《信息安全引论》第三次课程实验

作业要求

在以下的实验中任选两个进行学习，简单撰写实验报告并回答问题。在教学网进行提交，请交**单个 pdf 文件**。

SET-UID 程序漏洞实验

前置知识：

1. C 语言编程基础
2. Linux 文件访问控制

实验环境：使用配套练习平台的环境

1. 参照蓝桥云课的实验步骤，完成实验并撰写实验。
2. 涉及 LD_PRELOAD 的部分可以不做

格式化字符串漏洞

前置知识：

1. C 语言编程基础
2. 二进制函数栈

实验环境：使用配套练习平台的环境

1. 参照蓝桥云课的实验步骤，完成实验并撰写实验报告。

Python 编写端口扫描工具

前置知识：

1. TCP/IP 协议
2. Python 网络编程基础

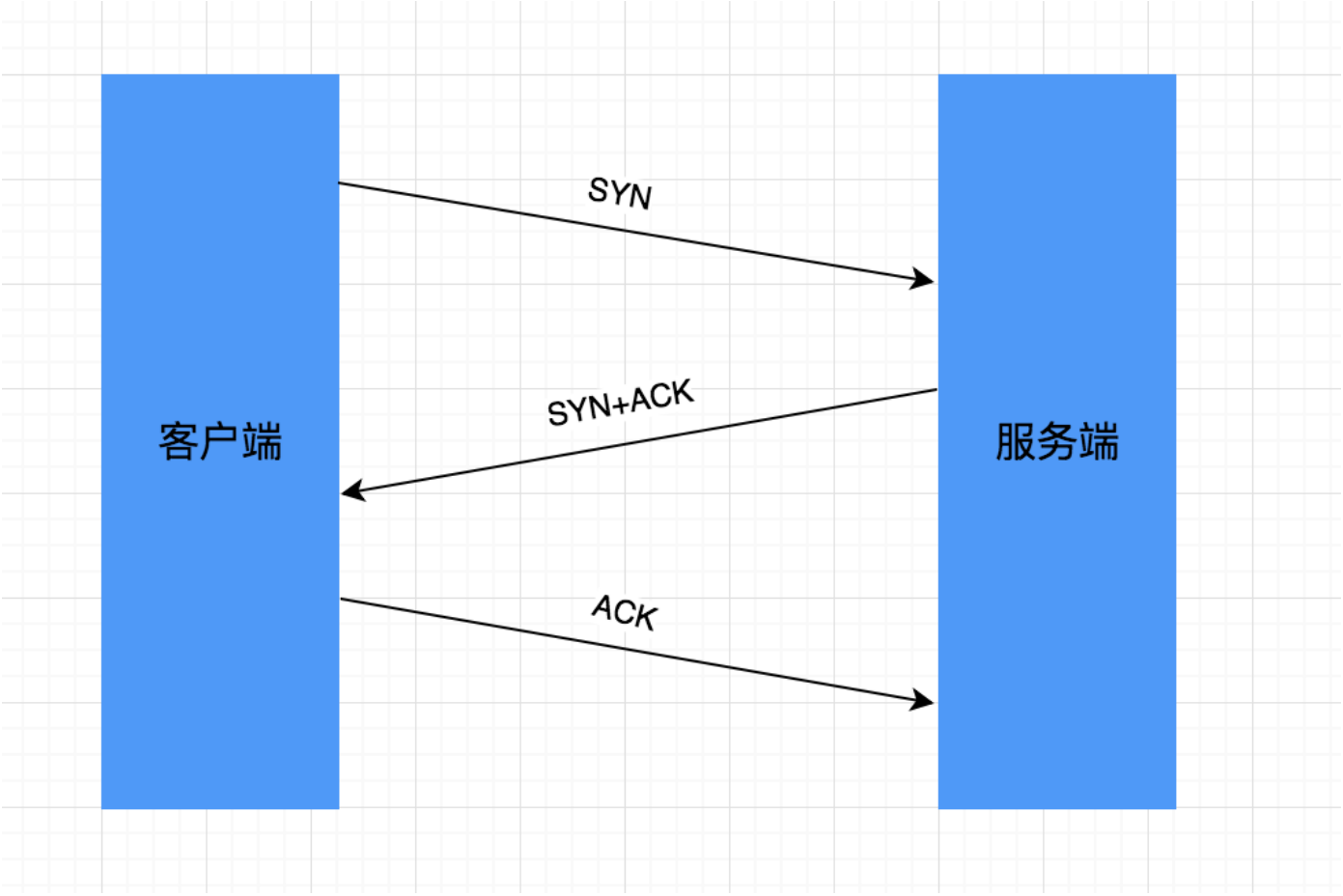
实验环境：装有 python3 的环境即可，接入校园网

TCP 协议：

1. TCP 协议是一种传输层协议，可以在两个设备之间建立逻辑连接，确保数据传输的稳定性与可靠性。一个 TCP 连接由一个四元组定义：

$$(src\_ip, src\_port, dst\_ip, dst\_port) \tag{1}$$

2. TCP 连接由三次握手协议完成。
    1. 服务端监听一个地址（dst_ip）和端口（dst_port），等待客户端连接。
    2. 客户端使用自己的地址（src_ip）和端口（src_port），向服务端发送 SYN 连接请求
    3. 服务端回复 SYN+ACK
    4. 客户端回复 ACK
    5. 至此，TCP 连接建立



端口扫描：

端口扫描用于确定服务器开放端口的情况。计算机管理员可依此确认安全策略；攻击者可用来识别目标主机上的可运作的网络服务，寻找攻击目标。

实验内容：使用对校园网内的一台机器进行端口扫描，确定其开放的 TCP 端口。

```
import sys
from socket import *

service_ports = {
    21: 'ftp',
    22: 'ssh',
    23: 'telnet',
    80: 'http',
    443: 'https',
    3306, 'mysql'
}

target_ip = '162.105.210.3'
opened_ports = []

for port in service_ports:
    sock = socket(AF_INET, SOCK_STREAM)
    sock.settimeout(5)
    result = sock.connect_ex((target_ip, port))
```

```
    if result == 0:
        opened_ports.append(port)

print("Opened ports:")

for i in opened_ports:
    print(f'{i} ({service_ports[i]})')
```

如果不能建立连接，除了端口关闭，也可能是连接请求被过滤了。请改进实验代码，使之能区分一个端口是“开放/被过滤/关闭”三种状态中的哪一种。

SQL Injection

前置知识：

1. SQL 语言基础
2. HTTP 请求

实验环境：使用配套练习平台的环境

1. 参照蓝桥云课的实验步骤，体验 SQL 注入攻击，结合课上所学内容撰写实验报告。
2. 简述如何防范 SQL 注入攻击