“网络安全综合实验（I）”实验任务书

Windows靶机安装与验证 （第2次实验）

实验者：

指导教师：付才 陈凯 刘铭 王美珍 肖凌

2020年11月

# 目　录

[目　录 I](#_Toc55812613)

[1 实验一：Win7靶机安装与测试 1](#_Toc55812614)

[1.1 实验环境及要求 1](#_Toc55812615)

[1.2 实验任务（共6个小任务关卡） 2](#_Toc55812616)

[2 小结：学习心得与体会 5](#_Toc55812617)

[参考文献： 6](#_Toc55812618)

# 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）**：

结合网络教学的实践课程，靶机安装与使用作为一项基本技能，本实验要求每位同学独立完成，可以与小组成员讨论。

**参考资料**：VMWare使用帮助、其他在线文档资源。

**最终提交文档及写作要求**：Win7靶机安装与测试相关内容，独立实验报告电子版一份，按指导老师要求提交。文件统一用docx文档，文件名：U2018XXXX（学号）-姓名-网络安全综合实验（I）。格式以当前指导书为准模板：正文小4号，仿宋字体，段首缩进2字符汉字，图保证清晰大小合适、每页尽量不留大段空白。

**文档中包含内容**：1.封面首页信息及作者、完成时间 2.目录 3.完成任务的过程，可在任务书基础上进行改写，补全主要截图及相应的过程说明文字4.小结：总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议 5.实验中查阅资料的页码、网址作为参考文献部分列表给出 6.参考资料通过浏览器的打印功能，以pdf文件方式保存，归档为：参考资料.zip，与报告一并提交。

**本次实验结束后，在一周之内提交本次实验的截图与说明，建议大家提交完整电子版报告。**

**虚拟机用户名**：

Windows 7虚拟机：用户名win7\_XXXX 口令：XXXX(XXXX为姓名全拼)

**场景设置：**

2021年夏天，你入职了一个网络安全公司，需要进行基础安全技能学习，并尝试对最近发生的Wannary病毒安全事件的样本分析。主要通过安装靶机进行。你需要掌握哪些技能呢？

根据场景，需要你完成以下操作，作为Windows基本操作实验通关考核。请你完成靶机安装与测试，遇到问题可以与其他同学讨论，各自保留实验中的完整虚拟机截图，遇到问题，寻找解决方案，并做好记录，最后，将通关过程、记录的文字，整理成报告提交。

## 实验任务（共6个小任务关卡）

### 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。

### 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

### 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)。

### 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)+[PHP](https://baike.baidu.com/item/PHP)+MySQL+ [phpMyAdmin](https://baike.baidu.com/item/phpMyAdmin)+[ZendOptimizer](https://baike.baidu.com/item/ZendOptimizer),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。

### 任务5 DVWA安装

[DVWA（Damn Vulnerable Web Application）](https://link.zhihu.com/?target=http%3A//www.dvwa.co.uk/)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/**](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。

### 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。

### 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

学生自己总结本次实验的内容，心得体会，意见和建议。

# 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。