**北京科技大学实验报告**

学院：计算机与通信工程学院 专业： 信息安全 班级： 信安192

姓名： 霍炟 学号：41824147 实验日期： 2022年 4月 20日

**实验名称：启动Kali**

## 实验目的

启动Kali，为后续实验做准备、学习安全渗透。

## 实验仪器

希冀平台

Linux kali 5.4.0-kali3-amd54

## 实验原理

渗透测试是对用户信息安全措施积极评估的过程。通过系统化的操作和分析，积极发现系统和网络中存在的各种缺陷和弱点，如设计缺陷和技术缺陷。本章将简要介绍Linux安全渗透及安全渗透工具的相关内容。其主要知识点如下：

什么是安全渗透； 安全渗透所需的工具； Kali Linux简介； 安装Kali Linux； 基本设置。

其主要知识点如下：

什么是安全渗透；

安全渗透所需的工具；

Kali Linux简介；

安装Kali Linux；

Kali更新与升级；

基本设置。

1. 什么是安全渗透

渗透测试并没有一个标准的定义。国外一些安全组织达成共识的通用说法是，渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法，这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析。这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

渗透测试与其他评估方法不同。通常的评估方法是根据已知信息资源或其他被评估对象，去发现所有相关的安全问题。渗透测试是根据已知可利用的安全漏洞，去发现是否存在相应的信息资源。相比较而言，通常评估方法对评估结果更具有全面性，而渗透测试更注重安全漏洞的严重性。

渗透测试有黑盒和白盒两种测试方法。黑盒测试是指在对基础设施不知情的情况下进行测试。白盒测试是指在完全了解结构的情况下进行测试。不论测试方法是否相同，渗透测试通常具有两个显著特点：

渗透测试是一个渐进的且逐步深入的过程。

渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。

2. 安全渗透所需的工具

了解了渗透测试的概念后，接下来就要学习进行渗透测试所使用的各种工具。在做渗透测试之前，需要先了解渗透所需的工具。渗透测试所需的工具如表1-1所示。

表1-1　渗透所需的工具

splint unhide scrub pscan examiner ht flawfinder srm driftnet rats nwipe binwalk ddrescue firstaidkit-gui scalpel gparted xmount pdfcrack testdisk dc3dd wipe foremost afftools safecopy sectool-gui scanmem hfsutils unhide sleuthkit cmospwd examiner macchanger secuirty-menus srm ngrep nc6 nwipe ntfs-3g mc firstaidkit-gui ntfsprogs screen net-snmp pcapdiff openvas-scanner hexedit netsed rkhunter irssi dnstop labrea powertop sslstrip nebula mutt bonesi tripwire nano proxychains prelude-lml vim-enhanced prewikka iftop wget prelude-manager scamper yum-utils picviz-gui iptraf-ng mcabber telnet iperf firstaidkit-plugin-all onenssh nethogs vnstat dnstracer uperf aircrack-ng chkrootkit nload airsnort aide ntop kismet pads trafshow weplab cowpatty wavemon

由于篇幅原因，这里只列了一部分工具。渗透测试所需的工具可以在各种Linux操作系统中找到，然后手动安装这些工具。由于工具繁杂，安装这些工具，会变成一个浩大的工程。为了方便用户进行渗透方面的工作，有人将所有的工具都预装在一个Linux系统。其中，典型的操作系统就是本书所使用的Kali Linux。

该系统主要用于渗透测试。它预装了许多渗透测试软件，包括nmap端口扫描器、Wireshark（数据包分析器）、John the Ripper（密码破解）及Aircrack-ng（一套用于对无线局域网进行渗透测试的软件）。用户可通过硬盘、Live CD或Live USB来运行Kali Linux。

Kali Linux简介

Kali Linux的前身是BackTrack Linux发行版。Kali Linux是一个基于Debian的Linux发行版，包括很多安全和取证方面的相关工具。它由Offensive Security Ltd维护和资助，最先由Offensive Security的MatiAharoni和Devon Kearns通过重写Back Track来完成。Back Track是基于Ubuntu的一个Linux发行版。

Kali Linux有32位和64位的镜像，可用于x86指令集。同时它还有基于ARM架构的镜像，可用于树莓派和三星的ARM Chromebook。用户可通过硬盘、Live CD或Live USB来运行Kali Linux操作系统。

## 实验内容与步骤

实验路径：

打开桌面Virtual Machine，选择kali-linux虚拟机进入实验环境。

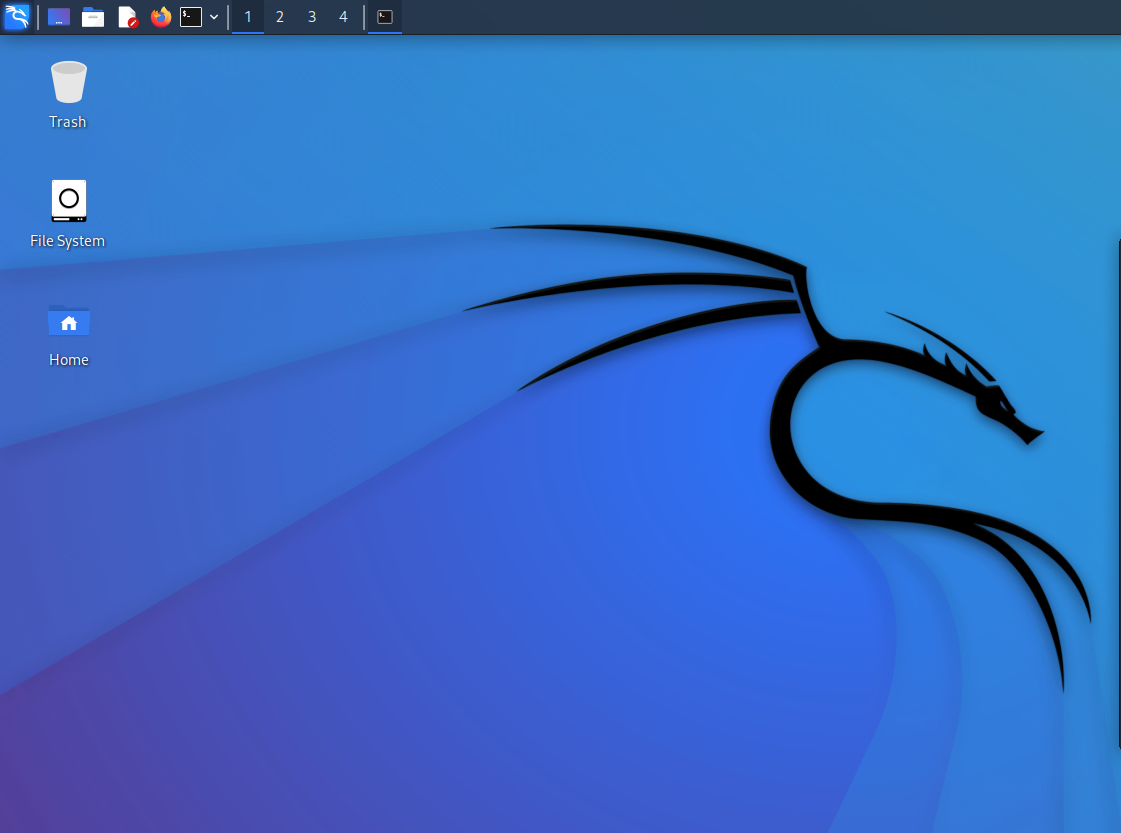
1. **打开kali**

**2.登陆系统**

账号：kali

密码：kali

输入账号密码登陆。



**2.1 启动网络服务**

Kali Linux 自带了多种网络服务，它们在多种情况下可能很实用，并且默认是禁用的。这个秘籍中，我们会涉及到通过多种方法设置和启动每个服务的步骤。

准备

需要满足下列要求以继续：

* 带有有效IP地址的网络连接。

鼠标右键或者左上角进入控制台：

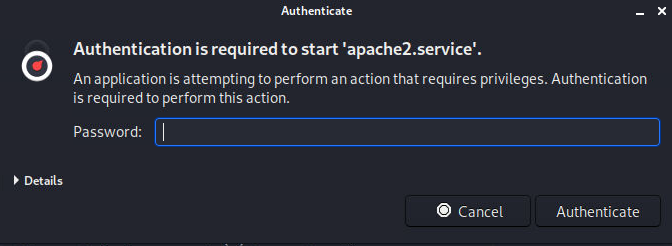
操作步骤

让我们开始启动默认服务：

1. 启动Apache服务器：

/sbin/service apache2 start

出现验证界面：

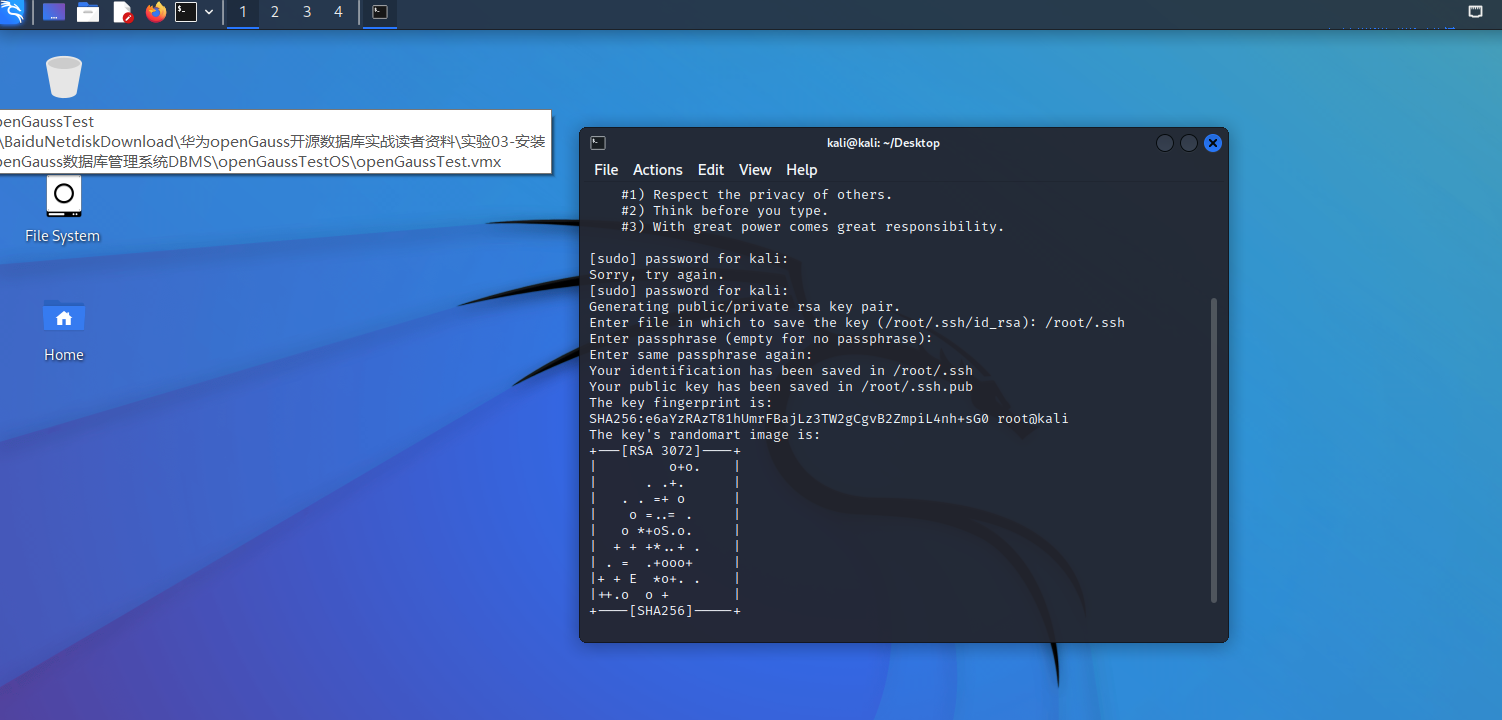


输入密码kali，即可，该密码为账号密码，与登陆密码一致。

我们可以通过浏览本地地址来验证服务器是否打开。

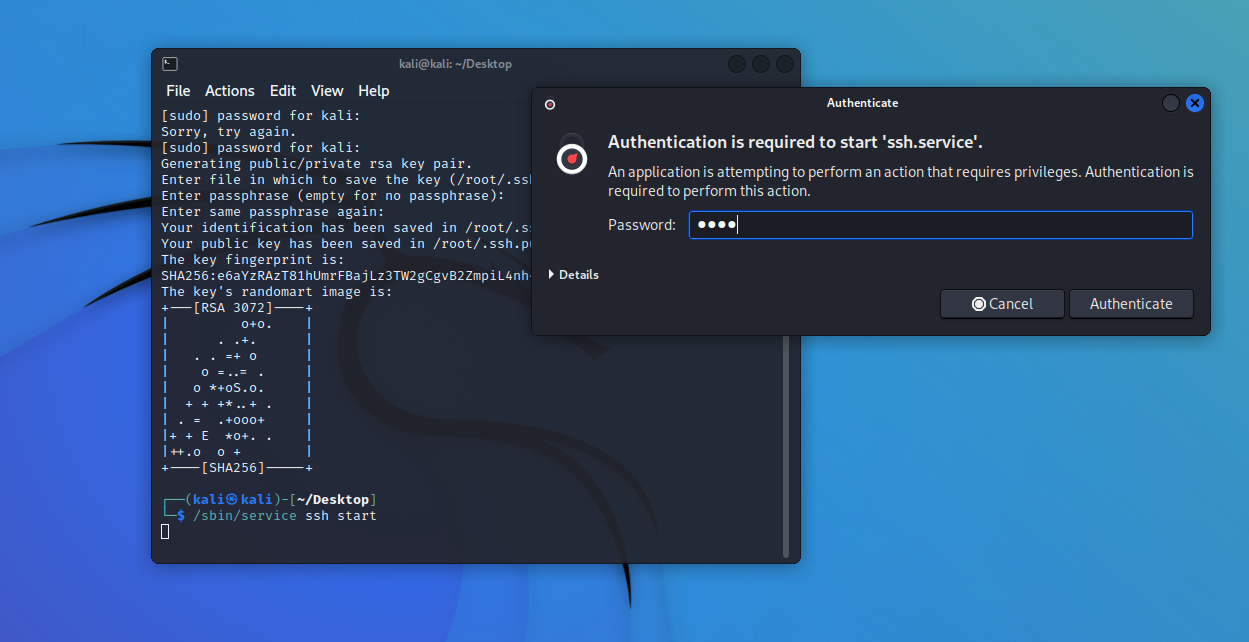
1. 为了启动SSH服务，首次需要生成SSH密钥：

sudo ssh-keygen



1. 启动SSH服务器：

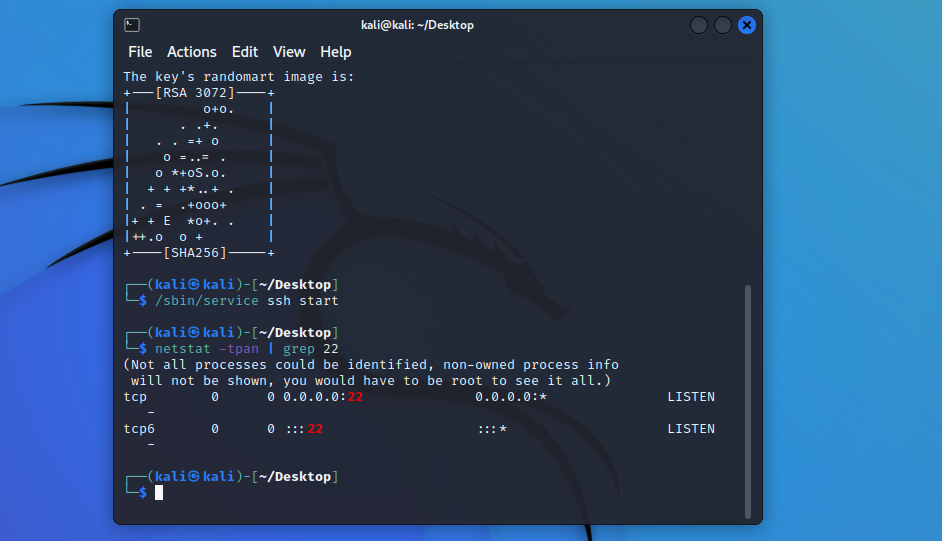
/sbin/service ssh start



输入kali密码即可

1. 使用netstat命令来验证服务器是否开启并正在监听：

netstat -tpan | grep 22



1. 启动FTP服务器：

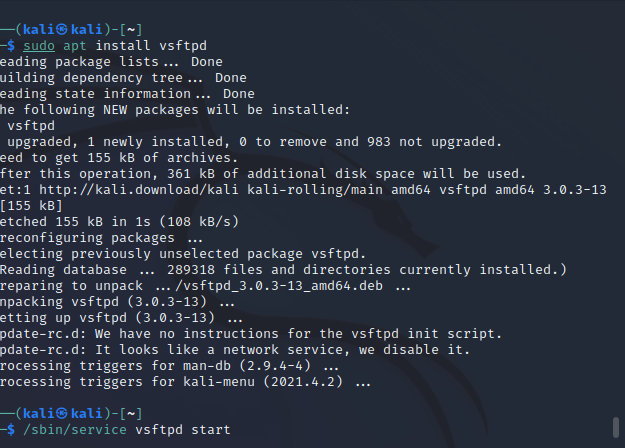
/sbin/service vsftpd start

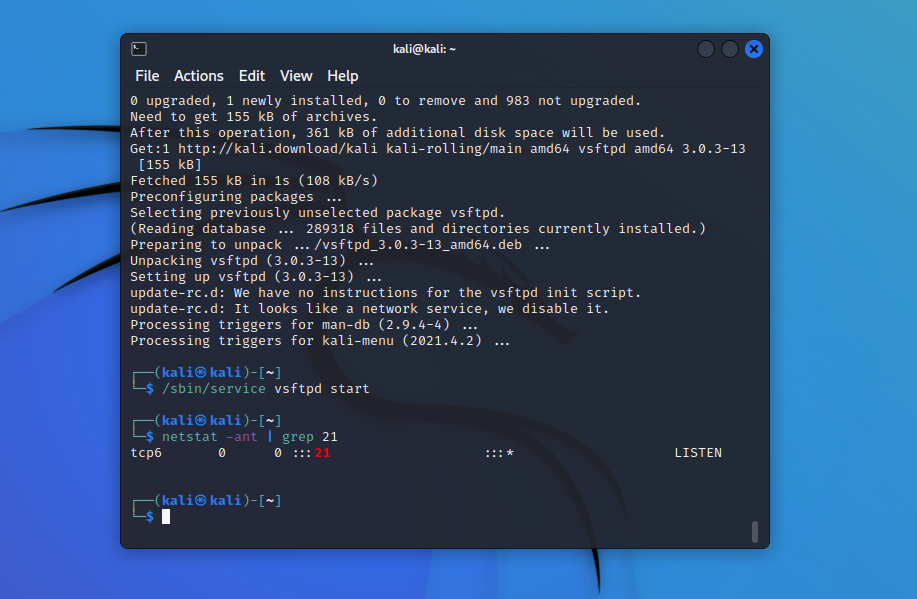
1. 使用下列命令来验证FTP服务器：

netstat -ant | grep 21

你也可以使用ps-ef | grep 21命令。

如果未安装FTP，则使用命令 sudo apt-get install vsftpd 来安装。





使用下列命令来停止服务：

service <servicename> stop

其中<servicename>代表我们希望停止的网络服务，例如：

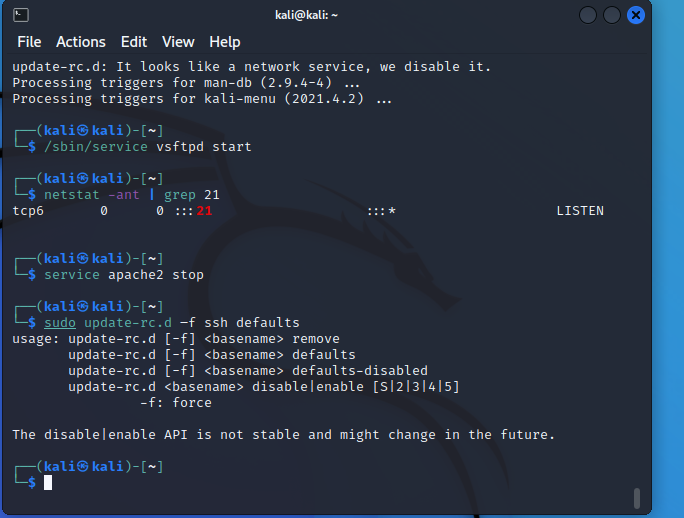
service apache2 stop

使用下列命令来在开机时启用服务：

sudo update-rc.d –f <servicename> defaults

其中<servicename>代表打算启动的网络服务，例如：

sudo update-rc.d –f ssh defaults



## 实验数据

见上图

## 实验数据处理

无

## 实验结果与分析

在官网下载kali后（密码是kali）需要换源才可以安装ftp，在/etc/apt/source.list文件中添加如下代码

deb http://mirrors.163.com/debian lenny main non-free contrib

deb http://mirrors.163.com/debian lenny-proposed-updates main contrib non-free

deb http://mirrors.163.com/debian-security lenny/updates main contrib non-free

deb-src http://mirrors.163.com/debian lenny main non-free contrib

deb-src http://mirrors.163.com/debian lenny-proposed-updates main contrib non-free

deb-src http://mirrors.163.com/debian-security lenny/updates main contrib non-free

deb http://mirrors.ustc.edu.cn/ubuntu/ bionic main restricted universe multiverse

deb http://mirrors.ustc.edu.cn/ubuntu/ bionic-security main restricted universe multiverse

deb http://mirrors.ustc.edu.cn/ubuntu/ bionic-updates main restricted universe multiverse

deb http://mirrors.ustc.edu.cn/ubuntu/ bionic main restricted universe multiverse

deb http://mirrors.ustc.edu.cn/ubuntu/ bionic-backports main restricted universe multiverse

deb-src http://mirrors.ustc.edu.cn/ubuntu/ bionic main restricted universe multiverse

deb-src http://mirrors.ustc.edu.cn/ubuntu/ bionic-security main restricted universe multiverse

deb-src http://mirrors.ustc.edu.cn/ubuntu/ bionic-updates main restricted universe multiverse

deb-src http://mirrors.ustc.edu.cn/ubuntu/ bionic main restricted universe multiverse

deb-src http://mirrors.ustc.edu.cn/ubuntu/ bionic-backports main restricted universe multiverse

deb http://cn.archive.ubuntu.com/ubuntu bionic main multiverse restricted universe

deb http://cn.archive.ubuntu.com/ubuntu bionic-updates main multiverse restricted universe

deb http://cn.archive.ubuntu.com/ubuntu bionic-security main multiverse restricted universe

deb http://cn.archive.ubuntu.com/ubuntu bionic main multiverse restricted universe

然后更新源 sudo apt-get update

即可安装ftp。