

网络攻防技术基础课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验一  网络渗透攻防实验环境本地搭建 |
| 实验日期： | 2024-2-27 |
| 实验地点： | 西部片区4号楼301 |
|  | |
| 学号： | 33920212204567 |
| 姓名： | 任宇 |
| 专业年级： | 软工2021级 |
| 学年学期： | 2023-2024学年第二学期 |

1. **实验目的**

网络渗透攻防实验环境本地搭建

包括：

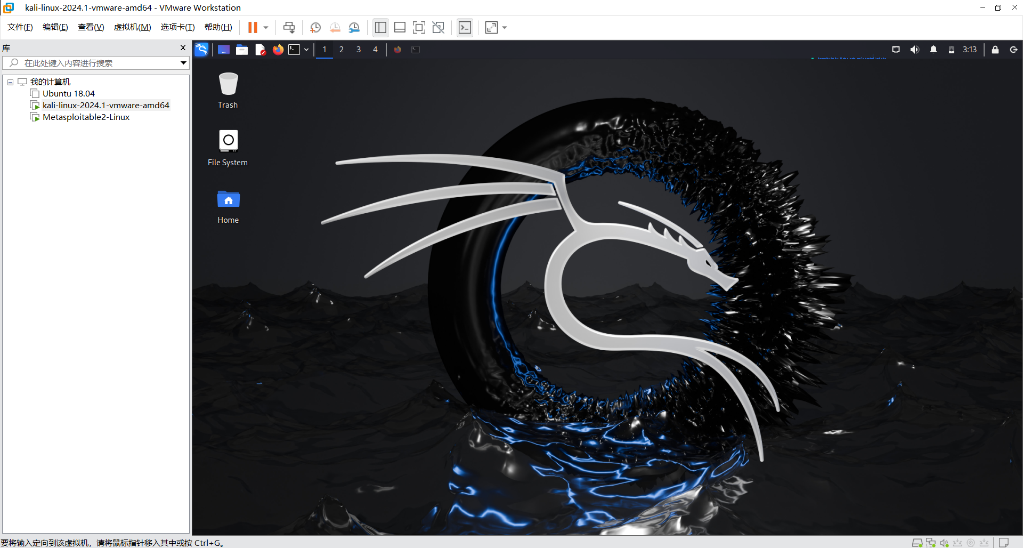
* 安装虚拟机软件（Virtualbox或VMware）
* 虚拟机下安装靶机：metasploitable-linux-2.0.0
* 虚拟机下安装攻击机：Kali
* 攻击机、靶机在虚拟机软件环境中能够网络通信（虚拟网络的配置），且攻击机能够访问实训平台靶机

1. **实验用到的软件或工具**

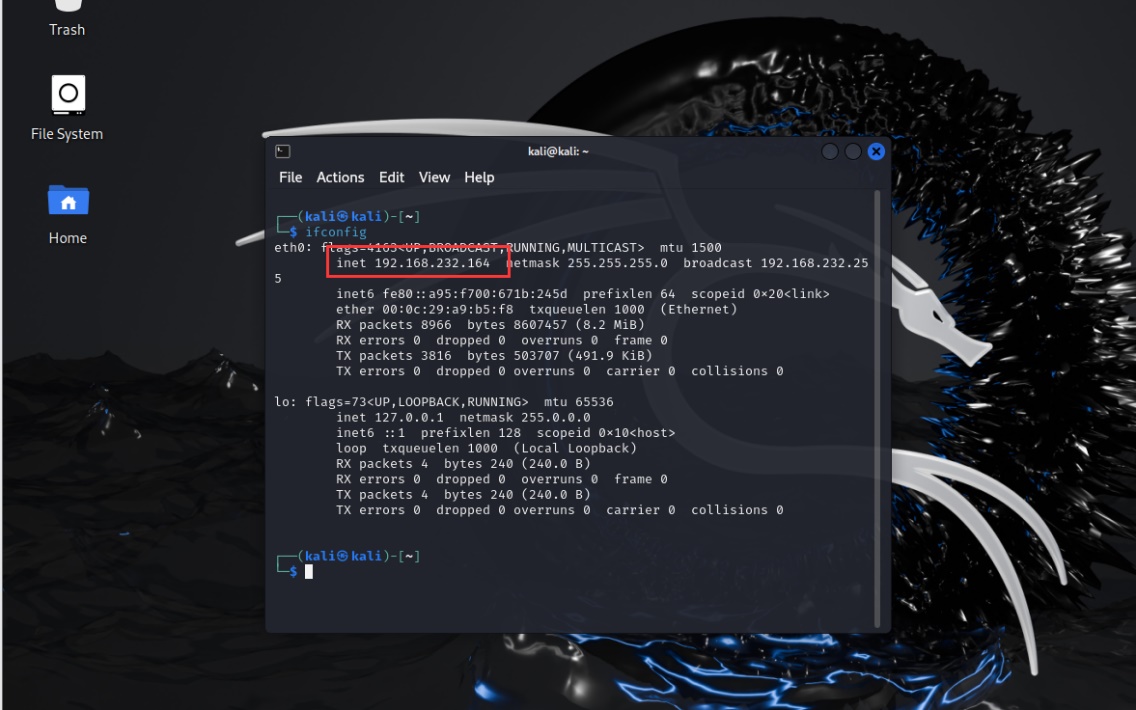
虚拟机软件：VMware Workstation Pro 17

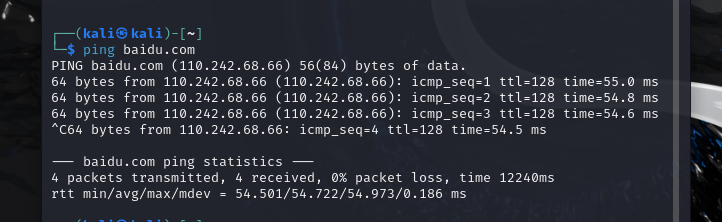
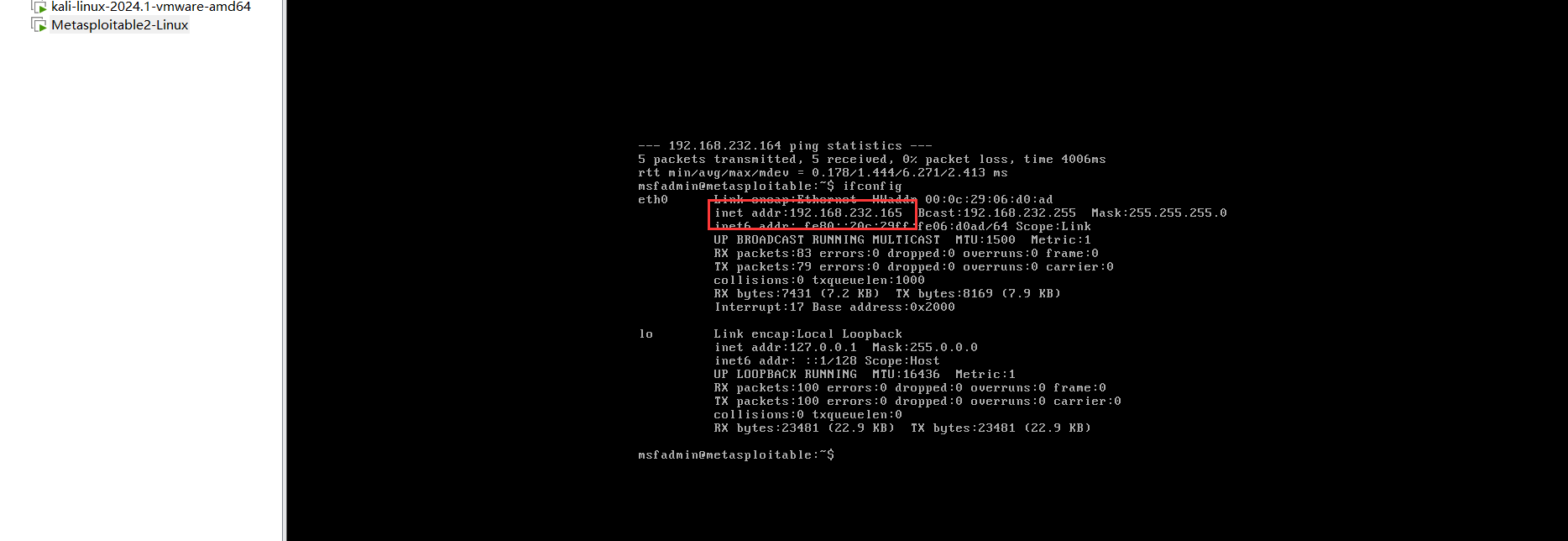
虚拟机系统：metasploitable-linux-2.0.0、Kali

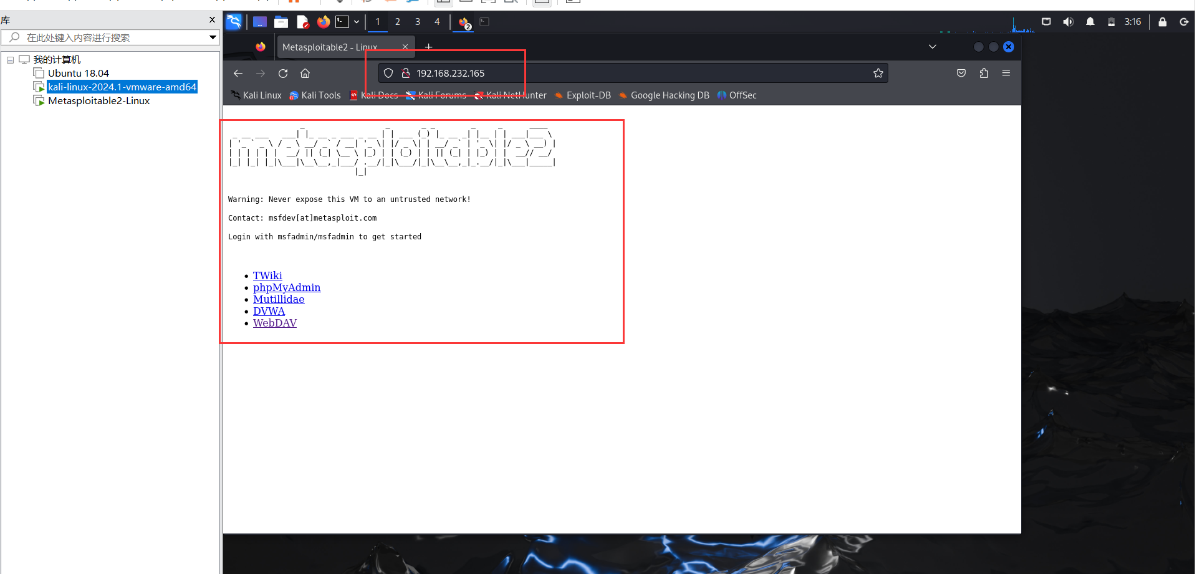
1. **实验过程**
2. 在本地搭建网络渗透攻防实验环境：



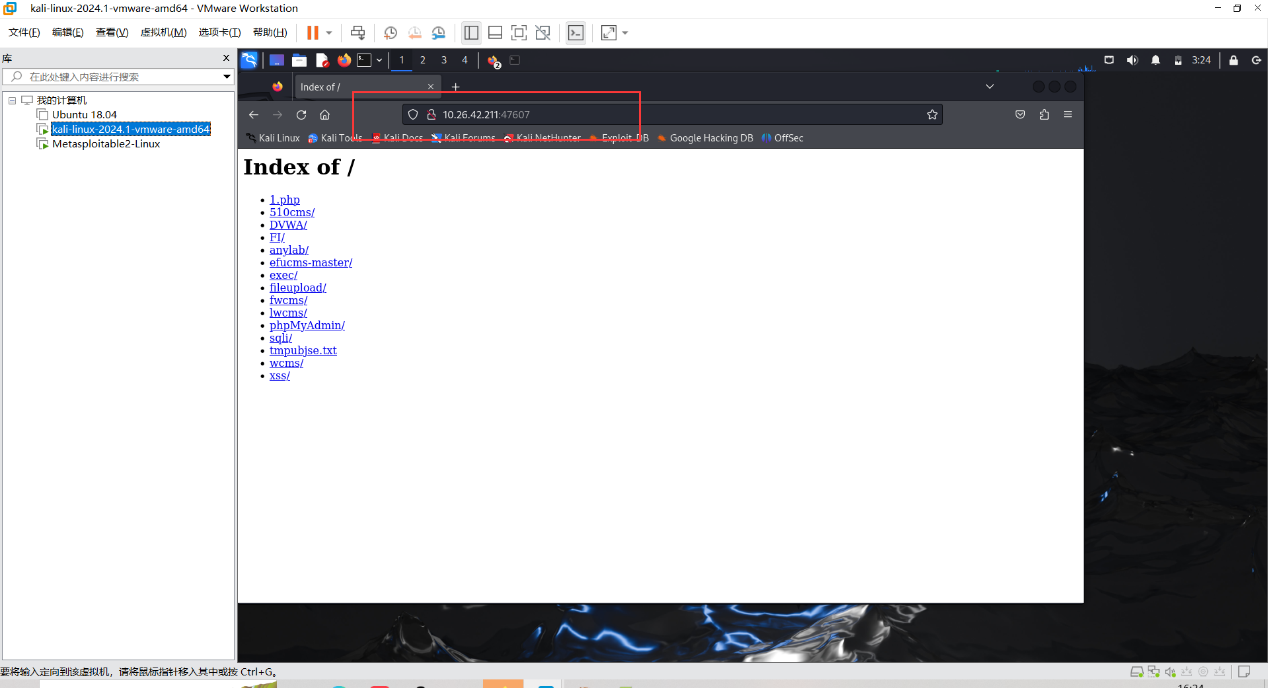
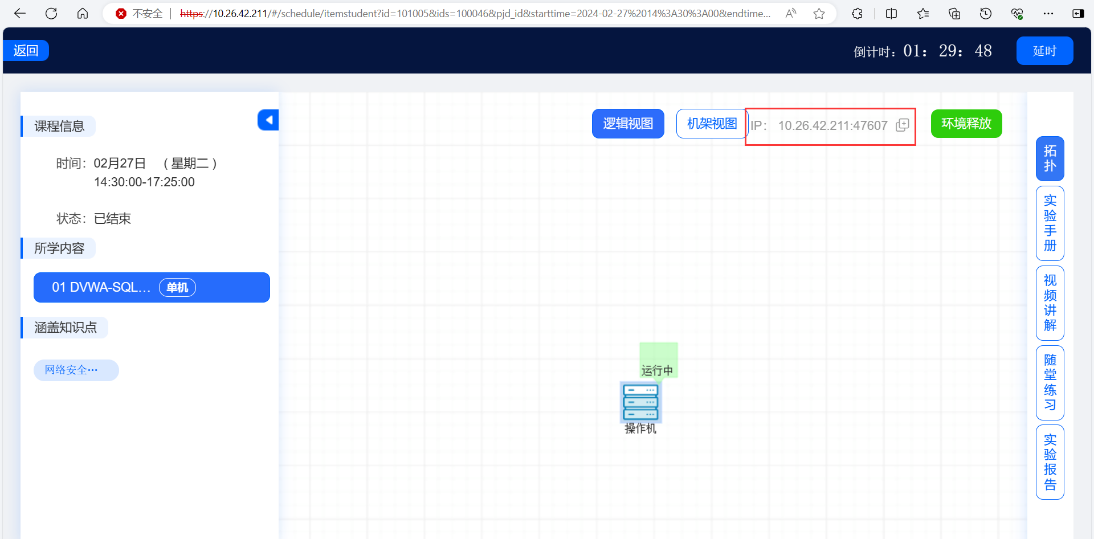
1. 测试攻击机和靶机在虚拟机环境中能否网络通信：





1. 测试攻击机能否访问实训平台靶机：



1. 对DVWA靶机进行调研：
2. 简介

DVWA(Damn Vulnerable Web Application)是一个PHP/MySQL的网络应用程序，特意设计成包含安全漏洞。这个应用程序允许那些对网络安全感兴趣的人，在一个合法的环境中，学习和实践他们的安全技能。DVWA的目的是帮助网络安全专业人员测试他们的工具和技术，同时帮助开发人员更好地理解网络应用程序安全的重要性。

1. 包含的漏洞类别
2. SQL注入：SQL注入漏洞允许攻击者在Web应用程序的数据库查询中插入恶意SQL代码，从而能够读取、修改甚至删除数据库中的敏感数据。DVWA提供了不同级别的SQL注入挑战，从最基础的错误信息引导型注入到更高级的盲注技术，帮助用户逐步深入学习和实践SQL注入的检测和防御方法。
3. 跨站脚本：跨站脚本漏洞允许攻击者在受害者浏览器中执行恶意脚本。这可以用于窃取cookie或其他敏感信息，甚至可以重定向用户到恶意网站。DVWA中的XSS挑战包括反射型XSS、存储型XSS和DOM-based XSS。
4. 文件包含：文件包含漏洞允许攻击者将文件注入到应用程序中，这些文件可能包含恶意代码，可被服务器执行。DVWA通过其LFI和RFI挑战向用户介绍了如何识别和利用这些漏洞，以及如何防御它们。
5. 命令注入：命令注入漏洞允许攻击者在受害的Web应用服务器上执行任意命令。这可以导致数据泄露、服务器被入侵甚至被完全控制。DVWA提供了命令注入的实践环境，让用户学习如何通过不当处理用户输入的应用程序来执行操作系统命令，以及如何采取措施防止这种攻击。
6. 跨站请求伪造（CSRF）：跨站请求伪造漏洞可以使攻击者诱使受害者在不知情的情况下，以他们的身份执行不安全的操作，如更改密码、转账等。DVWA的CSRF挑战向用户展示了如何构造和利用CSRF攻击，以及通过使用令牌、Referer检查等技术来防御CSRF攻击。
7. 会话劫持和固定：会话劫持涉及到攻击者截获或接管Web应用的用户会话，而会话固定则是攻击者强迫用户在服务器上使用一个由攻击者定义的会话ID。通过这些方法，攻击者可以绕过认证机制，以受害者的身份访问应用。DVWA通过实践教学用户识别这类攻击和实施有效的会话管理策略。
8. 文件上传漏洞：文件上传漏洞允许攻击者上传恶意文件，如包含恶意代码的脚本，这些文件上传到服务器后可能会被执行。DVWA中的文件上传挑战让用户练习如何检测和利用这种漏洞，以及如何通过文件类型验证、大小限制和文件内容扫描等技术来防御恶意文件上传。
9. 弱密码和强制浏览：弱密码漏洞指的是系统允许用户设置简单或常见的密码，易于被猜解。强制浏览则是指攻击者通过改变URL或直接访问未公开链接来访问未授权的资源。DVWA提供了这些场景的实际演练，教导用户如何采用强密码策略和正确配置访问控制，以提高安全性。
10. 部署过程

DVWA可以部署在任何支持PHP和MySQL的Web服务器上，部署过程如下：

1. 获取DVWA：首先从DVWA官方网站或者GitHub仓库中下载适合的DVWA版本。
2. 服务器准备：确保Web服务器，以及PHP和MySQL服务已经安装并运行。
3. 配置数据库：导入DVWA的数据库文件（位于DVWA的“/config”目录下）到MySQL数据库中，并修改配置文件“config.inc.php”中的数据库连接设置。
4. 访问DVWA：通过Web浏览器访问DVWA的URL，通常是“http://localhost/dvwa”。
5. 登陆方法

部署完成后，通过浏览器访问DVWA的地址，通常是http://[服务器IP]/。默认情况下，登录DVWA的用户名是admin，对应的密码则是password。登陆后，用户可以在DVWA的用户界面选择不同的漏洞类型进行实践。

1. 可以实现的功能
2. 学习和测试不同类型的漏洞：用户可以针对DVWA中提供的漏洞类别进行攻击尝试，了解它们的工作原理。
3. 安全配置和强化练习：通过调整DVWA的安全级别，用户可以学习如何通过配置和安全强化措施来降低Web应用的安全风险。
4. **实验思考及心得**

在本次实验中，我成功在本地搭建了一个包含靶机和攻击机的简易环境，它提供了一个安全、合法的环境，让我能够在实践中学习网络攻击技术以及如何保护网络应用免受类似攻击的侵害。