# 如何使用python写渗透测试脚本

常用的python库

python-nmap/requests/socket/sys/threading/time/re 等等

可以参考如下链接https://www.freebuf.com/sectool/94777.html

## 常见渗透测试脚本编写思路：

1. 在github/博客等找现有的脚本
2. 基于现有的脚本结合自己的需求进行修改
3. 调试并测试
4. #优化代码

举例：ftp匿名登陆批量测试工具

## 特定需求渗透测试脚本编写思路：

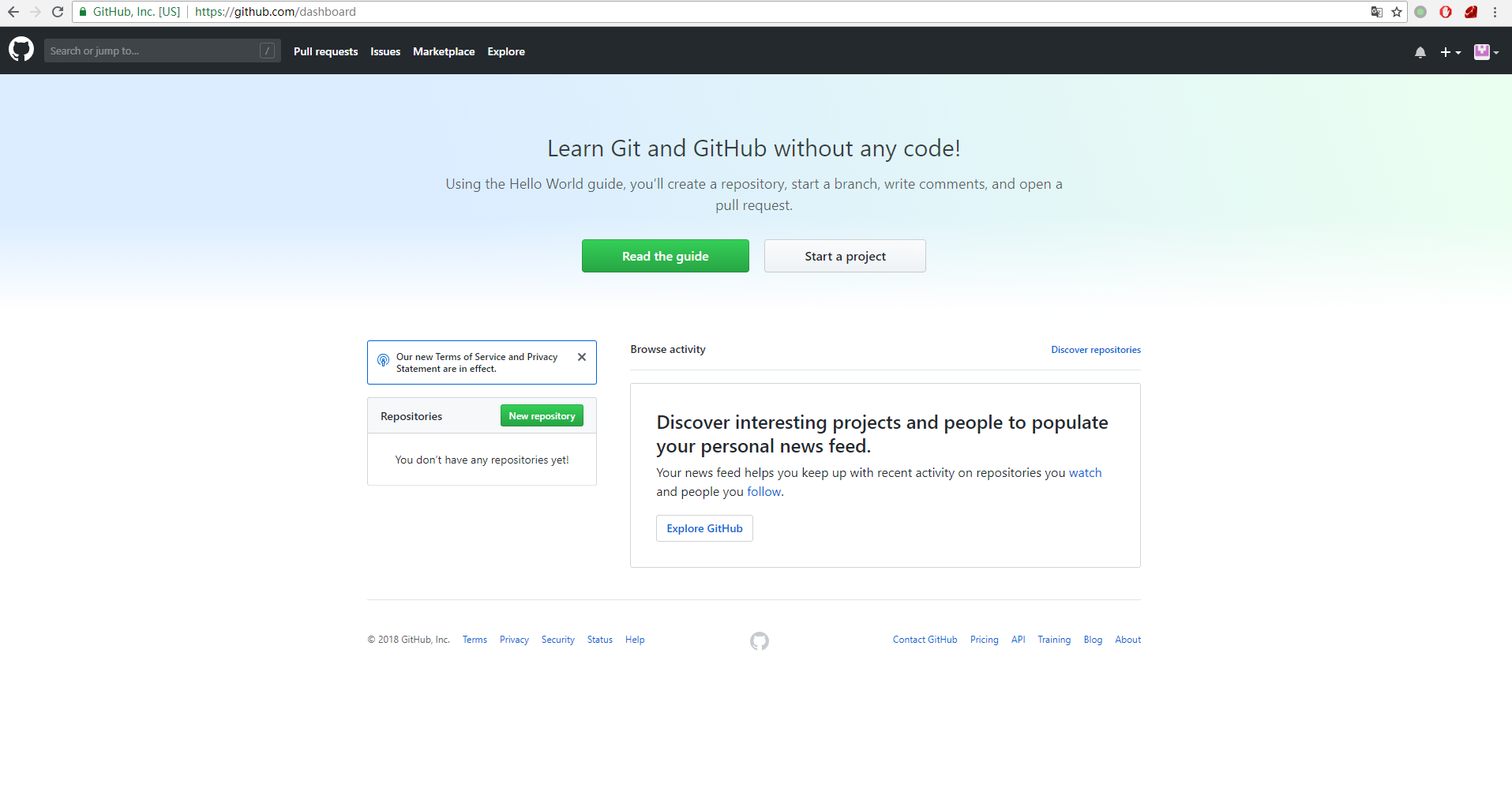
1. 实现核心功能
2. 封装核心功能
3. 围绕核心功能进行外层架构
4. 调试并测试
5. #优化代码

举例：某cms漏洞的批量测试脚本编写

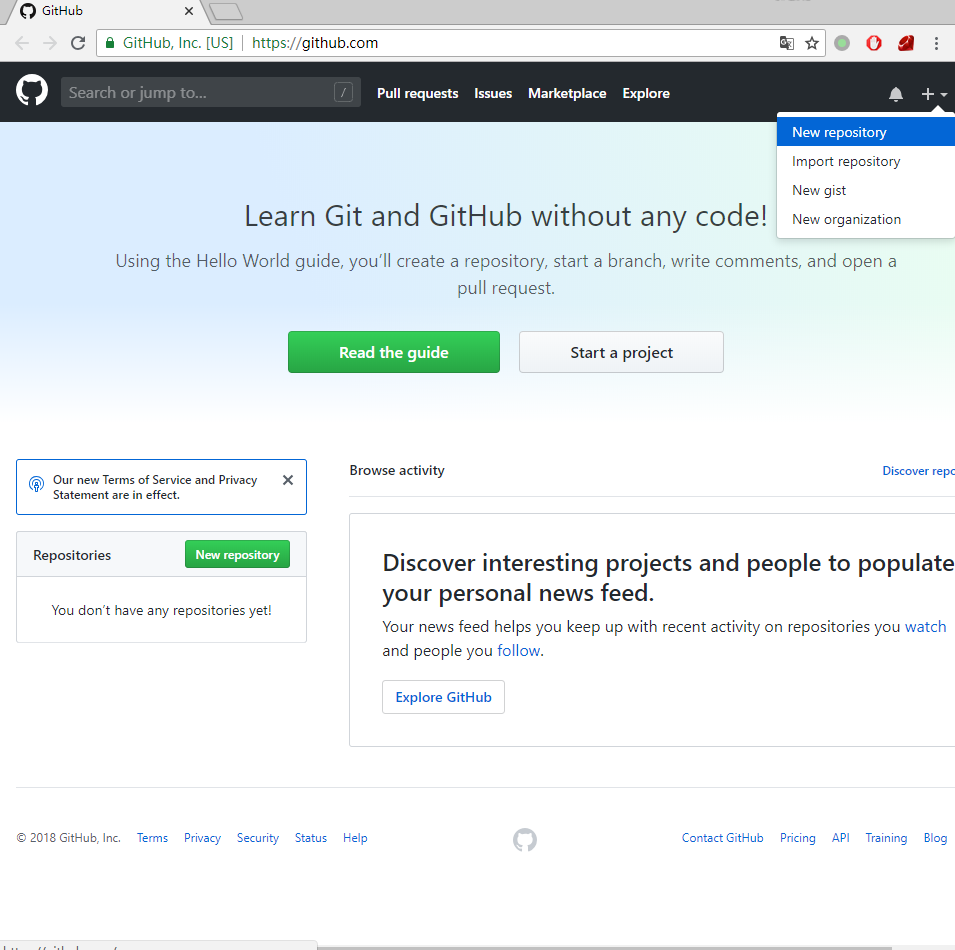
# Github 部署

## 注册

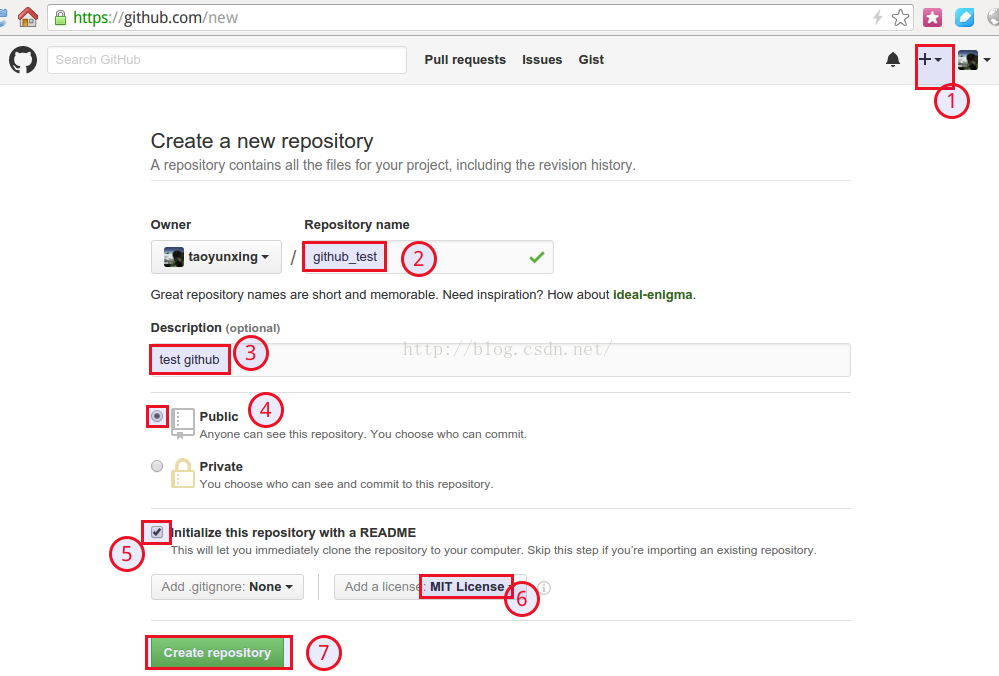
注册一个github账号，并进入邮箱验证



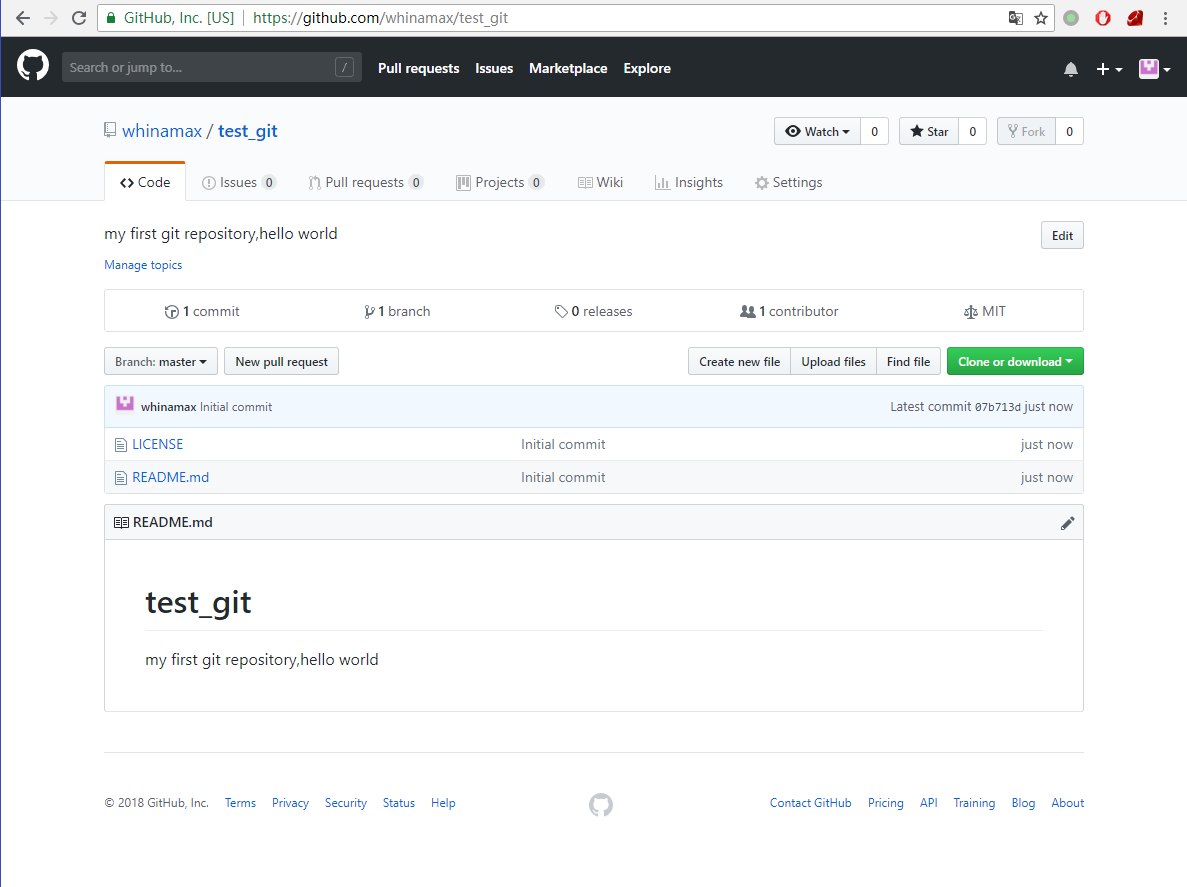
## 创建一个仓库



填写相关信息



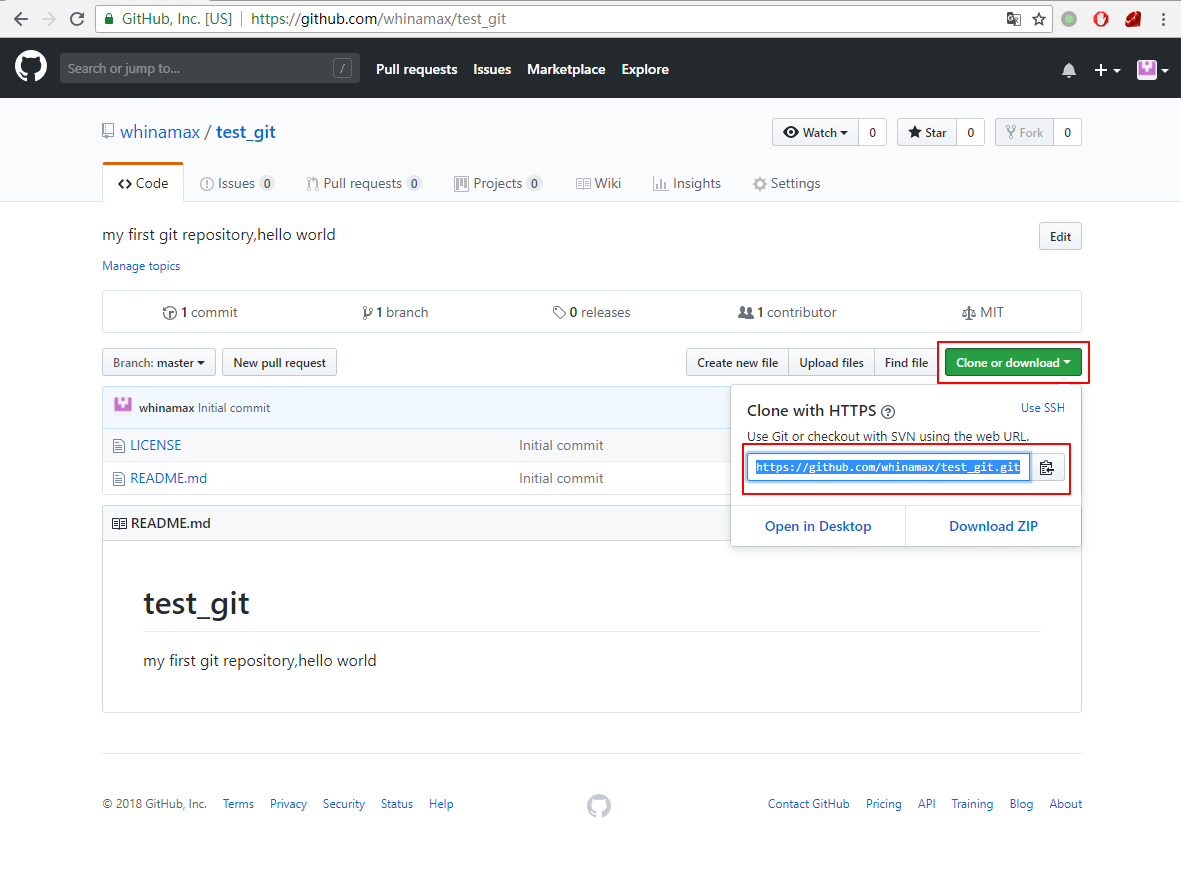
下图为已经创建好的项目



## 下载项目仓库代码，修改以及提交

从项目主页中得到链接为

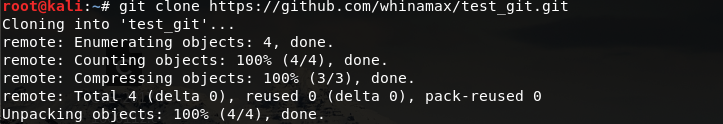
https://github.com/whinamax/test\_git.git



我们将其下载到本地, 修改代码然后提交给远程Github项目仓库，下面是相关的命令

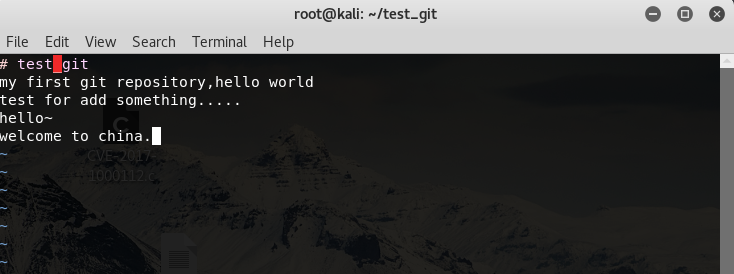
把项目checkout到本地来修改

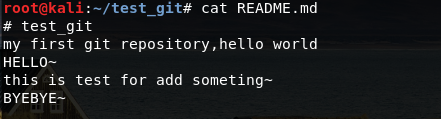
命令： git clone <https://github.com/whinamax/test_git.git>





使用vim修改README.md 以作示范

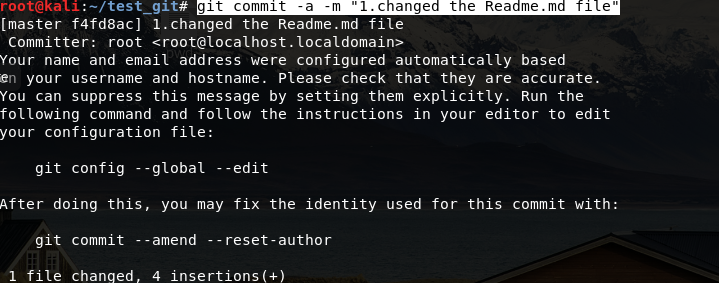




将修改代码提交到本地仓库

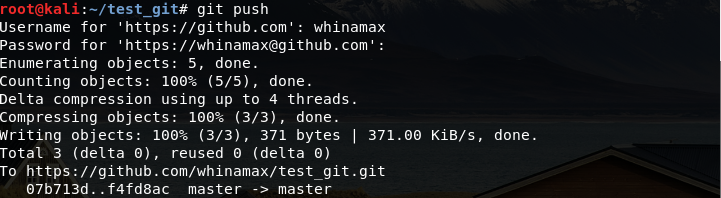
命令：

git commit -a -m "1.changed the Readme.md file"



将本地仓库更新同步到远程仓库：

命令: git push



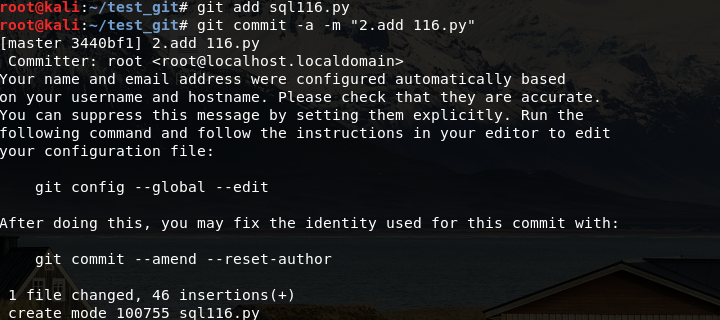
从远程仓库更新

命令：git pull



添加一个文件/文件夹

命令 git add 文件名/文件夹名

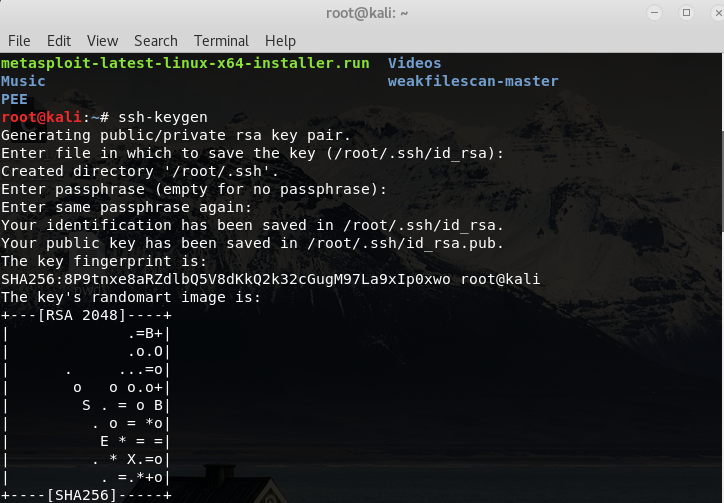


然后继续执行git push / git pull操作即可

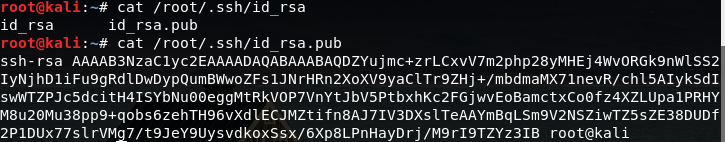
## 添加SSH，避免每次填写账号密码

添加ssh，github是采用ssh协议提交代码， 如果有多台工作机器，为了便于提交代码，可以在linux 下生成一对ssh密钥，把公钥放在github上，把私钥拷贝到每台机器就行。

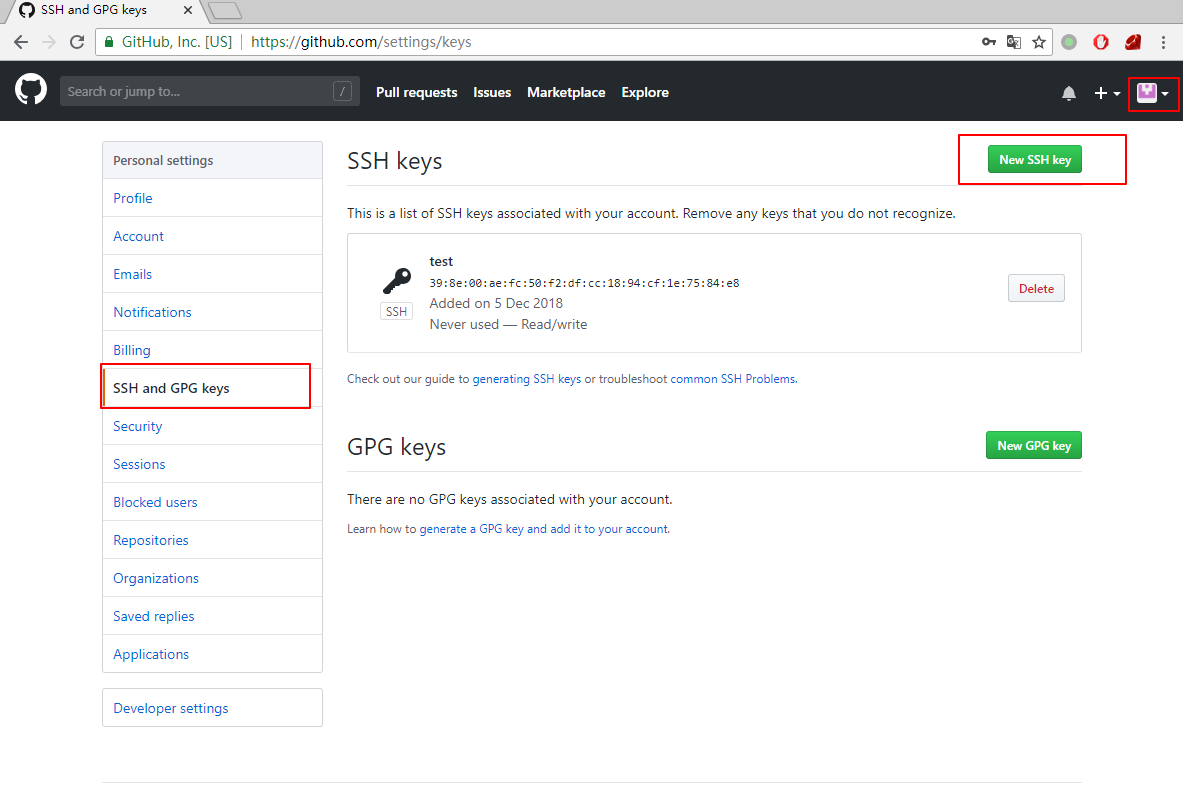
命令：ssh-keygen



查看公钥和私钥



复制公钥到github即可



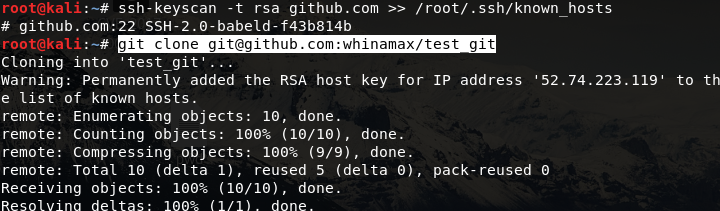
（1）将原有的项目删除

（2）将github添加到ssh主机中

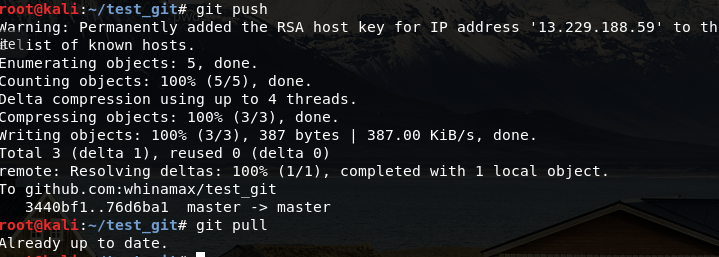
命令：ssh-keyscan -t rsa github.com >> /root/.ssh/known\_hosts

（3）使用ssh的方式来克隆项目到本地

命令：git clone [git@github.com:whinamax/test\_git](mailto:git@github.com:whinamax/test_git)



（4）git push /git pull



常用的git命令操作

https://www.jianshu.com/p/0f2ffa404ac1