

“网络安全综合实验（I）”实验报告

**题目： Linux主机基础实验**

院 系 网络空间安全学院

专业班级 xxxx

姓 名 xxx

学 号 xxxxx

日 期 2021 年 05 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | Linux主机基础实验报告评分  （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： xxx 学号： xxxxx

你给同组人评价： 优 （优 良 中 及格）；

理由： xxxx对于Linux的操作接触的比我更早，对于一些常用命令比较熟悉，配置网络地址的相关操作也很熟练，给了我很大帮助。同时，他善于去搜索、查阅资料，来解决他遇到的Linux操作问题。

# 

# Linux主机基础实验

## 实验环境及要求

### 实验平台及说明

虚拟机：Vmware 15或者VirtualBox；

操作系统：虚拟机内安装kali Linux；

其他配置：虚拟机IP 192.168.242.135；

截图说明：姓名和日期、时间在截图顶部，日期、时间格式为：xx日-xx月， xx时：xx分

**实验分组**

本实验2人一组，同组成员： xxxx 、 xxxxx ；

### 实验场景设置

2021年夏天，你入职了一个为“银河”机场提供数据服务的互联网公司，负责一台Linux服务器的维护工作。该公司的服务器上，保存机场进出航班的数据生产系统，并为各类订票公司客户的订票系统，提供信息接入服务。

你进入Linux系统后，首先查看系统中的目录结构、文件、服务情况；并在自己的工作目录下，建立两个子目录，分别保存自己编写的C语言代码和python语言代码；一个月之后，公司给你介绍新来的实习生Bob（由你的同组同学担任）。你需要在你负责的服务器上也给Bob建立一个工作目录，而后面工作中，为了你与Bob共同完成任务，需要让Bob能访问你的目录下的某些文件，合作开发一个helloworld项目。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Linux基本操作实验通关考核。请和你的同组伙伴一起完成，遇到问题，可以用即时通讯工具进行讨论、查阅资料；

## 过程记录/实验任务（共8个任务，20个小关卡）

## 任务1 我的世界Minecraft

**了解自己的工作环境** ：

进入终端模拟器，在$提示符下，运行并熟悉命令：pwd、ls、cd、man、clear、who、mkdir、cp；

1. 请列出当前目录下所有文件，并带详细信息列表；

**解答：**

执行ls -al命令，如图1-1所示。

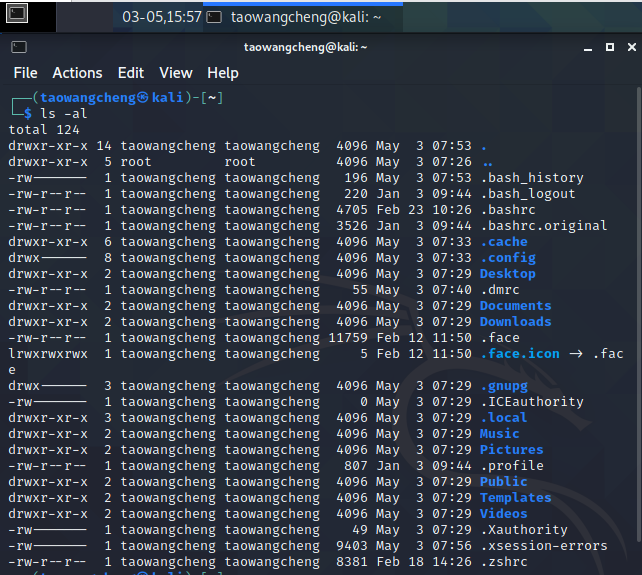


图1-1 任务1关卡1 ls命令的截图

1. 打印当前工作目录；

**解答：**

执行pwd命令，如图1-2所示。

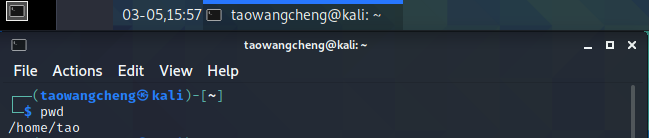


图1-2 任务1关卡2 pwd命令的截图

1. 查询关于命令ls的联机帮助信息；

**解答：**

执行man ls 命令，如图1-3所示。

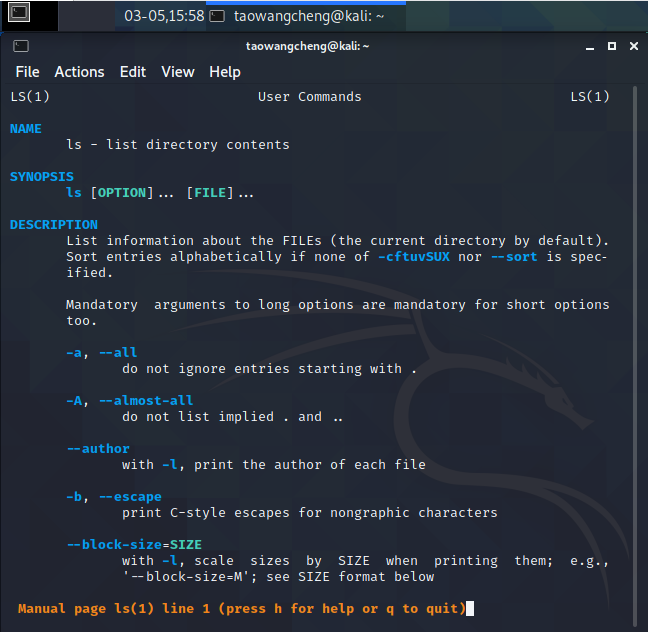


图1-3 任务1关卡3 man命令的截图

4) 查询目前系统中在线用户；

**解答：**

执行who命令，如图1-4所示。

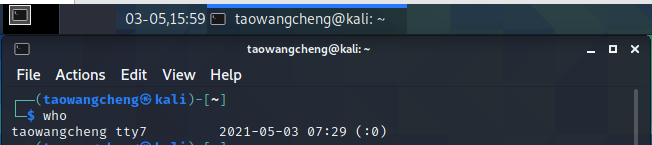


图1-4 任务1关卡4 who命令的截图

## 任务2 盖茨的车库：

**完成‘kali你好’的编程**：

5) 使用C语言完成任务：使用vi/vim，编写简单C程序，编译并运行，讲提示字符串到屏幕：Hello kali，I’m XXXX；

**解答：**

（a）先在当前用户主目录/home/tao下执行命令mkdir lab2创建新目录lab2，执行命令cd lab2切换到lab2目录下，再执行命令vim hello\_kali.c，编写C语言程序，编写完成后保存文件并退出，如图2-1所示。

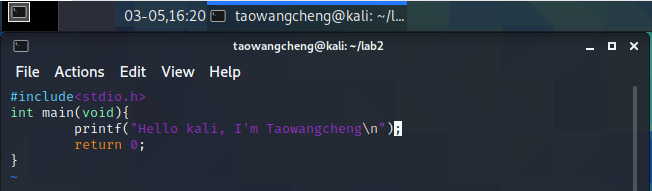


图2-1 任务2关卡5 编写C语言程序的截图

（b）执行命令gcc hello\_kali.c -o hellokali编译（a）中编写的C语言程序；再执行命令./hellokali运行编译后的程序，如图2-2所示。

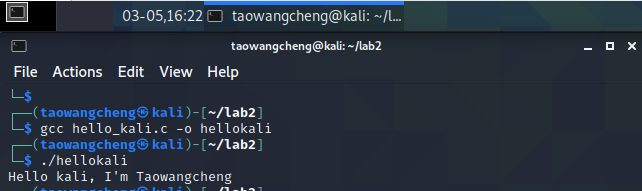
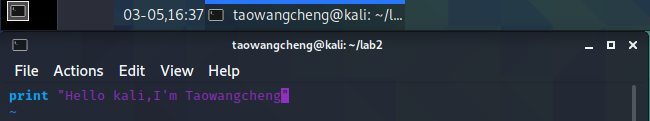


图2-2 任务2关卡5 编译并运行C语言程序的截图

6) 使用*python语言*完成5）中同样的任务。

**解答：**

（a）在lab2目录下，执行命令vim hello.py，编写python语言程序，编写完成后保存文件并退出，如图2-3所示。

图2-3 任务2关卡6 编写python语言程序的截图

（b）执行命令pyhon hello.py运行中编写的python程序，如图2-4所示。

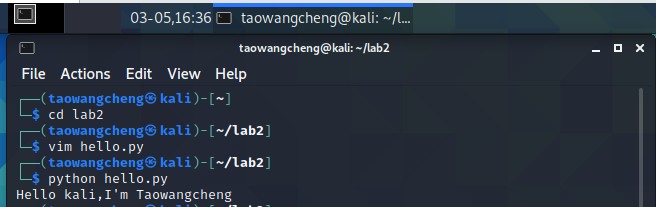


图2-4 任务2关卡6 运行python语言程序的截图

## 任务3 永远的Alice和Bob

7) 增加一个账号给同组的搭档使用。用该同学的姓名拼音作为用户名，并指定该用户的起始目录和默认shell(bash)；

**解答：**

执行命令sudo useradd -d /home/wang -m wangzhuo -s /bin/bash添加一个用户名为wangzhuo，起始目录为/home/wang，默认shell为/bin/bash的普通用户，如图3-1所示。

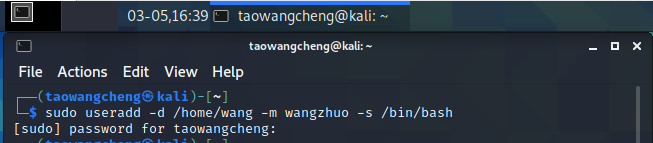


图3-1 任务3关卡7 创建新用户的截图

8) 然后为该账号指定一个初始密码；

**解答：**

在7）中创建新用户时，没有设置密码，账户处于锁定状态，此时用户账户将无法登录系统，执行命令sudo passwd wangzhuo为其设置密码，如图3-2所示。

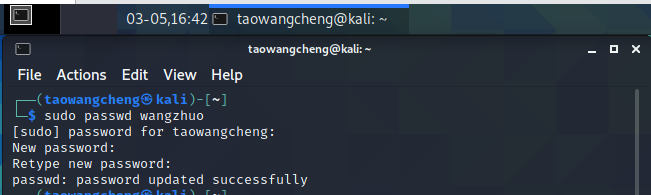


图3-2 任务3关卡8 为用户设置密码的截图

9) 查看系统中是否已经添加了该用户的信息；

**解答：**

结合管道操作实现新用户的查找，执行命令sudo cat /etc/shadow | grep wangzhuo，如图3-3所示。

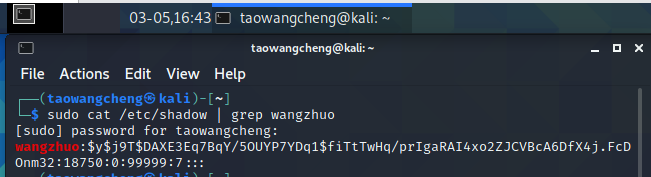


图3-3 任务3关卡9 查找新用户的截图

10) 切换到该新用户，并查看所在的目录；访问该用户的起始目录，列出所有文件详细信息；实习生自己修改密码。

**解答：**

先执行sudo su wangzhuo命令切换到新用户，执行pwd命令显示当前所在目录仍为/home/tao，执行cd ~命令访问新用户的起始目录，执行ls -al命令列出该目录下所有文件的详细信息，执行passwd命令修改密码，如图3-4所示。

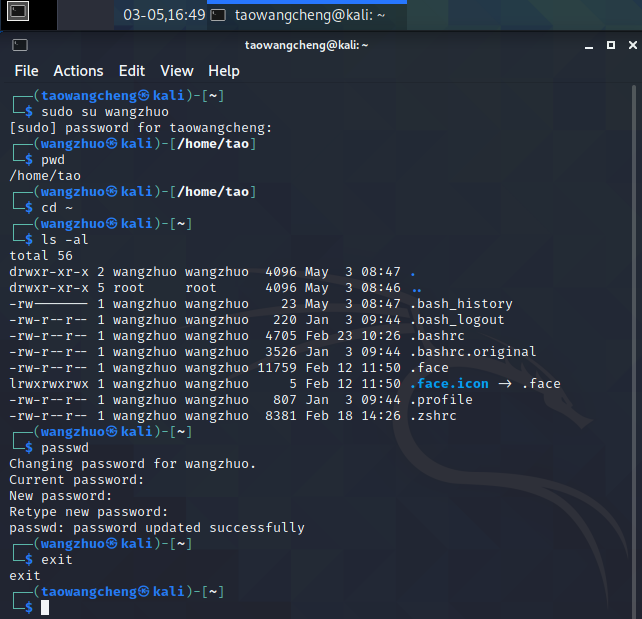


图3-4 任务3关卡10 切换新用户的截图

## 任务4 Teamwork团队协作：

11) 希望以Bob登录后，在Bob自己的工作目录下，建立一个目录，用来做项目测试，并将自己（Alice）前面编写的源程序hello\_kali.c，复制到测试目录下，改名为hello\_kali\_Bob.c；

**解答：**

以同伴身份登录系统，在起始目录下创建新目录ProjectTest,切换到新目录,并执行命令cp /home/tao/lab2/hello\_kali.c

/home/wang/ProjectTest/hello\_kali\_wang.c进行文件复制并重命名，如图4-1所示。

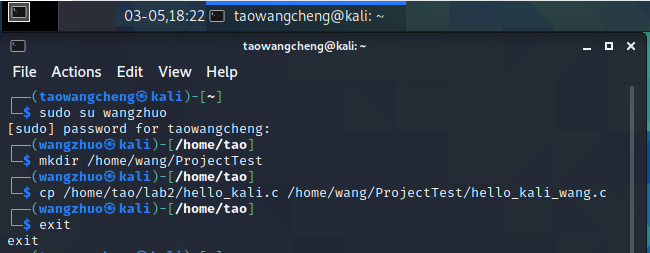


图4-1 任务4关卡11 跨用户复制文件的截图

12） 希望以Bob身份，能直接阅读、修改Alice工作目录下的源程序hello\_kali.c，增加功能，额外输出新的一行信息“I’m Bob，hi\n”；

**解答：**

（a）先以自己身份登录系统，查看同伴组，发现同伴和自己不在一个组，执行命令sudo usermod -a -G taowangcheng wangzhuo将同伴加入自己的主组。再执行命令chmod g+w ./lab2、chmod g+w ./lab2/hello\_kali.c修改lab2、hello\_klai.c两个文件的所属组权限，执行命令ls -l、ls -l ./lab2可看到修改结果,如图4-2所示。

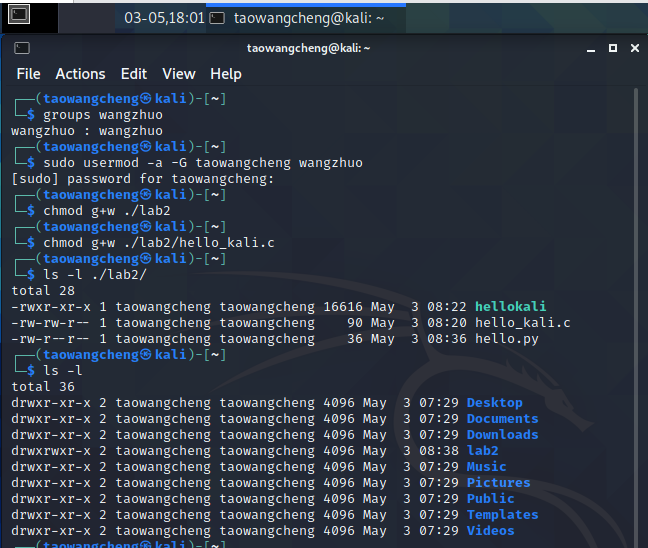
****

图4-2 任务4关卡12 修改权限的截图

（b）切换到同伴身份登录系统，执行命令echo "//I’m Wangzhuo, writing something into Taowangcheng’s file" >> ./lab2/hello\_kali.c在准备修改的文件里添加注释信息，执行命令vim ./lab2/hello\_kali.c对文件进行修改，接着执行命令gcc ./lab2/hello\_kali.c -o ./lab2/hellokali\_wang进行编译，执行命令./lab2/hellokali\_wang运行编译后的程序，如图4-3所示。

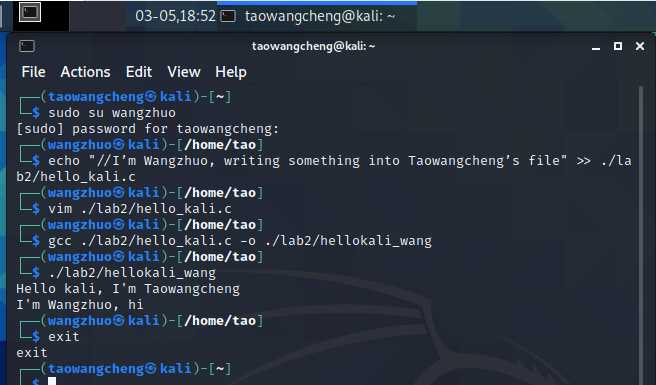
****

图4-3 任务4关卡12 修改程序的截图

（c）执行命令ln -s /home/tao/lab2/hello\_kali.c

/home/wang/ProjectTest/hello.c将自己目录下的文件共享到同伴目录下，执行命令ls -l /home/wang/ProjectTest可查看结果，如图4-4所示。

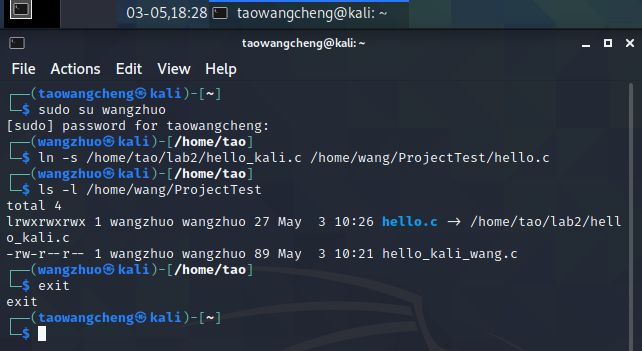
****

图4-3 任务4关卡12 创建链接的截图

## 任务5 人人都能查重：

13) Bob将自己写的源程序与Alice写的源程序进行比较，找中出不同之处；并统计源程序的字数、行数显示。

**解答：**

（a）以同伴身份登录系统，先进入项目目录，再执行命令diff hello.c hello\_kali\_wang.c进行文件内容比较，如图5-1所示。

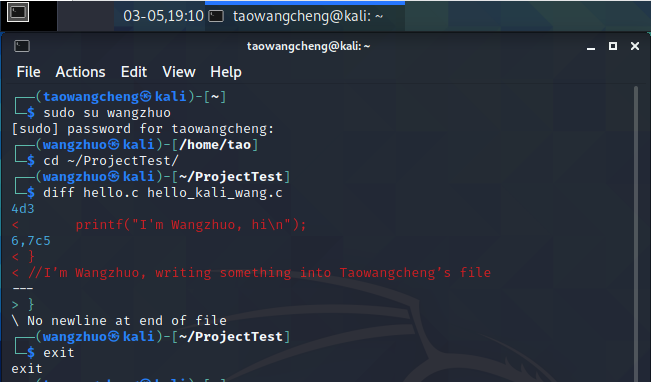


图5-1 任务5关卡13 比较不同源程序的截图

（b）以同伴身份登录系统，先进入项目目录，再执行命令wc hello.c、

wc hello\_kali\_wang.c进行文件内容统计，如图5-2所示。

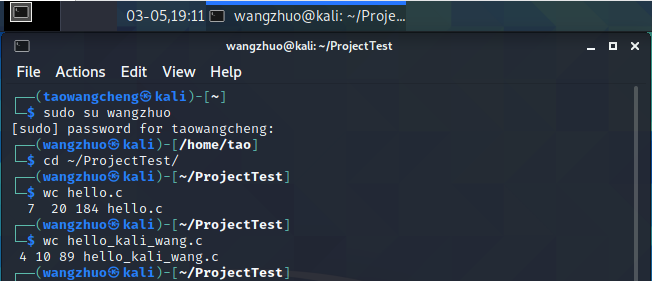


图5-2 任务5关卡13 源程序内容统计的截图

## 任务6 备份啊，当心Wannacry

14) Alice需要将自己编写的c语言源程序归档，归档文件保存为Project\_hello\_backup.tar，保存到子目录backup中；并在子目录中解压恢复。

**解答：**

（a）先在主目录下创建存放归档文件的backup目录，执行命令

tar -c -f ./backup/Project\_hello\_backup.tar ./lab2/\*.c对所有C语言源程序归档保存为backup目录下的Project\_hello\_backup.tar文件，进入backup目录，执行ls命令检查结果，如图6-1所示。

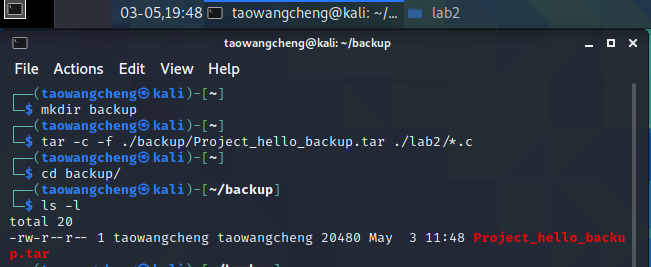


图6-1 任务6关卡14 压缩的截图

（b）再执行命令tar -x -f Project\_hello\_backup.tar对打包文件进行解压缩，执行ls 命令检查结果，如图6-2所示。

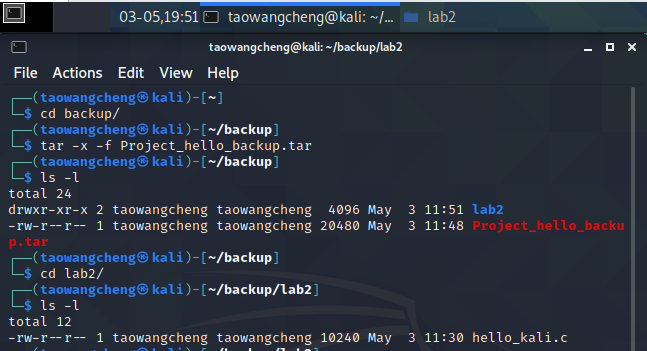


图6-2 任务6关卡14 解压缩的截图

## 任务7 我的地盘我做主My place, My rules

15）我的地盘我做主：作为Linux服务器的系统管理员，请查看目前服务器上安装好的各种服务程序的状态信息；了解目前系统中运行的程序是否有mysql，apache2、ssh服务；

**解答：**

执行命令systemctl status mysql apache2 ssh，检查结果发现目前三个服务都没有运行，如图7-1所示。

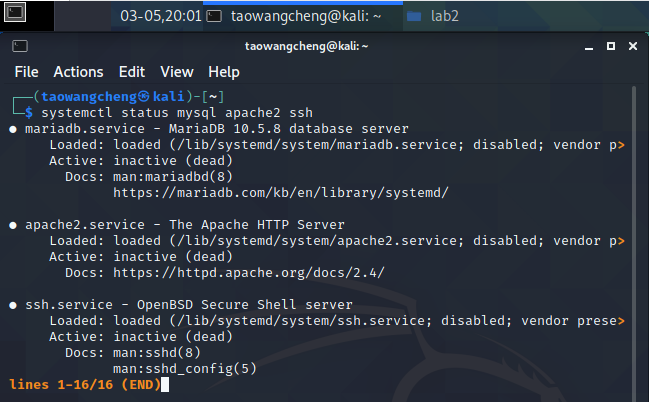
****

图7-1 任务7关卡15 查看服务状态的截图

16）尝试开启ssh服务并从host主机通过PuTTY访问kali服务器；

**解答：**

（a）先在kali上执行命令sudo systemctl start ssh启动ssh服务，再执行命令systemctl status ssh检查ssh服务运行状态，如图7-2所示。

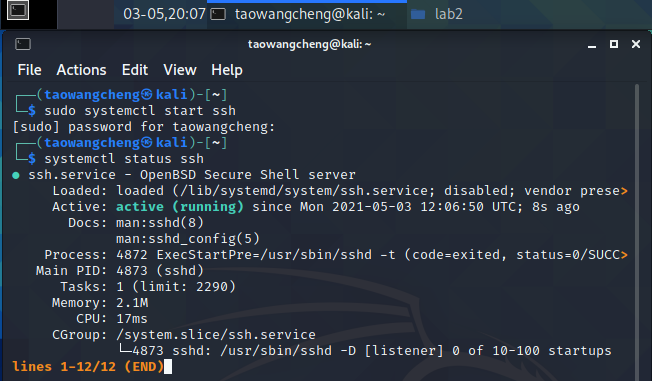


图7-2 任务7关卡16启动ssh服务的截图

（b）再打开PuTTY加载配置，访问kali虚拟机，如图7-3所示。

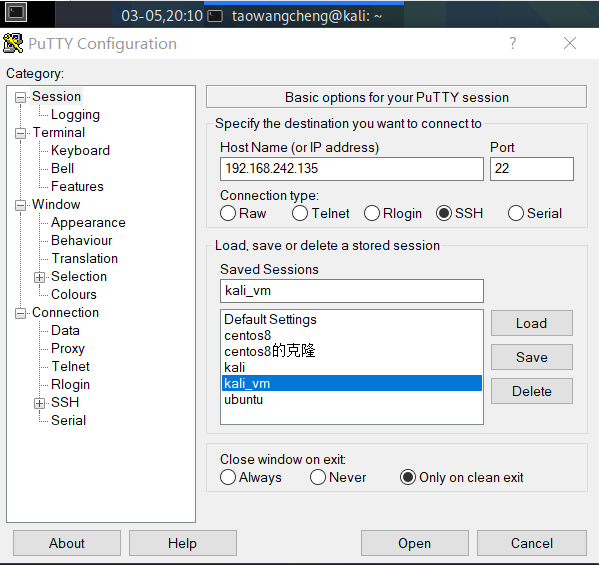


图7-3 任务7关卡16 加载PuTTY配置的截图

（c）输入用户名和密码后成功访问kali虚拟机，如图7-4所示。

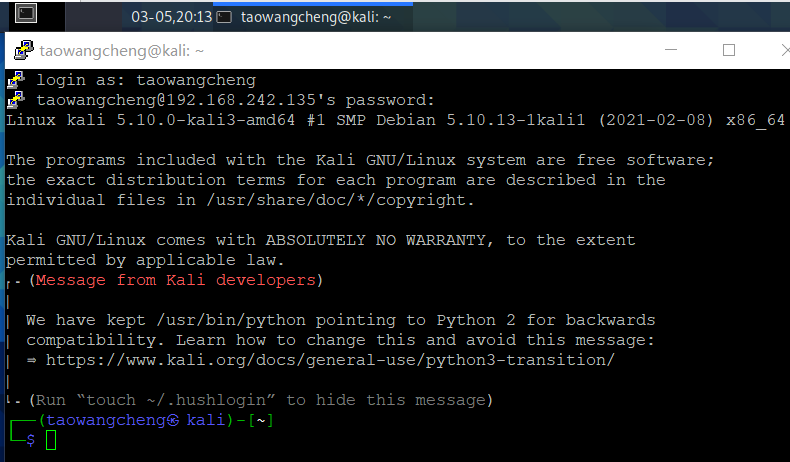


图7-4 任务7关卡16 访问kali虚拟机的截图

17）尝试开启apache2服务。

**解答：**

先执行命令sudo systemctl start apache2启动apache2服务，再执行命令systemctl status apache2检查apache2服务运行状态，如图7-5所示。

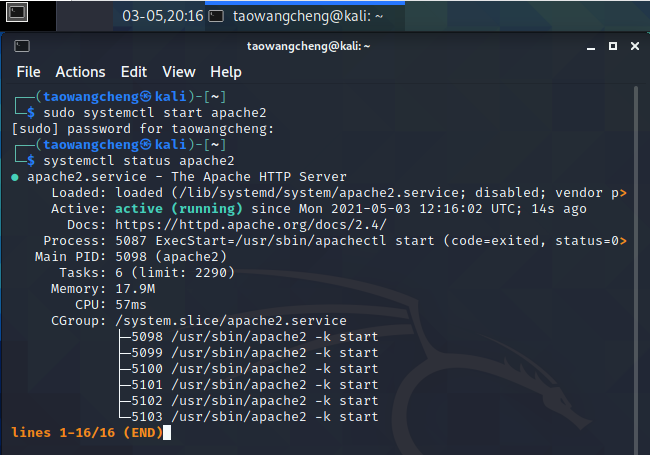
**

图7-5 任务7关卡17启动apache2服务的截图

18）问题：apache2服务如果已经开启了，可以通过浏览器访问，并打开首页index.html。该页面在kali Linux服务器的哪个目录里，请填写文件路径： /var/www/html/index.html；

**解答：**

打开浏览器，输入localhost/index.html访问首页，如图7-6所示。

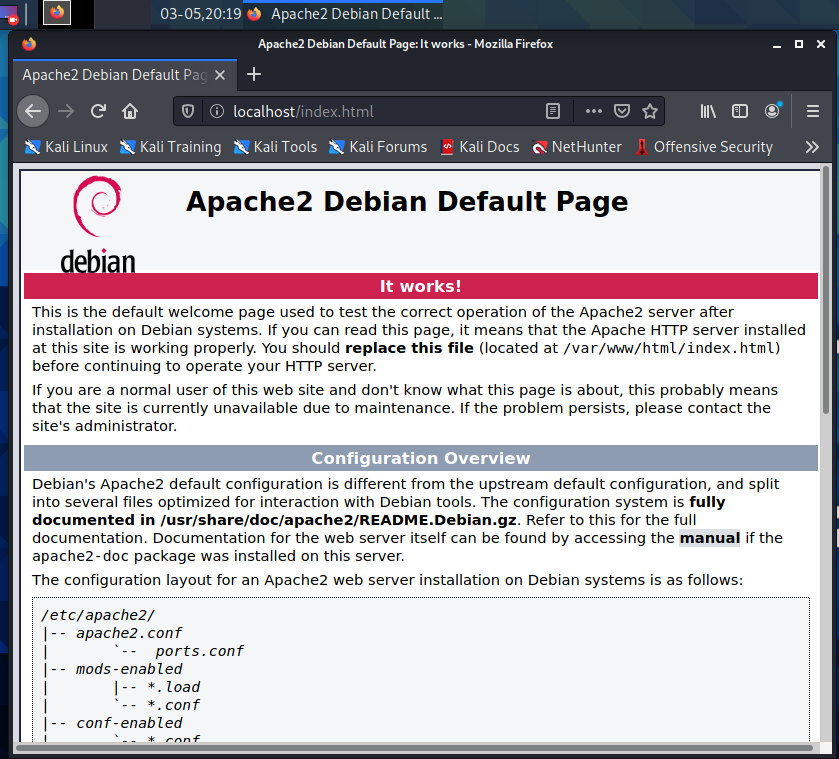


图7-6 任务7关卡18访问apache2首页的截图

## 任务8 Skywalker Vs. Yoda

19）创新设计：一年后，你将在公司里带新的成员了。请你运用Linux基础命令中的内容，查阅Linux相关资料，设计某个情景下的新关卡，用来检验新成员的Linux功底；如果关卡比较难，可以设置适当的提示信息，在合适的通关时间节点，提供给参与通关的成员。

**解答：**

备份是Linux系统管理员最重要的日常管理工作之一，以便将数据恢复到事故发生之前的状态。为了保证“银河”机场数据的完整性， Yoda让Luke Skywalker每天早上6:25都要对Apache2服务器的配置文件进行一次Full Backup。而Luke Skywalker和Mara Jade Skywalker相约“五一”假期去“天湖”风景区游玩，Luke Skywalker该怎么办呢？（通过自动化任务配置实现自动备份）

20）新关卡拟好后，给你的同组搭档通关尝试，请你的搭档将过程截图记录后，发给你并加入实验报告中。

**解答：**

（a）编写Shell脚本执行备份操作，如图8-1所示。

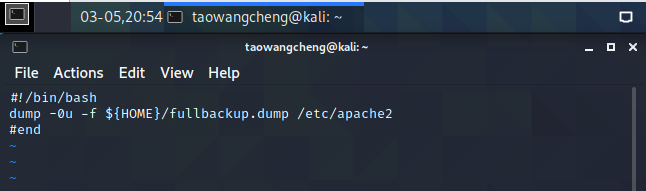


图8-1 任务8关卡20 编写Shell脚本的截图

（b）执行命令sudo vim /etc/crontab对Cron服务进行配置，发现配置已经完成，如图8-2所示。

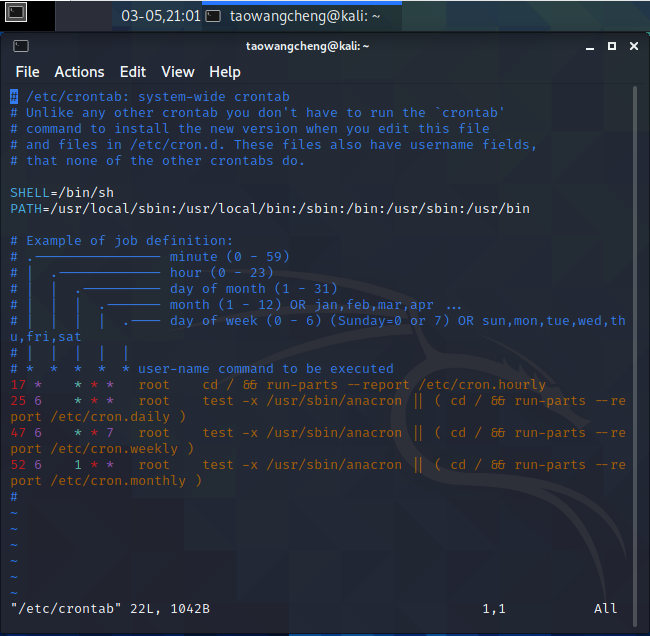


图8-2 任务8关卡20 配置Cron服务的截图

（c）将编写的Shell脚本移动到/etc/cron.daily目录下，并执行ls命令检查，如图8-3所示。

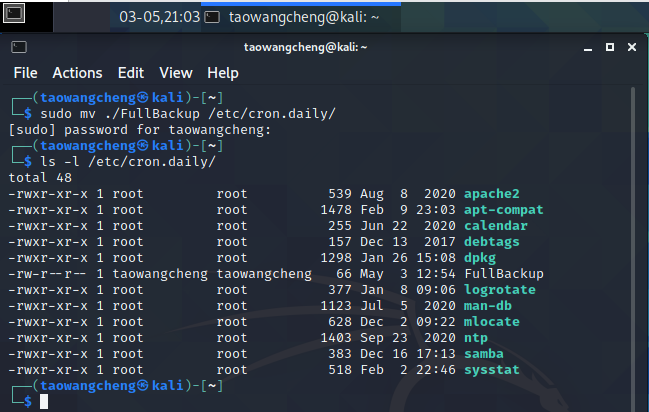


图8-3 任务8关卡20 任务调度的截图

## 扩展阅读

*1) 阅读*[*kali linux参考资料*](file:///C:\Users\liumi\AppData\Roaming\Microsoft\Word\1%20linux%20使用\Kali-Linux-Revealed-1st-edition.pdf)*，了解kali的功能；*

*2) 了解有关用户管理方面的信息，特别是用户、组、密码存放文件、进行资料搜集和总结；*

*3) 了解有关进程列表及管理、网络端口状态查看、ip地址配置的命令，比如ps、service、netsate、ifconfig；*

*4) 了解vim编辑工具的简单使用；*

*5) 通过开启ssh服务、选择虚拟机的IP配置与host主机在同一网段后，通过putty工具能远程访问虚拟机；*

*6) 了解对称密码、非对称密码、单向散列函数的知识，比如DES、AES、RSA、MD5;*

*7) 在kali中第一次使用sudo命令后，系统提示信息带来的启发*

## 实验问题分析与总结

## 实验任务小结：

（1）Linux命令行使用

主要内容：任务一主要学会Linux命令行使用，熟悉pwd、ls、cd、man、clear、who、mkdir、cp等常见命令的使用，以及各命令相关选项的作用。

关键分析：要熟练掌握Linux命令行操作，多多实践是关键。

经验总结：Linux命令行基本格式为：提示符 命令 选项 参数。

（2）用户与组管理

主要内容：任务三涉及添加用户账户的操作，任务四涉及管理组成员的操作。此外，还有删除用户账户、创建组账户等操作，也有相应的图形化配置管理工具来进行用户与组管理，有关用户与组管理的更多内容请参考[1]32-46页。

关键分析：具有最高权限的root账户可以对系统进行任何操作，这对于系统安全性可能有很大威胁。Kali Linux默认禁用root账户，但需要root权限的操作可以用由sudo组的成员执行sudo命令来代替。

经验总结：Kali对于用户和组管理体系比较完备，有着完善的权限划分等级。

（3）文件与目录管理

主要内容：任务一涉及查看文件与目录操作，任务二涉及创建文件与目录操作，任务四涉及文件的修改与移动、链接文件的创建、文件与目录权限管理，任务三和任务五五涉及文件内容操作，任务六涉及文件压缩与解压缩操作。此外，还有更多的命令来进行文件与目录管理，也有相应的图形化配置管理工具来进行文件与目录组管理，有关文件与目录管理的更多内容请参考[1]46-59页。

关键分析：文件与目录管理是软件包管理、系统高级管理等基础，需要熟练掌握。

经验总结：熟悉Linux目录结构，了解Linux文件类型，并在此基础上掌握文件与目录管理。

（4）C/Python编程

主要内容：任务二涉及C/Python编程。此外，Linux也支持C++/Java/PHP等更多编程语言，Linux上也可以部署IDE进行编程。

关键分析：C语言是编译型语言，Python是解释型语言，注意两者程序执行的区别。

经验总结：在掌握某一编程语言的基础上，学会在Linux上进行编程。

（5）系统高级管理

主要内容：任务七涉及使用systemd管控系统和服务，任务八涉及进程的调度启动。相关的更多内容请参考[1]106-134页。

关键分析：除了用户与组管理、文件与目录管理、磁盘管理等基础管理，作为Linux系统管理员，必须掌握系统高级管理的知识和技能。

经验总结：以某种服务为例（如Apache），学习并掌握系统高级管理技能。

## 课外拓展

（1）权限管理

Kali对于权限管理十分严格，对于系统核心配置文件的修改只能由root用户来操作，第一次使用sudo命令系统给出的提示信息也体现出系统对于权限管理的重视。但与此同时，Kali的权限管理又不缺乏灵活性，此处举出如下两个例子：其一，Kali虽然默认禁用root账户，但可以使用sudo命令代替；其二，文件访问权限除了所有者权限、所属组权限、其他用户权限以外，还有3中特殊权限suid、sgid、sticky，这3种权限与用户进程有关，可用于非正常情况下绕过正常权限体系的操作，具体内容这里不再赘述，最典型的例子是——用户密码以加密形式存放在/etc/shadow文件中，只允许root用户读写，但是当某个用户需要修改自己账户密码时，无须使用sudo命令；反之，需要使用sudo命令才让人困惑。

纵观Kali的权限管理体系，有如下启发：在进行权限体系构建时，需要对权限等级进行严格划分，尤其是系统最高权限，不轻易让攻击者获得较高权限来篡改系统配置。但是，权限体系也要具有灵活性，从实际出发，考虑实际中会遇到的非正常情况，避免权限体系过于僵硬。

（2）网络配置

有关借助PuTTY工具通过ssh服务访问Kali的问题，网络上相关的教程很多，但真正能解决问题的很少，甚至有的文章有知识错误，其中主要涉及计算机网络的相关知识，可参考教材[3]，网址[4]，网址[5]。此处简述一种基于Windows的解决办法：首先，查看Kali的ip地址，以192.168.242.135为例，将VMware Network Adapter VMnet8的IPv4地址改为192.168.242.1（前24位相同）。此外，最好事先将Kali的ip地址由通过DHCP服务动态获得改为使用静态地址。

其次，开启Kali上的ssh服务，配置PuTTY，即可成功访问Kali，此步骤可参考本文13-14页。

通过解决这一问题，有如下收获：遇到问题时，Google等搜索引擎仍然是寻找解决办法的重要途径。但是，对于网上的教程要持怀疑态度。值得思考三个问题：自己能否独立解决问题？搜索到的解决办法对不对？有没有更好的解决办法？更为重要的是，要善于阅读官方文档，例如，VMware官网对于虚拟机的网络配置给出了详细说明，可参考网址[4]。

（3）Kali特性

Kali Linux是Linux操作系统的特别发行版本，它的目标用户是从事网络空间安全工作的人。通过Kali，可以实现网络安全测试、漏洞查找与利用、密码破解等高级技术，详细内容可参考[2]。

## 总体感受

通过本次课的学习，对于以Kali为例的Linux操作系统有了基本了解，掌握了基本操作，但这只是网络安全知识的冰山一角。接下来，在学习网络安全基础知识的前提下，需要通过网络空间安全综合实践课的学习提升自己的实操能力。

最后，进行网络安全测试，必须在合法的前提下。此外，还要遵守职业道德，道德的要求往往高于法律。

## 参考文献

[1]张金石,钟小平,汪健.Ubuntu Linux操作系统.(第二版).北京:人民邮电出版社,2020.6

[2]Ric Messier.Learning Kali Linux.北京:O’Reilly Media,Inc,2020.6

[3]James F. Kurose,Keith W.Ross.Computer Networking: A Top-Down Approach(Seve

nth Edition).北京:机械工业出版社,2018,5

[4]VMware Workstation Pro Documentation,https://docs.vmware.com/cn/VMware-Workstation-Pro/index.html

[5] lsgxeva.VMware三种网络模式的区别.博客园网站, https://www.cnblogs.com/ lsgxeva/p/9995259.html. 2018-11-21