网络空间攻防基础与实践

2024 年春季-实践指导书

简介

本课程从零开始，采用“做中学”理念，使学生掌握网络空间攻防必备的知识基础、安全工具，具备开展网络空间攻防实践的能力。参与本课程学习没有先修要求，只需一份乐意动手实践的心情。

课程将基于 HTB 学院（https://academy.hackthebox.com/）开展知识点讲解与实验，要求学生能够建立自己的 Linux 学习环境，建立 Web 安全测试靶标，以不断巩固网络空间安全实践基础能力。请各位同学注册 HTB 学院账号，循序渐进开展学习，本课程对应 HTB 学院中“Path ==> Skill Paths”中“Information Security Foundations”学习路径，以及部分 Web 安全模块。

一、考核

本课程成绩由实验报告与技能竞赛两个部分组成，实验报告占 70%，技能赛 30%，具体要求如下。

1、实验部分（共 70 分）

考查实验报告的撰写是否认真，图表是否规范，逻辑思路是否清晰，运行结果是否正确，安全风险与法律风险分析是否合理，以及是否存在抄袭。

(1) Linux 实验（20 分）：提交实验报告，实验报告应包含思路与运行结果。

(2) Python 编程实验（30 分）：提交实验报告与代码，实验报告应包含思路与运行结果。

(3) HTB 技能评估（20 分）：提交实验报告，实验报告应包含思路与运行结果。

① 测试工具：https://academy.hackthebox.com/module/110/section/1055

② Js 混淆：https://academy.hackthebox.com/module/41/section/519

③ XSS：https://academy.hackthebox.com/module/103/section/1011

④ SQLi：https://academy.hackthebox.com/module/33/section/518

2、技能赛部分（共 30 分）

依据学校网络空间安全实验技能大赛规则：提交的 Flag 是否正确，提交的 writeup 情况是否充分合理。考查提交 Flag 是否正确，实验报告的逻辑思路是否清晰，以及是否存在抄袭。

二、教学安排

具体教学安排如下：

教学模块	二级模块	教学（实验）内容	学时
Linux 基础 12 学时	Linux 概述	重点：发展史、设计哲学、内核与发行版的区别	2
	Shell 概述	重点：常用快捷键、常用命令、获取帮助	2
	文件与权限	重点：文件操作及命令，文件权限及命令	3
	系统管理	重点：Linux 环境建立、包管理、周期任务、SSH 服务	4
	Linux 主机加固	重点：了解主机加固的工具	1
Python 基础 12 学时	Python 概述	重点：解释型、执行 Python 代码、Shebang line	0.5
	变量	重点：强类型、类型转换、字符串常用操作、切片	0.5
	数据结构	重点：列表、元组、字典	1
	程序控制	重点：迭代、in、range	0.5
	函数与类	重点：位置参数、关键字参数、默认参数、lambda 函数、None、命名空间与作用域、异常与错误处理、基本的类定义	1
	Python 库	重点：包、模块、导入、PIP 库管理、虚拟环境、	0.5
	实例一	重点：理解程序并复现	1
	实例二	重点：理解程序并复现	1
	编程练习	多练习	6
Web 基础	Web 概述		2

12 学时	Web Request		2
	Web 测试工具		4
	Js 混淆		2
Web 安全基础 12 学时	XSS		4
	SQLi		8
合计			**48**

三、线上资源

1. DVWA：https://github.com/digininja/DVWA

可以说是入坑必刷靶机了，没有之一。Damn Vulnerable Web Application (DVWA)，其主要目标是帮助安全专业人员在法律环境中测试他们的技能和工具，帮助 Web 开发人员更好地了解保护 Web 应用程序的过程，并帮助教师/学生在课堂环境中教授/学习 Web 应用程序安全性。

2. Pikachu：https://github.com/zhuifengshaonianhanlu/pikachu

一个好玩的 Web 安全漏洞测试平台，跟 DVWA 类似，不过看上去比前者清晰（中文的），有简单的漏洞页面，不那么单调。

3. Wargames：https://overthewire.org/wargames/

力推，内容丰富，因吹斯听，说它是一个网络安全百科全书也不为过。

不会没关系，一个字，学！

特色的闯关模式让你情不自禁的学习，知识涵盖 Linux 命令、web 安全、密码学、系统安全、逆向、代码审计等等。

4. XSS 弹窗专项练习：https://xss.haozi.me/#/0x00

一个 XSS 的弹窗挑战，一共 13 关，让你一个点一个点的理解 XSS。

页面上展现了源码，方便直接，更易理解其原理。

5. SQL 注入专项练习：https://github.com/Audi-1/sqli-labs

一个针对 SQL 注入的专项训练集，共 75 个挑战。分为基本 SQL 注入、高级 SQL 注入、

SQL 堆叠注入、SQL 挑战四个部分。

各种 SQL 注入姿势，让你一次注个痛快。

6. Hack The Box：https://www.hackthebox.com/

在里面的有很多靶机（但是会员才能玩历史靶机），各种难度层，从小白到大佬，都有适合你的靶机，并且经常更新，想要提升自我，不断挑战的同学可以尝试。

7. BUUCTF：https://buuoj.cn/

适合喜欢 CTF 方向的同学，整合了各大 CTF 赛事题目，没事就多刷题，刷刷刷！

7. 系统设计 101：https://github.com/ByteByteGoHq/system-design-101

使用视觉效果和简单术语解释复杂系统的工作原理，可以帮助准备系统设计面试。

四、赏金计划

本课程将发布若干任务，“明码标价”，邀请有兴趣的同学参与完成，根据完成质量予以积分奖励，积分按 1:1 兑换礼品。

任务成果将在学院在线平台共享给所有同学。

目录

预备知识

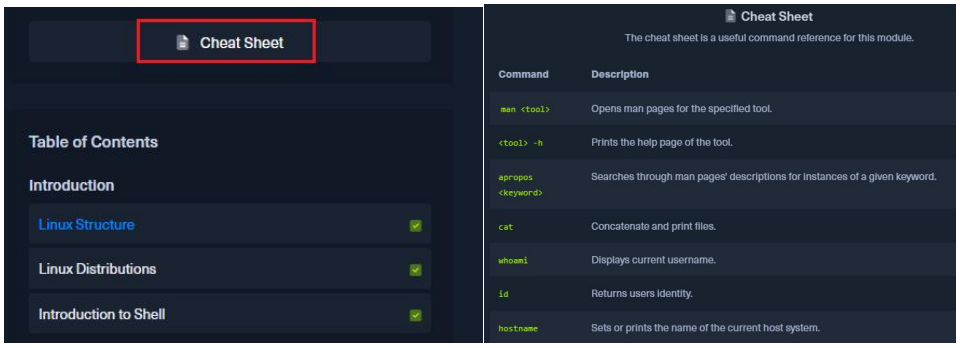
一、HTB 预备知识

1、HTB 学院网址：https://academy.hackthebox.com/

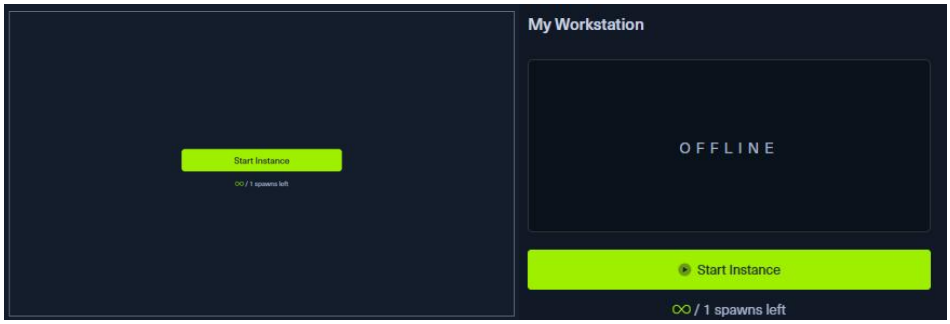
2、HTB 学院网站功能与使用介绍：INTRODUCTION TO ACADEMY

https://academy.hackthebox.com/module/details/15

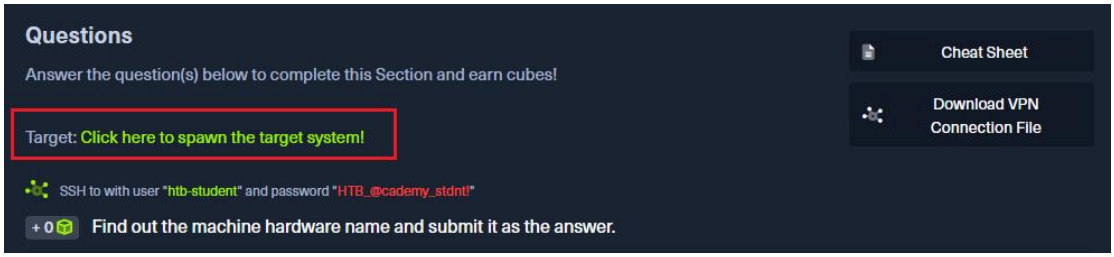
3、模块小抄：Cheat Sheet



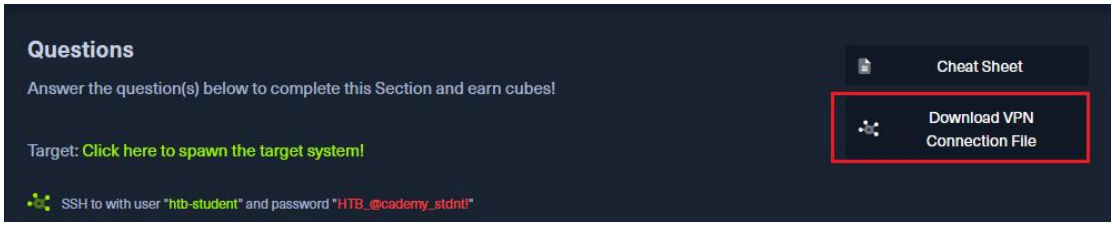
4、MyWorkStation：HTB 提供的免费云主机，与目标靶机可以直接联通，免费用户一天用一次，每次 2 小时



5、Target System：HTB 做题的目标靶机，通过 SSH 连接到目标靶机完成题目。



6、OpenVPN（带 GUI）：通过在本机安装 VPN 客户端，使用 HTB 提供的 VPN 连接文件，建立与目标靶机的 VPN 连接，即可在本机 SSH 连接到目标靶机。



(1) 下载地址：https://openvpn.net/community-downloads/

(2) 安装文档：

https://openvpn.net/community-resources/how-to-install-the-openvpn-gui-on-windows/

(3) Linux 安装和使用 OpenVPN：

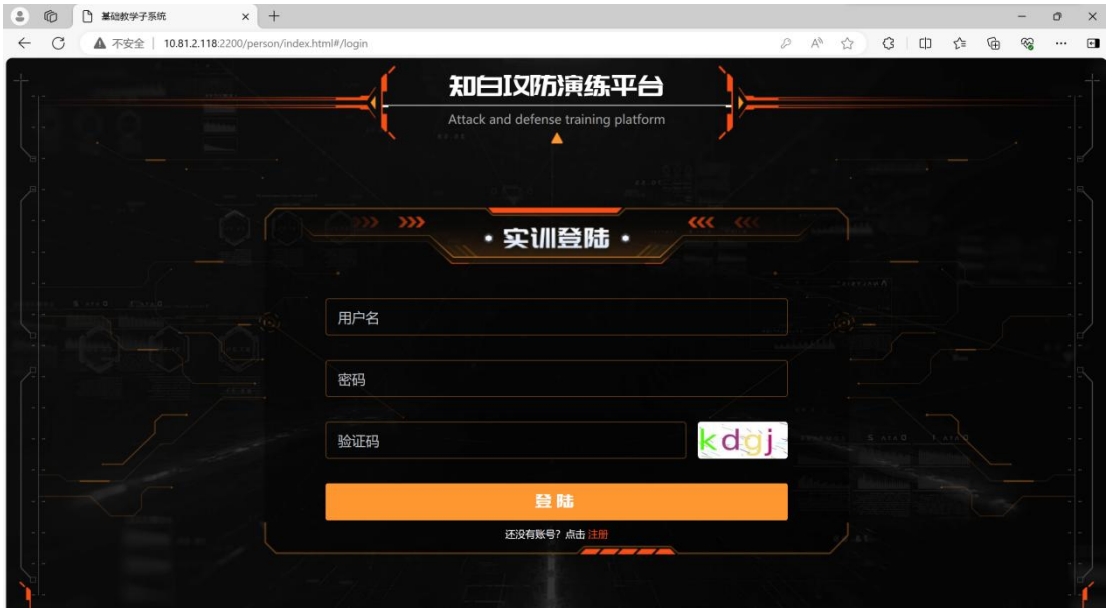
https://blog.csdn.net/qq_51690690/article/details/130612517

二、学院在线平台预备知识

1、学院在线平台网址：http://10.81.2.118:2200/

2、如何做实验：

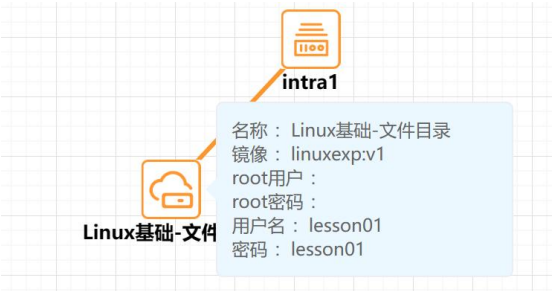
（1）打开浏览器，输入学院在线平台网址，进入实训登录界面。输入用户名、密码和验证码登录。用户名：jcxl+学号（例如：jcxl2023264609），初始密码：Aa123456



（2）点击主页热门课程中的“Linux 基础操作”进入。如果热门课程中没有此课程，点击页面上方的“课程体系”一栏后，展开左侧列表中的“安全技术”类，选择其中的最后一项“信息安全基础能力”，进入体系。打开位于该体系中的“Linux 基础操作”课程，开始学习。

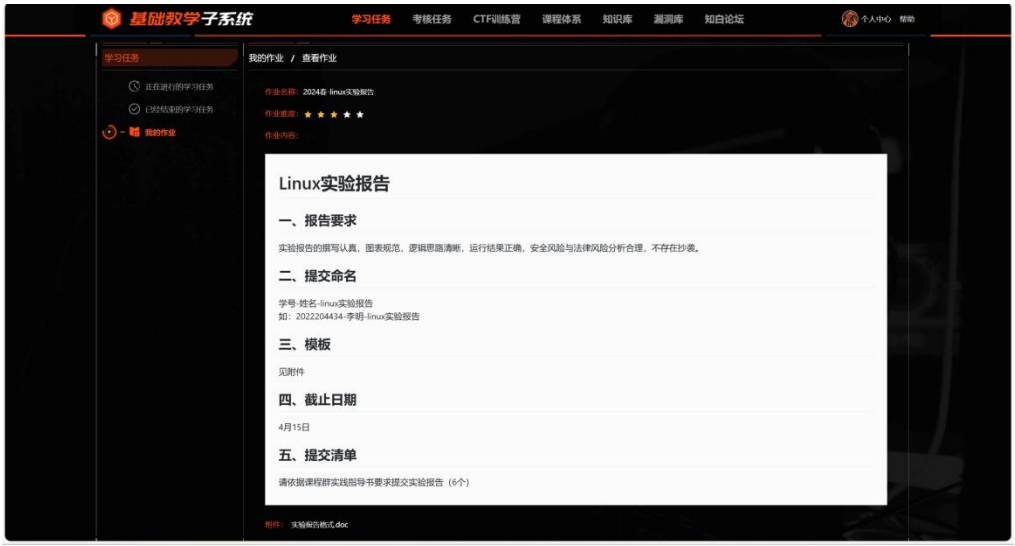
在该课程的“Linux 实验”部分中，第一项是实验指导书（**指导书请以课程群发布为准**），其余项是实验。**按照顺序完成**“Linux 基础-实验 2”-“Linux 基础-实验 7”。点击“开始实验”，跳转到实验手册。

（3）进入实验手册，点击“开启默认环境”后，鼠标移动到页面中间的小图标可看到登录用户名和密码。展开右侧的隐藏栏，点击“实验环境”后查看 IP 和端口号，使用 MobaXterm 或其他 ssh 软件进行远程 ssh 连接登录，按照指导书要求进行实验。



（4）注意事项：靶机开放时间默认为半小时，请注意点击实验延时。

3、如何交作业和实验报告：登陆进入首页： 学习任务->我的作业->查看作业要求->上传实验报告。注意实验报告提交有截止日期，逾期系统关闭。



第一部分：Linux

参考资料

1、鸟哥的 Linux 私房菜：基础学习篇，https://linux.vbird.org/

2、LINUX FUNDAMENTALS：https://academy.hackthebox.com/module/details/18

赏金计划

1、（50 积分）如何使用 OpenVPN 刷 HTB 学院靶机，提供 GIF 录屏。

(1) Windows 环境下安装 OpenVPN-GUI

(2) Linux 虚拟机环境下安装 OpenVPN

(3) 以 System Information 为例演示：

https://academy.hackthebox.com/module/18/section/70

2、（50 积分）Linux 各发行版（含国产操作系统）的联系与区别，各自的特色是什么？提供 PPT。

3、（50 积分）Git 入门，如何利用 Github 与 Gitee 做版本管理，提供 PPT。

4、（50 积分）主要开源协议的内涵与区别，提供 PPT。

实验清单

一、HTB 实验清单

(1) System Information：https://academy.hackthebox.com/module/18/section/70

(2) Navigation：https://academy.hackthebox.com/module/18/section/75

(3) Working with Files and Directories：https://academy.hackthebox.com/module/18/section/78

(4) Find Files and Directories：https://academy.hackthebox.com/module/18/section/81

(5) File Descriptors and Redirections：https://academy.hackthebox.com/module/18/section/79

(6) Filter Contents：https://academy.hackthebox.com/module/18/section/80

(7) User Management：https://academy.hackthebox.com/module/18/section/71

(8) Service and Process Management：https://academy.hackthebox.com/module/18/section/73

(9) Working with Web Services：https://academy.hackthebox.com/module/18/section/74

二、建立 Linux 环境（提交报告）

1、实验目标

(1) 熟悉 Vmware、VirtualBox 等虚拟机用法，并配置 Linux 实验环境，Linux 发行版本不限，建议 Kali、Parrot、Ubuntu。

(2) 了解和使用 Linux 常用 shell 工具，并掌握通用的帮助或手册用法

(3) 能够使用基础命令查看主机名、网络配置

(4) 能够查看 CPU、内存配置与使用状态以及系统内核版本与发行版本

(5) 能够完成与宿主机的网络配置，理解不同网络配置类型的区别

(6) 能够对常用软件镜像源进行修改

(7) 能够在 Linux 环境中配置 SSH 服务

(8) 熟练使用命令行或 GUI 工具通过 SSH 远程连接 Linux

2、实验内容

(1) 下载 Vmware、VirtualBox 等虚拟机并安装

(2) 下载 Parrot 系统镜像，并在虚拟机中安装

(3) 在 Parrot 系统中打开终端，使用常见的命令进行操作，尝试执行`ls`、`ps`命令观察输出结果。尝试“Tab”、“↑”、“↓”来进行补全和查看 bash 历史记录

(4) 使用`man`命令查看`ls`手册，执行`ls --help`查看帮助，观察两种不同的帮助文档的

区别。进阶操作：查看任意一个命令的说明文档，并简述其功能

(5) 使用 date、hostname、top、uname 命令来查看系统时间、主机名、实时系统占用情况和内核版本

(6) 通过`cat`命令查看当前系统中 CPU 信息（`/proc/cpuinfo`）、内存信息（`/proc/meminfo`）验证是否与虚拟机配置相同

(7) 在虚拟机中对所安装的系统进行网络配置，分别使用 NAT 网络、桥接网卡以及 Host-Only 来进行配置，使用`ip`命令来查看系统当前网络配置，比较不同配置的区别。在宿主机中使用 ping 命令来测试与虚拟机的连通性。最后使用一种合适的网络配置使虚拟机中系统可以连接互联网。

(8) 进行 apt 软件源的更换，使用`apt update`命令进行更新

(9) 使用 apt 安装 openssl 服务端，进行 ssh 服务端配置

(10) 在宿主机中使用支持 ssh 连接的程序（ssh、mobaxterm、windterm 等）对 Ubuntu/Parrot 进行远程连接

3、注意事项

(1) 对于陌生命令学会使用`-h/--help`来查看帮助

(2) 在更换 apt 源时使用选用国内镜像源，如清华镜像源、阿里镜像源

(3) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

(4) 推荐镜像站 https://mirrorz.org/

4、Parrot OS：下载 HTB 版本

(1) 官网：https://www.parrotsec.org/download/

(2) 清华镜像：https://mirrors.tuna.tsinghua.edu.cn/parrot/iso/

(3) 安装文档：https://www.parrotsec.org/docs/installation/

(4) 安装文档：https://www.parrotsec.org/docs/virtualization/parrot-on-vmware

三、Linux 文件与目录管理（提交报告）

1、实验目标

(1) 学习使用常用命令：ls，cd，cat，find，file

(2) 理解基本的用户与文件权限

2、实验内容

(1) 通过 SSH 远程连接给定目标

(2) 在登录账户的主目录中，查看文件名为“readme”的内容

(3) 使用 lesson01-1 用户重新登录该虚拟主机，密码为上一步骤中的文件内容，使用用户名：lesson01-1 登陆，查看文件名为“-”的内容

(4) 使用 lesson01-2 用户重新登录该虚拟主机，密码为上一步骤中的文件内容，使用 lesson01-2 登陆，查看文件名为“spaces in this filename”的内容

(5) 使用 lesson01-3 用户重新登录该虚拟主机，lesson01-3 用户密码为上一步骤中的文件内容，使用 lesson01-3 登陆，查看主目录下隐藏文件内容

(6) 使用 lesson01-4 用户重新登录该虚拟主机，密码为上一步骤中的文件内容，使用 lesson01-4 登陆，查看主目录下 ASCII 格式的文本文件内容

(7) 使用 lesson01-5 用户重新登录该虚拟主机，密码为上一步骤中的文件内容，使用 lesson01-5 登陆，查找 maybehere 目录，查看该文件夹满足以下条件文件的内容：“文件大小为 1008 字节，文本文件，不可执行”（题目待改进）

(8) 使用 lesson01-6 用户重新登录该虚拟主机，密码为上一步骤中的文件内容最后 8 字符，查找满足以下条件文件：“在/var 路径下，属于用户 lesson01-6、属于用户组 lesson01-5、文件大小为 50 字节”，查看该文件内容

(9) 使用 lesson01-7 用户重新登录该虚拟主机，密码为上一步骤中的文件内容最后 8 字符，获取`/etc/lesson01_pass`内容。观察主目录中文件内容及权限，使用`md5sum`来观察主目录下的两个文件是否相同，说明为什么会造成差异。（两个同样的可执行程序，但权限设置不一样，setuid 权限）

3、注意事项

(1) 对于陌生命令学会使用`-h/--help`来查看帮助

(2) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

四、Linux 文件处理（提交报告）

1、实验目标

(1) 巩固使用常用命令：ls，cd，cat，find，file

(2) 学习使用常用命令：grep，sort，uniq，strings，diff

2、实验内容

(1) 通过 SSH 远程连接给定目标。

(2) 查找文件`data.txt`中，单词“millionth”后到段落结尾的文本内容。

(3) 使用 lesson02-1 用户登录，密码为上一步骤中得到的内容，查找文件`data.txt`中，仅出现一次的文本行。

(4) 使用 lesson02-2 用户登录，密码为上一步骤中得到的内容，查找文件`data.txt`中，查找以几个“=”开头的 ASCII 字符串。（data.txt 为 binary 格式，使用 strings 看更清晰）

(5) 使用 lesson02-3 用户登录，密码为上一步骤中结果的其中一个，查找文件`passwords.old`和`passwords.new`，比较`password.old`和`password.new`文件内容，获取已更改的行内容。

3、注意事项

(1) 对于陌生命令学会使用`-h/--help`来查看帮助

(2) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

五、Linux 周期任务和 Shell 脚本理解（提交报告）

1、实验目标

(1) 学习使用常用命令：crontab

(2) 能够阅读理解简单的 Shell 脚本

2、实验内容

(1) 通过 SSH 远程连接给定目标

(2) 在`/etc/cron.d`查找定时任务 cronjob_lesson03_1，思考该任务的执行周期是多长？分析该定时任务写入临时文件的内容；

(3) 在`/etc/cron.d`查找定时任务 cronjob_lesson03_2，分析该定时任务写入临时文件的内容。

3、注意事项

(1) 对于陌生命令学会使用`-h/--help`来查看帮助

(2) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

六、Linux Shell 脚本 1（提交报告）

1、实验目标

(1) 理解 cron 配置文件和 shell 脚本

(2) 编写简单的 shell 脚本

(3) 文件权限

2、实验内容

(1) 通过 SSH 远程连接给定目标；（登录用户为 lesson04-1）

(2) 分析已经存在的定时任务；（依然在该位置：/etc/cron.d；cronjob_leeson04_1 这个定时任务具有 root 可执行权限，脚本定时执行 lesson04_1.sh，该 sh 将执行特定文件夹下的可执行程序）

(3) 获取/etc/lesson04_2_pass 内容。（lesson04_2_pass 的 owner 为 lesson04-root）

3、注意事项

(1) 实验报告中放出 shell 脚本

(2) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

七、Linux Shell 脚本 2（提交报告）

1、实验目标

(1) 编写简单的 shell 脚本

(2) 理解 linux 中管道的使用

(3) 文件输入重定向

2、实验内容

(1) 通过 SSH 远程连接给定目标，密码为“Linux Shell 脚本 1”所得结果

(2) 主目录有一个程序，他需要一个正确的口令来告诉你下一关的密码。提示：口令格式为`lesson04-2xxxx`，其中 xxxx 为纯数字。

3、注意事项

(1) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

(2) 实验报告中给出破解 shell 脚本或其他代码

(3) 实验所提供脚本需要在一次实验中完成，尽量减少申请环境次数

八、Linux Shell 脚本 3（提交报告）

1、实验目的

(1) 编写简单的 shell 脚本

(2) 了解 SSH，以及日志分析

2、实验内容

(1) 通过 SSH 远程连接给定目标，密码为实验“Linux Shell 脚本 2”所得结果；

(2) 主目录下有一个 ssh 登录日志文件，帮忙分析文件，将登录失败超过 20 次（不含 20）的 IP 加入到主目录的 ban_waitlist 中，已有 IP 不重复加入；

(3) 执行主目录中 check 程序，获取下一关密码。

3、注意事项

(1) 实验报告中体现自己的操作步骤，可通过截图来展示实验结果

(2) 实验报告中放出 shell 脚本或其他代码

(3) 日志文件较大请使用 less 命令查看

第二部分：Python 程序设计基础

参考资料

1、Introduction to Python 3：https://academy.hackthebox.com/module/details/88

2、Python 语言程序设计，嵩天，

https://www.bilibili.com/video/BV1JL4y1x7xC/?vd_source=4ffbaa6d7bb311ade493c2a6d6882fa4

3、Python - 100 天从新手到大师：https://github.com/jackfrued/Python-100-Days

实验清单

一、HTB 实验清单

(1) Conditional Statements and Loops：https://academy.hackthebox.com/module/88/section/916

(2) Defining Functions：https://academy.hackthebox.com/module/88/section/917

(3) The First Iterations：https://academy.hackthebox.com/module/88/section/922

(4) Continuously Improving The Code：https://academy.hackthebox.com/module/88/section/923

(5) Further Improvements：https://academy.hackthebox.com/module/88/section/924

(6) Managing Libraries in Python：https://academy.hackthebox.com/module/88/section/934

二、建立 Python 编程环境

1、实验目标

(1) 安装 Python3.X 最新版本

(2) 安装 IDE：PyCharm 社区版（或者其他 IDE 亦可，推荐 PyCharm、VSCode）

2、实验内容

(1) 获取并安装 Python

(2) 环境变量设置：确保 Python 可在命令行运行（安装 GUI 界面勾选或者安装后设置）

(3) 查看 Python 之禅

(4) 查看 Python 官方文档

(5) 基于 IDE 了解 PEP8 规范：安装对应插件或者 IDE 直接支持 PEP8 检查

3、注意事项

(1) 请安装社区版：PyCharm（https://www.jetbrains.com/pycharm/）

(2) 尽可能理解 PEP8 规范（https://peps.python.org/pep-0008/），并在开发中应用

三、Python 编程练习（提交代码）

请按题目要求，将代码规整到不同的文件夹与 Python 源代码文件。训练题代码按文件夹组织，源代码文件命名采用小写字母。为了保证 PyCharm 能正确识别各个模块，请以 ExCode 作为项目的根目录（即在使用 PyCharm 打开项目时，选择 ExCode 文件夹）。如果选到高一级文件夹，可能会导致测试用例代码中 import 报错。最外层文件夹为 Sec+学号。

可利用 forStudent.zip 压缩包提供的 PyCharm 工程框架编写代码，可利用提供的单元测试来查看代码的基本功能是否正确。

参考目录结构如下图所示，最后整个文件夹打包为 zip 提交。

```
Sec2014201325
  |  ExCode
    |  numEx
       |  num_hw.py
    |  textEx
       |  text_hw.py
       |  filter_hw.py
    |  dataEx
       |  xml_hw.py
       |  data_hw.py
       |  db_hw.py
    |  classEx
       |  class_hw.py
```

1. 寻找水仙花数 （模块：numEx，所在文件名 num_hw.py，Level：★）

水仙花数（Narcissistic number）是指一个 3 位数，它的每个位上的数字的 3 次幂之和

等于它本身（例如：1^3 + 5^3+ 3^3 = 153）。本题要求寻找所有的水仙花数。

函数原型：def narcissistic_number()

返回值： 返回一个 list，包含了所寻找到的全部水仙花数的数值，要求这些数从小到大排列。每一个数都应当为整形，如[153, 370, 371]。

2. 寻找完美数（模块：numEx，所在文件名 num_hw.py，Level：★）

完全数（Perfect number），又称完美数或完备数，是一些特殊的自然数。它所有的真因子（即除了自身以外的约数）的和（即因子函数），恰好等于它本身。如果一个数恰好等于它的因子之和，则称该数为“完全数”。第一个完全数是 6，它有约数 1、2、3、6，除去它本身 6 外，其余 3 个数相加，1+2+3=6。第二个完全数是 28，它有约数 1、2、4、7、14、28，除去它本身 28 外，其余 5 个数相加，1+2+4+7+14=28。第三个完全数是 496，有约数 1、2、4、8、16、31、62、124、248、496，除去其本身 496 外，其余 9 个数相加，1+2+4+8+16+31+62+124+248=496。题目要求寻找参数规定所有完美数。

函数原型：def perfect_number(limit=1000)

参数 limit：整数，搜寻的上限，比如 limit=1000，表示寻找 1-1000 之间所有的完美数。1000 为 limit 的默认参数。注意处理异常参数

返回值： 返回一个 list，包含了函数所寻找到的全部完美数的数值，要求这些数从小到大排列。每一个数都应当为整形，如[6, 28, 496]。如果参数异常，返回错误“Parameter Error.”

3. 百钱百鸡问题（模块：numEx，所在文件名 num_hw.py，Level：★）

鸡翁一值钱五，鸡母一值钱三，鸡雏三值钱一。百钱买百鸡，问鸡翁、鸡母、鸡雏各几何？

函数原型：def buy_chicken()

返回值：返回一个 list，数列的元素为三元组，代表（鸡翁、鸡母、鸡雏）的数量，如：[[0,25,75], [4,18,78], [8,11,81]]，表示返回三组解，每一组解以三元 list 表示。

4. 最大公约数和最小公倍数（模块：numEx，所在文件名 num_hw.py，Level：★）

（1） 函数原型：def gcd(x, y)，求取最大公约数

（2） 函数原型：def lcm(x, y)，求取最小公倍数

参数 x，y：正整数

返回值：正整数，其中 gcd(x, y)返回 x 与 y 的最大公约数，lcm(x, y)求取 x 与 y 的最小公倍数。如果参数异常，返回错误“Parameter Error.”

5. 回文数（模块：numEx，所在文件名 num_hw.py，Level：★）

如果一个数反过来与原数相同，那么这就是一个回文数。比如，121 就是一个回文数，-121 不是一个回文数。设计函数验证一个数是否为回文数。

函数原型：def is_palindrome_number(n)

参数 n：输入待测试的数字，可能是正数、负数、整数、浮点数等数值

返回值：布尔型，如果这个数是回文数返回 True，否则返回 False

6. 素数（模块：numEx，所在文件名 num_hw.py，Level：★）

素数指的是除了 1 和它本身以外没有其他因数的数。设计函数验证一个数是否为素数。

函数原型：def is_prime_num(n)

参数 n：正整数，输入待测试的数字。负数、小数归为异常参数。

返回值：布尔型，如果这个数是回文数返回 True，否则返回 False。如果参数异常，返回错误“Parameter Error.”

7. 约瑟夫环问题（模块：numEx，所在文件名 num_hw.py，Level：★★）

有 15 个基督徒和 15 个非基督徒在海上遇险，为了能让一部分人活下来不得不将其中 15 个人扔到海里面去，有个人想了个办法就是大家围成一个圈，由某个人开始从 1 报数，报到 9 的人就扔到海里面，他后面的人接着从 1 开始报数，报到 9 的人继续扔到海里面，直到扔掉 15 个人。由于上帝的保佑，15 个基督徒都幸免于难，问这些人最开始是怎么站的，哪些位置是基督徒哪些位置是非基督徒。假设初始有 m 人，最后有 n 人存活，设计函数计算存活者的初始站立位置。

函数原型：def jose_prob(n, m)

参数 n：正整数，小于 m，表示基督徒的人数，即存活下来的人数。

参数 m：正整数，表示初始所有的人数。

返回值：返回一个长度为 m 的 list，数值为 0 或 1，其中 1 代表基督徒，0 代表非基督徒。该 list 即指明了基督徒初始站立的位置。如果参数异常，返回错误“Parameter Error.”

8. 万年历（模块：numEx，所在文件名 num_hw.py，Level：★★）

给出一个年月日，计算这一天是那一年的第几天。

函数原型：def calendar(year, month, day)

参数 year：四位正整数，年，如 2000。

参数 month：1-12 的正整数，月

参数 day：1-31 的正整数，日

返回值：正整数，表示这一天是那一年的第几天。如果参数异常，返回错误“Parameter Error.”

9. 两地之间距离计算（模块：numEx，所在文件名 num_hw.py，Level：★）

利用 Python 实现地球上两点之间的距离计算，地球上点的位置以经纬度坐标形式提供。距离计算采用 Haversine 公式：

$$d = 2r\arcsin\left(\sqrt{\operatorname{hav}(\varphi_2 - \varphi_1) + \cos(\varphi_1)\cos(\varphi_2)\operatorname{hav}(\lambda_2 - \lambda_1)}\right)$$
$$= 2r\arcsin\left(\sqrt{\sin^2\left(\frac{\varphi_2 - \varphi_1}{2}\right) + \cos(\varphi_1)\cos(\varphi_2)\sin^2\left(\frac{\lambda_2 - \lambda_1}{2}\right)}\right)$$

这里 r 是地球半径 6371Km，(φ, λ)代表点的（纬度，经度）坐标。

参考网站：https://en.wikipedia.org/wiki/Haversine_formula

完成距离计算函数：

函数原型：def sphere_distance(p1, p2)

参数 p1：tuple 元组类型，二元组，（纬度，经度），坐标精确到小数点后 7 位

参数 p2：tuple 元组类型，二元组，（纬度，经度），坐标精确到小数点后 7 位

纬度取值范围：[0-90]，经度取值范围：[0-180]，单位均为角度；而 Haversine 公式计算采用的是弧度，注意转换。

返回值：如果输入的坐标数据合规，则返回两点之间的距离，单位为 Km，保留两位小数；如果输入的坐标不合规，返回错误“Parameter Error.”

10. 计算 Fibonacci 序列的值（模块：numEx，所在文件名 num_hw.py，Level：★）

利用 Python 实现 Fibonacci 序列值的计算。实现两个函数：

（1）递归版本的 Fibonacci 序列值计算

函数原型：def fibonacci_recursion(number)

参数 number：Fibonacci 序列的第 number 项，number 为大于 0 的整数。

返回值：如果参数合规，则返回 Fibonacci 序列的第 number 项的值；如果参数不合规，返回错误“Parameter Error.”。

（2）循环版本的 Fibonacci 序列值计算

函数原型：def fibonacci_loop(number)

参数 number：Fibonacci 序列的第 number 项，number 为大于 0 的整数。

返回值：如果参数合规，则返回 Fibonacci 序列的第 number 项的值；如果参数不合规，返回错误“Parameter Error.”。

问题：

（1）查看 fibonacci_loop(36)与 fibonacci_recursion(36)的运行时间，哪个运行快？

（2）fibonacci_recursion 版本支持的最大输入是多少？最大值如何更改？

11. 摩斯码生成器（模块：textEx，所在文件名 text_hw.py，Level：★）

利用 Python 实现摩斯码符号生成，完成函数：

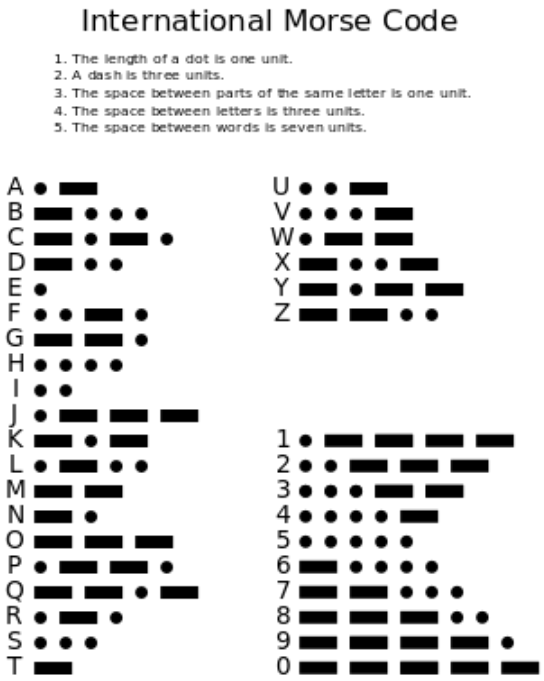
（1）摩斯码生成函数：

函数原型：def morse_code(usr_str)

参数 usr_str：字符串，需要转换为摩斯码的字符串。

返回值：输出 usr_str 对应的摩斯码字符串，用 . 代表点， - 代表破折号，点与点、破折号与破折号之间、点与破折号之间为一个空格，字符间为三个空格，单词之间为七个空格。注意输出的摩斯码首尾不含空格。

参考网站：https://en.wikipedia.org/wiki/Morse_code



12. 词频统计（模块：textEx，所在文件名 text_hw.py，Level：★★）

利用 Python 从文本文件中提取出现频次前十的单词，完成函数：

（1）词频提取函数：

函数原型：def word_freq(path)

参数 path：字符串，需要提取的文本文件路径。

返回值：列表，列表元素为二元组（单词，次数）；按从多到少的顺序列举出现最多的前十个单词与次数。如果单词出现的次数相同，则按单词的降序排序。统计时去除高频词（见 sight word.txt）。

可逐行读取文本内容，并按空格进行切分，逐个统计该行单词的数目信息，存储于字典中，最终对字典中的数据进行排序，可转化为列表之后排序，输出前 10 个出现频率最高的单词及其出现的次数。单词不区分大小写，处理时需去除一些非必要的符号（!`~@#$%^&*()_-+=[]{}/?,.:\"<\/>），只保留单词，连写词如 it's，don't 等算一个词汇。

13. C 程序文件处理（模块：textEx，所在文件名 filter_hw.py，Level：★★★）

利用 Python 实现将 C 源代码文件（后缀 .c，.cpp）读入，去除代码中的空格、块注释、行注释、include 语句、空行、回车换行符号，形成一个长字符串，并写入到新的文件。

实现函数：

（1）C/C++文件过滤函数：

函数原型：def filter_c_file(path)

从 path 中找到后缀为 .c，.cpp 的文件，逐个按要求删除不必要的字符，形成一个新字符串，该字符串被写入到同级目录下的新文件"XXX.txt"，其中"XXX"为原 C/C++文件文件名称。

参数 path：需要过滤的 C/C++文件路径，包含有多个文件。

返回值：无。

14. 敏感词过滤（模块：textEx，所在文件名 text_hw.py，Level：★★）

提供一个敏感词库文件 sensitive.txt，敏感词按类型进行分组，如"第一类 形容词"，每组中一行代表一个敏感词，如"可怕"。要求读取敏感词库，获得敏感词列表，根据敏感词列表对输入的敏感词进行过滤。敏感词是几个字，就将对应的文本替换成几个*符号。比如敏感词为脉动，则将"脉动真好喝"替换为"**真好喝"。

注意敏感词类型文本不归入敏感词，比如"第一类 形容词"不在过滤范围。敏感词库文件中的行可能只有空格，读入时请去除，不包含在过滤词库中。

函数原型：def filter_words(user_input)

参数 user_input：字符串，为输入待处理的字符串。

返回值：字符串，过滤后的字符串。

15. Base64 编解码算法（模块：textEx，所在文件名 base64_hw.py，Level：★★★）

理解 Base64 编码的原理，设计两个函数实现二进制数据的编解码。

（1） Base64 编码：

函数原型：def b64en(path_in, path_out)

参数 path_in：需要进行 base64 编码的图片文件路径。

参数 path_out：以 UTF8 编码生成的文本文件路径。

返回值：无。可使用 base64 内置库。

（2） Base64 解码：

函数原型：def b64de(path_in, path_out)

参数 path_in：需要进行 base64 解码的 UTF8 文本文件路径。

参数 path_out：解码生成的图片文件路径。

返回值：无。**不允许**使用 base64 内置库。

16. 计算图形面积及周长（模块：classEx，所在文件名 class_hw.py，Level：★）

利用 Python 尝试采用面向对象的设计方法。

（1）设计一个基类 Shape：

包含**两个成员函数**：

def cal_area(): 计算并返回该图形的面积，保留两位小数；

def cal_perimeter(): 计算并返回该图形的周长，保留两位小数。

def display(): 三行字符串，分别显示名称、面积、周长，数值四舍五入保留两位小数，如下：

名称是 rect

面积是 6

周长是 10

包含**三个变量**：

name：表示名称，字符串类型；

area：表示面积，数字；

perimeter：表示周长，数字。

（2）设计三个派生类：Rectangle、Triangle、Circle；派生类分别实现基类中的两个成

员函数。

Rectangle：构造函数参数（n, a, b），n 为名称，其他均为浮点数，两位小数，a、b 分别代表长和宽。

Triangle：构造函数参数（n, a, b, c），n 为名称，其他均为浮点数，两位小数，代表三边的长度。

Circle：构造函数参数（n, a），n 为名称，a 为浮点数，两位小数，代表圆的半径，圆周率取 3.14 进行计算。

17. XML 文件的生成与解析（模块：dataEx，所在文件名 xml_hw.py，Level：★★）

利用 Python 实现 XML 文件的读写，完成两个内容：

（1）创建 XML 文件，可使用 xml.dom.minidom，以生成 XML 文件。

函数原型：def create_xml(path)

参数 path：xml 文件的保存路径（包含文件名），要求支持相对路径。

返回值：无。

要求生成的 XML 文件结构与参考内容如下表所示。

```
<?xml version="1.0" ?>
<tilemap tilemapservice="http://tms.osgeo.org/1.0.0" version="1.0.0">
  <title>default</title>
  <abstract/>
  <srs>EPSG:4326</srs>
  <vsrs/>
  <boundingbox maxx="180.0" maxy="90.0" minx="-180.0" miny="-90.0" />
  <origin x="-180.0" y="-90.0" />
  <tileformat extension="tif" height="17" mime-type="image/tiff" width="17" />
  <tilesets profile="global-geodetic">
    <tileset href="" order="0" units-per-pixel="10.588" />
    <tileset href="" order="1" units-per-pixel="5.294" />
    <tileset href="" order="2" units-per-pixel="2.647" />
    <tileset href="" order="3" units-per-pixel="1.323" />
    <tileset href="" order="4" units-per-pixel="0.661" />
```

```
    <tileset href="" order="5" units-per-pixel="0.331" />
  </tilesets>
</tilemap>
```

（2）对指定的 XML 文件进行读取，可使用 xml.etree.ElementTree 解析 XML 文件。

函数原型：def parse_xml(path)

参数 path：要解析的 xml 文件路径，要求支持相对路径。

返回值：返回值类型为字典，如果解析成功，返回 dict 格式为：

{“tilemap service” : tilemap 节点 tilemapservice 属性的值，”title” : title 节点的值，”tileset count” : tileset 节点的个数，”tileset max” : tileset 节点中最大的 order 值（注意是整数）}

对应到上表的 XML 文件，返回值为：

{“tilemap service” : "http://tms.osgeo.org/1.0.0"，”title” : “default”，”tileset count” : 6，”tileset max” : 5}

解析过程中，如果缺少对应的值，则该项不在字典中出现；如果所有的值均不存在，就返回空的字典。

注意提供测试的 XML 中 tileset 节点的个数和属性值不是固定的。

18. 二进制数据报文构建与解析（模块：dataEx，所在文件名 data_hw.py，Level：★）

利用 Python 标准库中的 struct 模块实现二进制数据报文的构造与解析。完成两个内容：

（1）构建报文：

函数原型：def pack_message(data_dict)

参数 data_dict：报文字段值，为字典类型，例如：

{'type': 50, 'csum': 1, 'id': 'abcdefghigklmnop', 'dis1': 300, 'dis2': 100, 'count': 20}

返回值：二进制报文的字节序列。如果参数异常或者缺项，返回错误“Parameter Error.”

报文格式如下：共 27 字节

消息类型（type，1 字节，0-100 的整数） || 数据校验字节（csum，1 字节，后续的数据部分字节加法和）|| 禁飞区 ID（16 个字符，可按 UTF8 编码）| 禁飞区预警距离（dis1，整数，4 字节，大端序）| 禁飞区告警距离（dis2，整数，4 字节，大端序） | 禁飞区 1 点数（count，1 字节，0-255 整数）

（2）解析报文：

函数原型：def pack_message(message)

参数 message：经 pack_message 生成的二进制序列。

返回值：字典类型，包含有解析出来的数据。如果参数异常，返回错误“Parameter Error.”

19. 实现数据库的操作（模块：dataEx，所在文件名 db_hw.py，Level：★★）

利用 Python 实现针对 Sqlite3 数据库的操作，实现以下函数：

（1）初始化数据库：创建数据库文件、数据表

函数原型：def create_db(path)

参数 path：字符串，指明了数据库文件生成的位置。后续函数中的增删改查都是针对该数据库文件操作。在 dataEx 模块中可增加全局变量记录该路径。

在指定路径新建 Sqlite3 数据库，如果已经存在，则应首先删除原文件再创建。然后，建立两张数据表，即 Person 表与 Position 表。

返回值：创建成功，返回 0；失败返回-1。

人员信息表 Person：

序号	字段名称	字段类型	取值范围
1	NAME	字符串	姓名，32 字符
2	GENDER	字符串	性别，2 字符
3	BIRTH	日期	生日，2000 年 10 月 20 日
4	ID	字符串	身份证号，18 位身份证号，全局唯一，作为主键
5	POSITIONID	字符串	岗位名称，与岗位表关联

岗位表 Position：

序号	字段名称	字段类型	取值范围
1	POSITIONID	字符串	岗位名称，A、B、C、D；全局唯一，作为主键
2	SALARY	数字	薪水，10000，6000，3000，1000；每月的薪水

（2）新进人员：

函数原型：def new_employee(person，level)

参数 person：四元组，(姓名，性别，生日，身份证号)。

参数 level：字符串，岗位。

返回值：人员插入成功，返回 0；失败返回-1。

（3）删除人员：

函数原型：def delete_employee(person)

参数 person：字符串，被删除人员的身份证号。

返回值：删除成功，返回 0；失败返回-1。

（4）设置岗位薪水：

函数原型：def set_level_salary(level，salary)

参数 level：字符串，岗位级别，即 A、B、C、D 四个等级之一。

参数 level：整数，薪水。

返回值：设置成功，返回 0；失败返回-1。

（5）统计薪水开支：

函数原型：def get_total_salary()

返回值：整数，返回当前所有人员每月开支的薪水总和；失败返回-1。