

渗透工具环境安装

Java环境安装

Windows安装JDK8

Linux安装JDK8

Mac安装JDK8

Python环境安装

Windows安装Python2/3

Linux安装Python2/3

Mac安装Python2/3

Linux-Kali配置与使用

VMware软件安装

下载vmware

安装vmware

激活vmware

VMware安装Kali

Kali简介

Kali下载

Vmware安装Kali

Linux使用基础

Linux简介

Linux目录结构

Linux文件属性

文件目录管理

VIM编辑器

Kali配置

用户配置

网络配置

设置APT源

APT使用

设置中文

配置Python

Git使用

SSH登录

Kali工具

#2课时

渗透工具环境安装

Java环境安装

Windows安装JDK8

- 下载 **JDK8**

<https://www.oracle.com/java/technologies/javase-jdk8-downloads.html>

账号密码: https://blog.csdn.net/Virgil_K2017/article/details/90260880

账号: iwei@xiaostudy.com

密码: OracleTest1234

- 安装 **JDK8**

1. 双击打开下载的 `jdk-xx-windows-x64.exe`，进入安装向导



2. 点击下一步，进入定制安装界面，可以按需要修改 JDK 安装目录



3. 下一步，进入 `jre` 安装界面



4. 下一步，等待安装完成



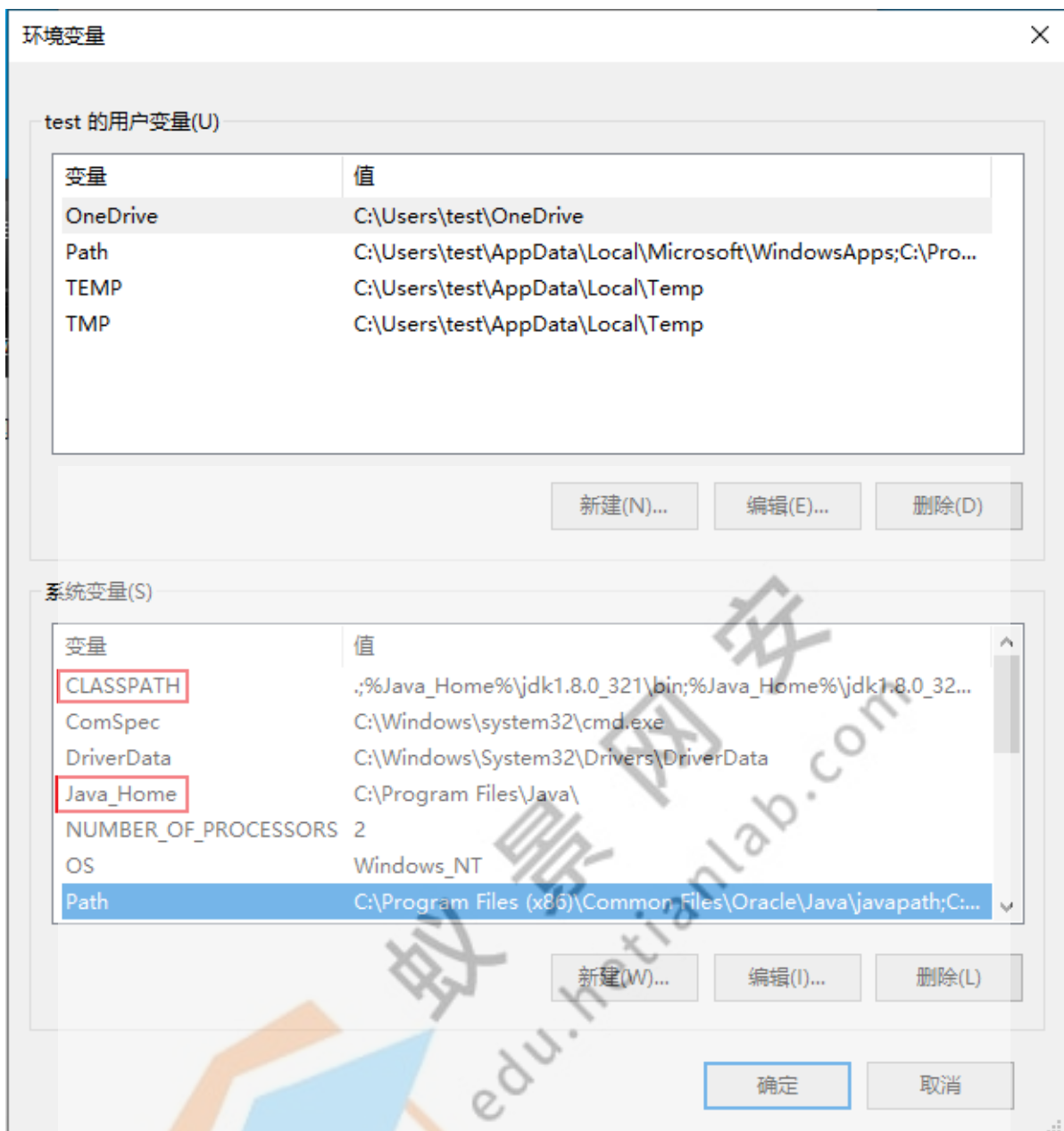
5. 配置 PATH 环境变量

win + R 快捷键打开运行窗口, 输入 `sysdm.cpl` 打开系统属性, 选择高级, 环境变量

新建如下环境变量及值:

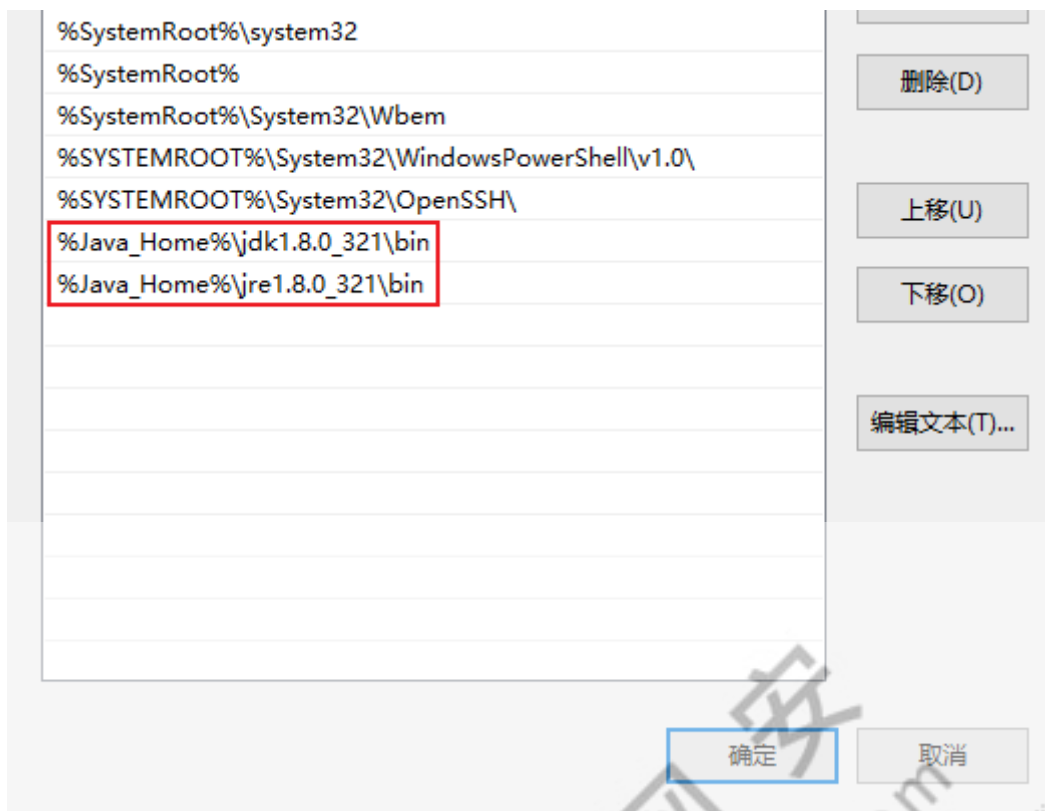
```
变量: Java_Home
值: C:\Program Files\Java

变量: CLASSPATH
值: .;%Java_Home%\jdk1.8.0_321\bin;%Java_Home%\jdk1.8.0_321\lib\dt.jar;%Java_Home%\jdk1.8.0_321\lib\tools.jar
```



新增如下环境变量的值





6. 验证安装

Win + R 运行窗口输入 `cmd` 打开命令提示符，输入 `java -version`、`javac -version`

```
命令提示符
C:\Users\test>java -version
java version "1.8.0_321"
Java(TM) SE Runtime Environment (build 1.8.0_321-b07)
Java HotSpot(TM) 64-Bit Server VM (build 25.321-b07, mixed mode)

C:\Users\test>javac -version
javac 1.8.0_321

C:\Users\test>
```

Linux安装JDK8

- 包管理器安装（新手推荐）：

```
# centos、redhat等
yum -y list java*
yum install java-1.8.0-openjdk* -y
```

```
[root@centos7 ~]# yum -y install java-1.8.0-openjdk*
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ap.stykers.moe
 * extras: ftp.sjtu.edu.cn
 * updates: mirrors.ustc.edu.cn
Resolving Dependencies
--> Running transaction check
--> Package java-1.8.0-openjdk.x86_64 1:1.8.0.242.b08-0.el7_7 will be installed
--> Processing Dependency: xorg-x11-fonts-Type1 for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libpng15.so.15(PNG15_0)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9.0rc4)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libXcomposite(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: gtk2(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: fontconfig(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libpng15.so.15()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libgif.so.4()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libasound.so.2()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libXtst.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libXrender.so.1()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libXi.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libXext.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Processing Dependency: libX11.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
--> Package java-1.8.0-openjdk-accessibility.x86_64 1:1.8.0.242.b08-0.el7_7 will be installed
--> Processing Dependency: java-atk-wrapper(x86-64) for package: 1:java-1.8.0-openjdk-accessibility-1.8.0.242.b08-0.el7_7.x86_64
```

```
# debian、ubuntu、kali等
apt-cache search java | grep jdk

apt install openjdk-8-jre-headless
apt install openjdk-8-jdk-headless

apt install openjdk-11-jdk
```

```
+ ~ # apt install openjdk-11-jdk
Reading package lists... done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libboost-fsystem1.65.1 libboost-iostreams1.65.1 libboost-program-options1.65.1 libboost-system1.65.1 libgoogle-perftools4 libpcrepp
  libyaml-cpp0.5v5 linux-headers-4.15.0-55 linux-headers-4.15.0-55-generic linux-image-4.15.0-55-generic linux-modules-4.15.0-55-generic
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  at-spi2-core ca-certificates-java fonts-dejavu-extra libatk-bridge2.0-0 libatk-wrapper-java libatk-wrapper-java-jni libatk1.0-0 libatk1
  libdrm-nouveau2 libdrm-radeon1 libfontenc1 libgif7 libgl1 libgl1-mesa-dri libglapi-mesa libglvnd0 libglx-mesa0 libglx0 libice-dev libice
  libx11-dev libx11-doc libx11-xcb1 libxau-dev libxaw7 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0 libxcb-present0 libxcb-shape0 libxcb-sync1
  libxft2 libxinerama1 libxmu6 libxpm4 libxrandr2 libxshmfence1 libxt-dev libxt6 libxv1 libxxf86dgal libxxf86vml openjdk-11-jdk-headless
  x11proto-core-dev x11proto-dev xorg-sgml-doctools xtrans-dev
Suggested packages:
  libice-doc libsm-doc libxcb-doc libxt-doc openjdk-11-demo openjdk-11-source visualvm libnss-mdns fonts-ipafont-gothic fonts-ipafont-mino
The following NEW packages will be installed:
  at-spi2-core ca-certificates-java fonts-dejavu-extra libatk-bridge2.0-0 libatk-wrapper-java libatk-wrapper-java-jni libatk1.0-0 libatk1
  libdrm-nouveau2 libdrm-radeon1 libfontenc1 libgif7 libgl1 libgl1-mesa-dri libglapi-mesa libglvnd0 libglx-mesa0 libglx0 libice-dev libice
  libx11-dev libx11-doc libx11-xcb1 libxau-dev libxaw7 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0 libxcb-present0 libxcb-shape0 libxcb-sync1
  libxft2 libxinerama1 libxmu6 libxpm4 libxrandr2 libxshmfence1 libxt-dev libxt6 libxv1 libxxf86dgal libxxf86vml openjdk-11-jdk openjdk-1
  x11proto-core-dev x11proto-dev xorg-sgml-doctools xtrans-dev
0 upgraded, 64 newly installed, 0 to remove and 134 not upgraded.
Need to get 259 MB/291 MB of archives.
After this operation, 758 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrors.cloud.aliyuncs.com/ubuntu bionic-updates/main amd64 openjdk-11-jre-headless amd64 11.0.13+8-0ubuntu1~18.04 [37.2 MB]
Get:2 http://mirrors.cloud.aliyuncs.com/ubuntu bionic-updates/main amd64 openjdk-11-jre amd64 11.0.13+8-0ubuntu1~18.04 [174 kB]
Get:3 http://mirrors.cloud.aliyuncs.com/ubuntu bionic-updates/main amd64 openjdk-11-jdk-headless amd64 11.0.13+8-0ubuntu1~18.04 [220 MB]
Get:4 http://mirrors.cloud.aliyuncs.com/ubuntu bionic-updates/main amd64 openjdk-11-jdk amd64 11.0.13+8-0ubuntu1~18.04 [1,545 kB]
Fetched 259 MB in 5s (47.7 MB/s)
```

- 源码安装（新手不推荐）：

```
mkdir /usr/java
cd /usr/java
tar -zxvf jdk-8u241-linux-x64.tar.gz
mv jdk-1.8._241 jdk8

vim /etc/profile # 编辑profile配置文件，添加如下内容
export JAVA_HOME=/usr/java/jdk8
export JRE_HOME=${JAVA_HOME}/jre
export CLASSPATH=.:${JAVA_HOME}/lib:${JRE_HOME}/lib:$CLASSPATH
export JAVA_PATH=${JAVA_HOME}/bin:${JRE_HOME}/bin
export PATH=$PATH:${JAVA_PATH}
```

- 验证安装：

```
source /etc/profile
java --version
```

```
→ ~ → java -version
openjdk version "1.8.0_232"
OpenJDK Runtime Environment (build 1.8.0_232-8u232-b09-0ubuntu1~16.04.1-b09)
OpenJDK 64-Bit Server VM (build 25.232-b09, mixed mode)
→ ~ →
```

Mac安装JDK8

[Java Downloads | Oracle: https://www.oracle.com/java/technologies/downloads/#java8-mac](https://www.oracle.com/java/technologies/downloads/#java8-mac)

```
cd ~
vim .bash_profile
export
JAVA_HOME=/Library/Java/JavaVirtualMachines/jdk1.8.0_201.jdk/Contents/Home/(java
安装目录)
source .bash_profile
```

Python环境安装

Windows安装Python2/3

- 方法一：Microsoft Store安装python3（不推荐）



- 方法二：Python官网下载安装（推荐）

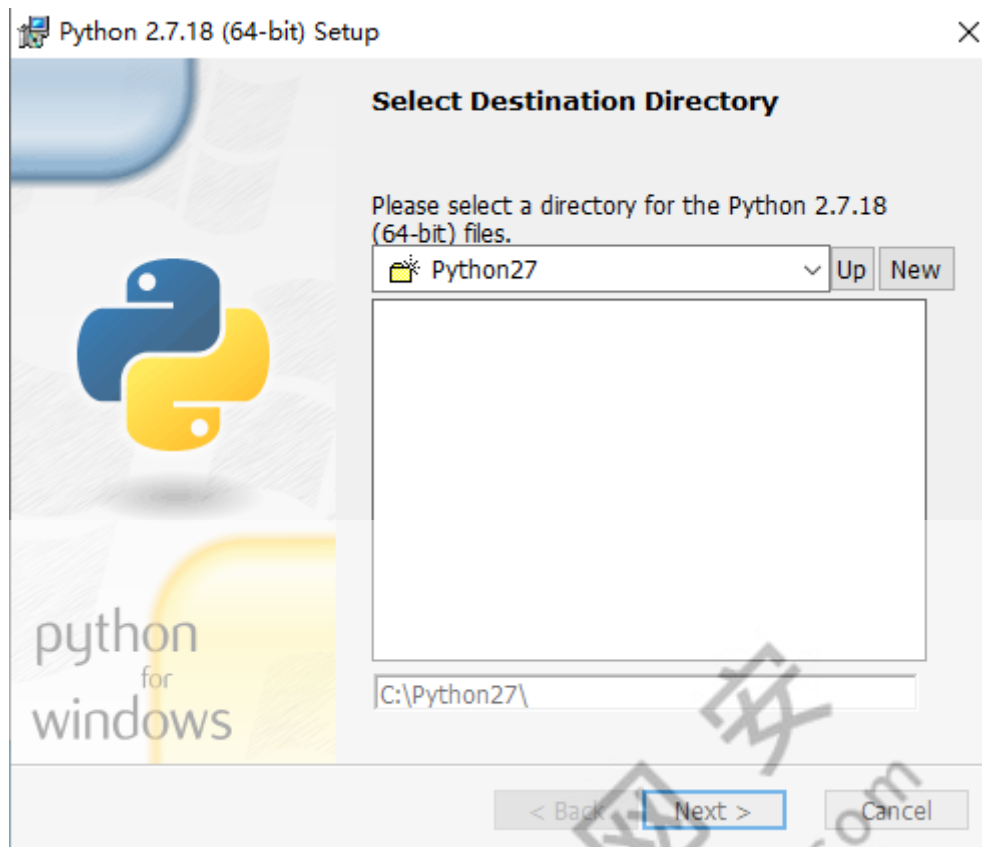
下载安装程序：

<https://www.python.org/downloads/>

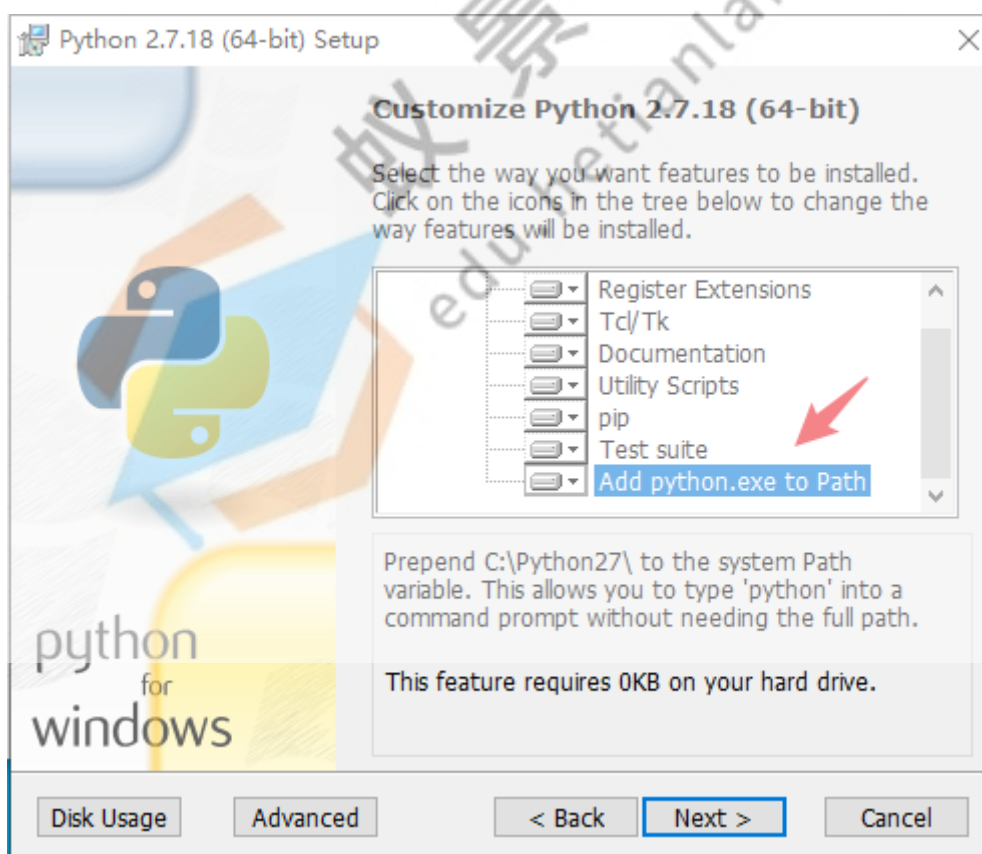
<https://www.python.org/ftp/python/>

- Python2 安装

双击打开 `python-2.7.18.amd64.msi`，进入安装引导界面：



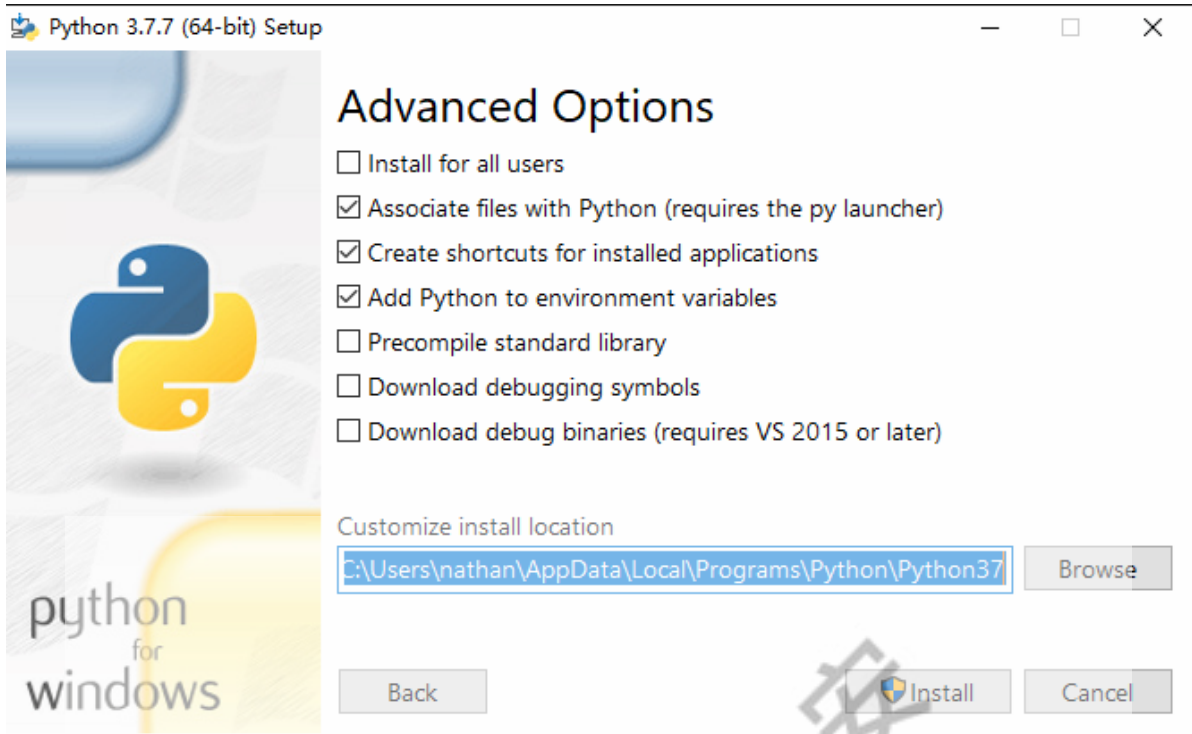
Next, 勾选最后一项, 添加 python.exe 到 Path 环境变量:



Next, 等待安装完成, 打开命令提示符窗口, 输入python, 进入 python 命令控制台, 则表示 python2 安装成功。

- Python3 安装

选择 Customize installation, 自定义安装 pip、IDLE、安装路径等



Linux安装Python2/3

- 安装Python2

一般Linux系统默认安装Python2.7, 因此无需额外安装

- 安装Python3

```
mkdir -p /usr/local/python3
yum -y install wget gcc libffi-devel
wget https://www.python.org/ftp/python/3.7.7/Python-3.7.7.tgz
tar -zxf Python-3.7.7.tgz
cd Python-3.7.7
./configure --prefix=/usr/local/python3
make && make install
```


Mac安装Python2/3

系统默认安装Python2.7，因此无需额外安装

- 安装Python3

```
brew install python3
```

- 不同版本Python路径

来源	python安装路径
系统默认(2.7)	/System/Library/Frameworks/Python.framework/Versions/2.7
brew安装(2.7/3.x)	/usr/local/Cellar/python
官网pkg安装(3.x)	/Library/Frameworks/Python.framework/Versions/3.x

- 配置Python2和Python3

```
vim ~/.bash_profile

# Setting PATH for Python 2.7
PATH="/System/Library/Frameworks/Python.framework/Versions/2.7/bin:${PATH}"
export PATH
# Setting PATH for Python 3.x
PATH="/usr/local/Cellar/python/3.x/bin:${PATH}"
```

```
vim ~/.bashrc

alias
python2='/System/Library/Frameworks/Python.framework/Versions/2.7/bin/python2.7'
alias python3='/usr/local/Cellar/python/3.x/bin/python3.x'
```

```
source ~/.bash_profile
source ~/.bashrc
```

Linux-Kali配置与使用

VMware软件安装

下载vmware

Vmware官网: <https://www.vmware.com/>

Download VMware Workstation Pro

Select Version: Select the relevant installation package to download from the tabs below. You may be prompted to log in to complete the download. If you do not have a profile, you may be asked to create one before being able to complete the download process.

15.0

[Read More](#)

Product Resources

[View My Download History](#)

[Product Info](#)

[Documentation](#)

[Community](#)

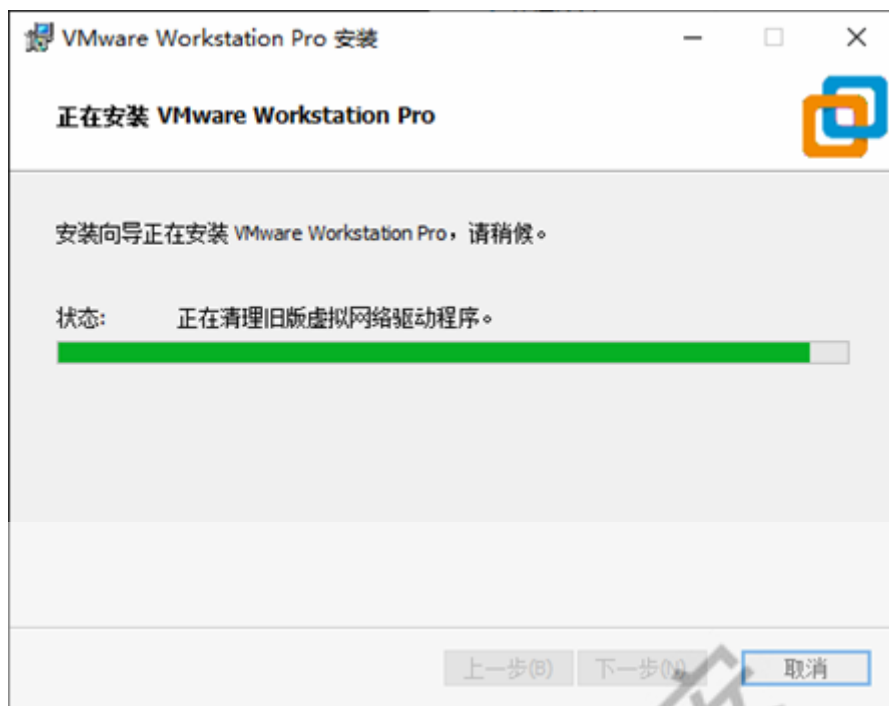
[Download Free Trial: Windows | Linux](#)

[Product Downloads](#) [Drivers & Tools](#) [Open Source](#) [Custom ISOs](#)

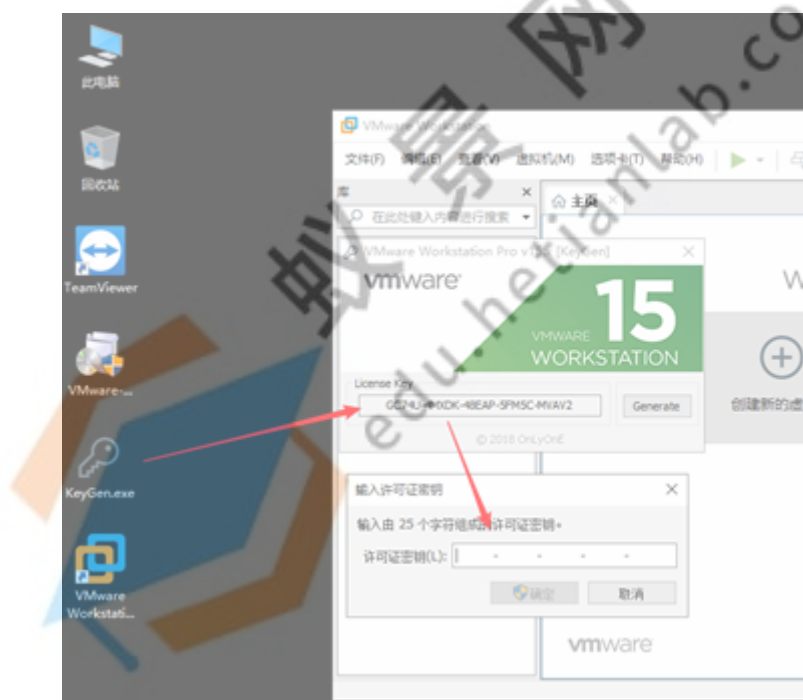
Product	Release Date	
VMware Workstation Pro 15.5.2 for Windows		
VMware Workstation 15.5.2 Pro for Windows	2020-03-12	Go to Downloads
VMware Workstation Pro 15.5.2 for Linux		
VMware Workstation 15.5.2 Pro for Linux	2020-03-12	Go to Downloads

安装vmware





激活vmware





VMware安装Kali

Kali简介

Kali Linux是基于Debian的Linux发行版，旨在进行高级渗透测试和安全审核。Kali包含数百种工具，可用于各种信息安全任务，例如渗透测试，安全研究，计算机取证和逆向工程。Kali Linux由领先的信息安全培训公司Offensive Security开发、资助和维护。

Kali官网：<https://www.kali.org>

为什么使用Kali？

1. 包括600多个渗透测试工具：<https://tools.kali.org/tools-listing>
2. 完全免费
3. 多语言（中文）

.....

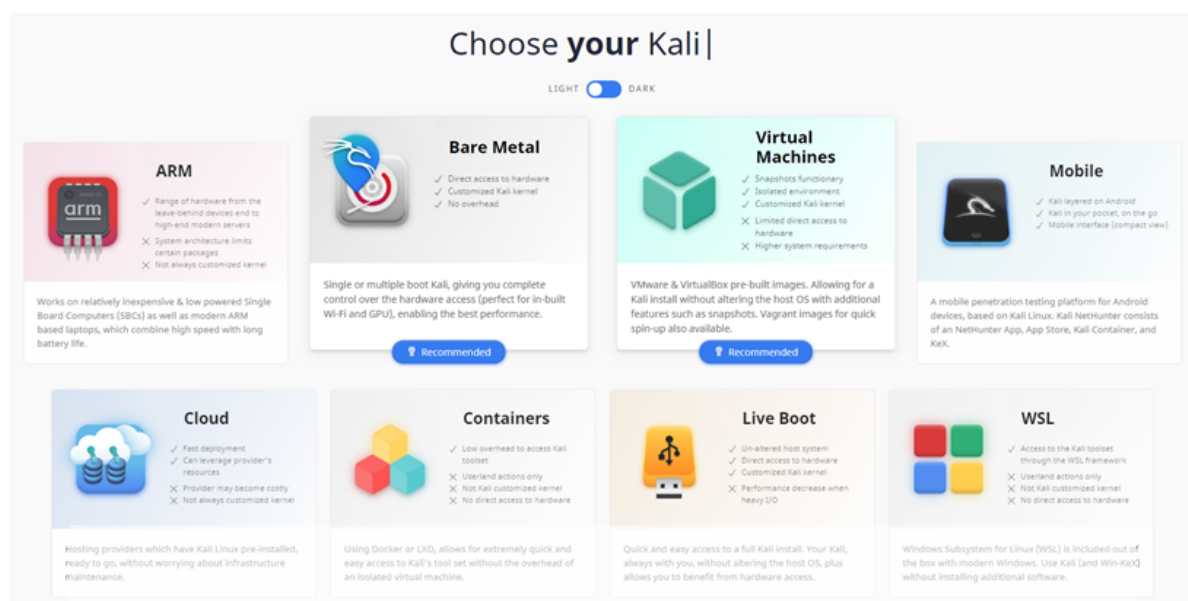
<https://www.kali.org/docs/introduction/what-is-kali-linux/>

Kali下载

Kali官网下载：

[Get Kali | Kali Linux: https://www.kali.org/get-kali/](https://www.kali.org/get-kali/)

<https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-vmware-amd64.7z>



Vmware安装Kali

解压下载的压缩包 kali-linux-2022.1-vmware-amd64.7z , 双击打开下图 .vmx 文件:

kali-linux-2022.1-vmware-amd64.nvram	2022/2/11 15:24	VMware 虚拟机非易...	9 KB
kali-linux-2022.1-vmware-amd64.vmdk	2022/2/11 15:30	VMware 虚拟磁盘文...	2 KB
kali-linux-2022.1-vmware-amd64.vmsd	2022/2/11 14:06	VMware 快照元数据	0 KB
kali-linux-2022.1-vmware-amd64.vmx	2022/2/11 15:40	VMware 虚拟机配置	4 KB
kali-linux-2022.1-vmware-amd64.vmx	2022/2/11 14:06	VMware 组成员	1 KB
kali-linux-2022.1-vmware-amd64-s001.vmdk	2022/2/11 15:41	VMware 虚拟磁盘文...	3,519,872 KB
kali-linux-2022.1-vmware-amd64-s002.vmdk	2022/2/11 15:42	VMware 虚拟磁盘文...	3,582,464 KB
kali-linux-2022.1-vmware-amd64-s003.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	1,155,968 KB
kali-linux-2022.1-vmware-amd64-s004.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	136,576 KB
kali-linux-2022.1-vmware-amd64-s005.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	344,896 KB
kali-linux-2022.1-vmware-amd64-s006.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	176,768 KB
kali-linux-2022.1-vmware-amd64-s007.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	193,664 KB
kali-linux-2022.1-vmware-amd64-s008.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	194,112 KB
kali-linux-2022.1-vmware-amd64-s009.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	640 KB
kali-linux-2022.1-vmware-amd64-s010.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	523,456 KB
kali-linux-2022.1-vmware-amd64-s011.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	704 KB
kali-linux-2022.1-vmware-amd64-s012.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	896 KB
kali-linux-2022.1-vmware-amd64-s013.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	640 KB
kali-linux-2022.1-vmware-amd64-s014.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	832 KB
kali-linux-2022.1-vmware-amd64-s015.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	275,008 KB
kali-linux-2022.1-vmware-amd64-s016.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	241,152 KB
kali-linux-2022.1-vmware-amd64-s017.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	195,264 KB
kali-linux-2022.1-vmware-amd64-s018.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	206,592 KB
kali-linux-2022.1-vmware-amd64-s019.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	225,792 KB
kali-linux-2022.1-vmware-amd64-s020.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	102,080 KB
kali-linux-2022.1-vmware-amd64-s021.vmdk	2022/2/11 15:43	VMware 虚拟磁盘文...	128 KB

kali-linux-2022.1-vmware-amd64

▶ 开启此虚拟机
🔧 编辑虚拟机设置
🔧 升级此虚拟机

▼ 设备

内存	2 GB
处理器	4
硬盘 (SCSI)	80 GB
CD/DVD (IDE)	自动检测
网络适配器	NAT
USB 控制器	存在
声卡	自动检测
显示器	自动检测

▼ 描述

Kali Rolling (2022.1) x64
2022-02-10

Username: kali
Password: kali
(US keyboard layout)


* Kali Homepage:
<https://www.kali.org/>

* Documentation:
<https://www.kali.org/docs/>

* Kali Tools:
<https://www.kali.org/tools/>

* Forum/Community Support:
<https://forums.kali.org/>

* IRC Channel:
<irc://irc.oftc.net:6697/#Kali-Linux>
<https://www.kali.org/docs/community/kali-linu>

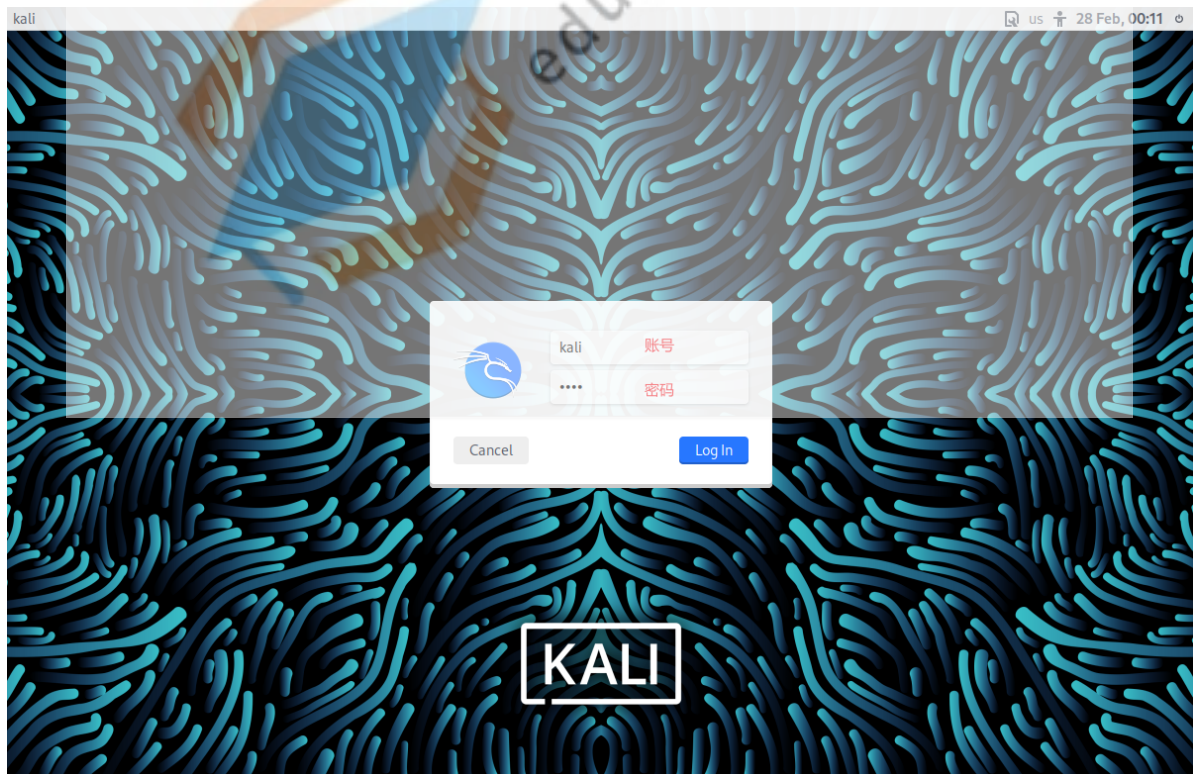


▼ 虚拟机详细信息

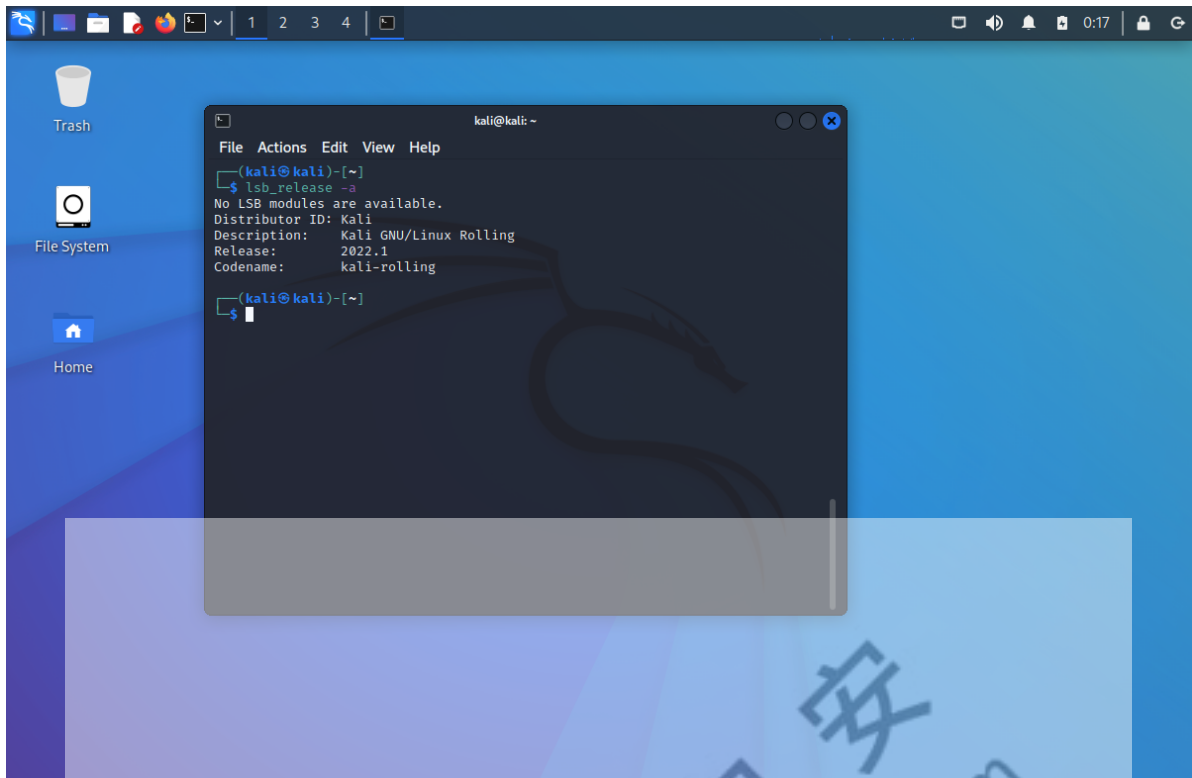
状态: 已关机
配置文件: E:\VM\Kali2022.1\kali-linux-2022.1-vmware-amd64.vmx
硬件兼容性: Workstation 8.x 虚拟机
主 IP 地址: 网络信息不可用

点击“开启此虚拟机”，即可启动。

系统已经配置好默认普通用户 `kali`，默认密码 `kali`：



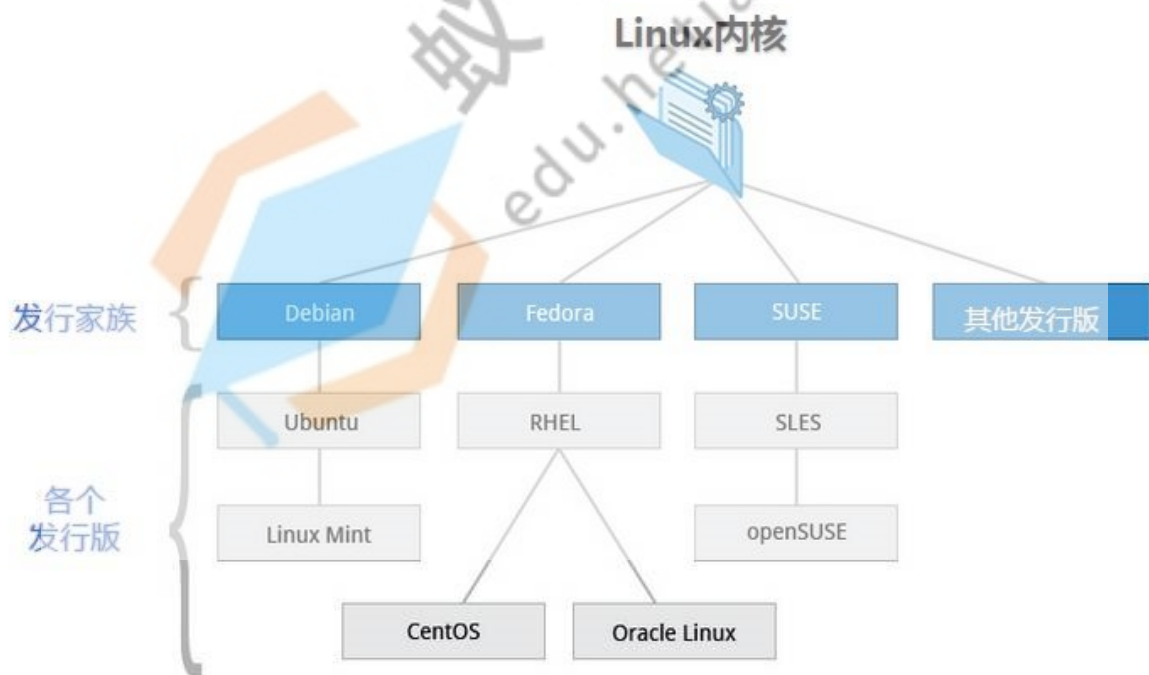
成功登录系统：



Linux使用基础

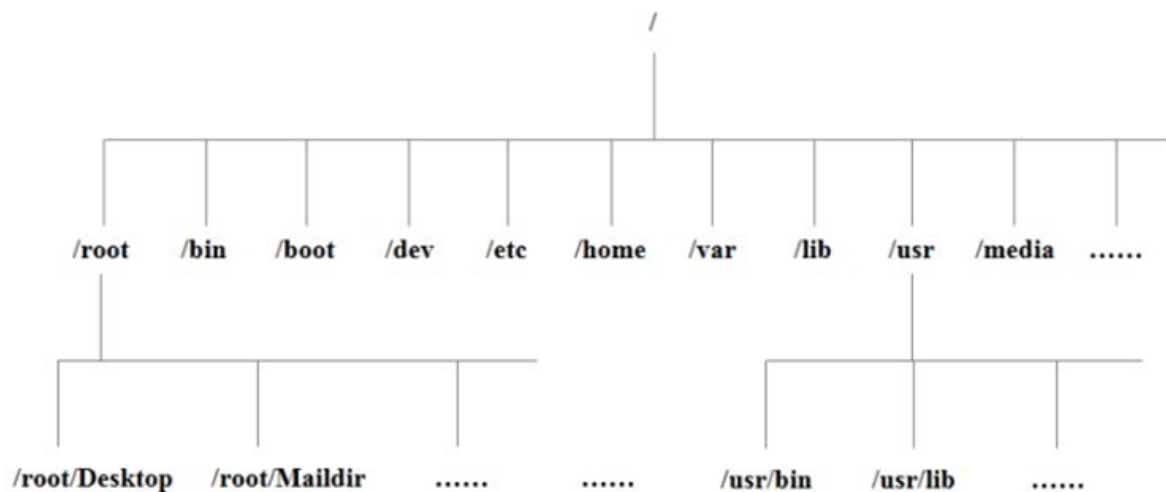
Linux简介

Kali Linux是基于debian的发行版。



<http://hetianlab.com/pages/search.html?wk=linux>

Linux目录结构



/:

根目录，每一个文件和目录都从这里开始。只有root用户具有该目录下的写权限。

/bin:

用户二进制文件，包含二进制可执行文件。系统的所有用户使用的命令都设在这里，例如：ps, ls, ping, grep, cp等。

/boot:

这里存放的是启动Linux时使用的一些核心文件，包括一些连接文件以及镜像文件。

/dev :

设备文件，dev是Device(设备)的缩写，该目录下存放的是Linux的外部设备，在Linux中访问设备的方式和访问文件的方式是相同的。

/etc:

这个目录用来存放所有的系统管理所需要的配置文件和子目录。

/home:

用户的主目录，在Linux中，每个用户都有一个自己的目录，一般该目录名是以用户的账号命名的。

/lib:

这个目录里存放着系统最基本的动态连接共享库，其作用类似于windows里的DLL文件。几乎所有的应用程序都需要用到这些共享库。

/opt:

可选的附加应用程序，这是给主机额外安装软件所摆放的目录。比如你安装一个ORACLE数据库就可以放到这个目录下。默认是空的。

/root:

该目录为系统管理员，也称作超级权限者的用户主目录。

/sbin:

s就是Super User的意思，系统二进制文件，在这个目录下的linux命令通常由系统管理员使用。

/usr:

这是一个非常重要的目录，用户的很多应用程序和文件都放在这个目录下，类似于windows下的program files目录。

/usr/bin:

系统用户使用的应用程序。

/usr/sbin:

超级用户使用的比较高级的管理程序和系统守护程序。

/tmp:

这个目录是用来存放一些临时文件的。

/var:

这个目录中存放着在不断扩充着的东西，我们习惯将那些经常被修改的目录放在这个目录下。包括各种日志文件。

Linux文件属性

```
r: 4
w: 2
x: 1
```

属主: u (user)

数组: g (group)

其他: o (other)

```
chmod u+x test
```

```
chown root.root test
```

文件 类型	属主 权限			属组 权限			其他用户 权限		
0	1	2	3	4	5	6	7	8	9
d	r	w	x	r	-	x	r	-	x
目录 文件	读	写	执行	读	写	执行	读	写	执行

文件目录管理

```
ls
cd
pwd
mkdir
rmdir
cp
rm
mv
```

绝对路径: 由根目录写起 root@kali:~# cd /var/www/html

相对路径: 不是由根写起 root@kali:/var/www/html# cd ../../log/

VIM编辑器

- VIM简介

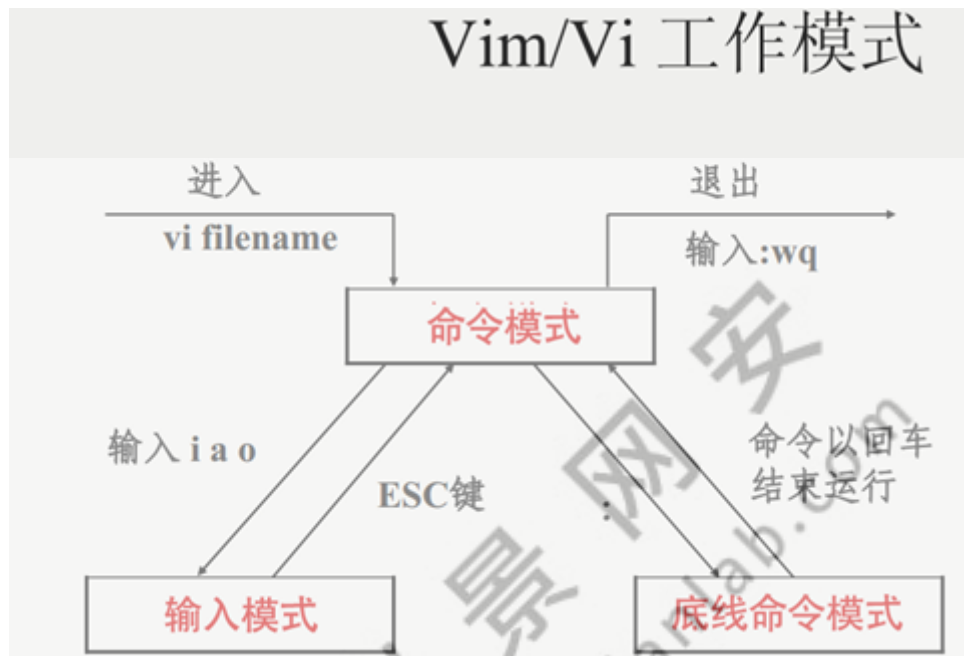
Vim是一个著名的功能强大、高度可定制的Unix及类Unix系统文本编辑器。

- VIM的三种模式

命令模式 (Command mode)

输入模式 (Insert mode)

底线命令模式 (Last line mode)



1. 命令模式

用户刚刚启动 vi/vim，便进入了命令模式。

此状态下敲击键盘动作会被Vim识别为命令，而非输入字符。比如我们此时按下i，并不会输入一个字符，i被当作了一个命令。

2. 输入模式

进行VIM输入模式的方式是在命令模式状态下输入 i、l、a、A、o、O 等插入命令

在输入模式下，Vim 可以对文件执行写操作，类似于在 Windows 系统的文档中输入内容。

3. 底线命令模式

在命令模式下按下 ":"(英文冒号)就进入了底线命令模式。

底线命令模式可以输入单个或多个字符的命令，可用的命令非常多。

在底线命令模式中，基本的命令有(已经省略了冒号)：

q 退出程序

w 保存文件

按ESC键可随时退出底线命令模式。

Kali配置

用户配置

- Kali

```
sudo apt update
```

- root

```
sudo su
```

```
sudo passwd root
```

网络配置

配置IP:
/etc/network/interfaces

```
auto eth0
iface eth0 inet static
address 192.168.1.228
netmask 255.255.255.0
gateway 192.168.1.1
```

配置DNS:
/etc/resolv.conf

重启服务
service networking restart
service network-manager restart

自动获取IP: dhclient

设置APT源

```
cp /etc/apt/sources.list /etc/apt/sources.list.bak
vim /etc/apt/sources.list
apt-get update
apt-get clean
```

```
#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
```

APT使用

- apt-get

`apt-get` 可以从认证软件源下载软件包及相关信息，以便安装和升级软件包，或者用于移除软件包。在这些过程中，软件包依赖会被妥善处理。

- 常用命令

```
update - 取回更新的软件包列表信息
upgrade - 进行一次升级
install - 安装新的软件包(注：软件包名称是 libc6 而非libc6.deb)
reinstall - Reinstall packages (pkg is libc6 not libc6.deb)
remove - 卸载软件包
```

- apt 与 apt-get的区别与解释

[Linux中apt与apt-get命令的区别与解释](#)

简单来说就是：`apt` = `apt-get`、`apt-cache` 和 `apt-config` 中最常用命令选项的集合。

虽然 `apt` 与 `apt-get` 有一些类似的命令选项，但它并不能完全向下兼容 `apt-get` 命令。也就是说，可以用 `apt` 替换部分 `apt-get` 系列命令，但不是全部。

`apt` 可以看作 `apt-get` 和 `apt-cache` 命令的子集，可以为包管理提供必要的命令选项。

`apt-get` 虽然没被弃用，但作为普通用户，还是应该首先使用 `apt`。

设置中文

- 安装中文字体

```
apt-get install xfonts-intl-chinese
apt-get install ttf-wqy-microhei
```

- 设置语言

```
dpkg-reconfigure locales
```

进入图形界面，选中 `en_US.UTF-8 UTF-8` 和 `zh_CN.UTF-8 UTF-8` 并将 `zh_CN.UTF-8` 选为默认。
(空格是选择，tab是切换，* 是选中)

- 重启

```
reboot
```

配置Python

- pip简介

`pip` 是一个 Python 包安装与管理工具。

`kali2022` 默认安装 `python2.7` 和 `python3.9`，但需自行配置 `pip`

- apt安装


```
apt install python3-pip
apt install python-pip
```

- 脚本安装

```
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip2.py
python2 get-pip2.py
```

```
curl https://bootstrap.pypa.io/get-pip.py -o get-pip3.py
python3 get-pip3.py & pip3 list
```

- pip安装Python 库

```
sudo pip3 install pwntools
```

pip使用国内代理:

```
pip3 install -r requirements.txt -i https://mirrors.ustc.edu.cn/pypi/web/simple
```

```
(kali@kali)-[~]
$ sudo pip3 install pwntools
Collecting pwntools
  Downloading pwntools-4.7.0-py2.py3-none-any.whl (11.7 MB)
    11.7/11.7 MB 1.4 MB/s eta 0:00:00
Collecting capstone>=3.0.5rc2
  Downloading capstone-4.0.2-py2.py3-none-manylinux1_x86_64.whl (2.1 MB)
    2.1/2.1 MB 1.0 MB/s eta 0:00:00
Collecting unicorn>=1.0.2rc1
  Downloading unicorn-2.0.0rc6-py2.py3-none-manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (7.4 MB)
    7.4/7.4 MB 479.0 KB/s eta 0:00:00
Requirement already satisfied: paramiko>=1.15.2 in /usr/lib/python3/dist-packages (from pwntools) (2.8.1)
Requirement already satisfied: requests>=2.0 in /usr/lib/python3/dist-packages (from pwntools) (2.25.1)
Collecting rpyc
  Downloading rpyc-5.1.0-py3-none-any.whl (69 kB)
    69.1/69.1 KB 319.4 KB/s eta 0:00:00
Requirement already satisfied: pygments>=2.0 in /usr/lib/python3/dist-packages (from pwntools) (2.7.1)
Requirement already satisfied: packaging in /usr/lib/python3/dist-packages (from pwntools) (21.3)
Requirement already satisfied: psocks in /usr/lib/python3/dist-packages (from pwntools) (1.7.1)
Collecting colored-traceback
  Downloading colored-traceback-0.3.0.tar.gz (3.8 kB)
  Preparing metadata (setup.py) ... done
Requirement already satisfied: mako>=1.0.0 in /usr/lib/python3/dist-packages (from pwntools) (1.1.3)
Requirement already satisfied: six>=1.12.0 in /usr/lib/python3/dist-packages (from pwntools) (1.16.0)
Requirement already satisfied: python-dateutil in /usr/lib/python3/dist-packages (from pwntools) (2.8.1)
Collecting psutil>=3.3.0
  Downloading psutil-5.9.0-cp39-cp39-manylinux_2_12_x86_64.manylinux2010_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (280 kB)
    280.4/280.4 KB 322.6 KB/s eta 0:00:00
Collecting ropgadget>=5.3
  Downloading ROPgadget-6.6-py3-none-any.whl (31 kB)
Requirement already satisfied: sortedcontainers in /usr/lib/python3/dist-packages (from pwntools) (2.1.0)
Requirement already satisfied: pyserial>=2.7 in /usr/lib/python3/dist-packages (from pwntools) (3.5b0)
Requirement already satisfied: pip>=6.0.8 in /usr/local/lib/python3.9/dist-packages (from pwntools) (22.0.3)
Collecting pyelftools>=0.2.4
  Downloading pyelftools-0.28-py2.py3-none-any.whl (155 kB)
    155.4/155.4 KB 329.3 KB/s eta 0:00:00
Collecting intervaltree>=3.0
  Downloading intervaltree-3.1.0.tar.gz (32 kB)
  Preparing metadata (setup.py) ... done
Collecting plumbum
  Downloading plumbum-1.7.2-py2.py3-none-any.whl (117 kB)
    117.8/117.8 KB 345.3 KB/s eta 0:00:00
Building wheels for collected packages: intervaltree, colored-traceback
  Building wheel for intervaltree (setup.py) ... done
```

Git使用

- Git简介

一个开源的分布式版本控制系统，用于敏捷高效地处理任何或小或大的项目。

- clone

```
git clone https://github.com/Hack-with-Github/Awesome-Hacking.git
```

```

(kali㉿kali)-[~]
└─$ git clone https://github.com/Hack-with-Github/Awesome-Hacking.git
Cloning into 'Awesome-Hacking' ...
remote: Enumerating objects: 313, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 313 (delta 4), reused 2 (delta 0), pack-reused 303
Receiving objects: 100% (313/313), 161.33 KiB | 718.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.

(kali㉿kali)-[~]
└─$ ls Awesome-Hacking
awesome_hacking.jpg  contributing.md  LICENSE  README.md

(kali㉿kali)-[~]
└─$

```

```
git clone git://github.com/Hack-with-Github/Awesome-Hacking.git
```

```

(kali㉿kali)-[~]
└─$ git clone git://github.com/Hack-with-Github/Awesome-Hacking.git
Cloning into 'Awesome-Hacking' ...
remote: Enumerating objects: 313, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 313 (delta 4), reused 2 (delta 0), pack-reused 303
Receiving objects: 100% (313/313), 161.33 KiB | 307.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.

(kali㉿kali)-[~]
└─$ ls Awesome-Hacking
awesome_hacking.jpg  contributing.md  LICENSE  README.md

(kali㉿kali)-[~]
└─$

```

- Git socks代理

前提是你本地有 socks5 代理，本地socks开启局域网连接

```

git config --global http.proxy 'socks5://127.0.0.1:1080'
git config --global https.proxy 'socks5://127.0.0.1:1080'

git clone https://github.com/shmily1ty/OneForAll.git

```

- Git教程

<https://www.runoob.com/git/git-tutorial.html>

SSH登录

- SSH简介

SSH 为 Secure Shell 的缩写，SSH 为建立在应用层基础上的安全协议。SSH 是较可靠，专为远程登录会话和其他网络服务提供安全性的协议。

- SSH配置

开启密码登录、允许root用户登录：

```
vim /etc/ssh/sshd_config  
  
#PermitRootLogin prohibit-password  
  
PermitRootLogin yes
```

开启或重启ssh:

```
service ssh start  
service ssh restart
```

查看22端口是否开启监听:

```
netstat -anltup | grep 22
```

添加开机启动:

```
systemctl enable ssh  
  
update-rc.d ssh enable
```

终端连接:

```
ifconfig  
  
ssh root@192.168.123.136
```

Kali工具

<https://tools.kali.org/tools-listing>
<https://github.com/Jack-Liang/kalitools>

1. 信息收集
2. 漏洞分析
3. WEB应用分析
4. 数据库评估
5. 密码攻击
6. 无线攻击
7. 逆向工程
8. 利用工具
9. 嗅探&欺骗
10. 后渗透攻击
11. 取证工具
12. 报告工具
13. 社会工程学工具



蚁景网安

edu.hetianlab.com