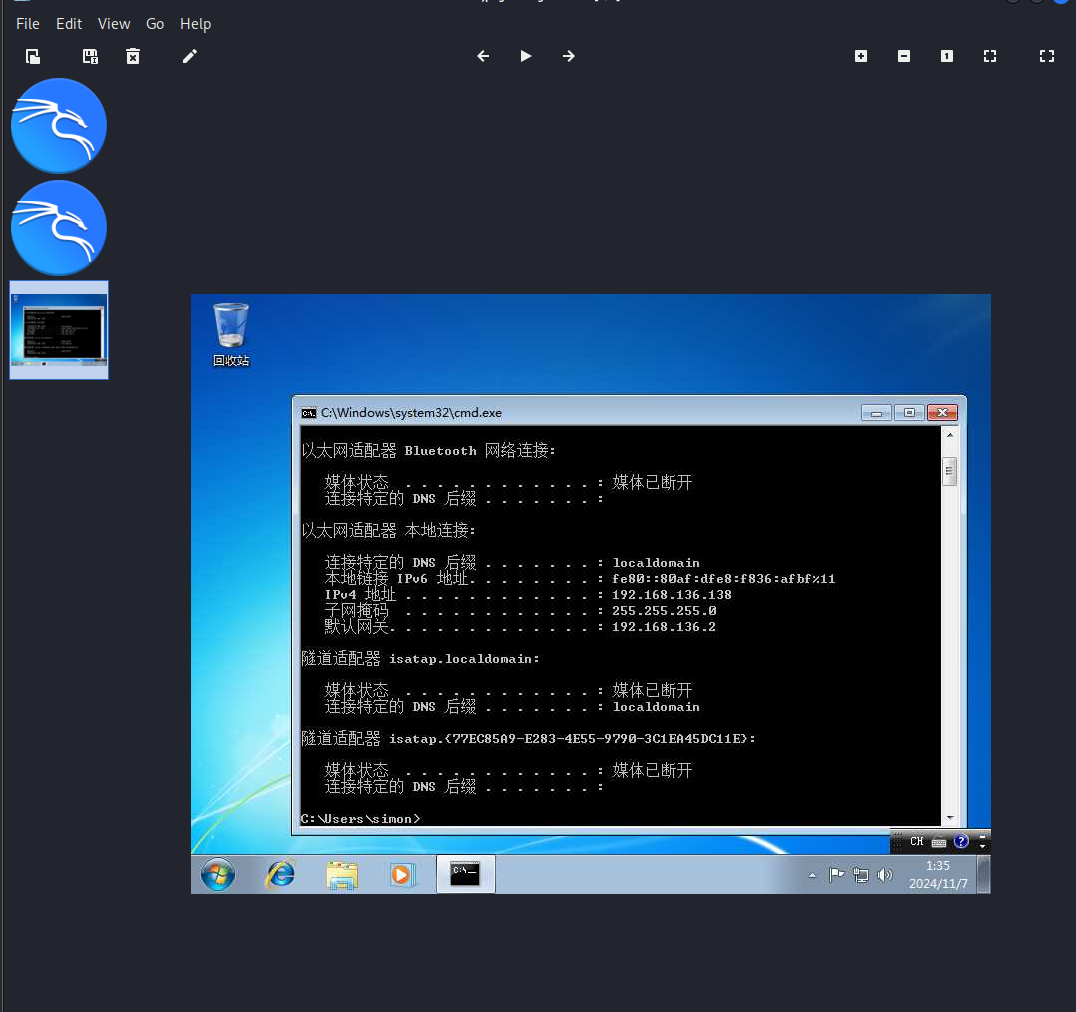
发现漏洞



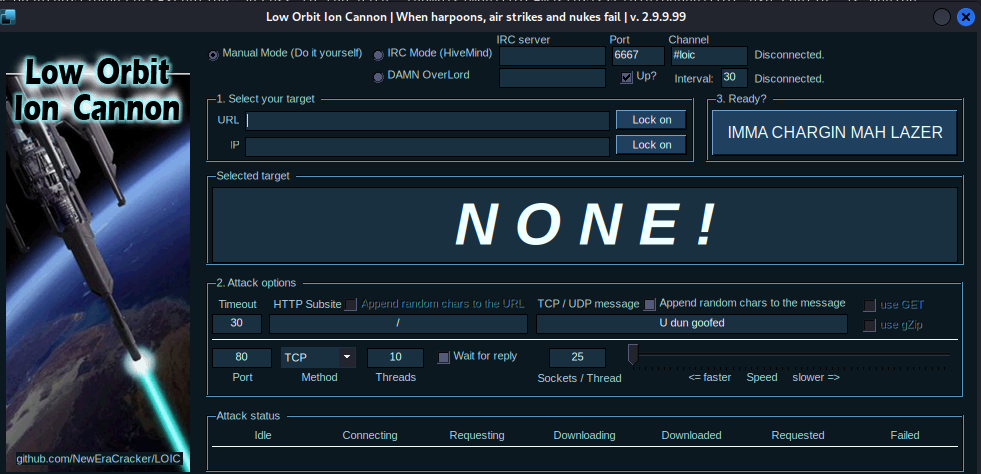
进入渗透成功

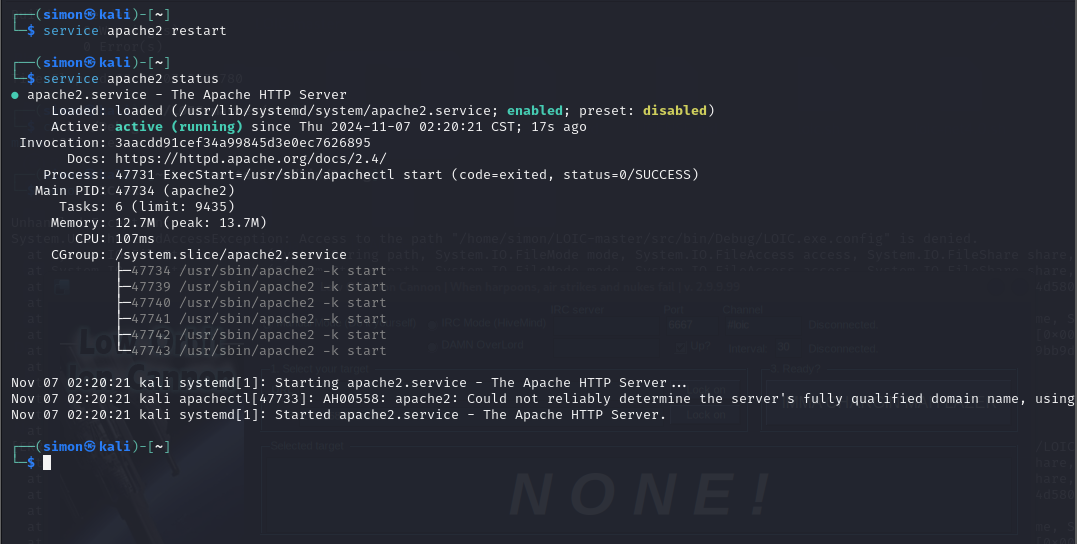


后渗透阶段查看截屏



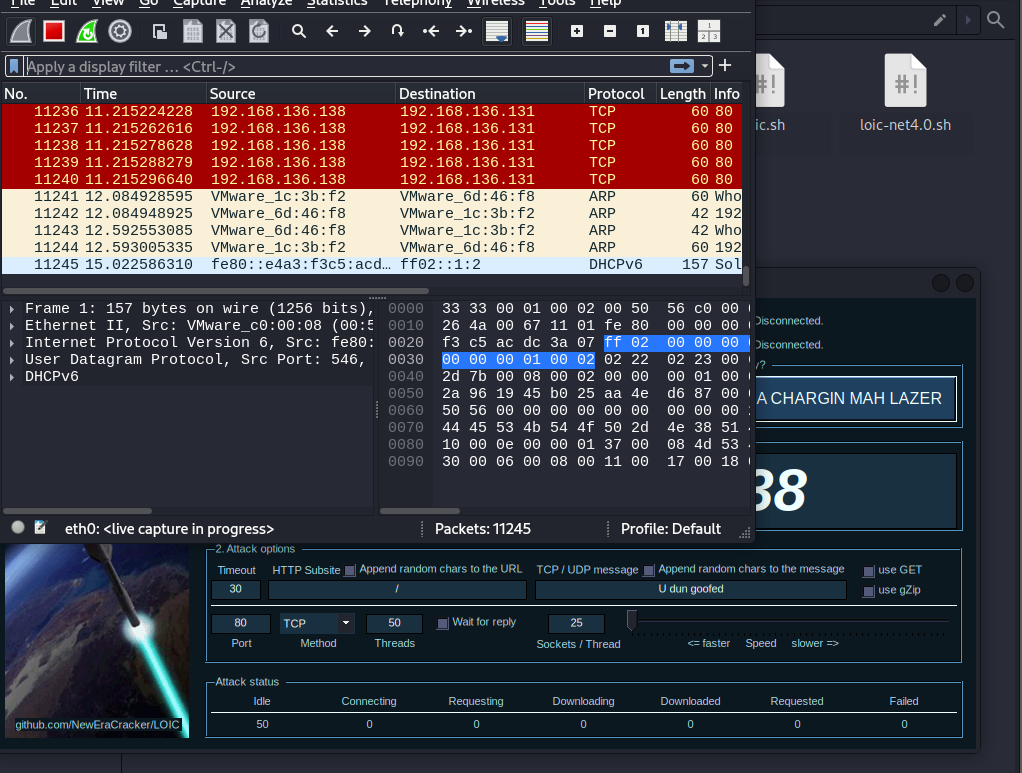
1. 安装LOIC，并使用LOIC进行TCP、UDP协议的Dos攻击

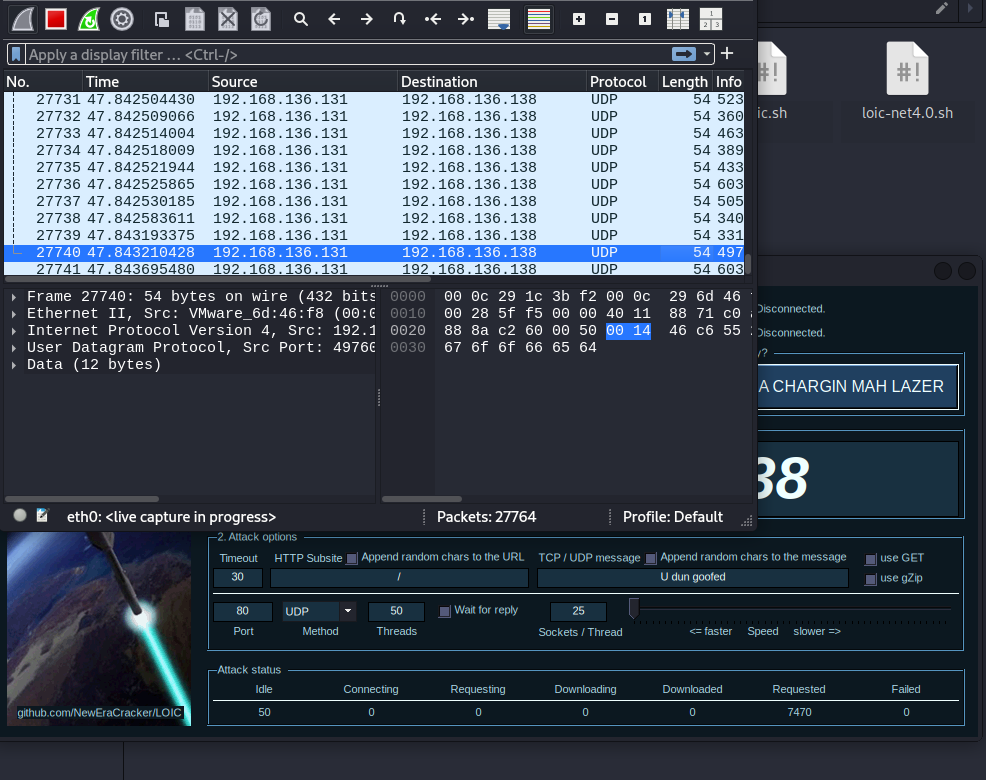
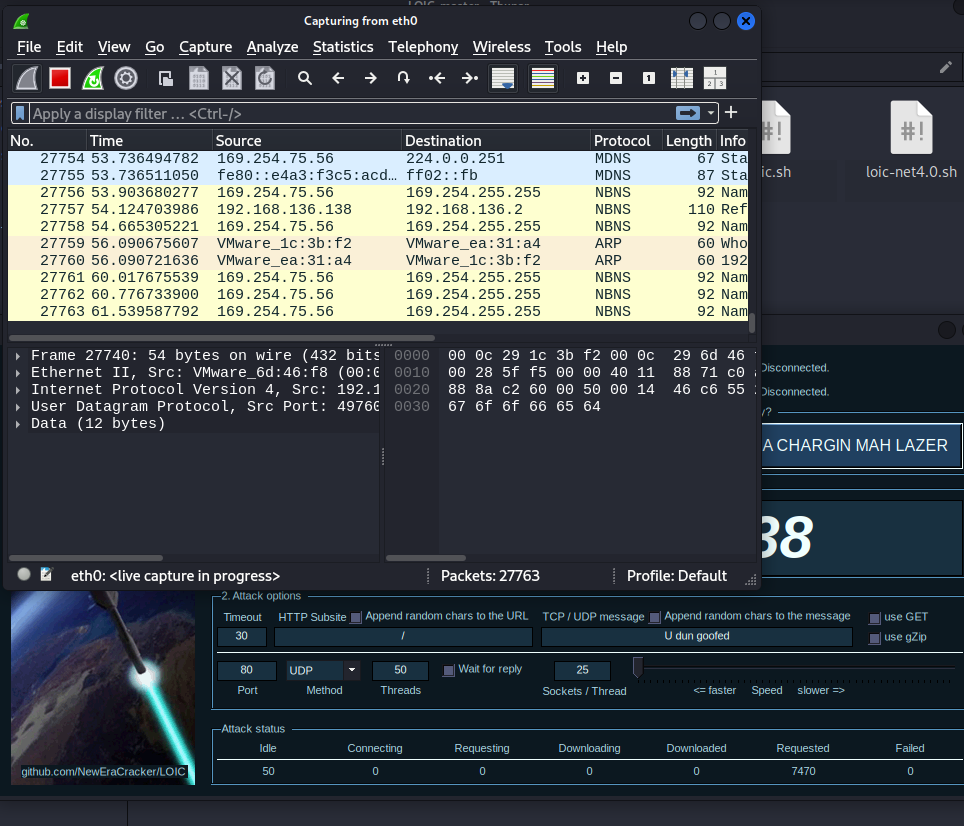


下载完成进入

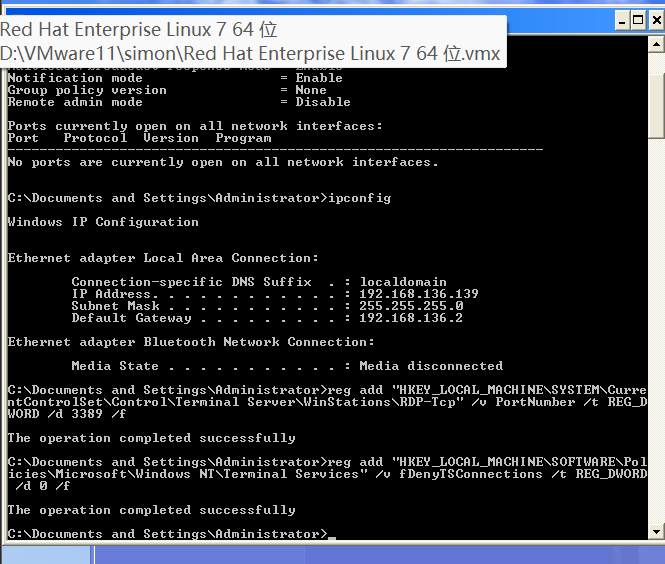
开启阿帕奇服务

开始用wireshark捕获包



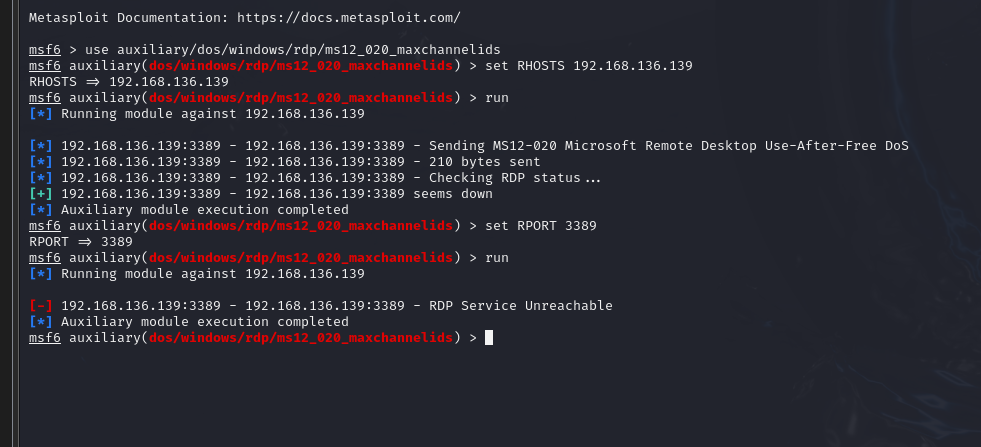
再改为udp

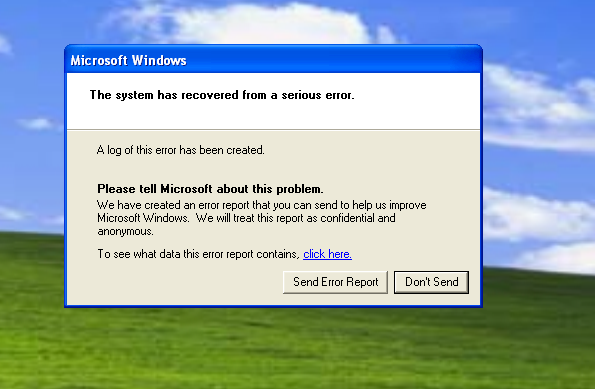
1. 应用MS12-020漏洞对服务器进行逻辑攻击



关闭防火墙并打开3306端口

攻击1



看结果：

成功