

“网络安全综合实验（I）”实验报告

**题目： Windows靶机安装与验证实验**

院 系 网络空间安全学院

专业班级 信安1901班

姓 名 李欣宇

学 号 U201911658

日 期 2020 年 11 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | Windows靶机安装与验证（50分） | | | | 完成（50分） | 成绩 | |
| 评分 项目 | 过程 | 分析与小结 | 撰写 | 创新 | 完成任务 | 合计 | 教师 |
| 分值 | 20 | 20 | 5 | 5 | 50 | 100 | 签名 |
| 评分 |  |  |  |  |  |  |  |

报告要求及评分规则

1.请按照模板给出的格式，包括行距、字体、段落格式等，完成报告；

2.报告封面保持一致(如实填写基本信息及完成日期)；

3.实验报告内容应包括：封面、评分规则、实验过程记录、实验问题分析与总结、参考文献及资料列表；

4提交：电子材料应包括本实验电子版（doc）、实验参考文献资料的电子资源文件（pdf）。

5.主要考察能力： 实验动手能力、问题分析与归纳能力、文档规范撰写能力、创新能力；

6.其他要求：可按指导老师要求的时间和提交方式提交；每次课实验报告可以单独提交；如果需要最终纸质报告的，可去掉模板中说明文字（斜体）之后，双面打印；

7.总评分=课程每次实验分数之和/课程实验次数。

其中：

每次实验分=实验完成分（50分）+实验报告分（50分）-扣分+加分；

计算方法：

实验完成分=（完成任务数量/总任务数量）\*50；

实验报告分=以下1-4项合计；

1）过程（要求：实验过程完整、清晰）(满分20)（优秀：18+ 良好：16+ 一般：14+）；

2）问题分析与小结（要求：有条理、细致）（满分20）（优秀：18+ 良好：16+ 一般14+）；

3）撰写（要求：语句通畅、格式规范）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

4）创新（要求：见解独到、有创意）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

扣分=报告迟交天数\*2分（满分10分）  （发现雷同抄袭的内容，该次实验不得分）；

加分=搜集整理与实验相关的学习资料作为附件，资料能帮助同学更好掌握相关知识的；获得同组人互评优秀的；提交最终报告时间为班级前3名。（满分5分）（项数\*1分）；

同组评价：

本实验中你的同组人姓名： 刘颖 学号： U201911663

你给同组人评价： 优 （优 良 中 及格）；

理由： 任务完成迅速，面对问题懂得利用搜索引擎，解决问题能力强。

# 实验一：Win7靶机安装与测试

## 实验环境及要求

**实验平台（1-2个虚拟机）：**

Vmware 12以上 或者 Virtual Box6.0以上。

配合安装1：windows7虚拟机、2：Wireshark截包工具 3：VC6/VS2010开发环境 4：IIS web服务,DVWA+phpstudy 5:WannaCry病毒测试(可快照恢复) ,上述软件下载地址由教师在线公布。

网络ip配置：采取NAT方式接入网络，IP动态获取

**实验分组（2人）**：

2人一组，本组名单 刘颖, 李欣宇。

## 实验任务（共6个小任务关卡）(在下述任务下面列上截图与说明)

### 任务1安装VMWare与windows7虚拟机：

**注意下载VMWare12与windows7安装ISO文件，根据自己的CPU选择32位或者64位windows7, Virtual Box6.0也可以作为靶机安装环境：**

在安装完成VMWare后，新建虚拟机，注意将windows7 的ISO文件作为虚拟光盘进行安装。

1) 在安装VMWare Tools后，请分别采用Unity/全屏/控制台视图使用虚拟机，观察虚拟机显示有什么区别；

2) 使用快照功能，测试快照恢复能够实现什么功能；

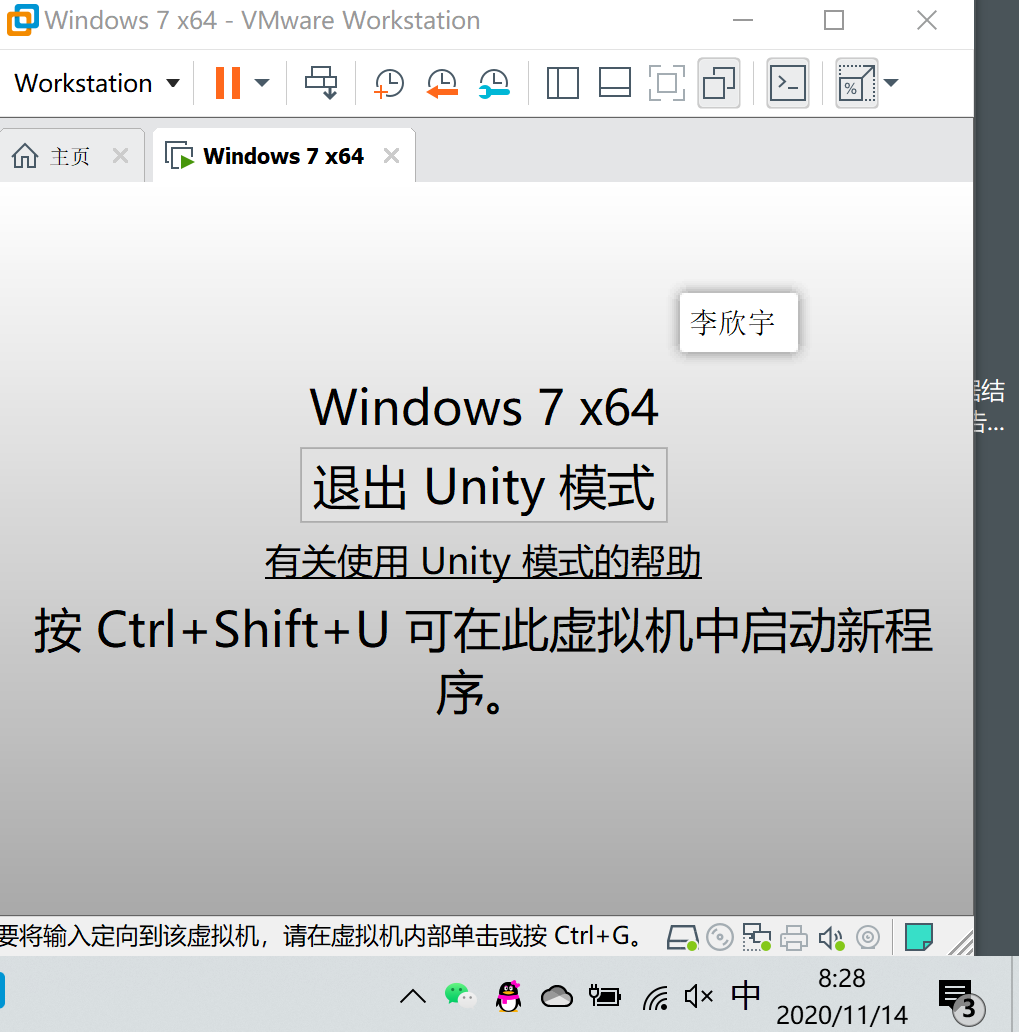
3) 增加一个虚拟磁盘或者物理磁盘，查看虚拟机的状态变化；

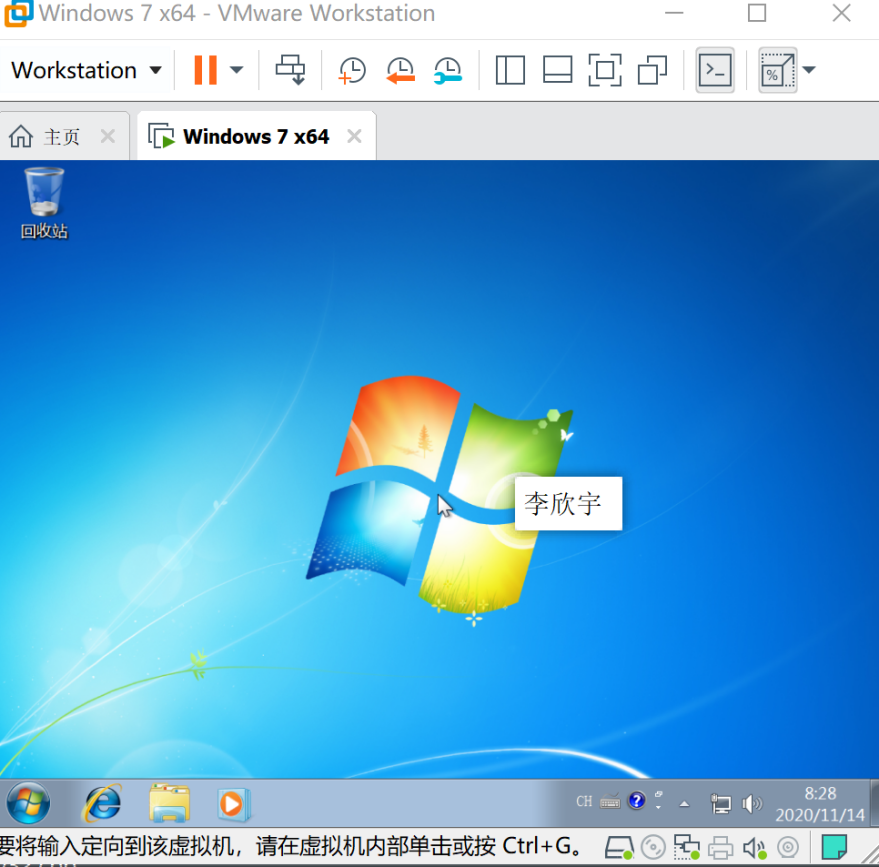
4) 进入虚拟机后，用IPConfig命令列出虚拟机的网络配置；

5) 进入系统与安全，打开防火墙，尝试关闭某个应用程序通信，测试是什么效果。

**过程记录：**

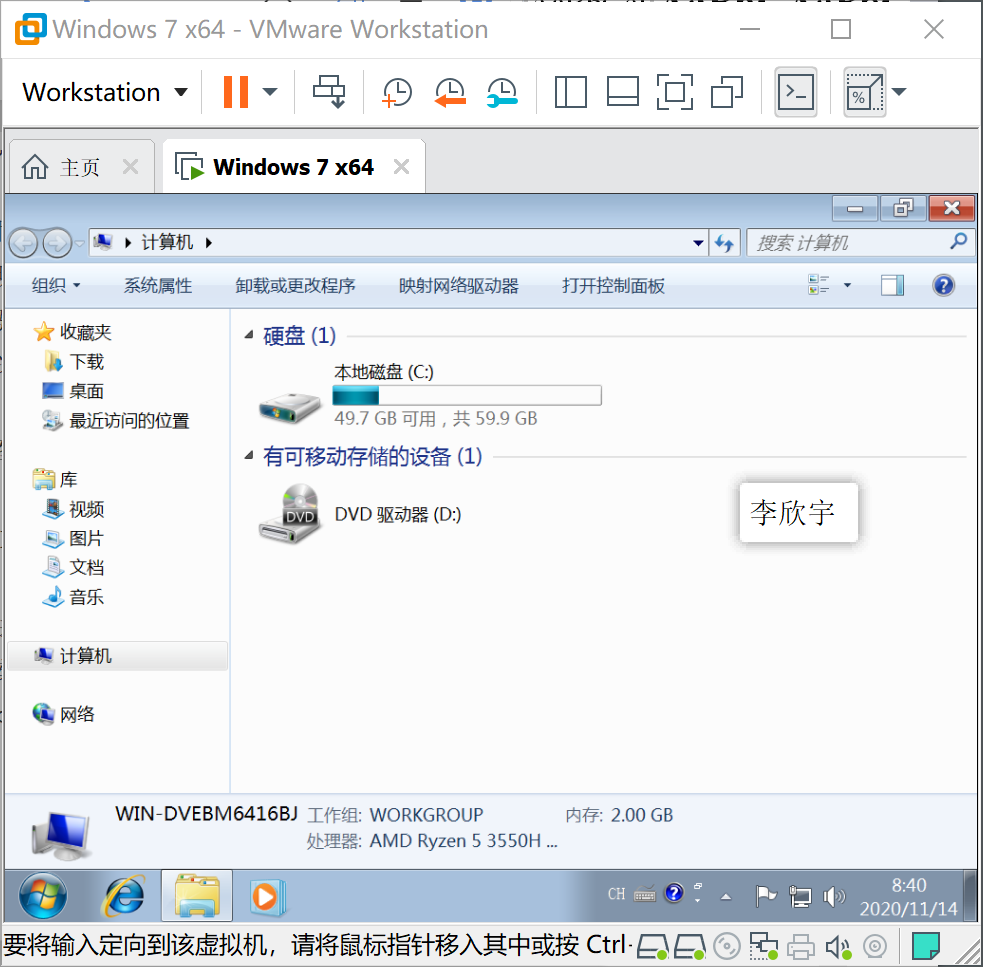
1）以下分别为unity模式与控制台视图，全屏模式即为全屏显示。全屏模式下可以隐藏宿主机的界面，U nity下可以从从宿主机的桌面启动虚拟机的程序而且隐藏其余的虚拟机用户界面。控制台界面下以程序软件的形式使用虚拟机。

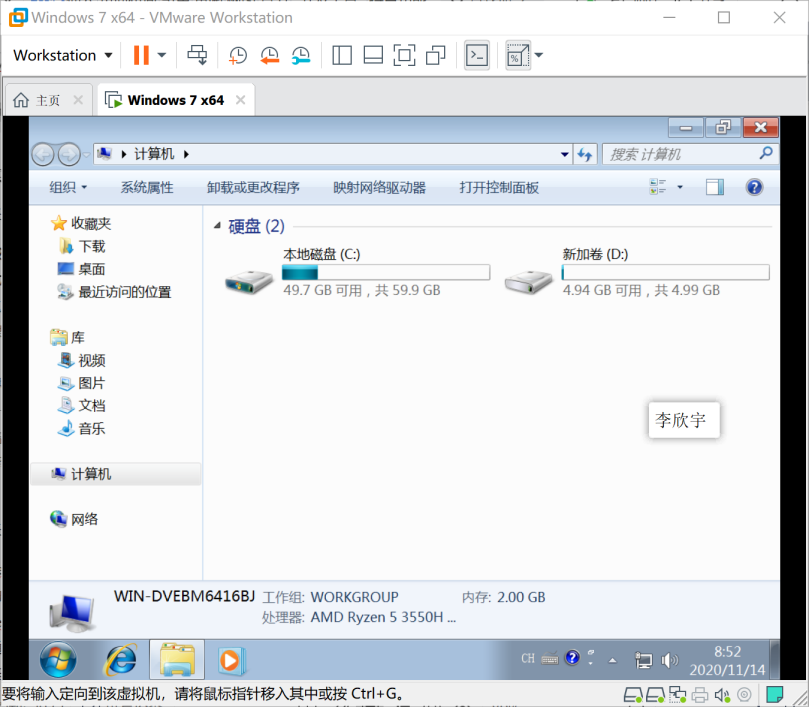
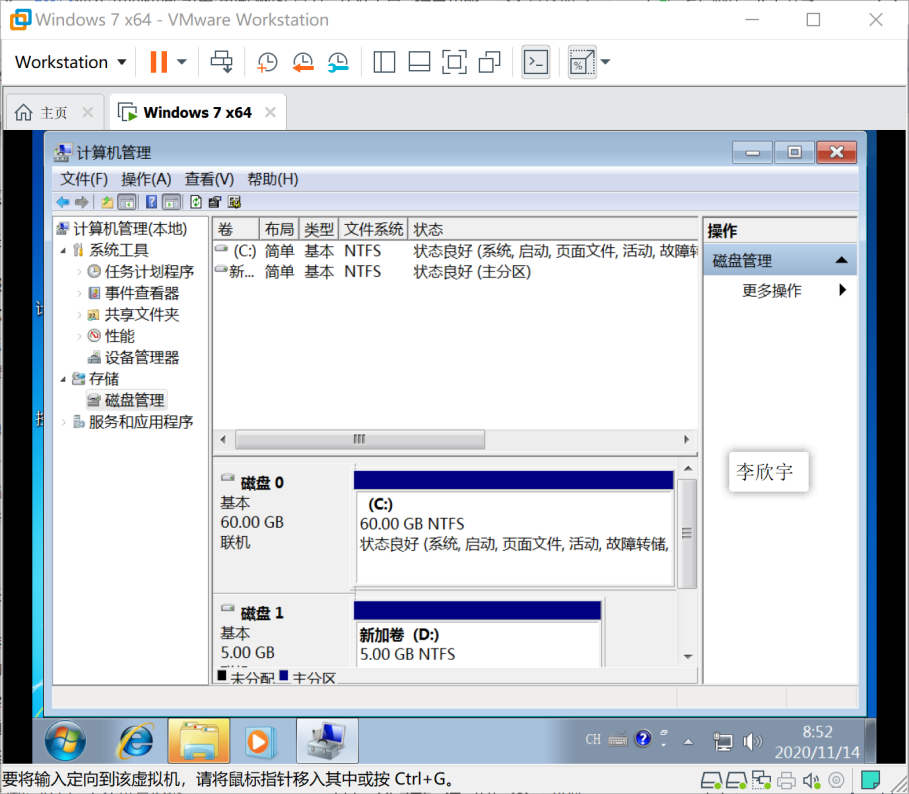




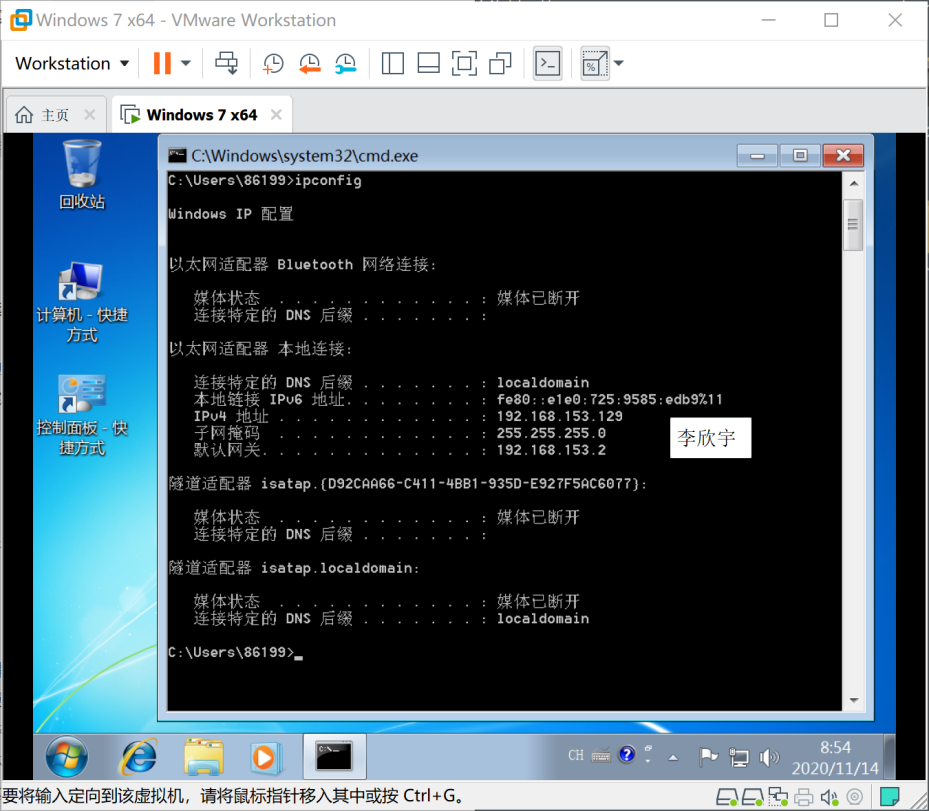
2）快照功能可以恢复拍下快照时系统的状态。

3）添加一个虚拟硬盘后，虚拟机会多出一个未进行初始化的磁盘，初始化后会多出一个盘

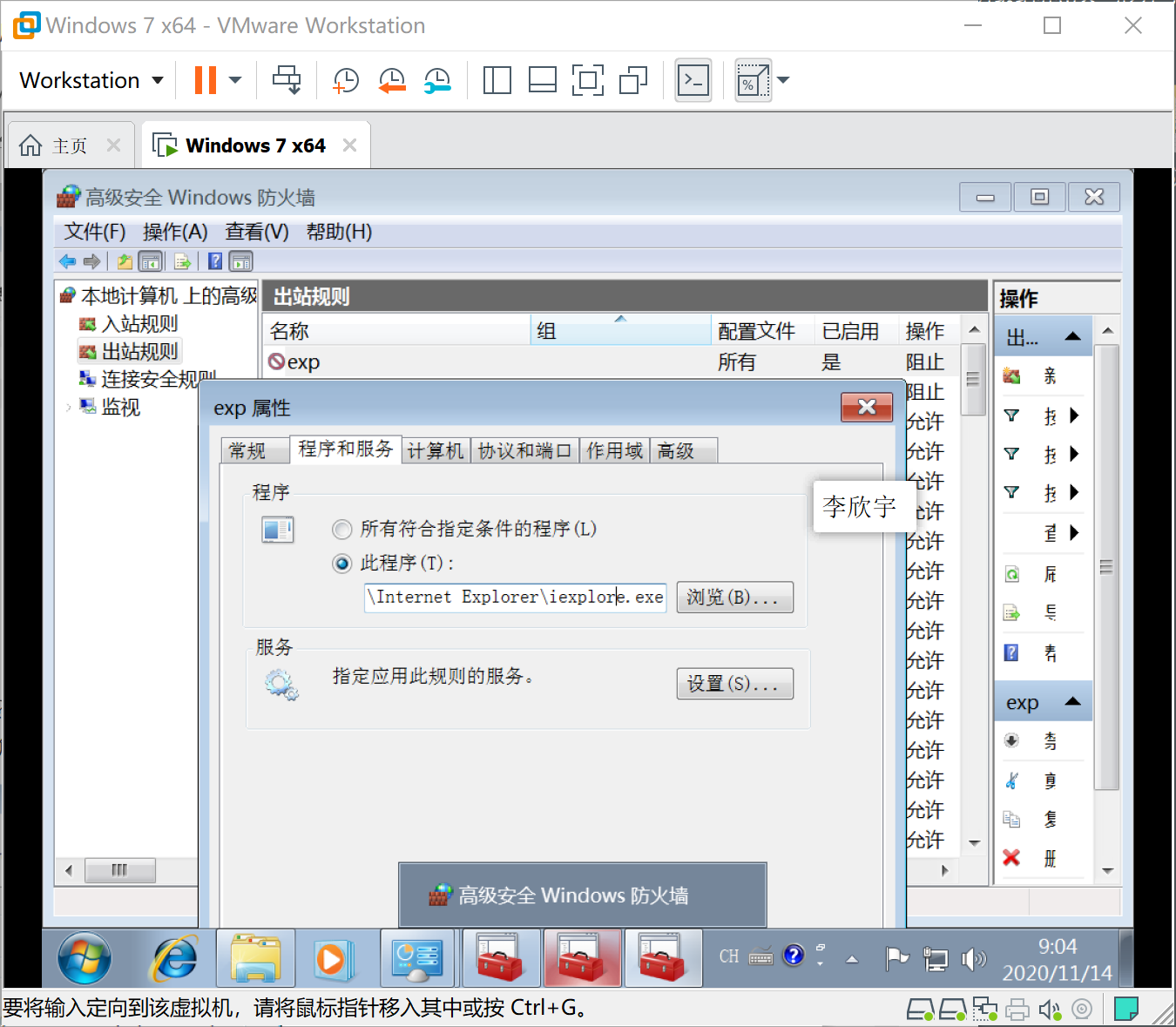


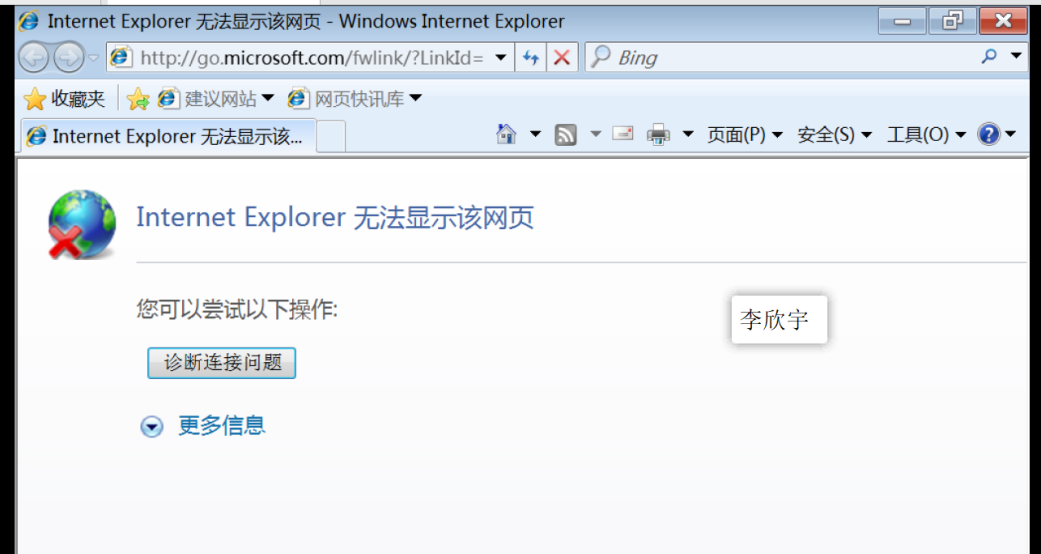


4）Ifconfig



5）添加一条高级规则中的出站规则，将浏览器禁用后，无法打开网页





### 任务2 安装Wireshark：

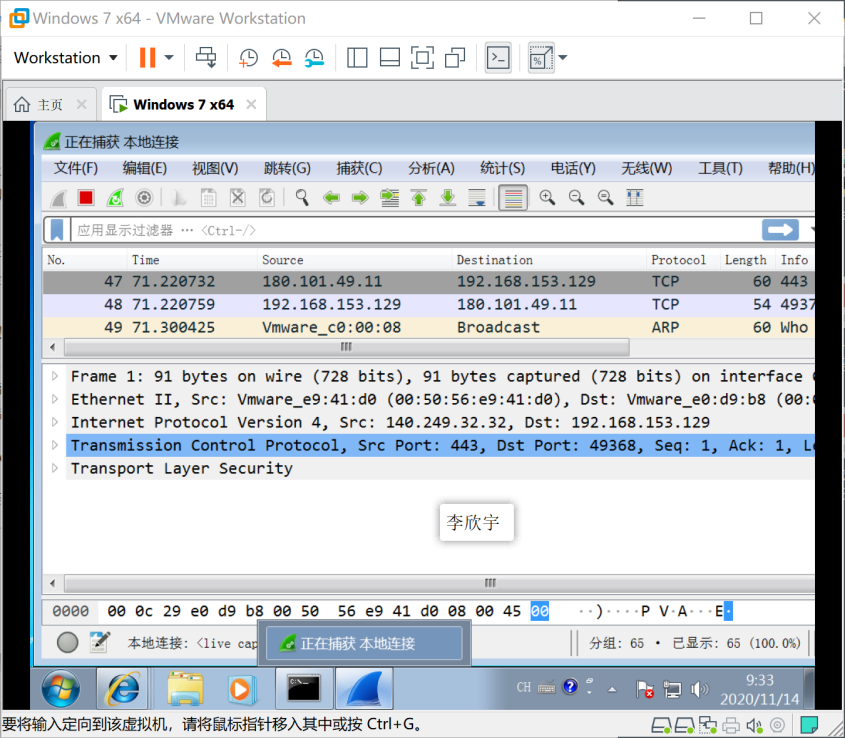
W**ireshark**是一款用途较广的网络报文分析工具。主要作用是尝试捕获网络包，并尝试显示包的尽可能详细的情况。网络管理员使用Wireshark来检测网络问题，网络安全工程师使用wireshark最新版来检查资讯安全相关问题，开发者使用Wireshark来为新的通讯协定除错，普通使用者使用Wireshark官方版来学习网络协定的相关知识。本次任务中，主要完成安装与基本的验证，后续的分级实践网络安全实验，可以使用Wireshark做网络报文的协议分析。

**注意在虚拟机中访问网络下载wireshark或者直接使用课堂提供的版本。**

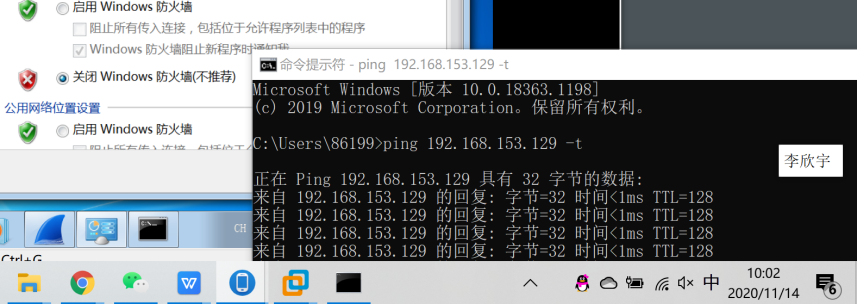
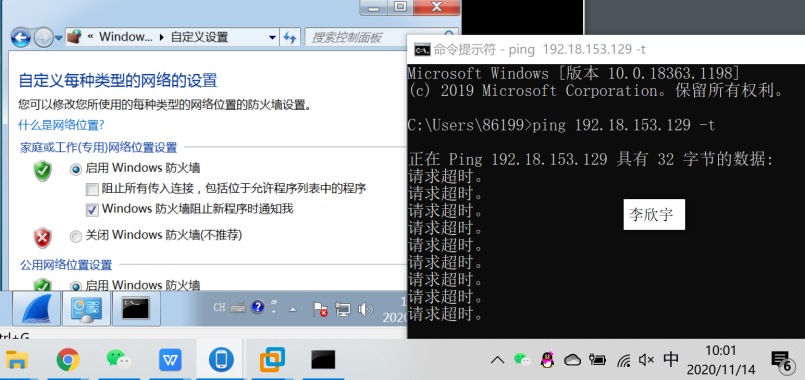
1. 打开wireshark, 选择不同的网卡，开始监听，观察监听数据结果；
2. 打开或者关闭Windows 7防火墙，同样监听，查看监听数据不同效果；
3. 在win7防火墙打开或者关闭某个应用，同样监听，查看监听数据不同效果

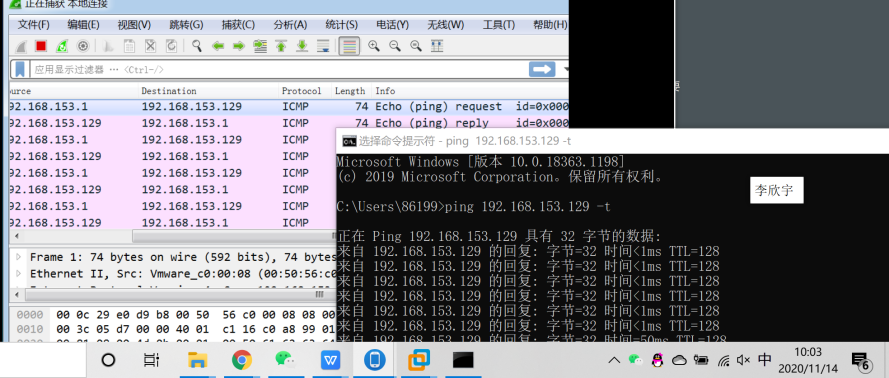
过程记录：

1）

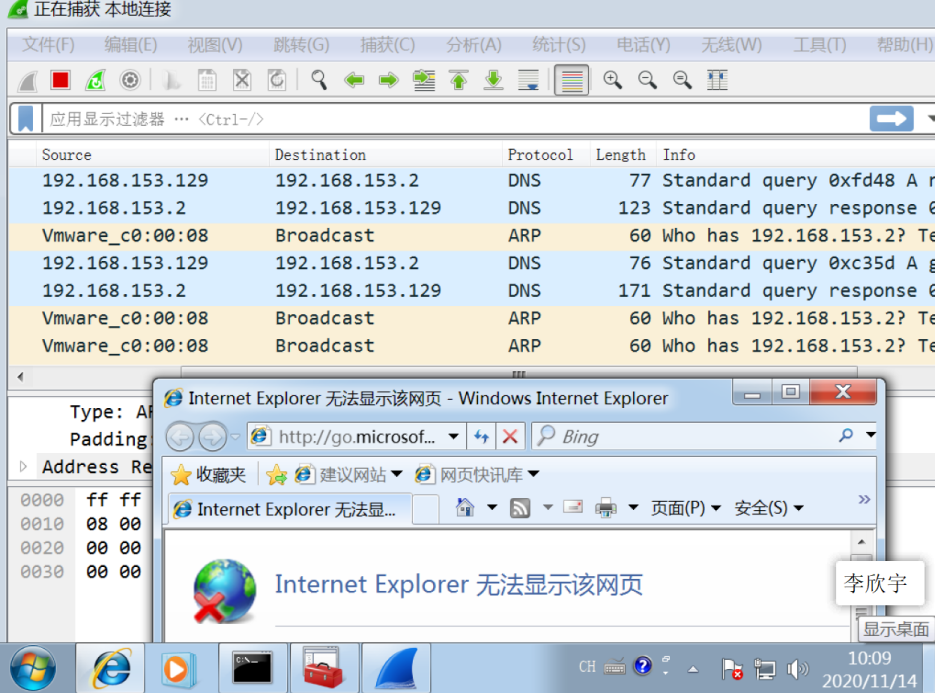


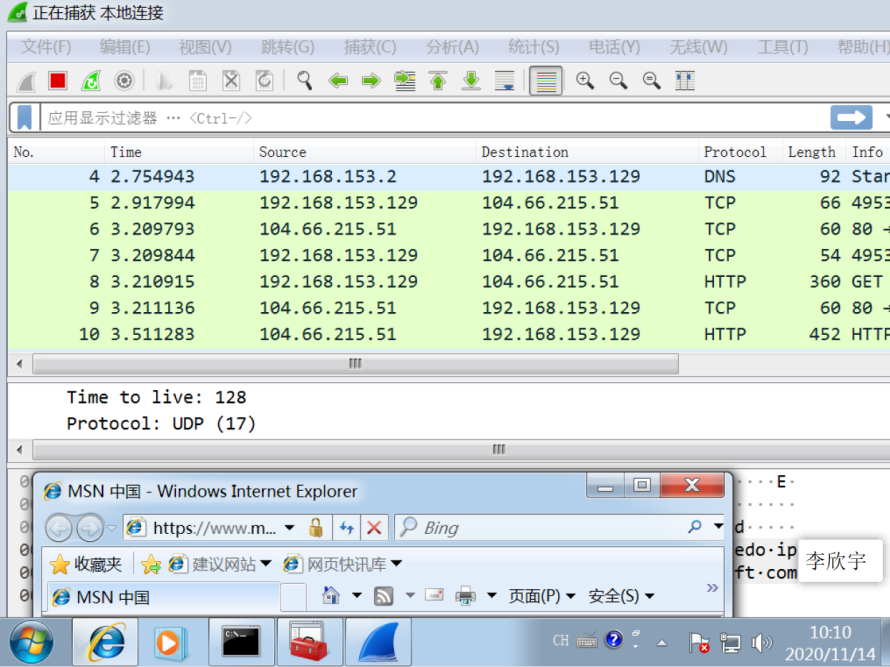
2）打开防火墙在宿主机不能ping通虚拟机的ip，关闭防火墙可以在宿主机下ping通虚拟机的ip





3）对ie浏览器限制出站与不限制出站





### 任务3 基础windows开发环境VC++6或者VS2010

VC6/VS2010是Windows操作系统中比较普及的开发工具，后续实践中需要通过开发工具调试代码体验Windows系统中的比如进程、线程、网络连接的基本知识。本次任务中，主要完成安装与基本调试编译的验证。

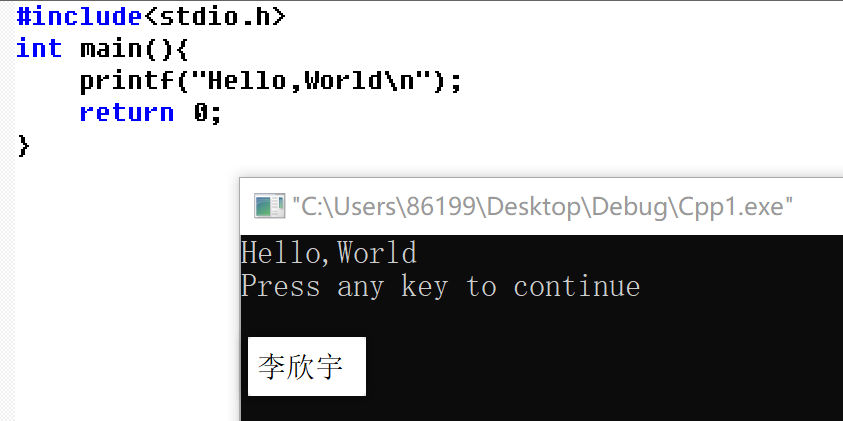
**在虚拟机中访问网络下载VC6或者VS2010,注意同时下载补丁包vcpp5与vs6SP5,VS2010 SP1，其中VC6(含SP5)比较精简，但可能在部分系统中存在兼容性问题，VS2010体积比较大，但是在Windows系统中兼容性较好，可以根据自己的情况灵活选择，只需要安装并使用其中一套。**

1. 安装完成后，打开VC6/VS2010并编写一个基本的控制台程序，打印HelloWord.
2. 新建一个MFC对话框程序，按照向导一步一步完成后编译运行。
3. 尝试再对话框上添加一个按钮，双击该按钮，再对应代码处弹出消息提示框MessageBox(“0”,”测试”,0)。

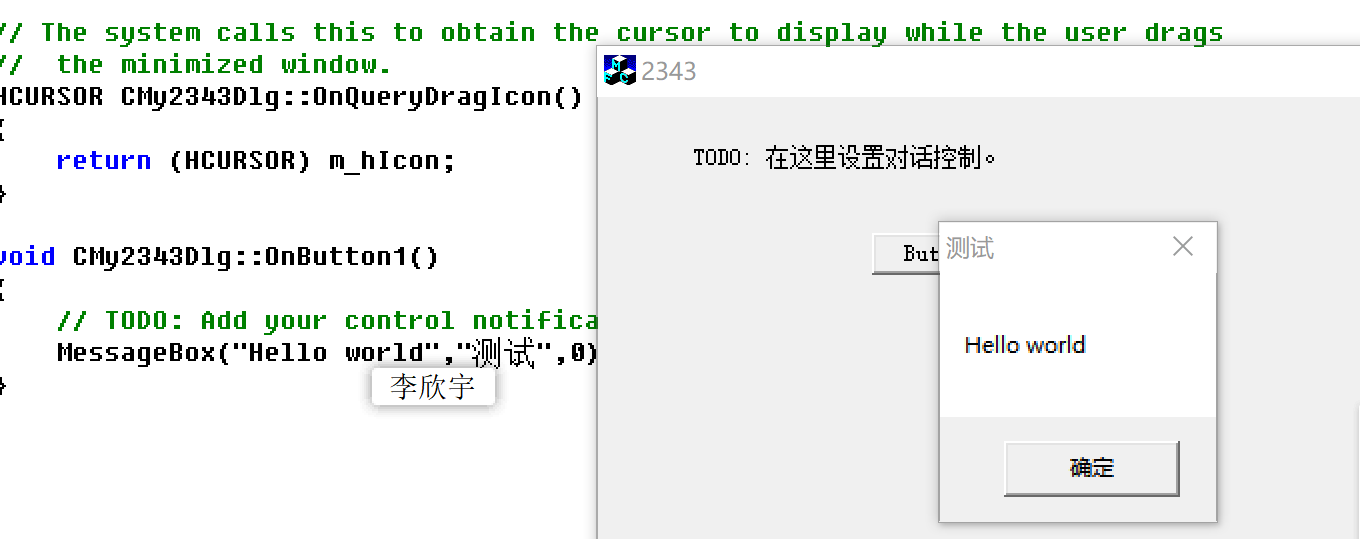
VC6与VS2010生成测试程序的过程请参考教学视频

**过程记录：**

1）使用VC6实现



2） 添加一个按钮，使用语句MessageBox（“Hello World”，“测试”，0）；实现



### 任务4 phpstudy安装

PhpStudy是一个PHP调试环境的程序集成包。该程序包集成最新的[Apache](https://baike.baidu.com/item/Apache" \t "_blank)+[PHP](https://baike.baidu.com/item/PHP" \t "_blank)+MySQL+ [phpMyAdmin](https://baike.baidu.com/item/phpMyAdmin" \t "_blank)+[ZendOptimizer](https://baike.baidu.com/item/ZendOptimizer" \t "_blank),一次性安装,无须配置即可使用,是非常方便、好用的PHP调试环境.该程序不仅包括PHP调试环境,还包括了开发工具、开发手册等。学习PHP只需一个包。该程序包的安装主要为后面的DVWA提供运行环境。

**在[www.phpstudy.net下载phpstudy](http://www.phpstudy.net下载phpstudy)8.1 ,解压缩后安装。**

注意:安装路径不能包含“中文”或者“空格”，否则会报错（例如错误提示：Can't change dir to 'G:\\x65b0\x5efa\x6587\）；保证安装路径是纯净的，安装路径下不能有已安装的V8版本，若重新安装，请选择其它路径

1. 启动Apache Web服务器与MySQL数据库服务。windows防火墙会阻止apache HTTP Server与MySQLD服务选择运行访问，只需要确认允许访问即可。
2. 访问<http://127.0.0.1/>，检查网页是否可以正常打开。
3. 进入数据库界面，点击操作修改密码，输入数据库新密码。
4. 进入数据安装目录，phpstudy\_pro\Extensions\MySQL5.7.26\bin。
5. 执行mysql –uroot –p新密码
6. 检查是否正常显示mysql>
7. 输入查询语句show databases; 查看系统中安装的数据库。至此，数据库安装基本完成。

过程记录：

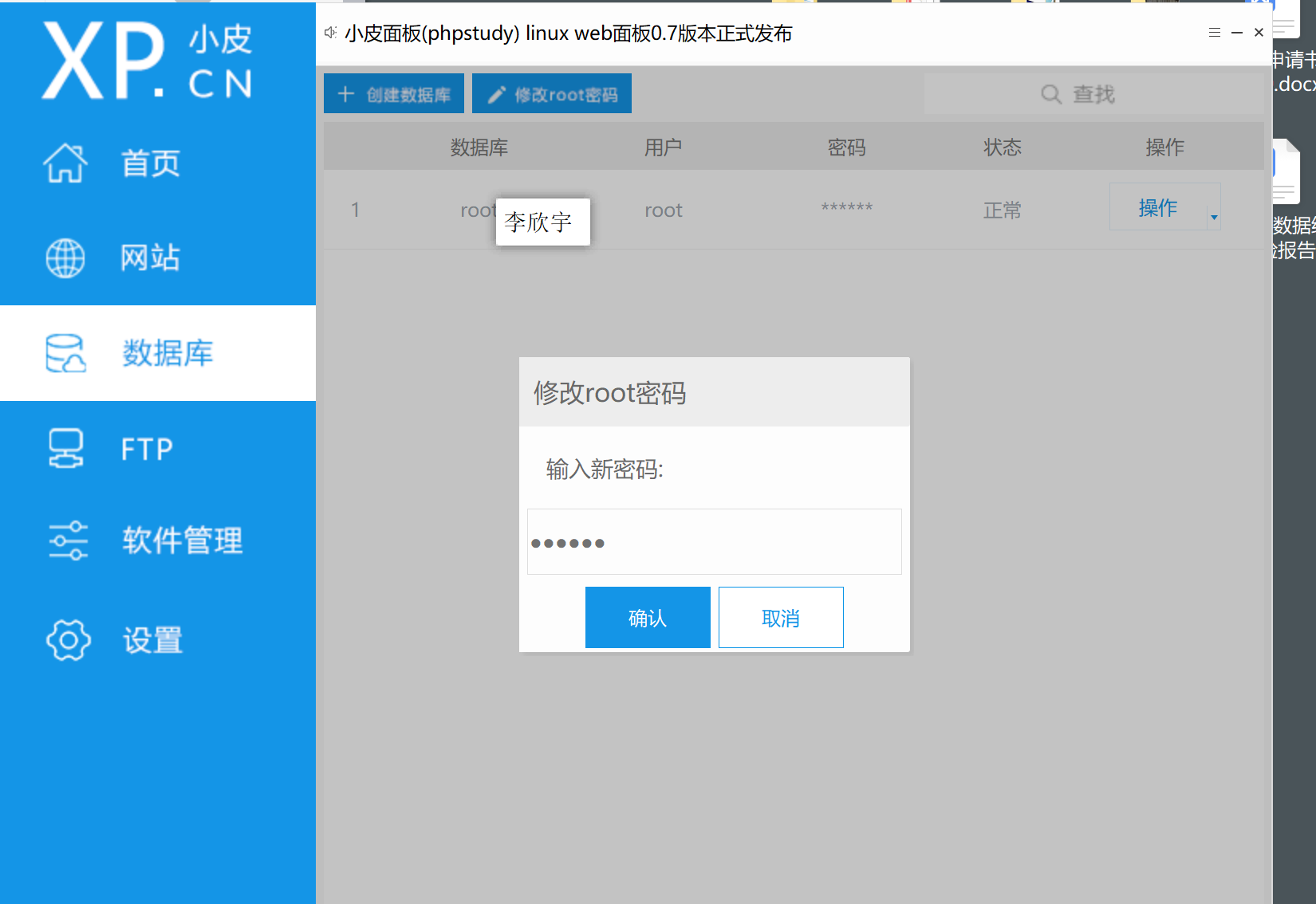
1）启动Apache Web服务器与MySQL数据库服务



2)访问<http://127.0.0.1/>

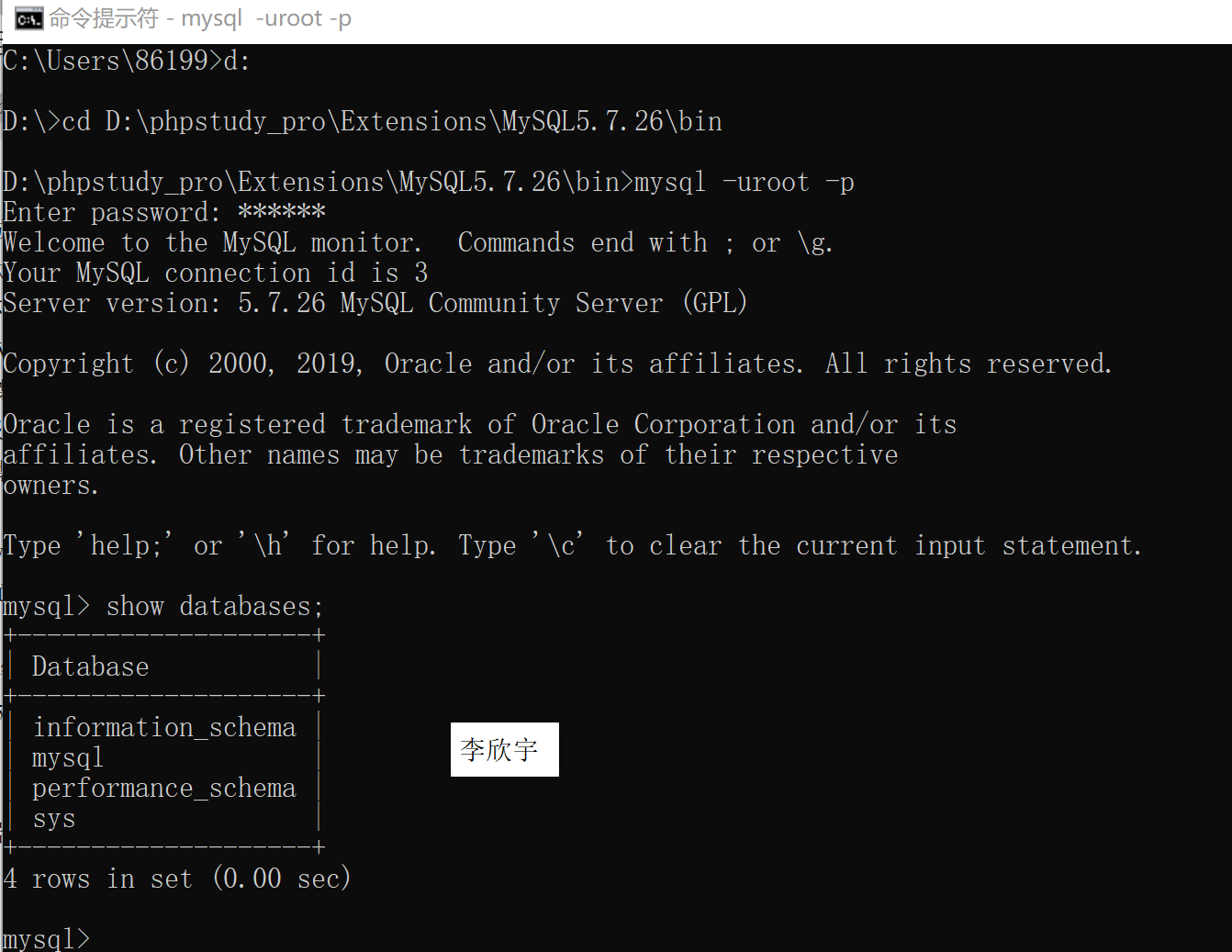


3)修改数据库密码



4）进入bin目录下，执行mysql –uroot –p 新密码

输入查询语句show databases; 查看系统中安装的数据库。



### 任务5 DVWA安装

[DVWA（Damn Vulnerable Web Application）](https://link.zhihu.com/?target=http%3A//www.dvwa.co.uk/" \t "_blank)是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。安装DVWA将用于分级实践后续的比如Web安全SQL注入提供一个学习与练习平台。本次实验要求完成安装，并按照实验步骤验证工作状态正常。

**进入<http://www.dvwa.co.uk/>下载DVWA(Damn Vulnerable Web App)**

1）打开phpstudy\_pro,查看网站的根目录。

2）将下载的压缩包解压缩到web服务器的根目录(比如：C:\phpstudy\_pro\WWW)。

3）在config目录config.inc.php.dist 改名为config.inc.php是修改数据库的配置文件，默认安装phpstudy情况下，将配置文件中$\_DVWA[ 'db\_password' ] = 'p@ssw0rd';修改为'root'；修改过密码的话就修改为更改过的密码。

4）访问<http://127.0.0.1/DVWA-master/>

5）点击创建数据库会跳转到DVWA的登录界面，DVWA的默认用户名是"admin",密码“password”登录。

6）点击确认出现DVWA的欢迎界面即DVWA部署成功。

7）部分Web返回消息会出现乱码，进入\dvwa\includes 打开DVWA目录includes文件夹中dvwaPage.inc.php，将dvwaPage.inc.php中charset=utf-8全部更改为charset=gb2312然后保存。

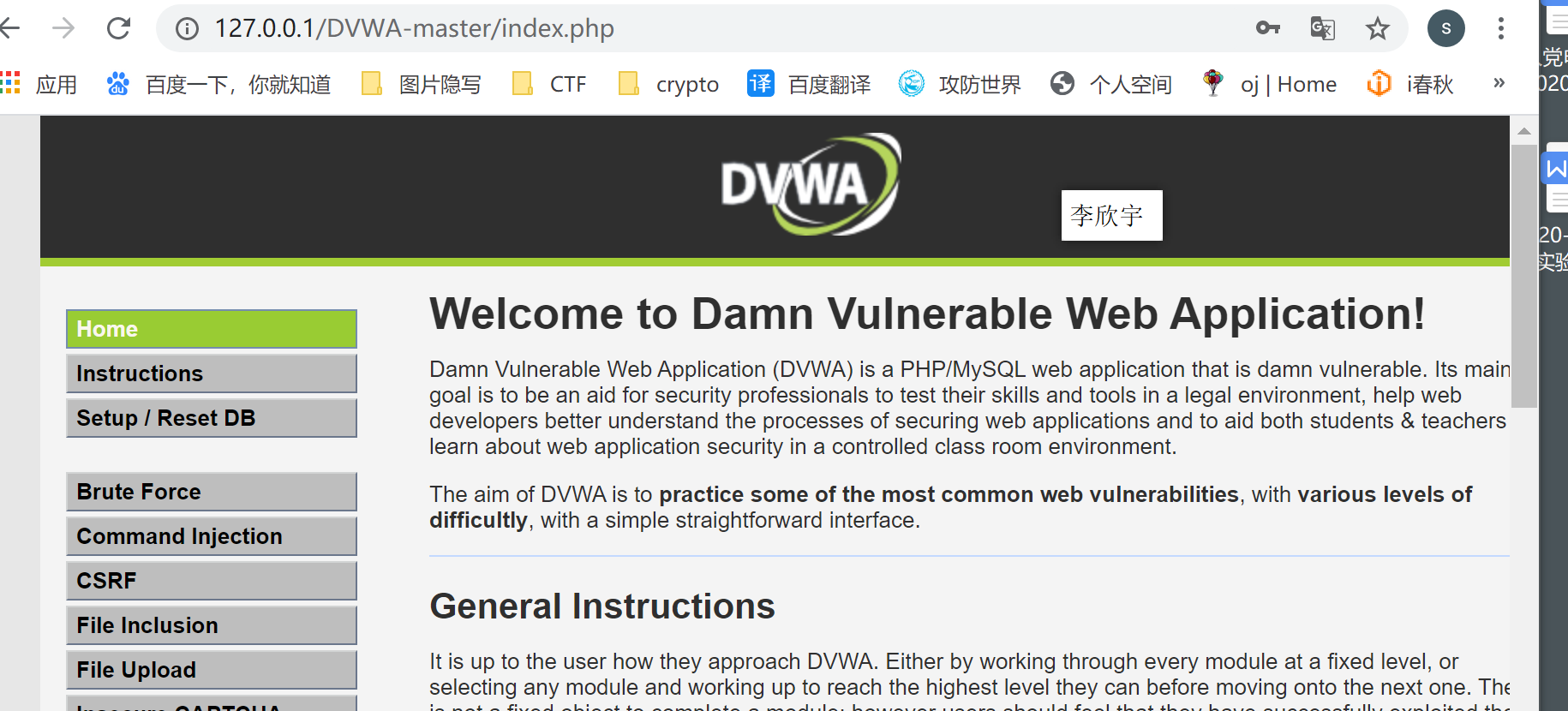
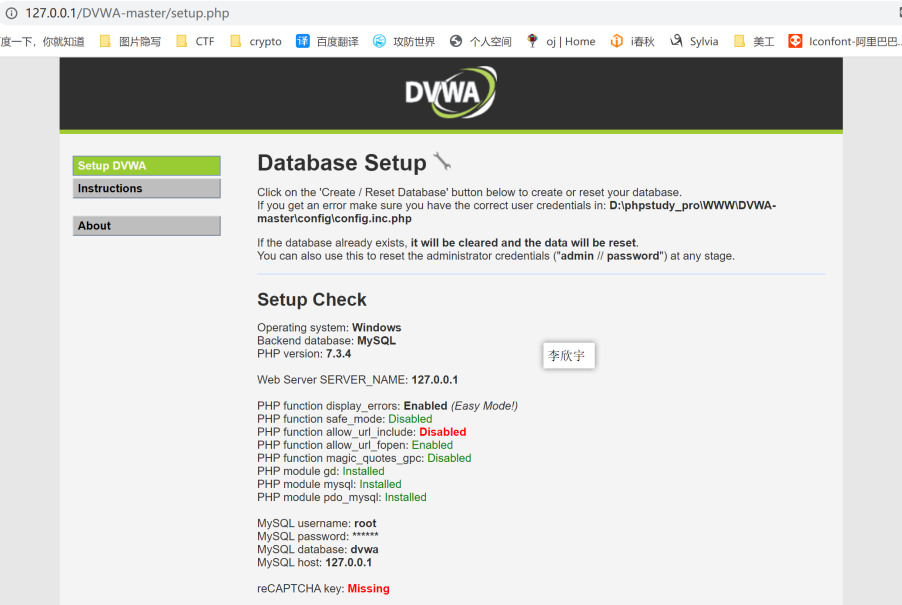
**过程记录：**

1）打开phpstudy\_pro,查看网站的根目录。



2）在config目录config.inc.php.dist 改名为config.inc.php是修改数据库的配置文件，默认安装phpstudy情况下，将配置文件中$\_DVWA[ 'db\_password' ] = 'p@ssw0rd';修改为新设置的密码![MYI}{]()3Q0BIKVK@FUEISD](data:image/png;base64,)

3）访问<http://127.0.0.1/DVWA-master/>



### 任务6 WannaCry勒索病毒测试与分析

此任务为突发任务，作为技术新手，主管将截获的病毒样本下发，要求采用虚拟机对其进行测试分析，找到其尽可能多的行为特征。但注意不能对外产生破坏作用。将自己分析的病毒行为截图，分析其可能的意图，并提出防御措施。

病毒样本已经作为压缩包拷贝到桌面。思考：测试前需要做哪些准备工作？

1. 检查防火墙是否打开。
2. 虚拟机做镜像备份。
3. 解压缩病毒压缩包。
4. 提取出WannaCry病毒。
5. 与同学讨论确认，是否做好准备工作。
6. 点击运行WannaCry病毒。
7. 分析WannaCry带来的系统变化。
8. 以某个已经被加密的doc文件为例，分析如何在没有解密程序的情况下，如何恢复该文件。
9. 恢复系统。
10. 多次恢复与运行病毒，对比测试系统变化，考虑：
11. 在系统增加了什么文件？
12. 对文件夹下面的文件做了什么操作？对哪些类型的文件做了修改？
13. 其它。比如是否对注册表做了修改等。

11）以自己提出的数据恢复方案，测试数据恢复的有效性。

12）完成课程平台思考题。

过程记录：

1）检查防火墙，做镜像备份，解压释放病毒

2）运行病毒



3）在运行wannacry后，照片，文件、压缩包等几乎所有类型的文件都变成了以WNCRY为扩展名的加密文件。在%TMP%下有很多WNCRY为扩展名的文件



4）

①对于存于c盘下（除桌面）小概率可恢复，使用数据恢复软件恢复出来的数据也是WNCRYT格式的文件，可以使用Hex查看文件头信息，根据文件头修改文件扩展名为doc，就可以恢复该文件

②对于存于非系统盘下的情况，如果磁盘有空余的情况，几乎可以100%恢复，在磁盘满的情况，只有部分文件加密，很多源文件被保留。

综上对于doc文件，存于桌面，无法恢复。存于系统盘小概率恢复，但恢复难度较大。存于其他盘容易被恢复，且可能性较高。

5）多次恢复与运行病毒，对比测试系统变化，发现在系统中增加了很多WNCRY文件，文件夹下的文件都被加密，还增加了@Please\_Read\_Me@、@wanaDecryptor@.exe文件 ，对照片、exe、压缩包、音频文件、文档、视频都进行了加密

### 扩展阅读：

请在病毒测试任务中，查找WannaCry技术分析报告，根据技术分析报告，验证真实WannaCry病毒的特征与表现。

# 小结：学习心得与体会

前期的靶机安装相对顺利，主要是学习了数据库的查看，最后浅显的了解了以下 wannacry，亲身体验了一把中病毒的感觉，查阅了很多资料，也了解到一些恢复数据的方法，对这一勒索病毒有了进一步认识，

# 参考文献：

这部分要求学生把查阅的资料整理出来，并附上pdf归档包，作为积累的内容。