基于Python技术设计的用户管理兼ARP欺骗系统

成员：付庭喜 张成双 梁星林

技

术

开

发

文

档

目录

[1引言 3](#_Toc165062573)

[1.1 课题学习的意义 3](#_Toc165062574)

[1.2 课题学习的目的及内容 3](#_Toc165062575)

[1.3 课题学习的特点 3](#_Toc165062576)

[1.4 开发及运行环境 4](#_Toc165062577)

[2 系统结构 5](#_Toc165062578)

[2.1 系统总体结构 5](#_Toc165062579)

[2.2 系统流程分析 5](#_Toc165062580)

[2.2.1系统总体业务流程 5](#_Toc165062581)

[2.2.2系统功能列表 6](#_Toc165062582)

[3 系统概要设计 8](#_Toc165062583)

[3.1 系统模块结构设计 8](#_Toc165062584)

[3.2 数据库设计 9](#_Toc165062585)

[3.2.1 数据库需求分析 9](#_Toc165062586)

[3.2.2 数据库设计 9](#_Toc165062587)

[4 系统测试 10](#_Toc165062588)

[4.1　软件测试的作用和意义 10](#_Toc165062589)

[4.2　测试内容 10](#_Toc165062590)

[4.3　测试结果 14](#_Toc165062591)

[5总结 15](#_Toc165062592)

[5.1 工作总结 15](#_Toc165062593)

# 1 引言

## 1.1 课题学习的意义

1、 有助于深入探究网络安全领域的技术与方法，增进对网络安全的全面理解。

2、 可为网络安全防护体系的优化提供有力支持，提升网络的安全性与稳定性。

3、 能推动网络安全技术的发展，为相关领域的创新提供新思路和新方法。

## 1.2 课题学习的目的及内容

**目的：**

深入剖析端口探测和 ARP 攻击的原理，为防范此类攻击提供坚实的理论基础。

实现用户登录功能的高效应用，提高系统的安全性和用户体验。

为网络安全领域的研究提供新的方向和思路，推动该领域的技术进步。

**内容：**

全面研究 Scapy 框架的特性和功能，以实现精准、高效的端口探测。

深入分析 ARP 攻击的手段和防范措施，为网络安全防护提供有效策略。

优化 Tinker 实现用户登录功能的流程和界面，提升用户使用的便捷性和安全性。

## 1.3 课题学习的特点

紧密贴合实际应用需求，具有显著的实践性，可为解决实际问题提供切实可行的方案。

涉及的专业知识和技术具有较高的专业性和复杂性，需要研究者具备扎实的专业基础。

强调研究的创新性和前瞻性，探索前沿技术和新的应用模式。

注重研究的系统性和综合性，全面考量各个因素对课题的影响。

具有较强的针对性，能够针对具体的网络安全问题提供个性化的解决方案。

## 1.4 开发及运行环境

* 系统开发平台：PyCharm professional Edition 2022.3.3
* 系统开发语言：Python
* 数据库管理系统：MYSQL
* 系统运行平台：Windows 11
* 系统运行环境：Python 3.11.5\python.exe

# 2 系统结构

## 2.1 系统总体结构

端口探测：使用 Scapy 进行端口探测，检测目标系统开放的端口。

ARP 攻击：实现 ARP 攻击的相关功能。

用户登录：利用 Tinker 实现用户登录的功能。

数据处理：对探测和攻击结果进行处理和分析。

配置管理：用于系统的配置和管理。

系统总功能如图所示。

基于python库实现的用户管理系统

登录

插入数据

删除数据

查询数据

ARP攻击

发送方IP

目标IP

实现攻击

端口扫描

更新数据

输入需要扫描的IP

扫描

源MAC地址

图3-1 系统总体结构图

## 2.2 系统流程分析

### 2.2.1系统总体业务流程

1. 启动系统：系统启动并进行初始化设置。

2. 配置参数：根据需求设置相关参数，如目标网络、端口范围等。

3.用户登录：

调用 Tinker 实现用户登录功能。

验证用户身份和权限。

4. 数据处理与分析：

对端口探测和攻击结果进行处理和分析。

生成相应的报告或通知。

5. 端口探测：

使用 Scapy 发送探测数据包。

接收并分析返回的数据包，确定目标系统开放的端口。

6. ARP 攻击（如需要）：

发起 ARP 攻击。

监控和记录攻击过程中的数据。

7. 系统监控与维护：

实时监控系统运行状态。

处理异常情况，进行系统维护和升级。

8. 数据存储与备份：

存储系统数据和日志。

定期进行数据备份。

在整个业务流程中，需要确保系统的安全性、稳定性和可靠性，同时遵循相关法律法规和道德准则。

### 2.2.2系统功能列表

系统具体功能列表如下所示：

表3.1系统功能列表

|  |  |
| --- | --- |
| 功能类别 | 功能介绍 |
| 个人信息管理 | 登陆（用户管理员、普通用户） |
| 修改个人信息（用户管理员、普通用户） |
| 端口扫描 | 发现开放端口：确定目标系统上哪些端口正在监听，了解系统提供的服务。  识别服务类型：通过端口号推测运行的具体服务或应用程序。 |
| 系统评估：帮助评估目标系统的安全性。  网络拓扑发现：了解网络中主机的分布和连接情况。 |
| 漏洞检测：辅助检测系统中可能存在的安全漏洞。 |
| ARP攻击 | 中间人攻击：截获或篡改网络通信数据。  网络干扰：造成网络连接故障或通信中断。 |
| 隐私窃取：获取敏感信息，如用户名、密码等。  拒绝服务：使目标系统无法正常提供服务 |

# 3 系统概要设计

本系统的开发工作分为以下5个主要阶段:

（1）系统需求分析与系统的功能设计。包括可行性分析、系统详细调查和用户需求分析，收集各种用户对系统功能的要求，整理相关信息资料，确定系统的开发范围。

（2）数据库设计。确定数据库结构，设计数据库的各种参数、创建数据库表、数据库关系表等。

（3）程序模块划分和实现。根据系统所管理的信息的类型和功能对系统进行模块划分，分别编写代码，逐一实现系统功能。

（4）安全策略设计。根据系统功能划分用户类型和权限，并进行安全模型的设计。

（5）测试。完成系统主体功能后，进行系统测试，查找设计缺陷与错误，对缺陷和错误进行改进和纠正。

## 3.1 系统模块结构设计

根据需求分析，系统可分为以下几个模块进行系统实现。

1. 端口扫描模块：

负责执行端口扫描操作。

检测目标系统的开放端口。

记录扫描结果。

2. ARP 攻击模块：

实现 ARP 攻击功能。

配置攻击策略。

监控攻击过程。

3. 用户登录模块：

集成 Tinker 进行用户登录管理。

验证用户身份和权限。

提供安全的登录界面。

4. 数据处理模块：

分析端口扫描和 ARP 攻击的数据。

生成相关报告。

5. 安全模块：

检测和防范网络攻击。

实施安全策略。

6. 配置模块：

允许用户设置系统参数。

管理系统配置。

7. 日志模块：

记录系统的操作和事件。

提供日志查询和分析功能。

8. 监控模块：

实时监控系统状态。

发送预警通知。

9. 数据库模：

存储系统数据。

确保数据的安全性和完整性。

## 3.2 数据库设计

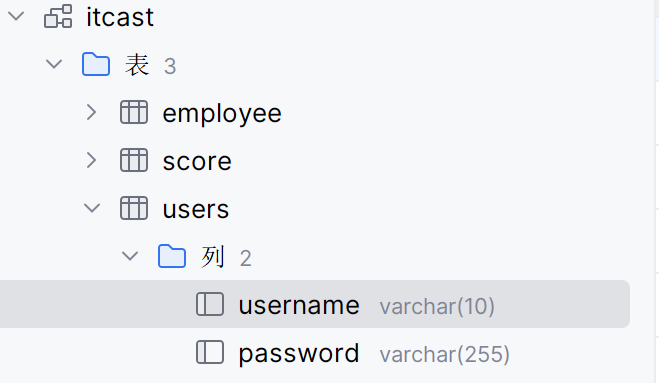
### 3.2.1 数据库需求分析

尽量合理地减少数据库的冗余，使重复的数据保持在最小限度，这样将尽量少的占用存储空间，减少产生混乱影响的危险，还能提高计算机的运行速度。根据需求，需要设计一个管理员表和一个用户表。

### 3.2.2 数据库设计

得到以上数据项和数据结构以后，就可以设计出实际的数据库实体，以及他们之间的关系，为后边的数据库逻辑结构设计打基础。这些实体包括各种具体信息，通过相互之间的作用形成数据的流动。

此系统包含以下实体：itcast 数据库表名：users ，字段：username password以及一个用户表。



# 4 系统测试

## 4.1　软件测试的作用和意义

系统测试是统的开发周期中的一个十分重要环节，尽管在系统开发周期的各个阶段均采用了严格的技术审查，但依然难免会留下错误，如果没有在投入运行前的系统测试阶段被发现并纠正，问题迟早会在运行中暴露出来，到那时候要纠正错误将会付出更大的代价，系统测试占用的时间、花费的人力和成本占软件开发的很大比例，统计表明，开发较大规模的系统，系统测试的工作量大的占整个软件开发工作量的40%-50%，而对于一些特别重要的大系统，测试的工作量和成本更大，甚至超过系统开发其他各阶段的总和的若干倍。

## 4.2　测试内容

（3）数据库的可维护性好，数据的录入、删除及更改均能顺利完成，并实现同台更新。登录时候能提示，如果登录失败，则会将出错原因报出来，有利于程序员的查错

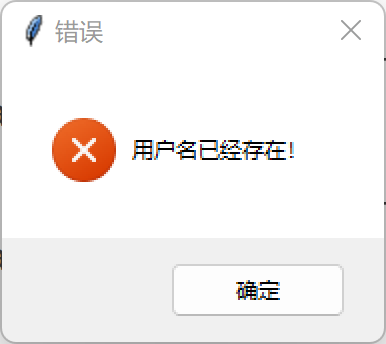
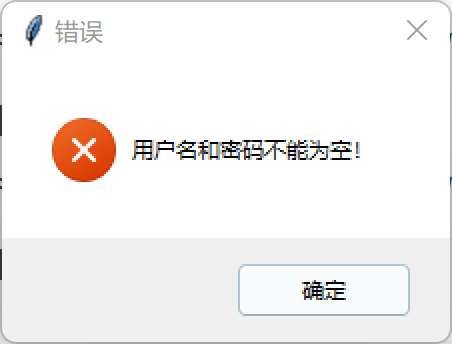


图7-2登录测试

**端口扫描测试：**

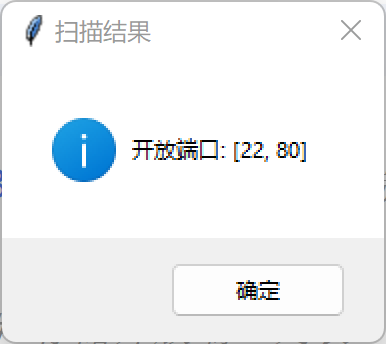
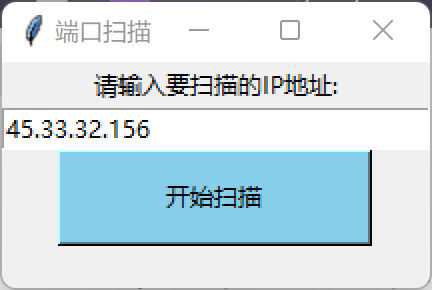
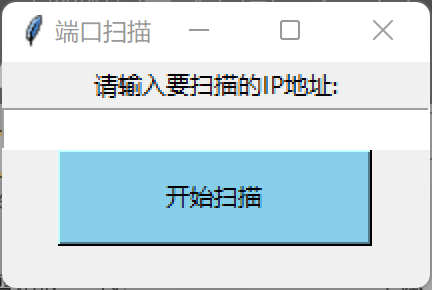


图7-3端口扫描测试

通过点击端口扫描按钮，然后键入需要扫描端口的IP地址，开始扫描之后就会扫描出此IP地址下开放的端口号。

**ARP攻击：**

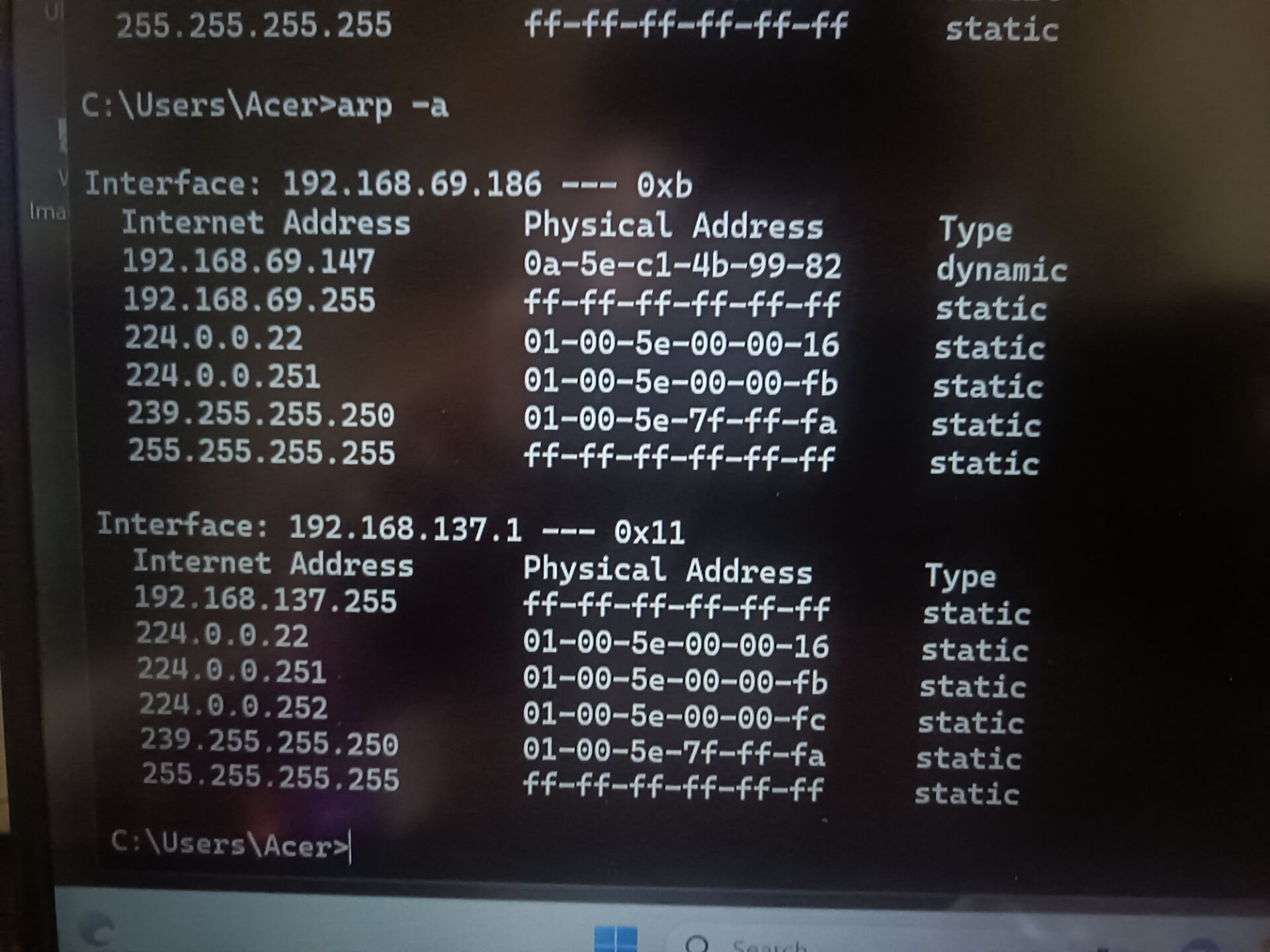
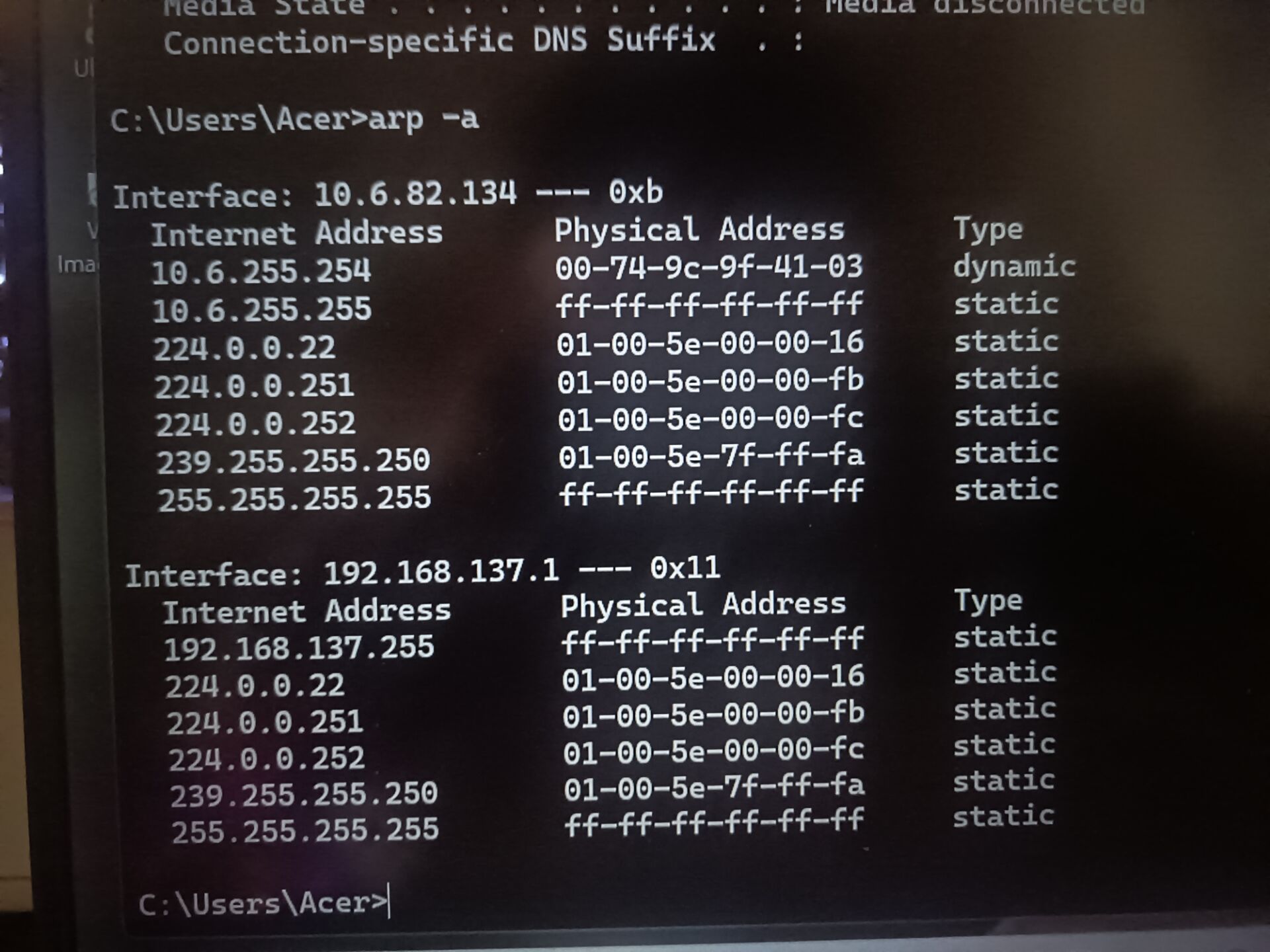
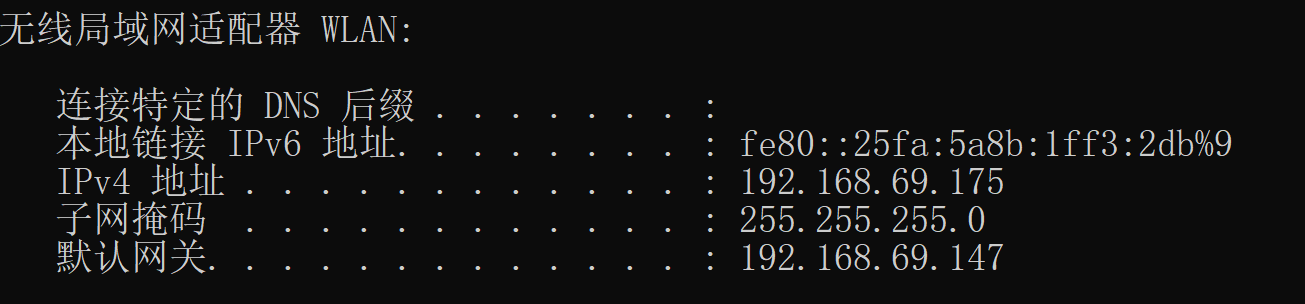
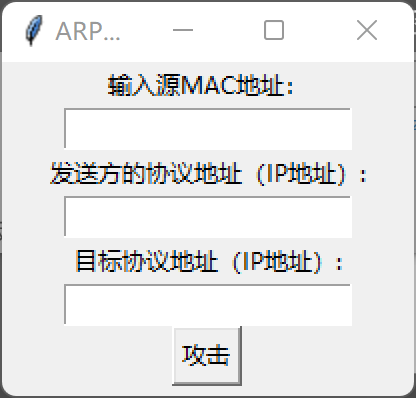


图7-4ARP攻击测试

可见ARP原来的网络IP地址被篡改成了发送方主机的默认网关IP地址，并且MAC地址也改变，证明ARP棋牌能成功。

此功能是用户输入一个源MAC地址，还有发送方主机的IP地址，以及需要欺骗的目标IP地址。点击攻击按钮，然后可以在欺骗的IP主机查看当前主机的ARP缓存。如果ARP的缓存动态的MAC地址变成了源MAC地址则说明ARP欺骗成功。前提是，需要保证目标主机和发送方的主机处在同一个局域网下才可以成功欺骗。

## 4.3　测试结果

（1）在网络无故障的前提下，系统可以正好访问操作界面。

（2）用户登录界面较友好，软件界面的色彩选择、搭配上考虑到了长期工作者眼睛疲劳问题，但依然显得不够专业。

（3）数据库的可维护性良好，数据的录入能顺利完成，并能实现动态更新，删除和修改也能顺利完成。

（4）端口探测功能良好，能顺利实现端口扫描

（5）ARP攻击虽然能够实现欺骗功能，但一旦攻击成功目标用户就不能上网了，可以改进为降低网速，此外，此攻击要遵循一定的协议，不能随便用。

# 5 总结

## 5.1 工作总结

该系统模块结构设计包括端口扫描、ARP 攻击、用户登录、数据处理、安全、配置、日志、监控和数据库等模块。

端口扫描模块检测开放端口，ARP 攻击模块执行攻击并监控过程。用户登录模块负责身份验证和权限管理。数据处理模块分析相关数据并生成报告。安全模块防范网络攻击并实施安全策略。配置模块用于设置系统参数。日志模块记录操作和事件。监控模块实时监控系统状态并发送预警通知。数据库模块存储系统数据，确保其安全性和完整性。

此设计体现了模块化和可扩展性，便于维护和升级，各模块协作实现系统功能。

5.2 待提高的地方

1. 简洁易用的界面：设计直观、简洁、易于操作的界面，降低用户的学习成本。

2. 良好的交互设计：提供清晰的反馈和提示，让用户清楚知道自己的操作结果。

3. 高效的性能：确保系统响应迅速，避免长时间的等待。

4. 稳定性和可靠性：减少故障和错误，保证系统的稳定运行。

5. 个性化设置：允许用户根据自己的需求和偏好进行定制。

6. 清晰的导航和布局：使用户能够轻松找到所需的功能和信息。

7. 及时的帮助和支持：提供在线帮助文档或客服支持。

8. 数据安全保护：让用户放心使用系统。