

# 黑客成长记：

## 7个有趣的信息安全实验

带你进入黑客的世界

## 黑客成长记：7个有趣的信息安全实验



实验楼官方微博

2016-11-09 17:39:42

举报

阅读数：1208

实验楼上有很多信息安全课程，有教程、有在线开发环境，非常适合学习信息安全.....

做一名白帽子黑客听起来就很酷，或许也是很多IT人选择学习编程的原因之一，可是黑客不是一蹴而就的，也是需要从基础知识学起，也是需要从小项目做起的。

实验楼上有很多信息安全课程，如果你对信息安全感兴趣的话，肯定会选择去看看的，有教程、有在线开发环境，随便折腾，这对于搞信息安全的实验来说非常的方便啊。

[实验楼](#)
[课程](#)
[路径](#)
[讨论区](#)
[训练营](#)
[会员](#)
[我的课程](#)

ShellShock 攻击实验

5143

缓冲区溢出漏洞实验

4827

密钥加解密实验

1754

SET-UID程序漏洞实验

1234

Python暴力猜解Web登录

1086

Collabative系统SQL注入实验

1085

Collabative系统跨站脚本攻击...

格式化字符串漏洞实验

Collabative系统跨站请求伪造...



本文就介绍7个有趣的信息安全项目，或许你可以从这里开始你的黑客之旅。

### 1.逆向分析简单Linux程序

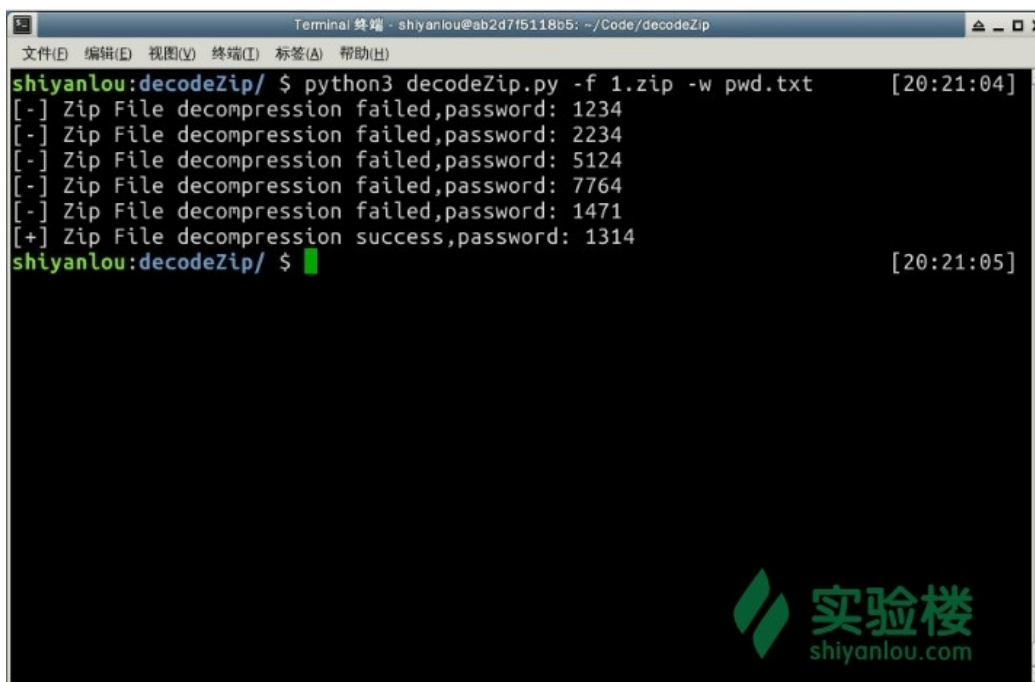
对软件的逆向分析被用于破解软件、查找漏洞等方面，因此，逆向分析是信息安全工程师必不可少的一项能力。

该项目通过对一个简单的Linux程序的逆向分析，带领大家熟悉汇编指令与GCC中objdump反汇编工具的简单使用

### 2.Python实现Zip文件的暴力破解

我们在网上好不容易下载到一个想要的zip资源却发现这个zip文件是加密的，或者忘掉自己压缩后的密码（一想到就头疼）。这时候我们就会想办法，将里面的内容提取出来。

我目前已知的破解zip的方式只有“Known plaintext attack”和“暴力破解”。这个项目带领大家用Python的zipfile模块实现Zip文件的暴力破解，涉及的知识点包括：zipfile、argparse的用法等等。



效果图

### 3.文件上传漏洞实例分析

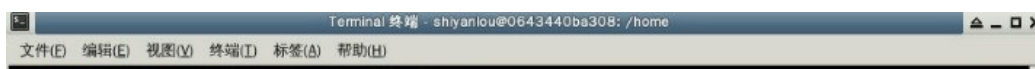
文件上传漏洞指攻击者利用程序缺陷绕过系统对文件的验证与处理策略将恶意程序上传到服务器并获得执行服务器端命令的能力。

该项目通过一个实例讲解文件上传漏洞，扩展分析文件漏洞利用的关键与防范。其中涉及文件上传漏洞的常见利用方式，部署web应用，编写恶意脚本程序，如何安全防范。

### 4.Python 实现 FTP 弱口令扫描器

FTP弱口令扫描其实就是暴力破解，为何我们不称为暴力破解呢？因为我们只是扫描一些简单的密码组合，并不是所有可能的密码组合。


项目通过使用Python实现一个FTP弱口令扫描器开始，入门Python渗透测试技术，项目涉及FTP协议原理，ftplib 库的使用等知识点。



```
shiyancelou:/home/ $ python3 ./ftpScanner.py [23:28:01]
usage: ftpScanner.py [-h] [-H HOSTNAME] [-f PWDFILE]

FTP Scanner

optional arguments:
  -h, --help      show this help message and exit
  -H HOSTNAME     The host list with ", "space
  -f PWDFILE      Password dictionary file
shiyancelou:/home/ $ [23:28:11]
```



效果图

## 5.BMP图像信息隐藏

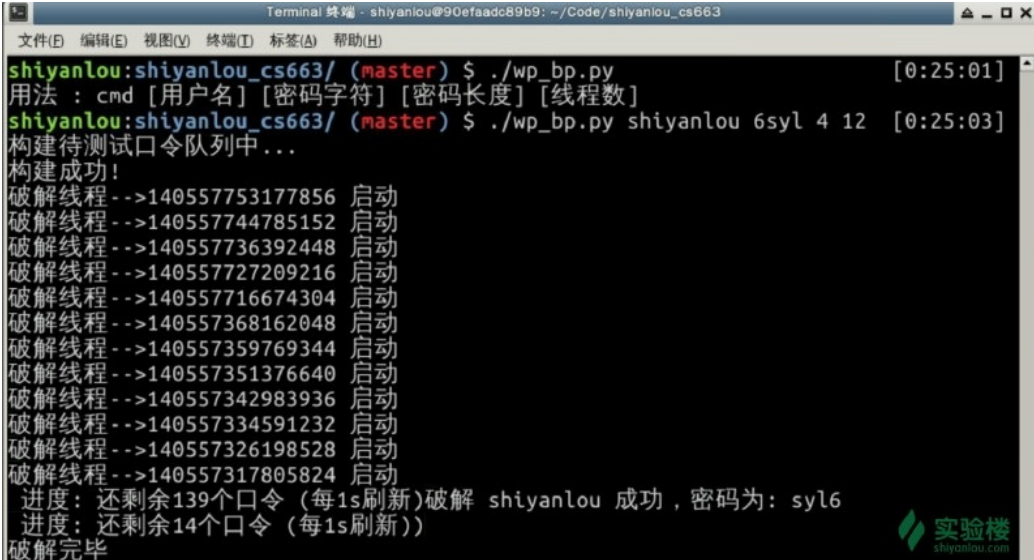
信息隐藏也称数据隐藏，将信息通过特定的方法隐藏于原始载体，使观察者无法察觉到隐秘载体里秘密信息。

通过C语言实现LSB信息隐藏算法来演示并讲解图像信息隐藏技术的基础与原理，带领初学者了解信息隐藏技术领域。


## 6.Python暴力猜解Web登录

暴力破解法就是列举法，将口令集合中的每一个口令一一尝试直到登录成功；有时候结合字典效率高一点，不过字典不一定猜得准。可以说它是一种“笨”办法，但有时候却是唯一的办法。

项目用Python实现暴力猜解wordpress管理员登录表单的功能，并用多线程、破解队列来优化破解过程。在实际应用中常结合弱口令和个人信息组成的口令集合来进行猜解，无论什么样的口令集合，破解过程都是相同的。



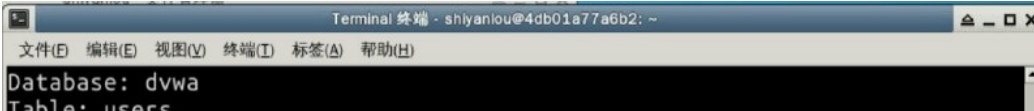
```
Terminal 终端 - shiyanlou@90efaadc89b9: ~/Code/shiyanlou_cs663
文件(F) 编辑(E) 视图(V) 终端(T) 标签(A) 帮助(H)
shiyanlou:shiyanlou_cs663/ (master) $ ./wp_bp.py [0:25:01]
用法 : cmd [用户名] [密码字符] [密码长度] [线程数]
shiyanlou:shiyanlou_cs663/ (master) $ ./wp_bp.py shiyanlou 6sylv 4 12 [0:25:03]
构建待测试口令队列中...
构建成功!
破解线程-->140557753177856 启动
破解线程-->140557744785152 启动
破解线程-->140557736392448 启动
破解线程-->140557727209216 启动
破解线程-->140557716674304 启动
破解线程-->140557368162048 启动
破解线程-->140557359769344 启动
破解线程-->140557351376640 启动
破解线程-->140557342983936 启动
破解线程-->140557334591232 启动
破解线程-->140557326198528 启动
破解线程-->140557317805824 启动
进度: 还剩余139个口令 (每1s刷新) 破解 shiyanlou 成功, 密码为: sylv
进度: 还剩余14个口令 (每1s刷新)
破解完毕
```



效果图

## 7.Sql注入之sqlmap+dvwa实例演练

sqlmap是当前最火热的自动化SQL注入工具,可以扫描、发现并利用给定URL的SQL注入漏洞;而DVWA是一套包含了一些常见安全漏洞的靶机web应用。该项目就通过实际演练来感受sql注入的实际威力。



```
Terminal 终端 - shiyanlou@4db01a77a6b2: ~
文件(F) 编辑(E) 视图(V) 终端(T) 标签(A) 帮助(H)
Database: dvwa
Table: users
```







# Mark! Android最佳的开源库集锦

Android开发库集锦

换一换 查看更多

转发 7

评论 3

3

**快速开通微博**你可以查看更多内容，还可以评论、转发微博。

## 微博精彩

- 热门微博
- 热门话题
- 名人堂
- 微博会员
- 微相册
- 微游戏
- 微指数

## 手机玩微博



扫码下载，更多版本  
戳这里

## 认证&合作

- 申请认证
- 开放平台
- 企业微博
- 链接网站
- 微博标识
- 广告服务
- 微博商学院

## 微博帮助

- 常见问题
- 自助服务