# windows安装AWVS

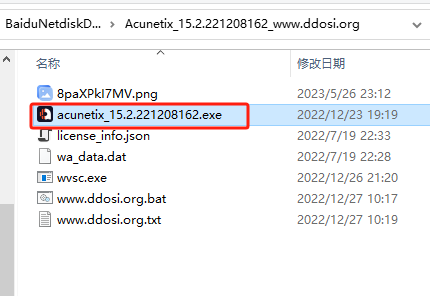
## 介绍

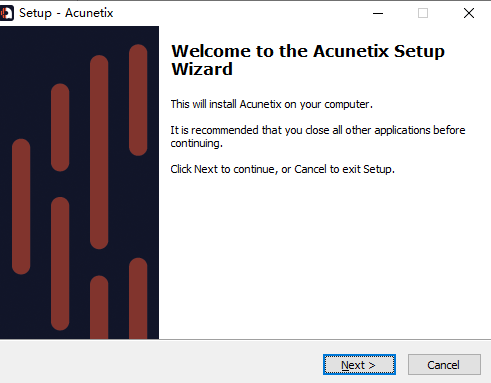
Acunetix Web Vulnerability Scanner(简称AWVS)是一款知名的Web网络漏洞扫描工具，它通过网络爬虫测试你的网站安全，检测流行安全漏洞。它包含有收费和免费两种版本，AWVS官方网站是：[http://www.acunetix.com/](https://link.zhihu.com/?target=http%3A//www.acunetix.com/)，官方下载地址：[https://www.acunetix.com/vulnerability-scanner/download/](https://link.zhihu.com/?target=https%3A//www.acunetix.com/vulnerability-scanner/download/)，官方免费下载的是试用14天的版本。

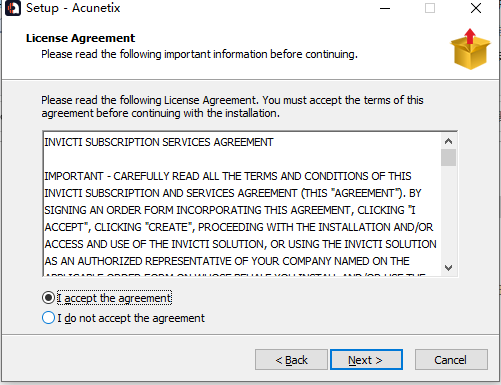
AWVS的功能及特点的功能及特点

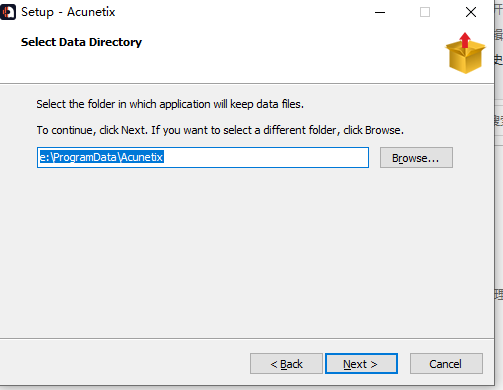
* 自动的客户端脚本分析器，允许对 Ajax 和 Web 2.0 应用程序进行安全性测试。
* 业内最先进且深入的 SQL 注入和跨站脚本测试
* 高级渗透测试工具，例如 HTTP Editor 和 HTTP Fuzzer
* 可视化宏记录器帮助您轻松测试 web 表格和受密码保护的区域
* 支持含有 CAPTHCA 的页面，单个开始指令和 Two Factor(双因素)验证机制f)、丰富的报告功能，包括 VISA PCI 依从性报告
* 高速的多线程扫描器轻松检索成千上万个页面
* 智能爬行程序检测 web 服务器类型和应用程序语言
* Acunetix 检索并分析网站，包括 flash 内容、SOAP 和 AJAX
* 端口扫描 web 服务器并对在服务器上运行的网络服务执行安全检查
* 可导出网站漏洞文件

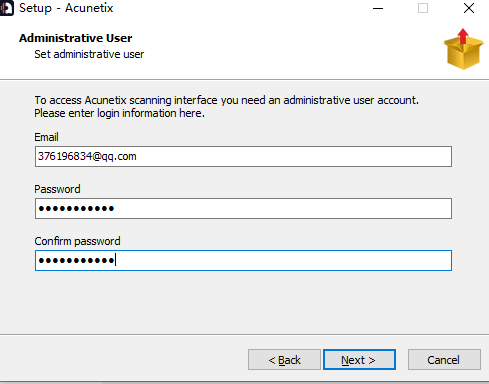
## 安装

双击

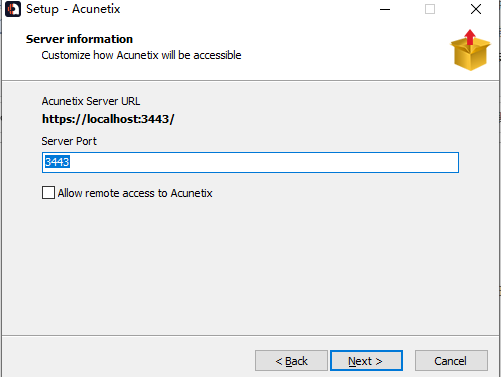


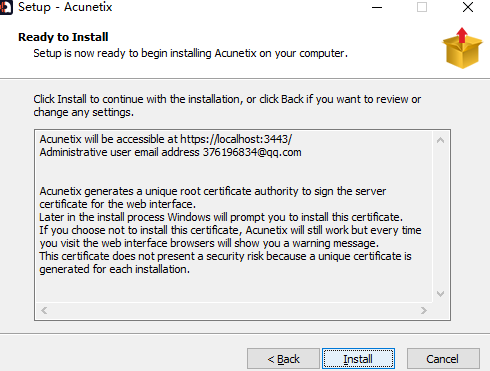




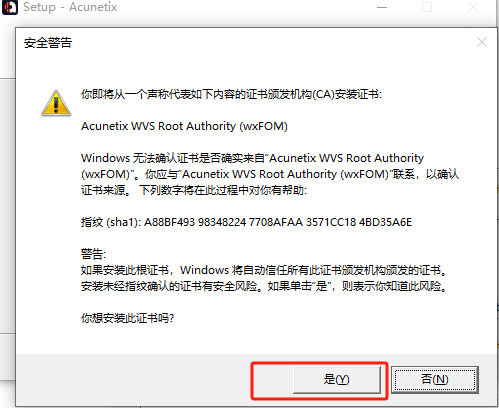


7106\*\*\*\*@jun





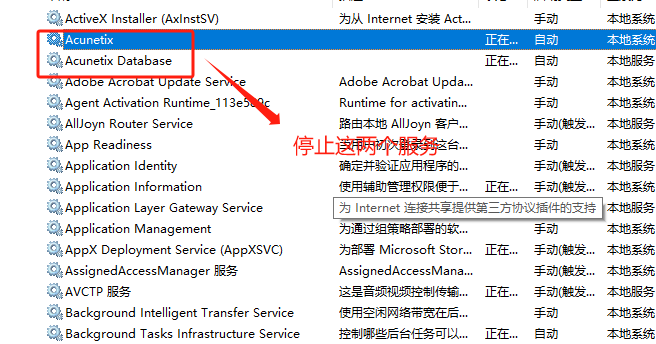
安装完成后，下载证书

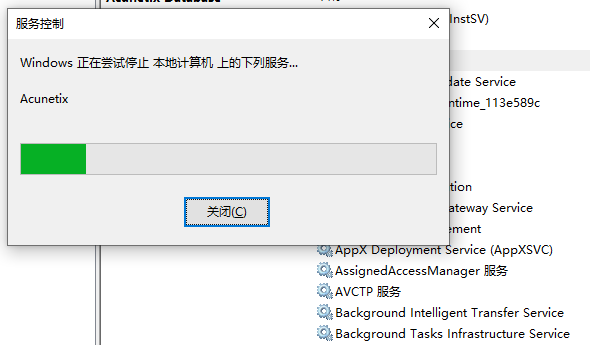


## 破解



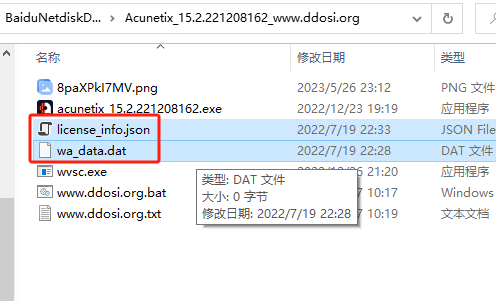
1. 进入服务界面



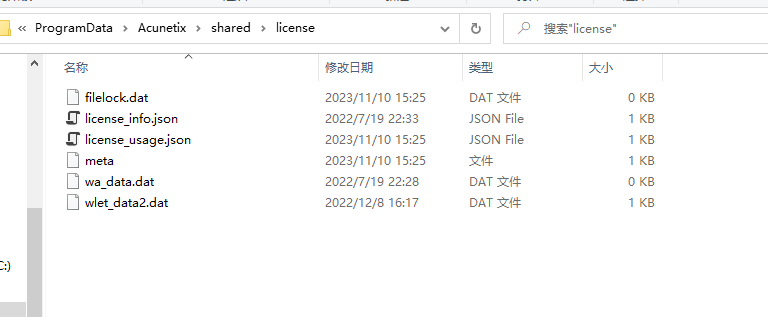


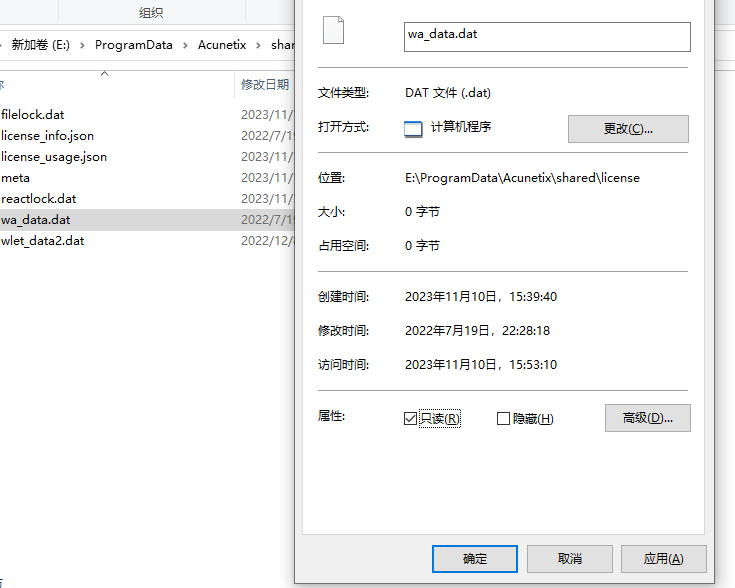


1. 将安装exe文件目录下的license\_info.json、wa\_data.dat这两个文件拷贝复制到软件安装目录下的E:\ProgramData\Acunetix\shared\license，覆盖掉原文件

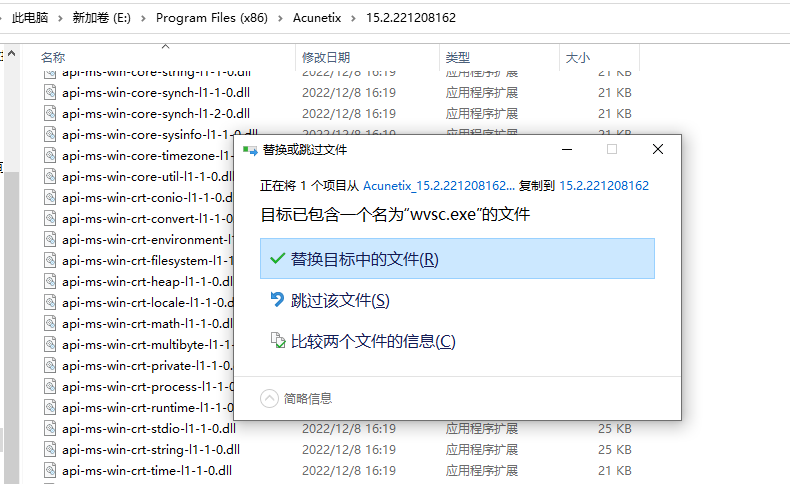


替换后如下：

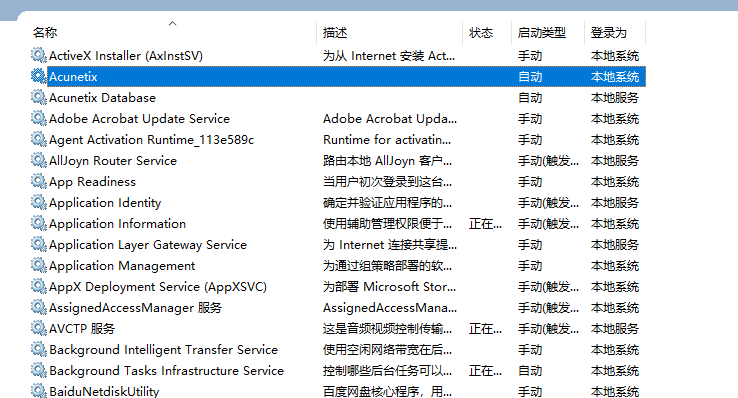
  
将这两个文件设为只读，记住，一定要



1. 将安装exe文件目录下的wvsc.exe文件拷贝复制到E:\Program Files (x86)\Acunetix\15.2.221208162下，覆盖掉原文件



1. 在服务中重新启动这两个服务



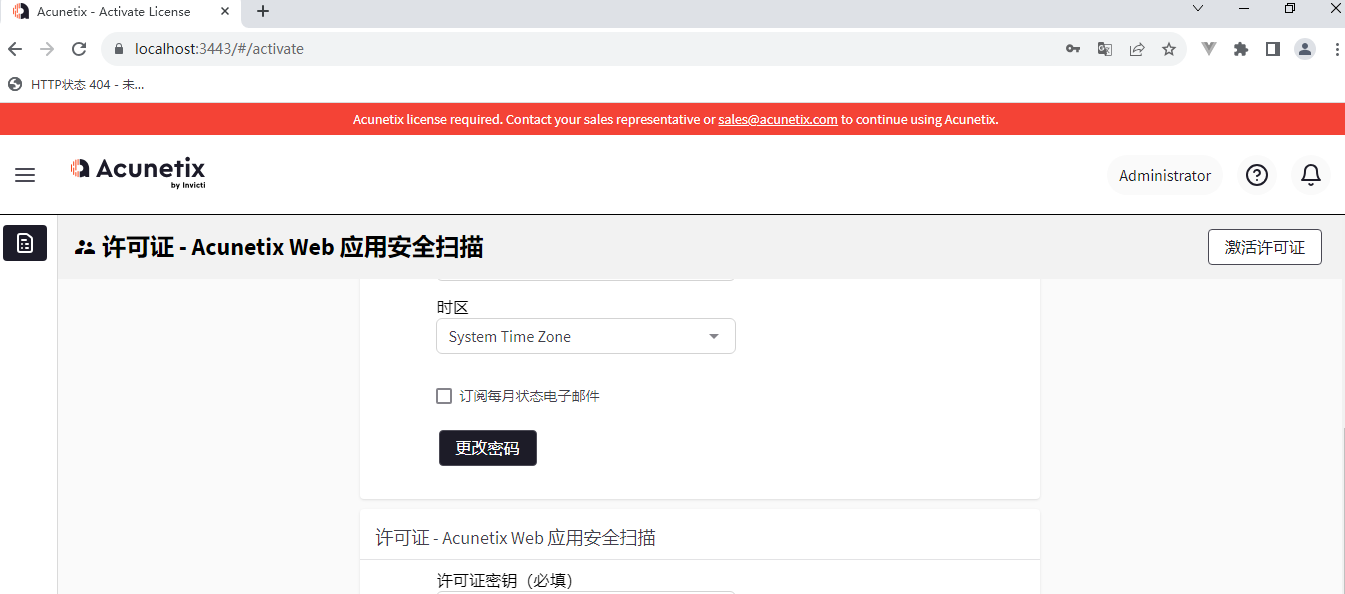
1. 登录，进入系统，输入

https://localhost:3443/#/login



账号和密码是我们安装时填写的邮箱地址和密码





# Kali环境下安装AWVS

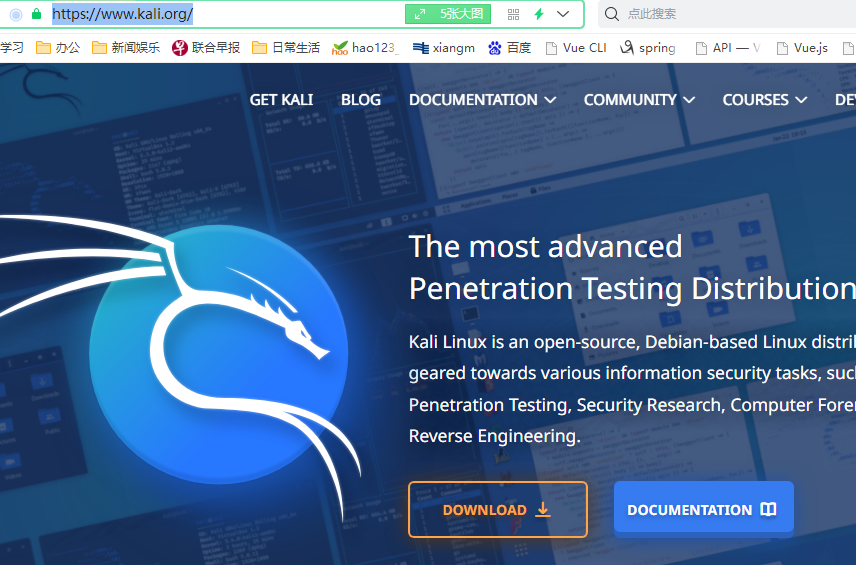
**Kali linux可以说是网络安全人员的专用系统，它是BackTrack系列的升级版。作为一个安全新手，如果你之前没有接触过BackTrack系列的话，建议直接学习使用Kali Linux。真的不要用windows学了，kali比它强多了。**

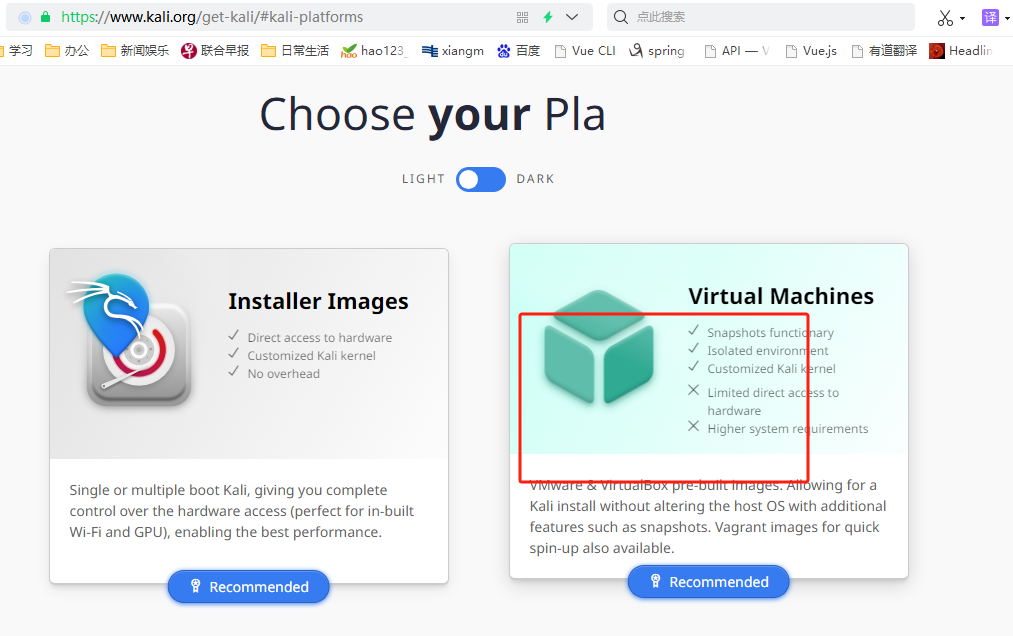
Kali Linux是一个高级渗透测试和安全审计Linux发行版。作为使用者，你可以把它理解为一个特殊的Linux发行版，集成了精心挑选的渗透测试和安全审计的工具，供渗透测试和安全设计人员使用，也可称之为平台或者框架。

## Kali 虚拟机环境下下载和使用

1. 下载虚拟机文件

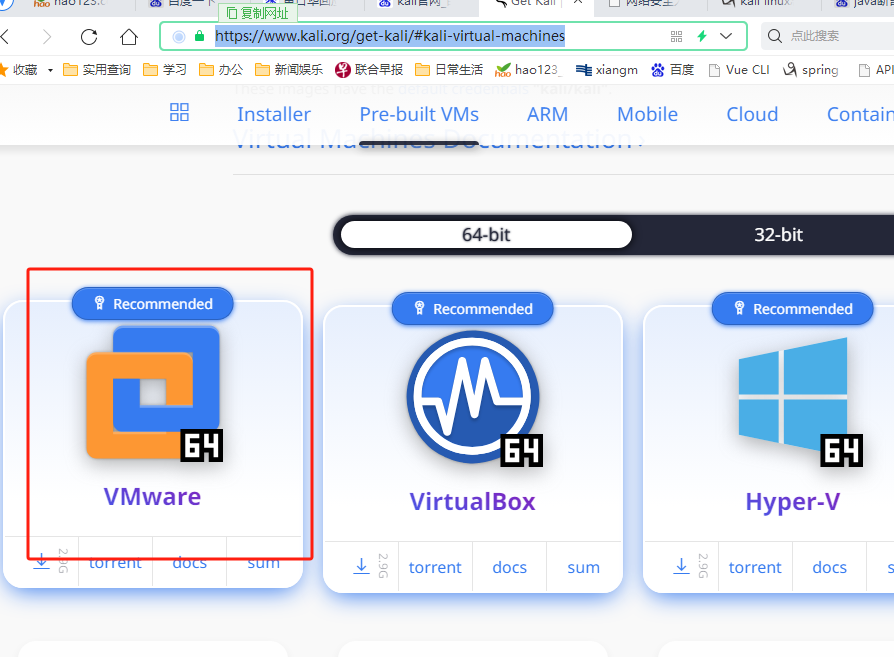
进入网站<https://www.kali.org/>，下载虚拟机环境，也可以是镜像环境自己安装



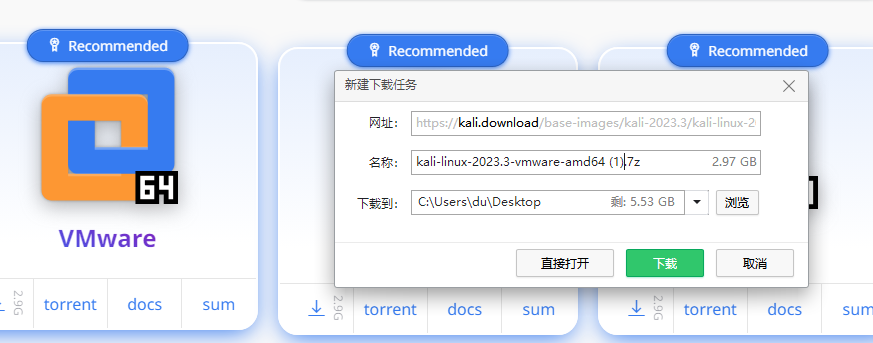


选择虚拟机直接安装

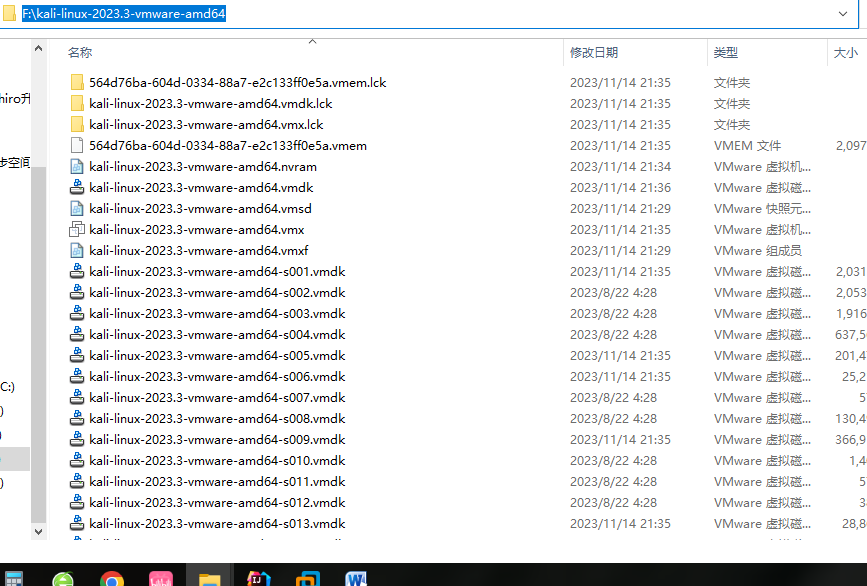
<https://www.kali.org/get-kali/#kali-virtual-machines>



下载

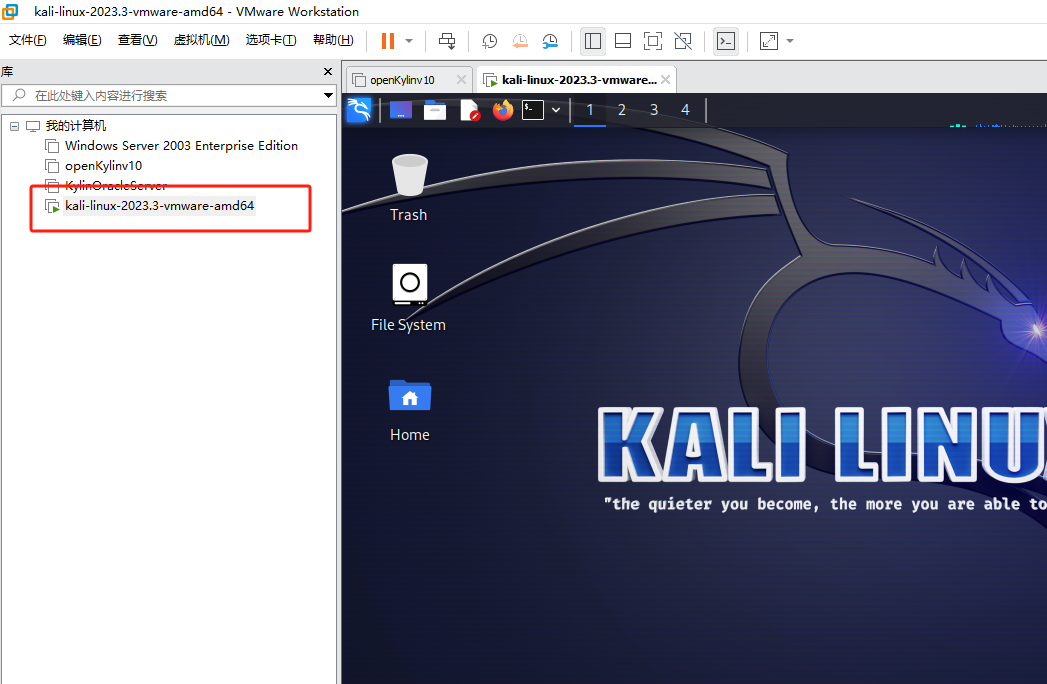


下载后解压，如下图所示：



2.打开虚拟机

通过Vmware进入虚拟机



**默认用户与密码均为kali**

用户名密码是：

**Kali/kali**

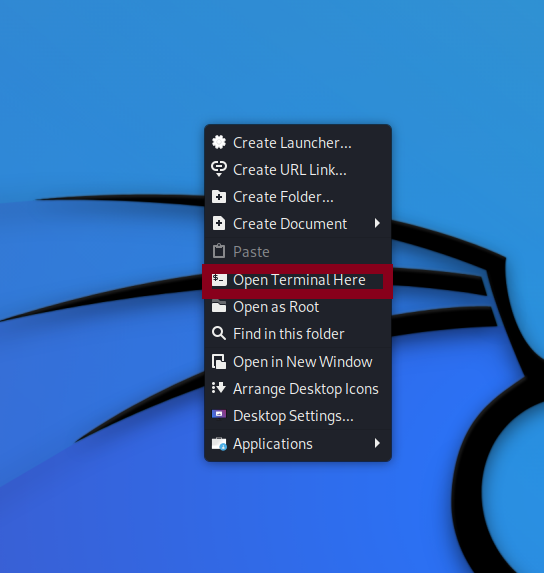


修改网络适配器

3.拿回root账号

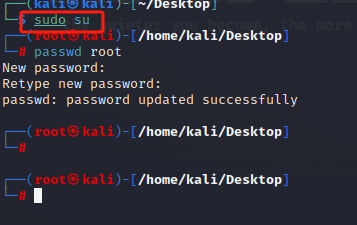
**最后是拿回root账号和密码**

进入系统，在桌面右键



在命令行

**进入root权限**  
**sudo su**  
**输入或更改密码**  
**passwd root**



密码改为12345678

1. 为了提高kali的使用速度以及获取资源，我们需要进行更换国内源。

# 官方源

deb http://http.kali.org/kali kali-rolling main non-free contrib

deb-src http://http.kali.org/kali kali-rolling main non-free contrib

#中科大

deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

#阿里云

#deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

#deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

#清华大学

#deb http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free

#deb-src https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free

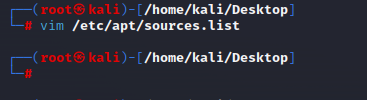
#浙大

#deb http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free

#deb-src http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free

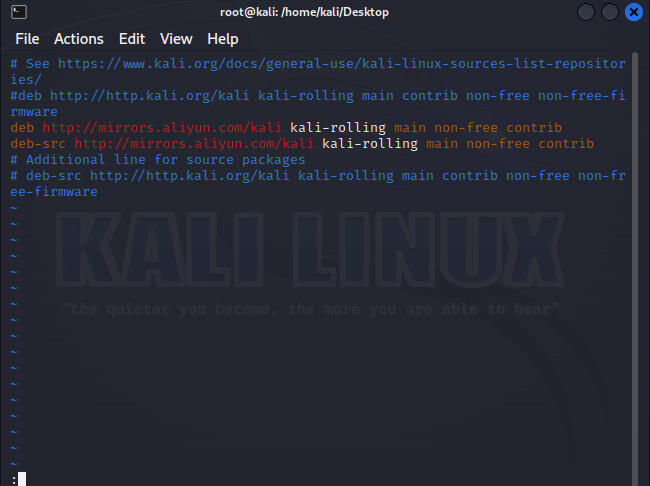
进入root权限，在终端内输入

**vim /etc/apt/sources.list**



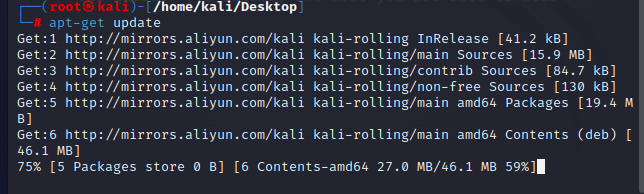
将官方源注释掉(#)或者删除，并输入国内源

按Insert键输入，按ESC后按 ' :+wq '保存



保存后进行更新，在root权限下的终端**分别依次**输入三条语句

**apt-get update**  
**apt-get dist-upgrade -y**  
**apt-get autoremove -y**

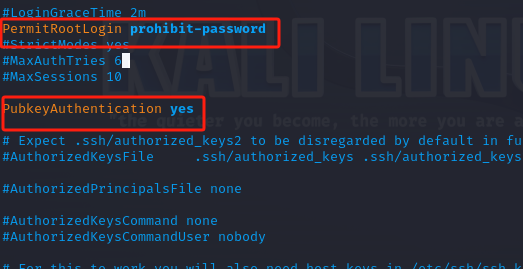


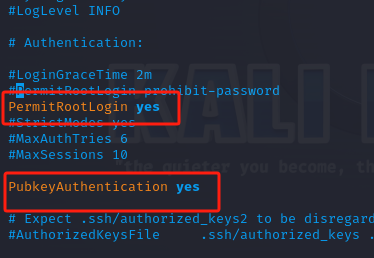
完成后

## Kali 虚拟机配置

1. 开通SSH

打开Kali [ssh配置](https://so.csdn.net/so/search?q=ssh%E9%85%8D%E7%BD%AE&spm=1001.2101.3001.7020" \t "_blank)文件，



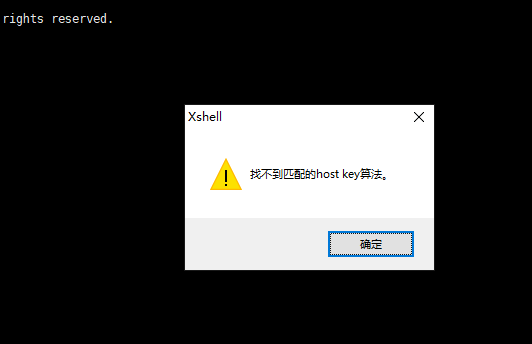


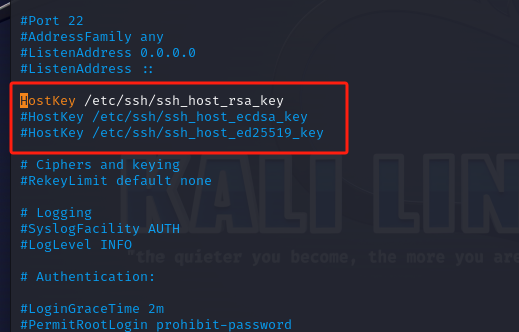
开启ssh

/etc/init.d/ssh start

查看状态

/etc/init.d/ssh status

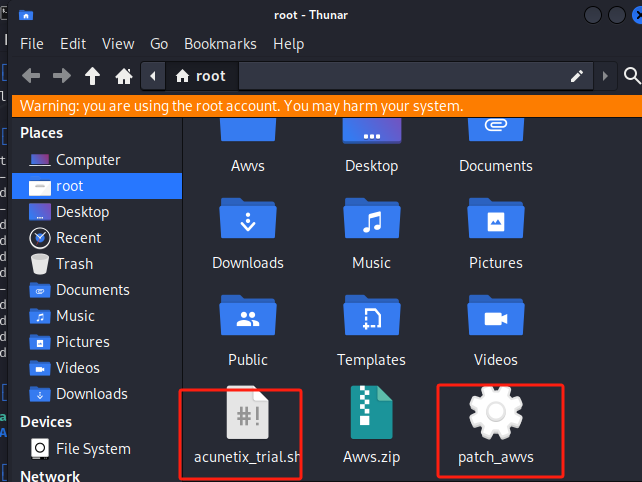




## Kali 安装AWVS

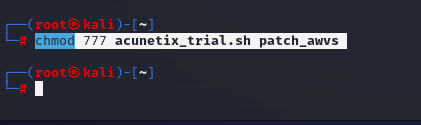
1.下载AWVS文件，把acunetix\_trial.sh和patch\_awvs两个文件拷贝到Kali，虚拟机下直接复制粘贴即可。

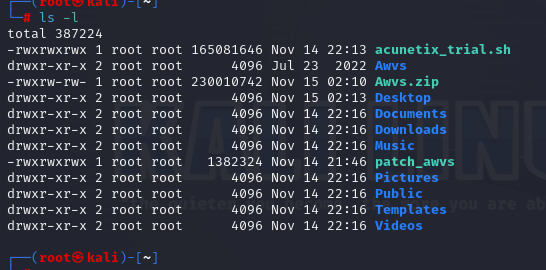




1. 赋最高权限给这两个文件

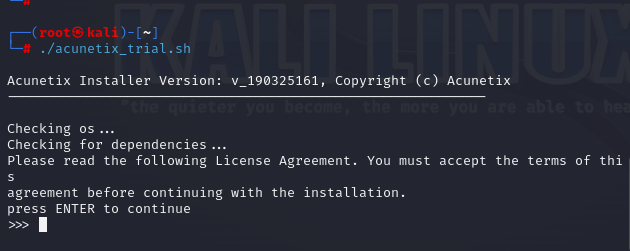
chmod 777 acunetix\_trial.sh patch\_awvs





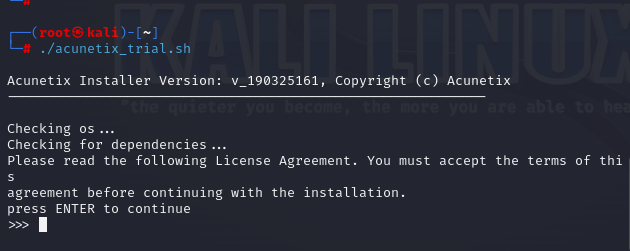
1. 安装

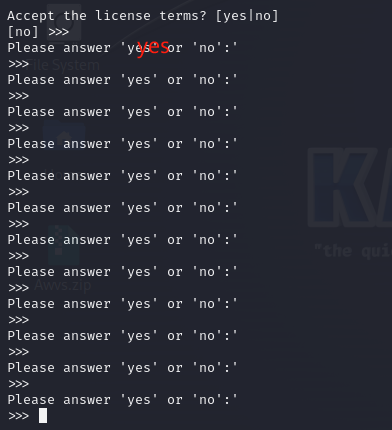
./acunetix\_trial.sh #执行安装，q退出信息提示

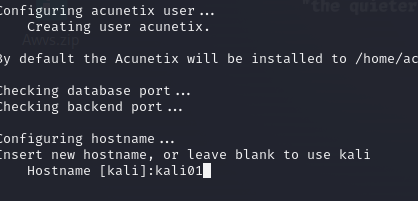


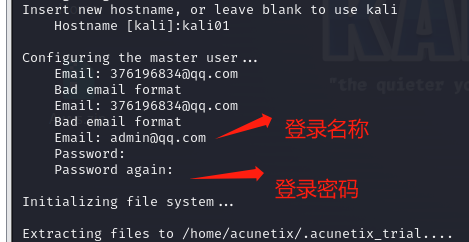
1. 按回车键继续

Yes

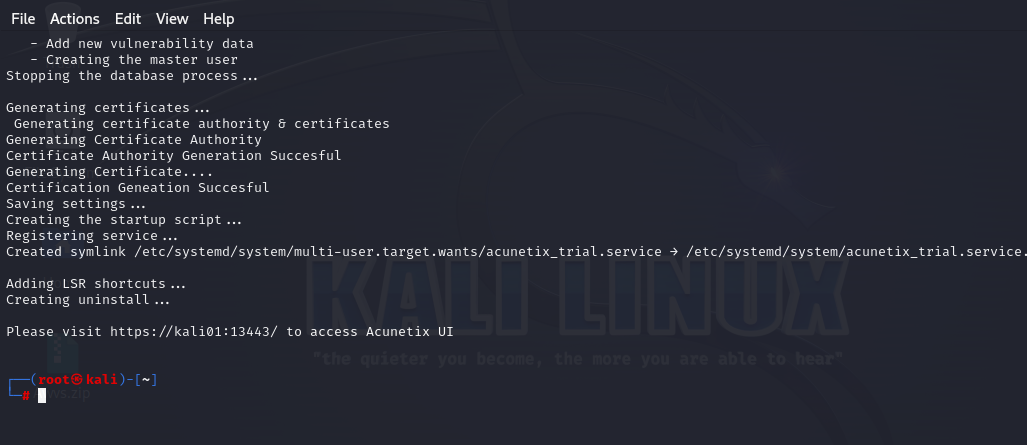








登录密码是：7106\*\*\*\*@jun



安装完成，访问如下地址进入登录界面

Please visit https://kali01:13443/ to access Acunetix UI



1. 激活，执行破解

拷贝激活文件到安装目录

cp patch\_awvs /home/acunetix/.acunetix\_trial/v\_190325161/scanner

然后进入安装目录

cd /home/acunetix/.acunetix\_trial/v\_190325161/scanner

授权

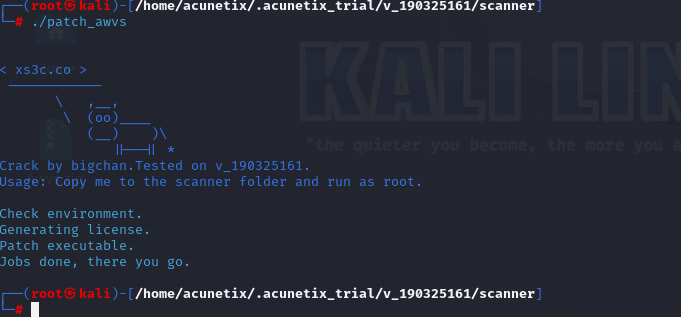
chmod 777 patch\_awvs



1. 激活

在 /home/acunetix/.acunetix\_trial/v\_190325161/scanner 执行如下命令

./patch\_awvs



1. 为了保证原始licence不失效，执行如下命令，否则licence会被修改，无法完全破解

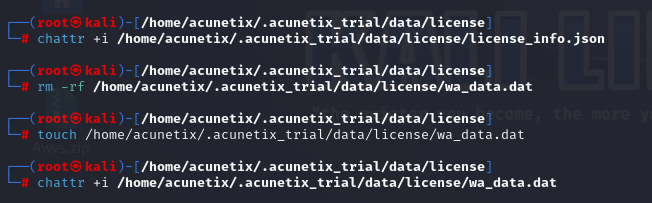
chattr +i /home/acunetix/.acunetix\_trial/data/license/license\_info.json

rm -rf /home/acunetix/.acunetix\_trial/data/license/wa\_data.dat

touch /home/acunetix/.acunetix\_trial/data/license/wa\_data.dat

chattr +i /home/acunetix/.acunetix\_trial/data/license/wa\_data.dat

chattr +I 命令的含义是：只允许以追加的方式读取文件

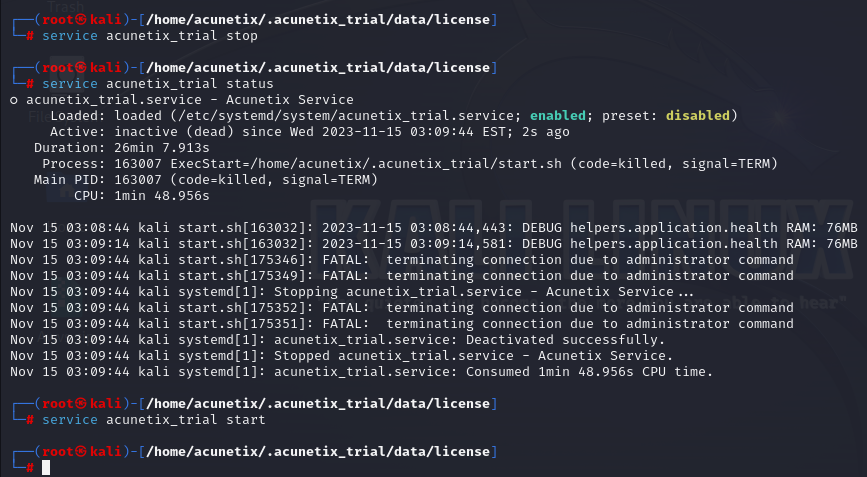


1. 重新启动服务

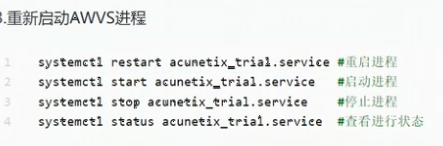
service acunetix\_trial status

service acunetix\_trial start

service acunetix\_trial stop

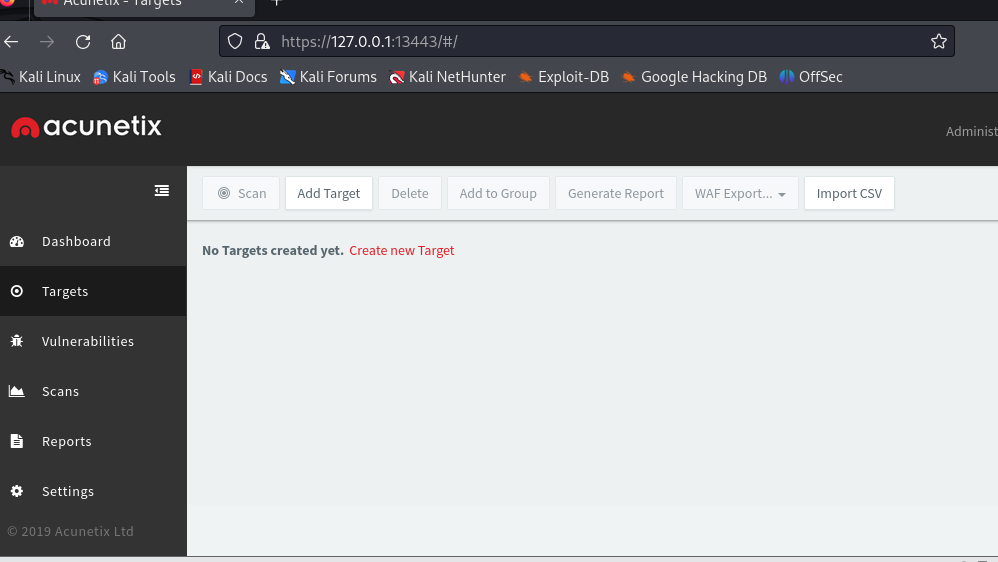


或者

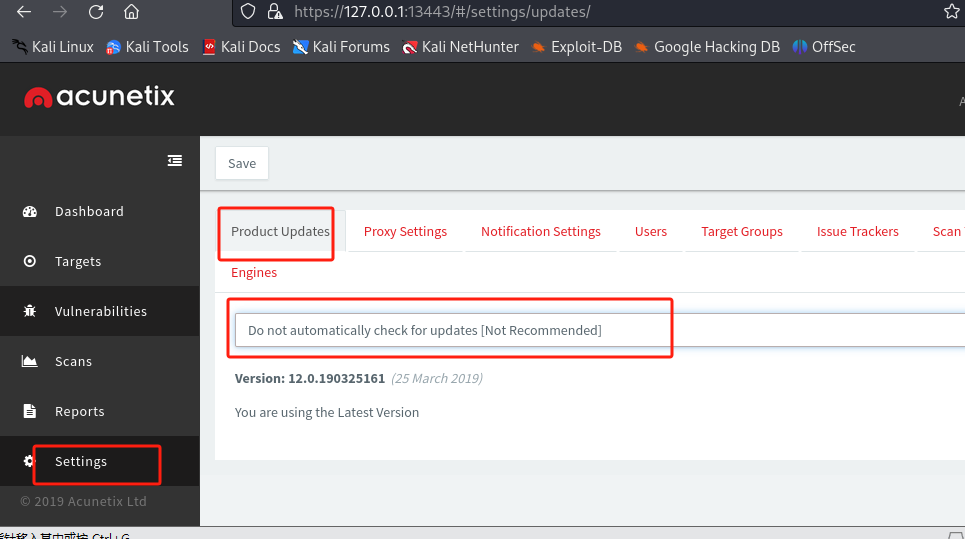


1. 访问<https://127.0.0.1:13443/> 进入登录页面

[输入admin@qq.com/7106\*\*\*\*@jun](mailto:输入admin@qq.com/7106****@jun)登录



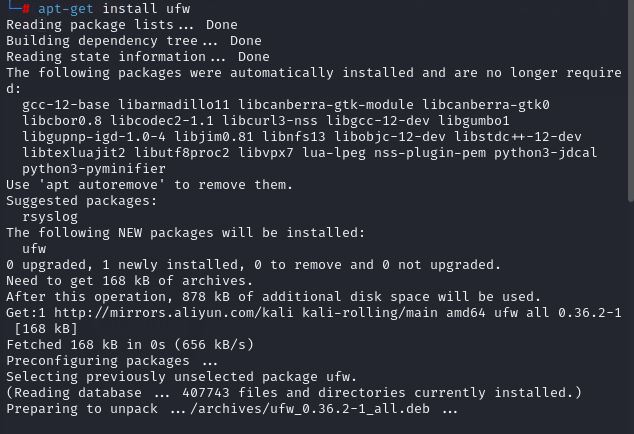
1. 设置不自动更新



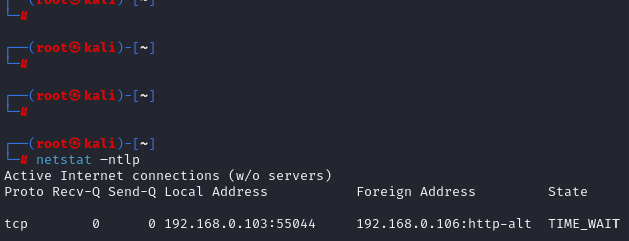
## Kali 开通防火墙

首先需要安装ufw命令

apt-get install ufw



netstat –ntlp #查看端口号



netstat -aptn #查看50050端口

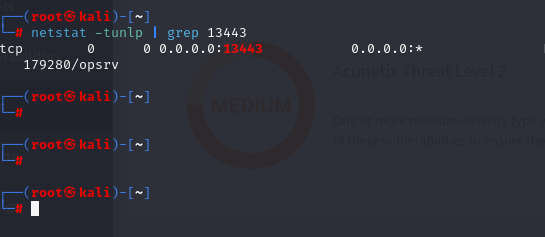
- 根据端口号，查询进程名称和进程ID

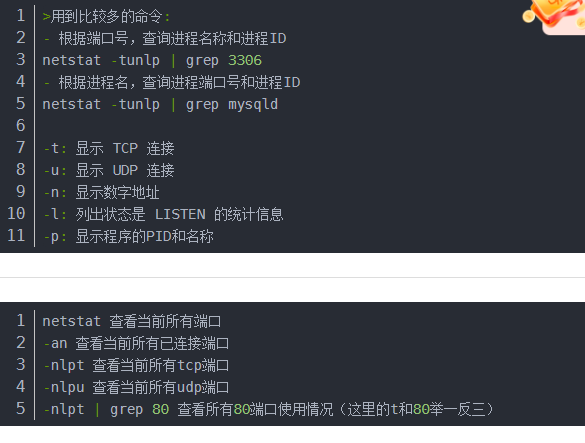
netstat -tunlp | grep 3306

netstat -tunlp | grep 13443

- 根据进程名，查询进程端口号和进程ID

netstat -tunlp | grep mysqld





ufw相关命令

ufw status #检查防火墙的状态(默认 inactive)

ufw version #防火墙版本

ufw enable # 启动ufw防火墙

ufw disable # 关闭ufw防火墙

ufw default deny # 默认禁止访问所有

ufw allow 22/tcp # 开放22/TCP端口

ufw allow 53 # 开放53端口(tcp/udp)

ufw deny 3306 # 禁止外部访问

ufw delete allow 22 #删除已经添加过的规则

ufw allow from 192.168.1.100 # 允许此IP访问所有的本机端口

ufw delete allow from 192.168.1.100 # 删除上面的规则

ufw status numbered #查看规则，显示行号

ufw delete 3 # 删除第三条规则

ufw disable # 关闭ufw

ufw deny 8888 # 禁止对8888端口的访问

ufw allow proto tcp from 192.168.0.1 to any port 22

-# 打开来自192.168.0.1的tcp请求的22端口

开通13443 端口

ufw allow 13443/tcp # 开放22/TCP端口

## Kali 使用MariaDB

MariaDB[数据库管理系统](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%BA%93%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F/1239101?fromModule=lemma_inlink" \t "_blank)是[MySQL](https://baike.baidu.com/item/MySQL/471251?fromModule=lemma_inlink)的一个分支，主要由[开源社区](https://baike.baidu.com/item/%E5%BC%80%E6%BA%90%E7%A4%BE%E5%8C%BA/1373560?fromModule=lemma_inlink" \t "_blank)在维护，采用[GPL](https://baike.baidu.com/item/GPL/2357903?fromModule=lemma_inlink)[授权许可](https://baike.baidu.com/item/%E6%8E%88%E6%9D%83%E8%AE%B8%E5%8F%AF/22991584?fromModule=lemma_inlink) MariaDB的目的是完全兼容MySQL，包括[API](https://baike.baidu.com/item/API/10154?fromModule=lemma_inlink" \t "_blank)和[命令行](https://baike.baidu.com/item/%E5%91%BD%E4%BB%A4%E8%A1%8C/196110?fromModule=lemma_inlink" \t "_blank)，使之能轻松成为MySQL的代替品。在[存储引擎](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%BC%95%E6%93%8E/8969956?fromModule=lemma_inlink" \t "_blank)方面，使用XtraDB来代替MySQL的InnoDB。 MariaDB由MySQL的创始人[Michael Widenius](https://baike.baidu.com/item/Michael%20Widenius/5446947?fromModule=lemma_inlink" \t "_blank)主导开发，他早前曾以10亿美元的价格，将自己创建的公司[MySQL AB](https://baike.baidu.com/item/MySQL%20AB/2620844?fromModule=lemma_inlink" \t "_blank)卖给了[SUN](https://baike.baidu.com/item/SUN/69463?fromModule=lemma_inlink" \t "_blank)，此后，随着SUN被[甲骨文](https://baike.baidu.com/item/%E7%94%B2%E9%AA%A8%E6%96%87/471435?fromModule=lemma_inlink" \t "_blank)收购，MySQL的所有权也落入[Oracle](https://baike.baidu.com/item/Oracle/301207?fromModule=lemma_inlink" \t "_blank)的手中。MariaDB名称来自Michael Widenius的女儿Maria的名字。

MariaDB基于事务的Maria[存储引擎](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%BC%95%E6%93%8E/8969956?fromModule=lemma_inlink)，替换了[MySQL](https://baike.baidu.com/item/MySQL?fromModule=lemma_inlink)的[MyISAM](https://baike.baidu.com/item/MyISAM?fromModule=lemma_inlink" \t "_blank)存储引擎，它使用了Percona的 XtraDB，InnoDB的变体，分支的开发者希望提供访问即将到来的MySQL 5.4 InnoDB性能。这个版本还包括了 PrimeBase XT (PBXT) 和 FederatedX[存储引擎](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%BC%95%E6%93%8E?fromModule=lemma_inlink" \t "_blank)。

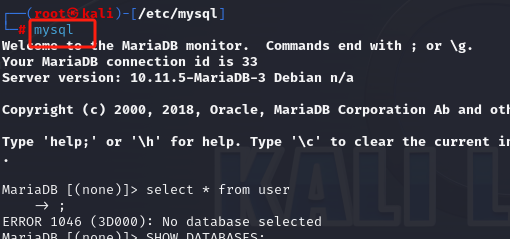
操作如下：

启动服务：service mariadb start

查看服务状态：service mariadb status

查看3306端口：netstat -tunlp | grep 3306

MariaDB 或者mysql 进入数据库



# Kali 安装mysql

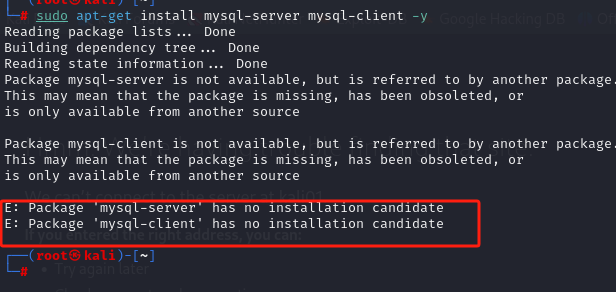
默认情况下，AWVS使用SQLite作为默认数据库。但是，为了实现最佳性能和可靠性，请考虑使用MySQL或Microsoft SQL Server等更强大的数据库。首先，如果您使用的是SQLite，可以跳过此步骤。

安装和配置MySQL，需要使用以下命令安装：

1. 安装MYSQL客户端和服务端

sudo apt-get install mysql-server mysql-client –y

出现如下错误



这个错误通常是由于apt-get源中没有包含mysql-server软件包而导致的。我们可以通过更新apt-get的源列表，从而获得更多的软件包。

阿里云数据源没有mysql，我们增加数据源

我们可以通过以下指令来新增mysql源：

sudo add-apt-repository 'deb http://archive.ubuntu.com/ubuntu trusty universe'

但是会报如下错误



sudo: add-apt-repository: command not found

先安装apt-get -y install software-properties-common

再增加数据源

具体安装命令如下：

apt-get -y install software-properties-common

sudo add-apt-repository 'deb http://archive.ubuntu.com/ubuntu trusty universe'

sudo apt-get update

再安装msql，验证也没有通过

apt-get install mysql-server mysql-client -y # 安装MySQL客户端和服务端

systemctl enable mysql.service # 开机自启服务

systemctl start mysql.service # 启动服务

mysql\_secure\_installation # 配置安全选项并设置密码

# Kali安装配置BurpSutepro

## burpsuite介绍

**Burp Suite**是Web应用程序测试的最佳工具之一，其多种功能可以帮我们执行各种任务.请求的拦截和修改，扫描web应用程序漏洞，以暴力破解登陆表单，执行会话令牌等多种的随机性检查。由于Burpsuite功能强大，各项参数十分复杂，下面我们只着重于软件的主要功能，更多细节见https://support.portswigger.net/。由于Burp的强大性，本文完整的讨论其功能特点（Burp软件版本1.6）：

**Target（目标）**，渗透测试的目标URL。

**Proxy（代理）**，Burp使用代理，默认端口为8080，使用此代理，我们可以截获并修改从客户端到Web应用程序的数据包。

**Spider（抓取）**，其功能是用来抓取Web应用程序的链接和内容等，它可以扫描出网站上的所有链接，通过这些链接的详细扫描来发现Web应用程序的漏洞。

**Scanner（扫描器）**，主要用来扫描Web应用程序的漏洞。

**Intruder（入侵）**，此模块有多种功能，如漏洞利用，Web应用程序模糊测试，暴力破解等。

**Repeater（中继器）**，重放，用来模拟数据包的请求与响应过程。**Sequencer**，此功能主要用来检查Web应用程序提供的会话令牌的随机性，并执行各种测试。

**Decoder（解码）**，解码和编码。

**Comparer（比较）**，比较数据包之间的异同。

**Extender（扩展）**，

Burp的一些高级功能。

**Options（选项）**，Burp通用设置选项。

**Alerts（警告）**，Burp的一些状态提示。

## 删除原burpsuite社区版

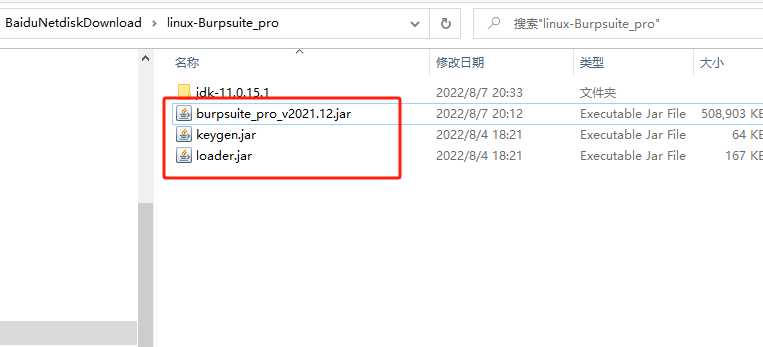
cd /usr/bin

sudo rm -rf /usr/share/burpsuite

sudo rm -rf burpsuite

## 安装

1、把下图三个文件拷贝到/usr/local/BurpsuitePro/,并对该目录授权

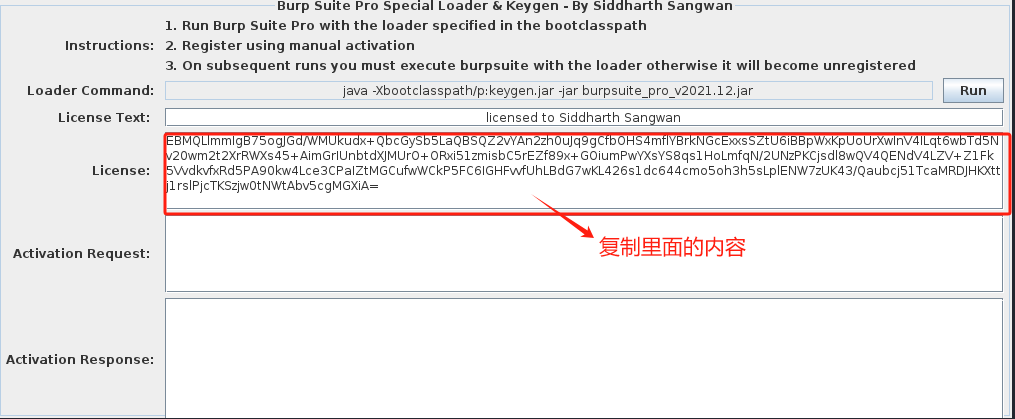


2、授权 chmod 777 BurpsuitePro

3、启动激活程序

java -jar keygen.jar

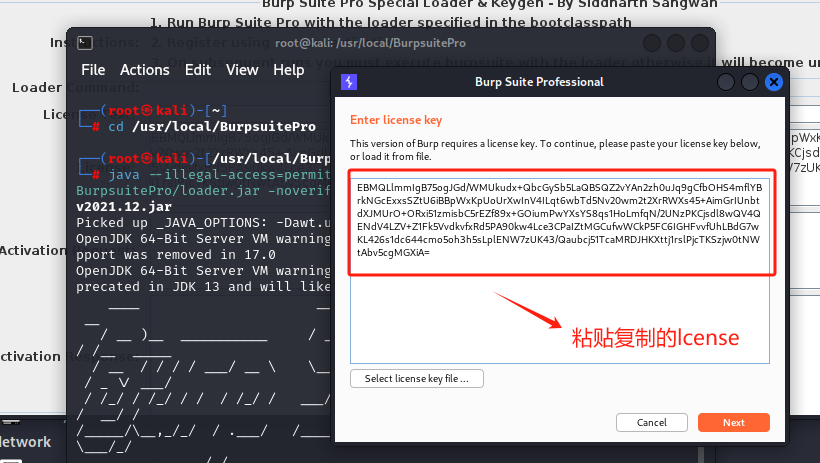
弹出如下窗口，复制License的内容



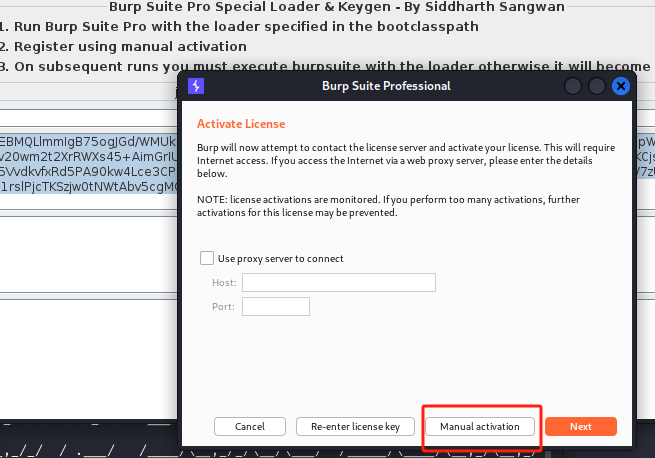
然后在启动BurpSuite

java --illegal-access=permit -Dfile.encoding=utf-8 -javaagent:/usr/local/BurpsuitePro/loader.jar -noverify -jar /usr/local/BurpsuitePro/burpsuite\_pro\_v2021.12.jar

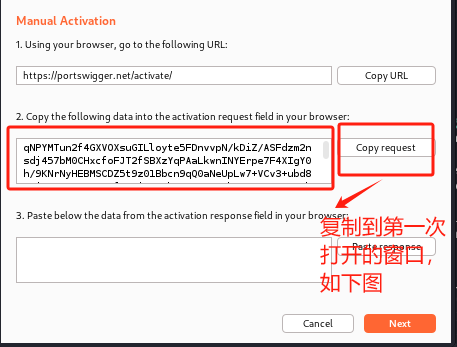




点击Next，进入下一个窗口；在下一个窗口，不要点击Next，点击Manual Activation,进入破解页面，



进入破解页面，然后点击Copy request ,拷贝数据，到第一次打开的窗口中把拷贝的数据粘贴到，会自动生成

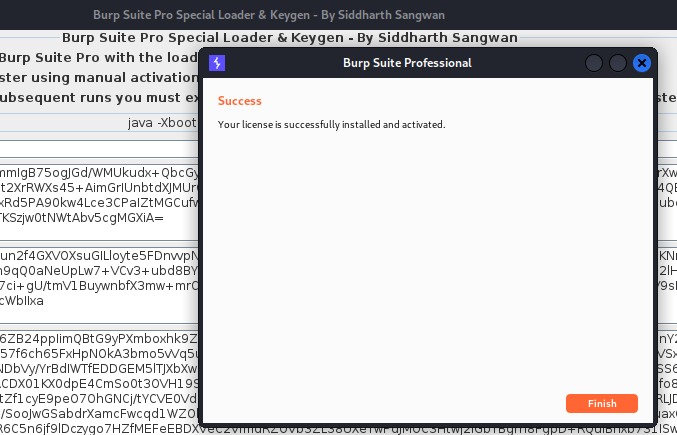






然后把生成的拷贝到下图所示区域





总的流程是：



4、在/usr/bin下添加专业版的burpsuite

添加之前要删除社区版本

cd /usr/bin

sudo rm -rf burpsuite

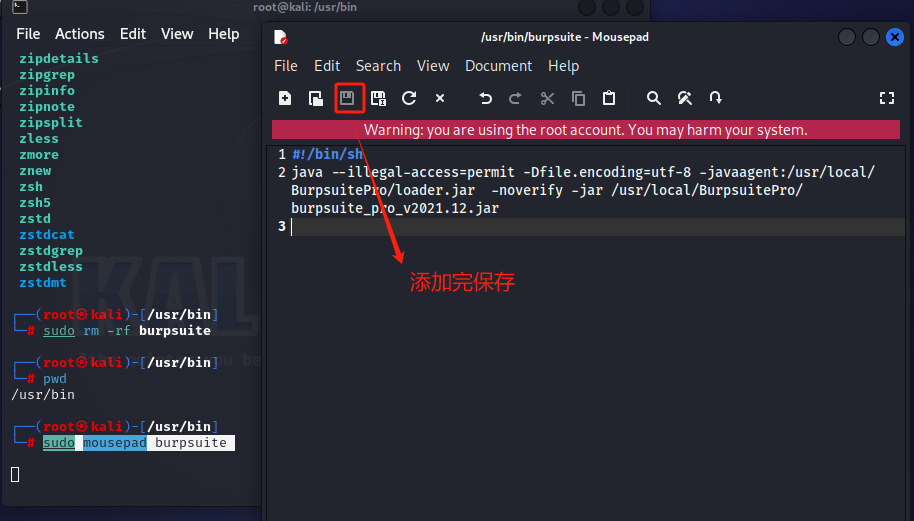
在/usr/bin下添加专业版的burpsuite

sudo mousepad burpsuite

在文本中添加如下内容：

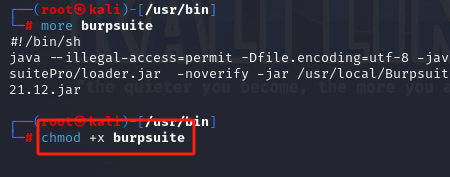
#!/bin/sh

java --illegal-access=permit -Dfile.encoding=utf-8 -javaagent:/usr/local/BurpsuitePro/loader.jar -noverify -jar /usr/local/BurpsuitePro/burpsuite\_pro\_v2021.12.jar



添加可执行权限

chmod +x burpsuite



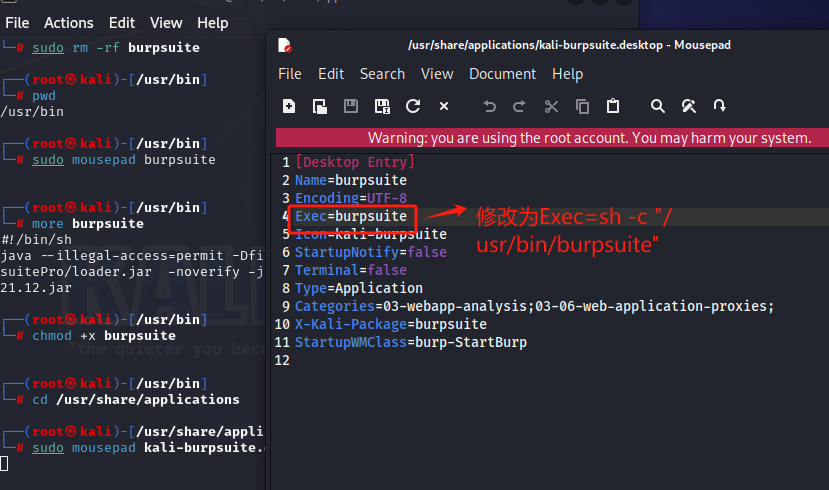
添加快捷访问：

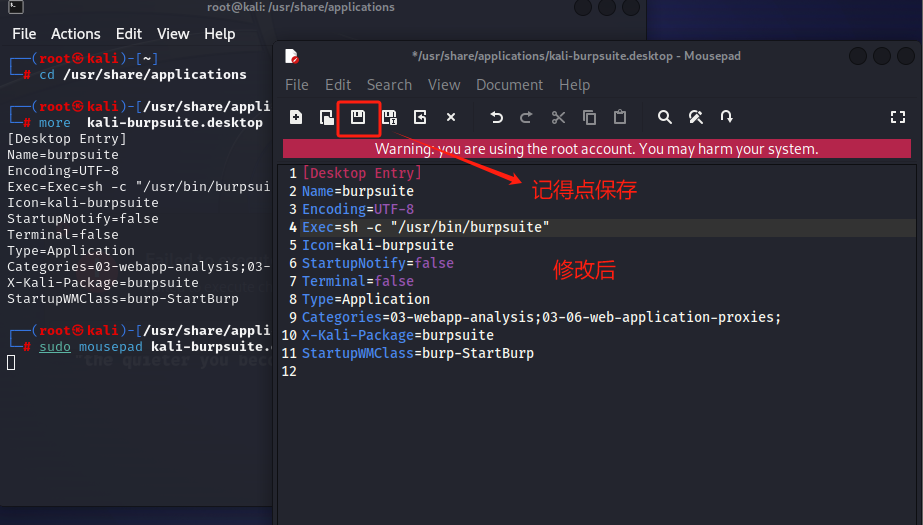
cd /usr/share/applications

sudo mousepad kali-burpsuite.desktop

弹出的文本中修改内容为

Exec=sh -c "/usr/bin/burpsuite"



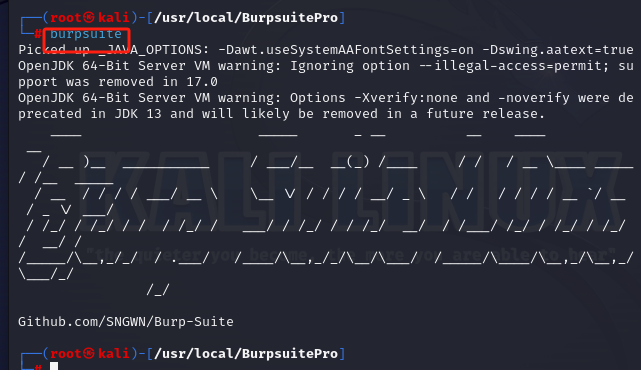


## 启动

**方式1：**

在命令行输入：

burpsuite



**方式2：**



**方式3：**

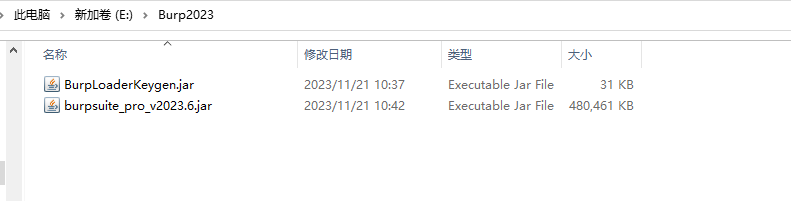
如下命令：

java --illegal-access=permit -Dfile.encoding=utf-8 -javaagent:/usr/local/BurpsuitePro/loader.jar -noverify -jar /usr/local/BurpsuitePro/burpsuite\_pro\_v2021.12.jar

# Windows配置BurpSuitepro

环境：jdk1.8,windows10

## 下载BurpSuitepro



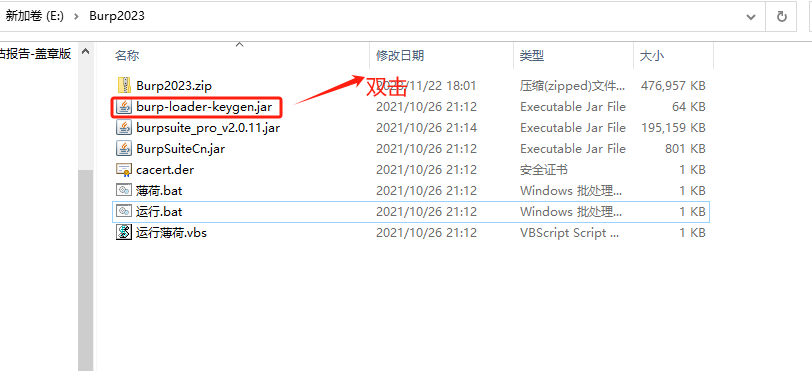
## 安装

1、下载安装包后，如下图所示：

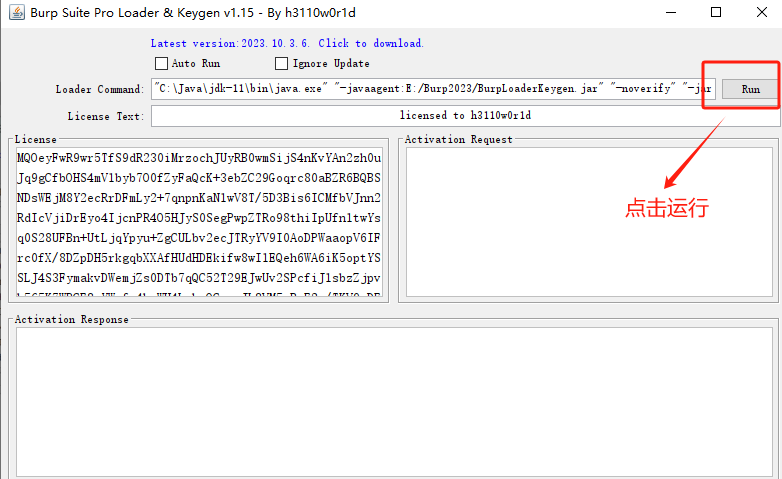


2、安装

在“E:\Burp2023”路径下双击文件“burp-loader-keygen.jar”进行运行。



打开如下界面：



运行程序后，效果如上图所示，接着点击run

**补充：可能遇到双击“burp-loader-keygen”没反应的情况，如果遇到这种情况，可以在cmd中用java打开它。（这里打不开大概率是环境变量配置有问题，可以检查一下环境变量配置的是否有问题）**

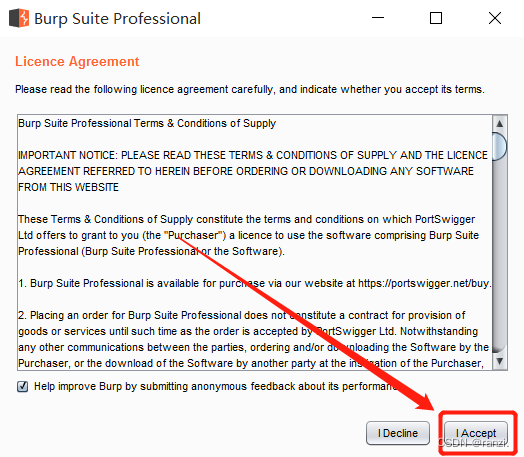
**在文件路径栏输入cmd即可在当前文件打开cmd，然后输入：**

**java -jar burp-loader-keygen.jar**

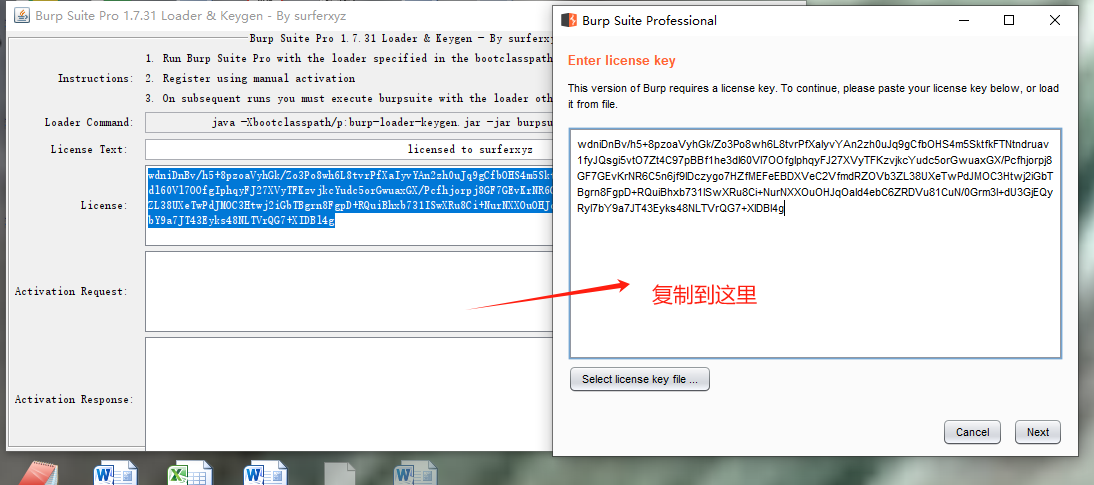
如果**还可能遇到点击“run”没反应的情况，如果遇到这种情况，可以回到文件列表手动点击“运行薄荷.vbs”或者点击“运行.bat”。**

Next

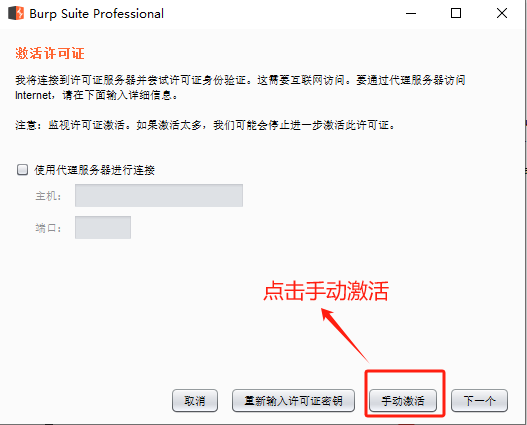
等待约7s后点击【I Accept】



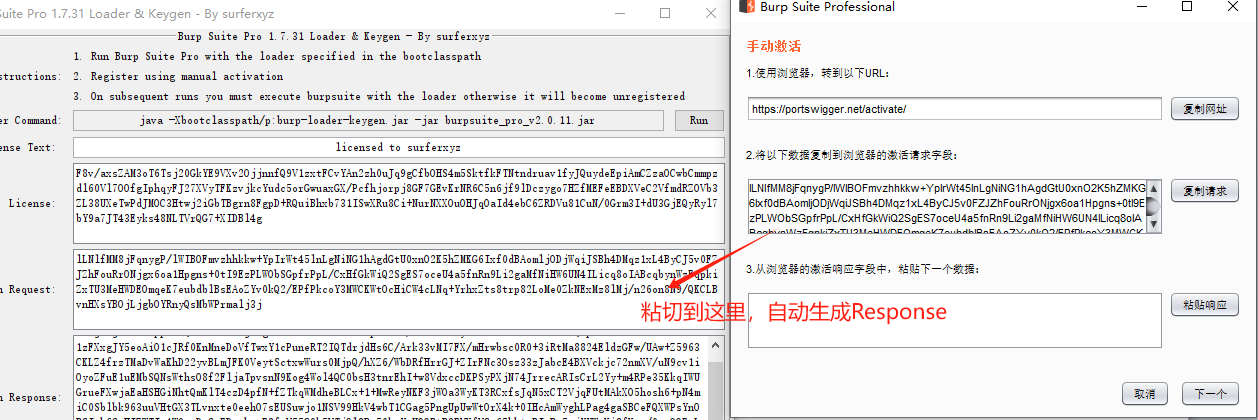
将左边窗口里的代码复制后粘贴到右面窗口

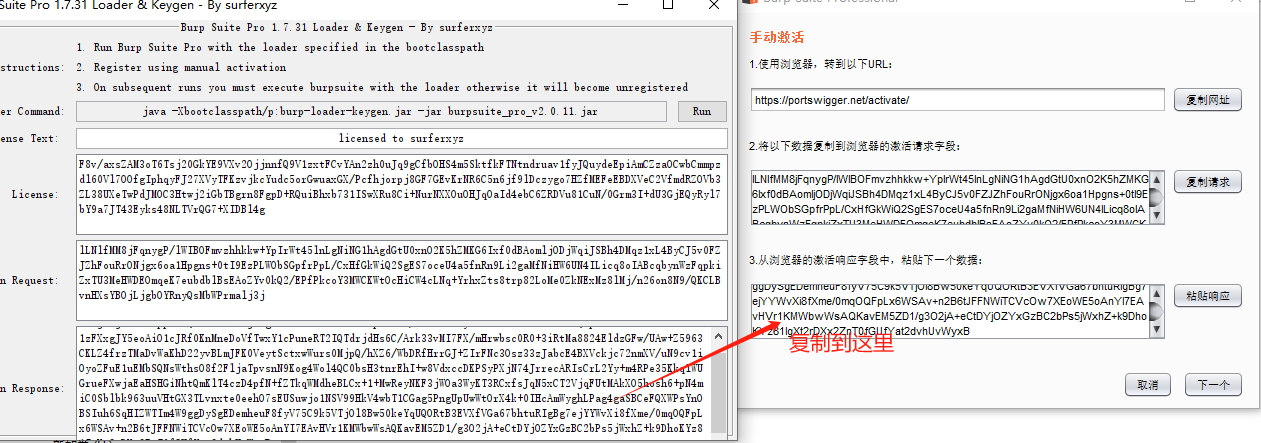


点击Next

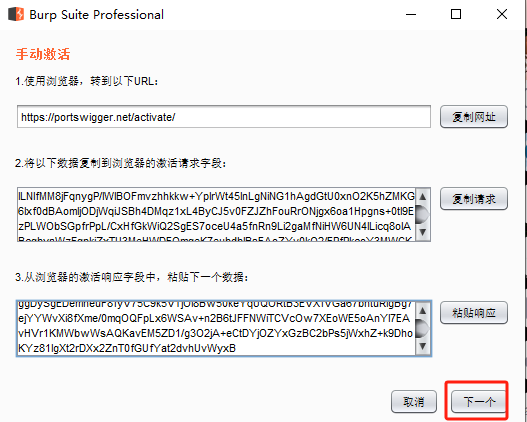


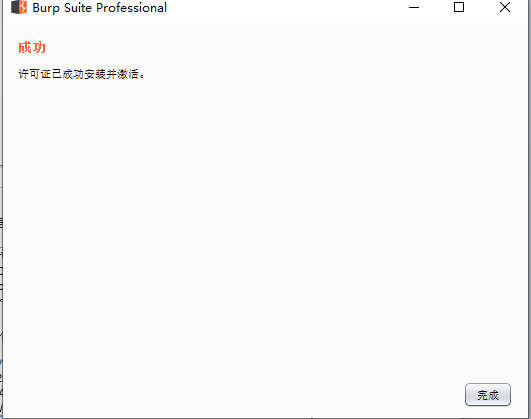
打开如下界面，在右面窗口点击【Copy request】后将代码粘贴到左面窗口

将左边窗口里的代码复制后粘贴到右面窗口



点击next





**点击【**Start Burp**】**

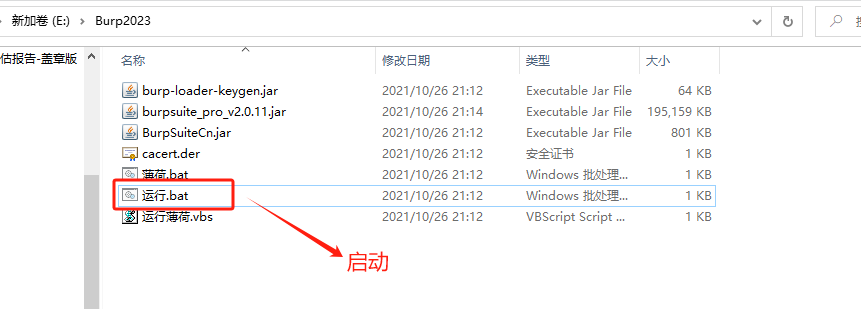


**至此，BurpSuit就已经破解并成功打开了！**

## 设置快捷方式

每次点“运行.bat”即可打开burpsuite。

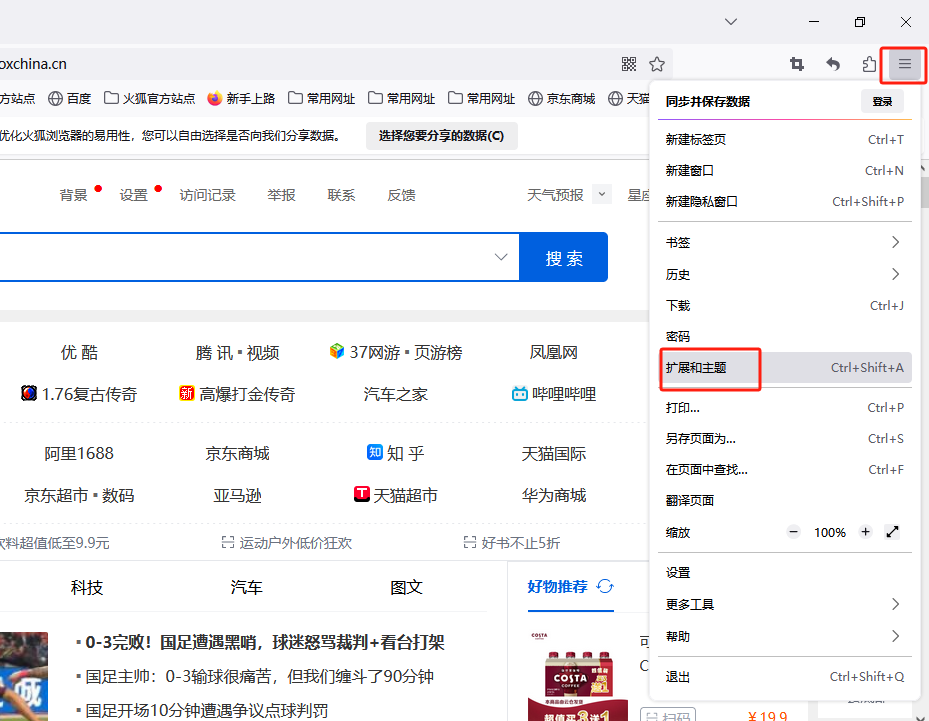
可以将此bat文件右键添加快捷方式方便打开。



## 配置代理

**这里推荐大家使用火狐浏览器**

**1.打开火狐浏览器，点击【扩展和主题】**



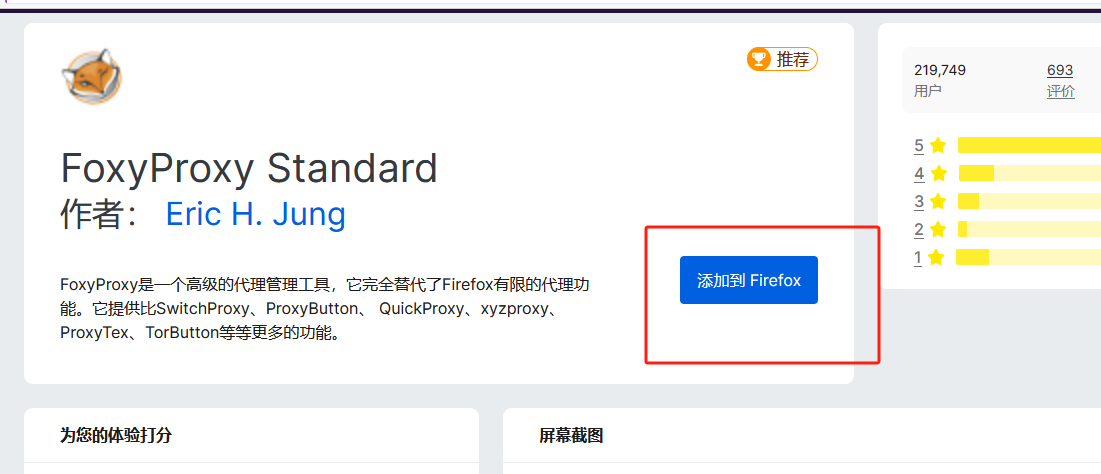
**2.在搜索框输入“FoxyProxy Standard”后搜索**



3.点击第一个



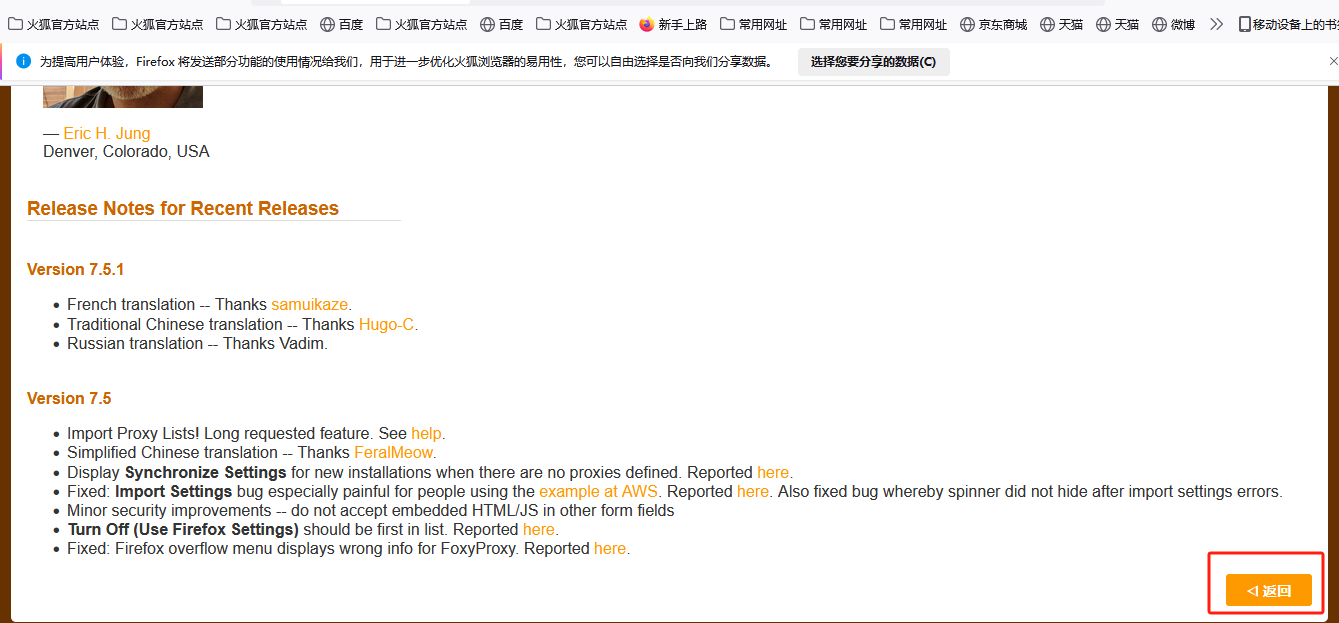
4.点击【添加到 Firefox】



点击“添加”



5.在弹出的页面下滑后**点击【返回】**



6.**点击【添加**



7.代理ip地址和端口处分别输入“127.0.0.1”、“8080”后点击【保存】



8.**得到以下页面即配置完成**



9.**结束**

**至此，浏览器代理配置就已经完成了！**

# Nessus（漏洞扫描工具）

## 说明

Nessus 是一款知名的漏洞扫描工具，由 Tenable Network Security 公司开发和维护。它被广泛用于评估计算机系统和网络中的漏洞和安全风险。Nessus 通过扫描目标系统，自动化地检测和识别系统中存在的已知漏洞、弱点和配置错误，然后生成相应的报告，帮助安全专业人员评估和修复系统中的安全问题。

Nessus 具有广泛的漏洞检测能力，包括操作系统漏洞、网络服务漏洞、应用程序漏洞等。它支持多种扫描类型，如主机扫描、网络扫描、Web 应用程序扫描等，可以灵活地满足不同环境和需求的安全评估和扫描任务。

Nessus 提供了用户友好的图形界面，以及强大的漏洞库和定期更新的漏洞签名，使其成为企业和安全专业人员进行漏洞扫描和评估的重要工具之一。