01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

1. **作业内容**

2025夏令营第六条-渗透测试环境搭建作业

1.完成vm环境搭建

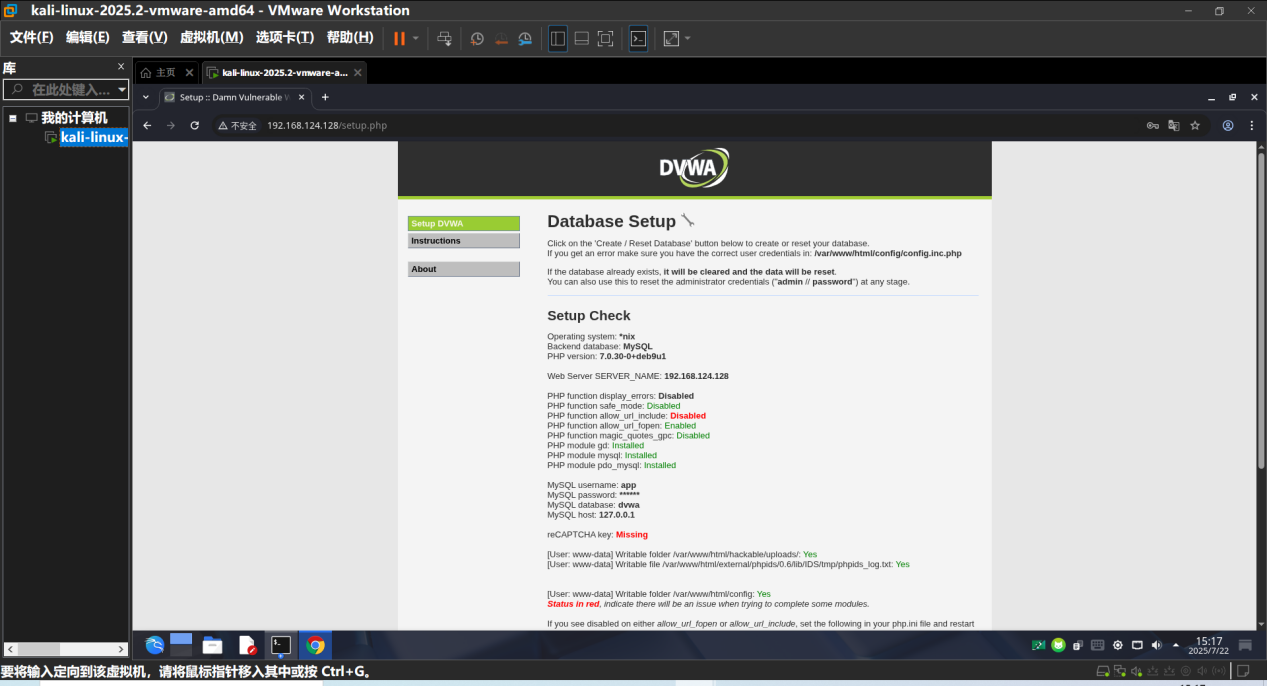
2.完成kali机器安装

3.完成dvwa环境搭建

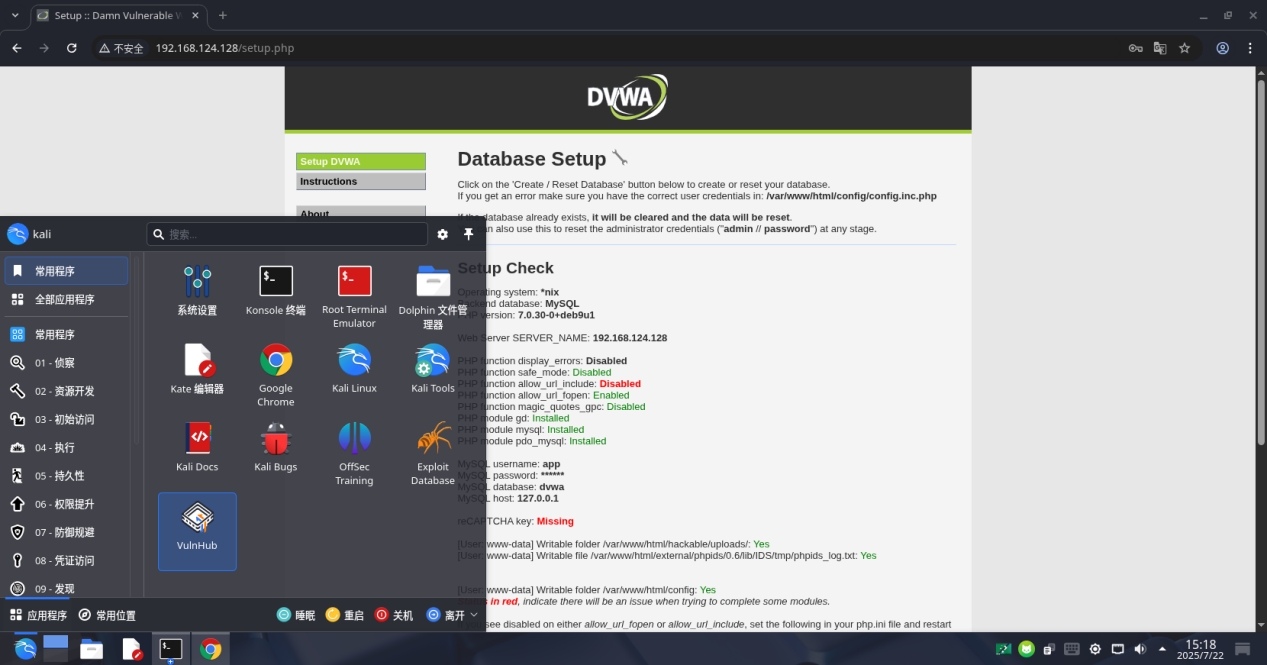
任务要求:安装完成截图写进word文档中即可

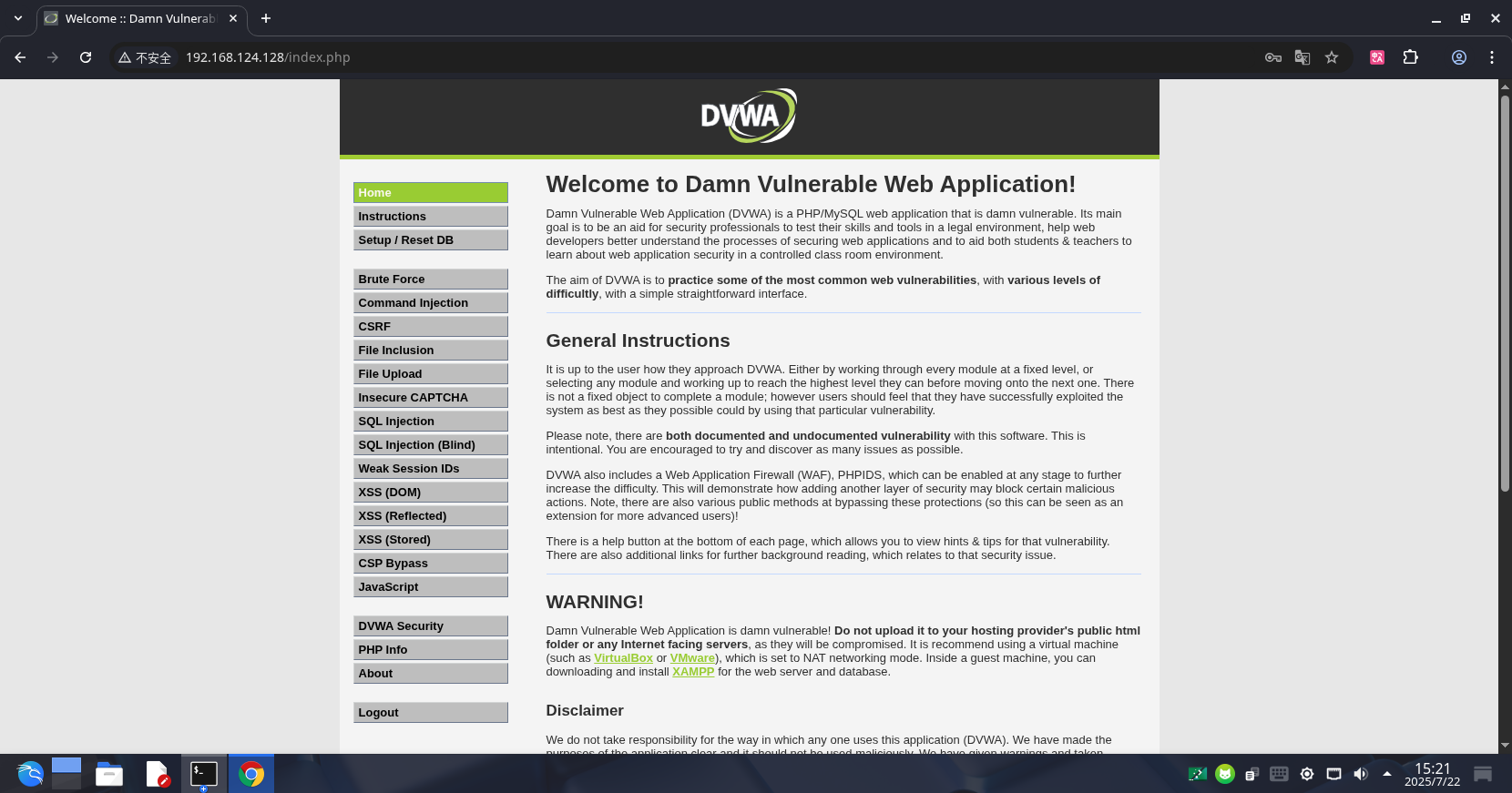
1. **操作步骤**

1.完成vm环境搭建



2.完成kali机器安装



3.完成dvwa环境搭建  


1. **作业总结**

本次作业让我完整地体验了从零开始搭建一个基础渗透测试实验环境的全过程。通过亲手实践，我不仅掌握了基本的操作流程，更在解决问题的过程中获得了宝贵的经验。

1. 理论与实践的结合：

课程PPT清晰地指明了方向和步骤，但在实际操作中，理论必须结合实践才能落地。例如，简单的一句“安装Docker”，在实际操作中就可能因为网络环境的不同而遇到各种问题。只有亲手去敲命令、去看报错信息，才能真正理解每一步的意义。

2. 问题解决能力的锻炼：

本次作业中最有价值的部分就是排错过程。

apt的403错误 让我明白了“网络通”不等于“所有资源都能访问”，软件源的可用性、CDN节点的策略都可能成为障碍，学会检查和修复软件源问题是一项基本功。

docker pull的超时错误 让我深刻体会到在国内网络环境下，配置镜像加速器的必要性和重要性。这不仅是技术问题，更是对网络环境现实情况的认知和适应。这两个问题的解决过程，极大地锻炼了我的故障排查和独立解决问题的能力。

3. 对基础环境架构的理解：

通过本次作业，我对渗透测试环境的“三层”架构有了更清晰的认识：

底层（虚拟化层）： VMware Workstation提供了一个安全、隔离的沙箱环境，让所有实验操作都不会影响到物理主机。

中层（攻击机系统层）： Kali Linux作为一个预装了大量工具的操作系统，是渗透测试者手中的“瑞士军刀”，是发起攻击和分析的平台。

顶层（靶场应用层）： 使用Docker部署的DVWA，则是一个标准化的、可复现的、专门用来练习的“靶子”。

总而言之，这次作业不仅是完成了几项安装任务，更是一次宝贵的实战演练。一个稳定、可靠的实验环境是后续深入学习所有渗透测试技术的基础。这次经历让我对后续的学习充满了信心和期待。