**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：高级测试环境**

## 实验目的

熟悉Virtual Machine

攻击 WordPress

## 实验仪器

希冀平台

Linux kali 5.4.0-kali3-amd54

wordpress 虚拟机

## 实验原理

既然我们已经了解了 Kali Linux 所包含的工具，现在我们要调查一些真实世界的场景。我们进行的许多攻击都有意在有漏洞的软件和系统上执行。但是，当你使用 Kali 攻击一个系统时，它不可能像我们当前的测试平台那样没有防护。

这一章中，我们会探索一些技巧，来建立起一些真实的测试环境。在当前的信息技术水平中，多数公司都使用平台即服务（PAAS）解决方案，云服务器主机，或者使用小型网络，它们由桌面、服务器和防火墙（单独）或防火墙和路由的组合组成。我们会建立这些环境，之后对它们发起攻击。

我们所有攻击的目的都是获取 root 级别的访问。

## 实验内容与步骤

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

Virtual Machine Manager 是桌面 Linux 用户的强大工具。它是开源的，是专有和封闭虚拟化产品的绝佳替代品。

如果你需要在虚拟机中配置更多详细信息，那么你就需要一个工具，为磁盘、网卡（NIC）和其他硬件提供全面的选项。这时就需要 虚拟机管理器（Virtual Machine Manager）（virt-manager）了。

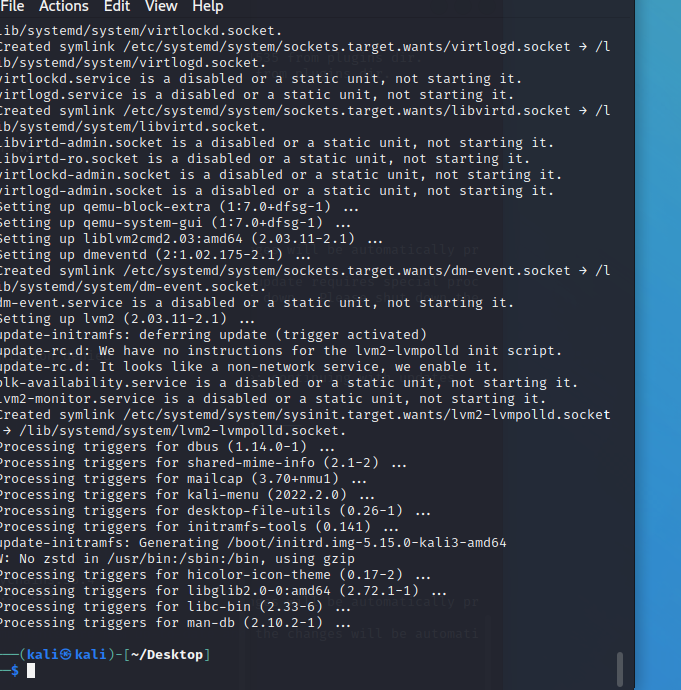
**1. 安装并运行Virtual Machine Manager**

如果在应用菜单中没有看到它，你可以从包管理器或命令行安装它：

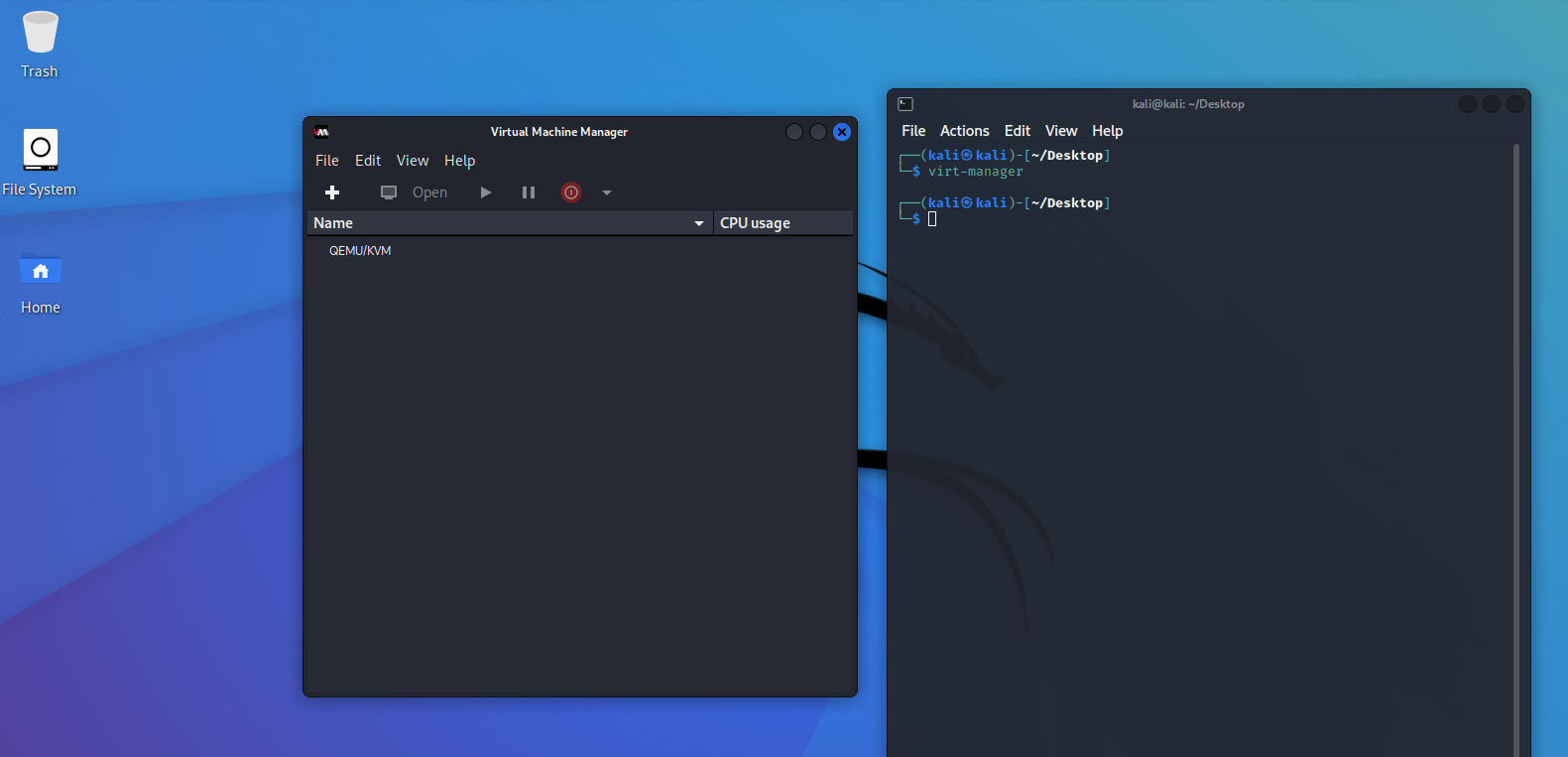
在 Fedora 上：sudo dnf install virt-manager

在 Ubuntu 上：sudo apt install virt-manager





安装完成后，在命令行输入virt-manager启动。

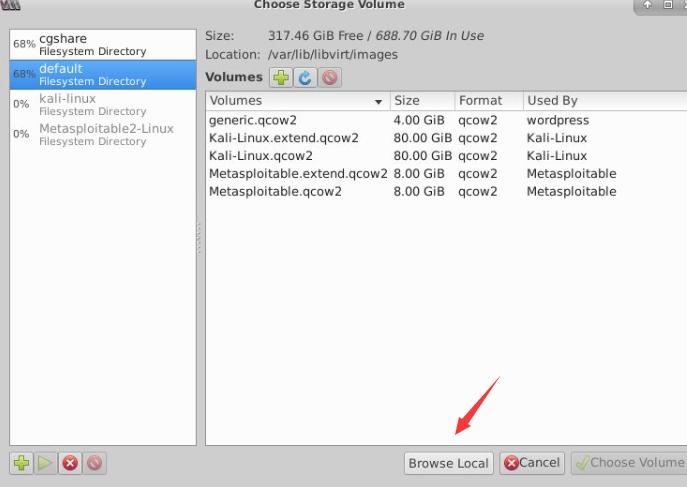


**2. 如何使用virt-manager 创建虚拟机**

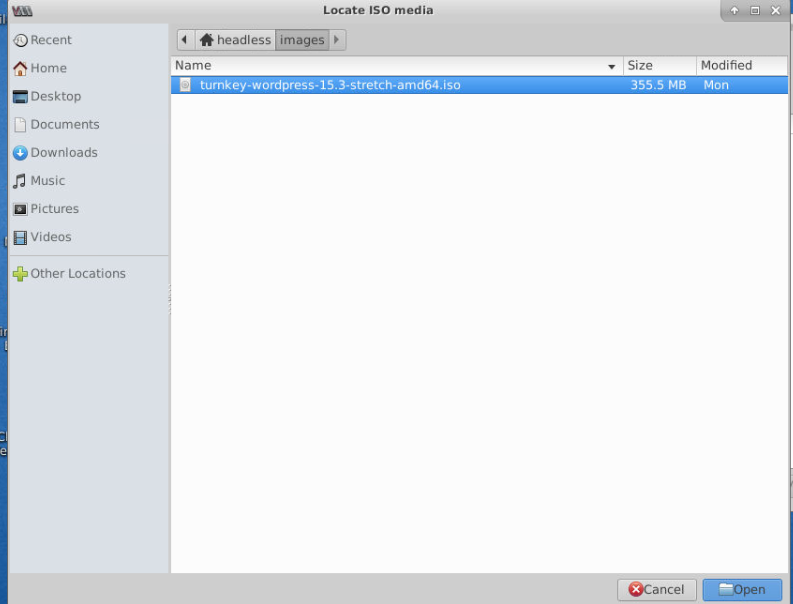
为了演示如何使用 virt-manager 创建虚拟机，我将设置一个 wordpress 虚拟机。

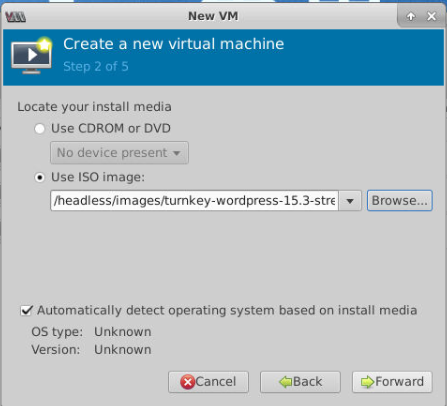
首先，单击 “ 文件(File)” 然后点击 “ 新建虚拟机(New Virtual Machine)”。Virt-manager 的开发者已经标记好了每一步（例如，“ 第 1 步，共 5 步(Step 1 of 5)”）来使其变得简单。单击 “ 本地安装介质(Local install media)” 和 “ 下一步(Forward)”。



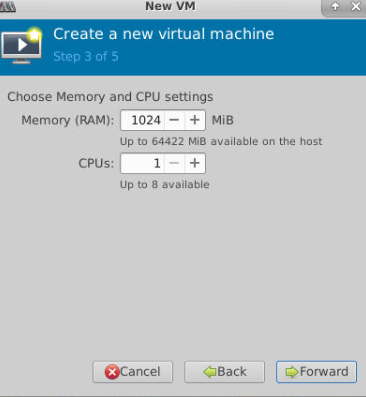


在下个页面中，选择要安装的操作系统的 ISO 文件。（wordpress镜像位于/headless/images目录中。）Virt-manager 自动检测操作系统。

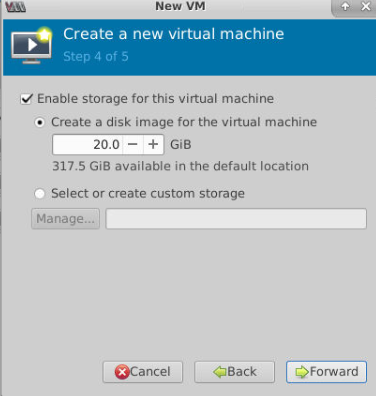


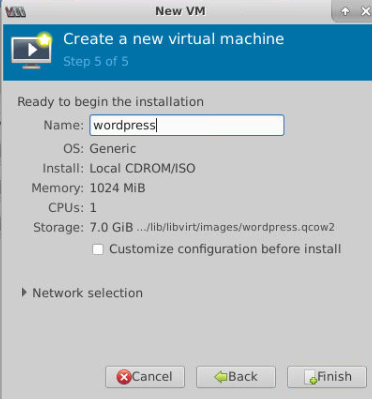


在步骤 3 中，你可以指定虚拟机的内存和 CPU。默认值为内存 1,024MB 和一个 CPU。

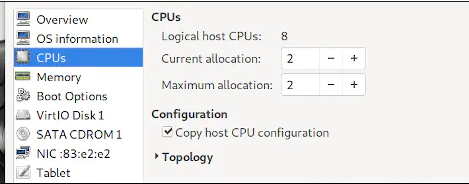


下一步为虚拟机配置存储。默认设置是 20GB 硬盘。（我保留此设置，但你可以根据需要进行调整。）你还可以选择现有磁盘镜像或在自定义位置创建一个磁盘镜像。

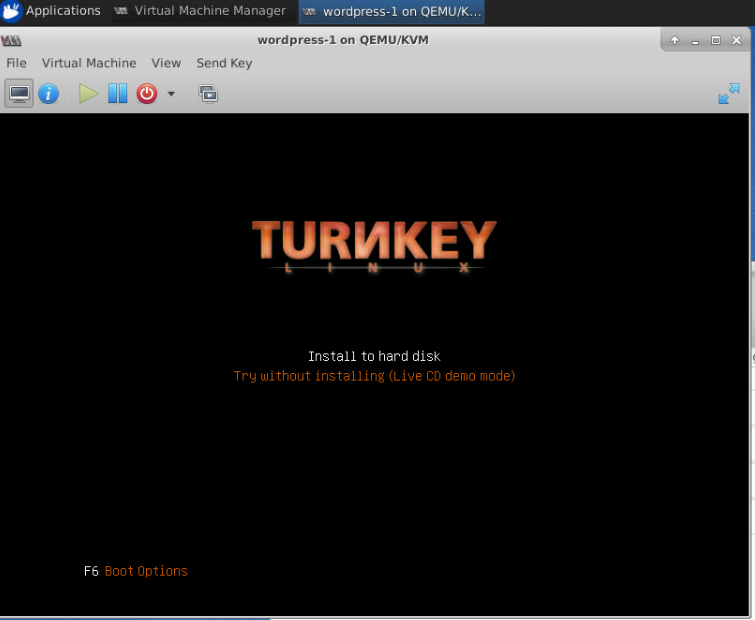




步骤 5 是命名虚拟机并单击“ 完成(Finish)”。这相当于创建了一台虚拟机，也就是 GNOME Boxes 中的一个 Box。虽然技术上讲是最后一步，但你有几个选择（如下面的截图所示）。由于 virt-manager 的优点是能够自定义虚拟机，因此在单击“ 完成(Finish)”之前，我将选中“ 在安装前定制配置(Customize configuration before install)”的复选框。



对 VM 配置感到满意后，单击 “ 开始安装(Begin Installation)”，系统将启动并开始从 ISO 安装指定的操作系统。



完成后，它会重新启动，你的新虚拟机就可以使用了。

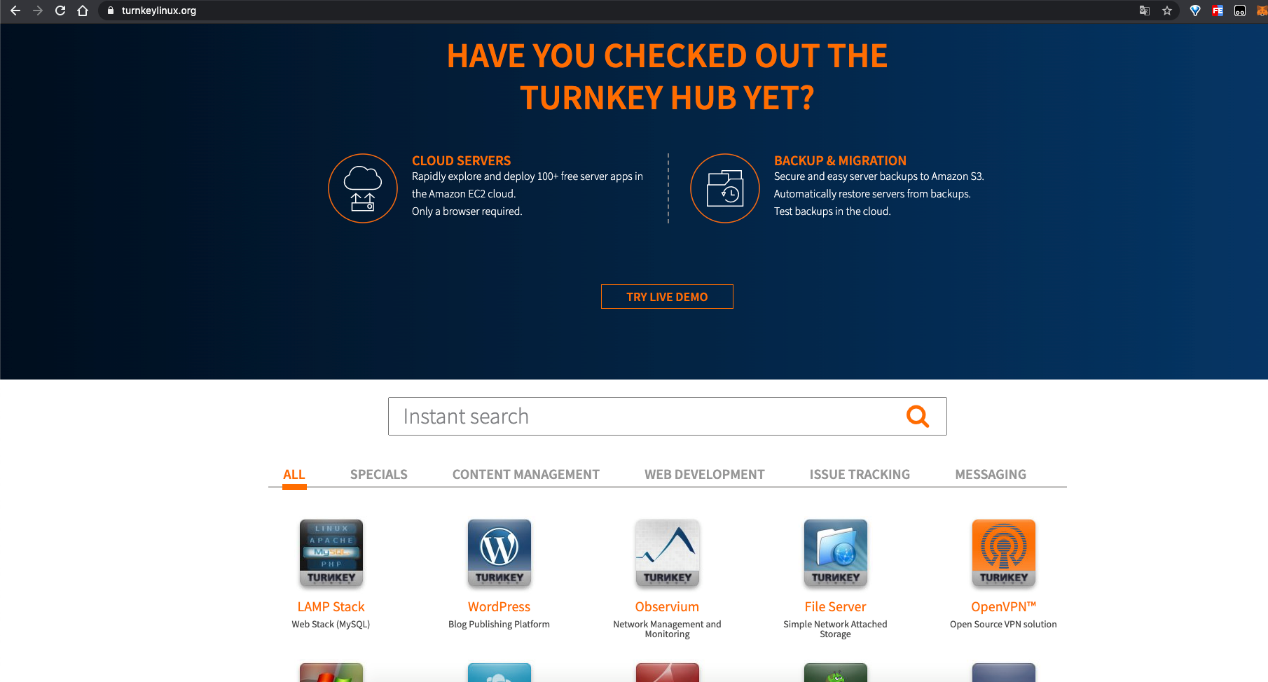
选择越来越多的公司在日常业务中使用 SAAS （软件及服务）工具。例如，公司普遍使用 WordPress作为网站的内容管理系统，或 Drupal 作为内部网络。在这些应用中定位漏洞的能力具有极大的价值。

收集被测试应用的一个很好的方式就是在这个网址 [http://www.turnkeylinux.org](http://www.turnkeylinux.org/) 。这个实验中，我们会下载流行的 WordPress Turnkey Linux 发行版。

**1. 下载wordpress镜像**

[http://www.turnkeylinux.org](http://www.turnkeylinux.org/)

主页如图所示：



搜索wordpress，下载我们所需要的镜像文件：



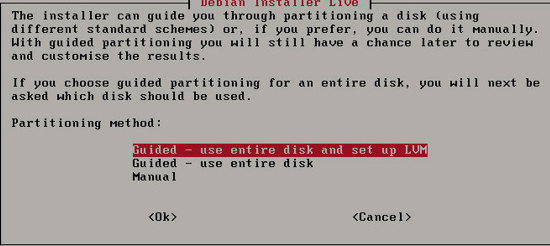
下载完成后，安装实验步骤1的教程，在虚拟机中安装好wordpress即可。

**2. 安装WordPress Turnkey Linux**

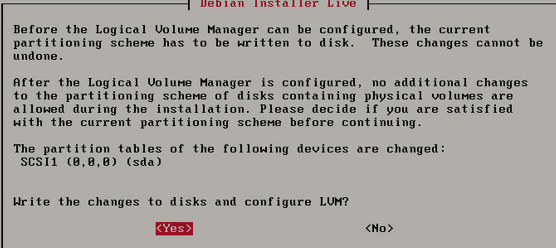
（1）使用虚拟机安装此镜像，然后启动此虚拟机，将显示如图 所示的界面。



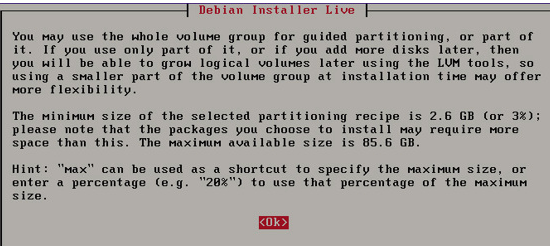
（2）在该界面选择Install to hard disk选项，按下“回车键”，将显示如图所示的界面。



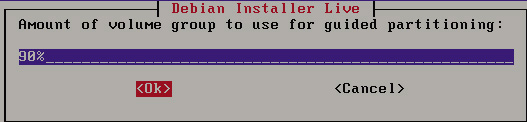
（3）该界面是选择分区的方法。该系统提供了三种方法，分别是使用整个磁盘并设置LVM、使用整个磁盘和手动分区。这里选择第一种，然后单击OK按钮，将显示如图所示的界面。



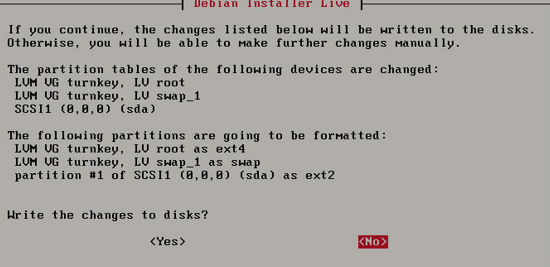
（4）该界面显示了分区的信息，这里提示是否将写入改变磁盘并配置LVM呢？如果想要重新分配分区的话，就单击No按钮，否则单击Yes按钮。本例中单击Yes按钮，将显示如图所示的界面。



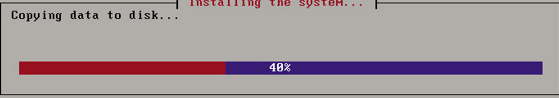
（5）该界面显示了LVM的配置信息。单击OK按钮，将显示如图所示的界面。



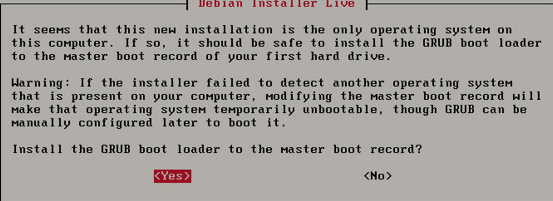
（6）该界面提示使用引导分区的卷组来安装系统。此时，单击OK按钮，将显示如图所示的界面。



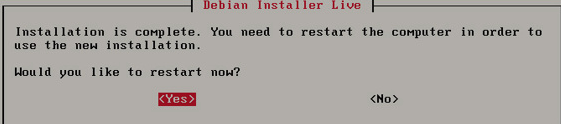
（7）该界面显示了磁盘的分区表信息，此时提示是否要写入数据。这里单击Yes按钮，将显示如图所示的界面。



（8）该界面显示了复制数据的磁盘的一个进度。复制完后，将显示如图所示的 界面。



（9）该界面提示是否安装GRUB引导加载程序的主引导记录。这里单击Yes按钮，将显示如图所示的界面。



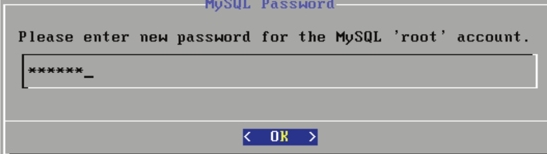
（10）该界面显示WordPress Turnkey Linux已经安装完成，是否现在重新启动系统。单击Yes按钮，将显示如图所示的界面。



（11）在该界面为Root用户设置一个密码。输入密码后，单击OK按钮，将显示如图所示的界面。



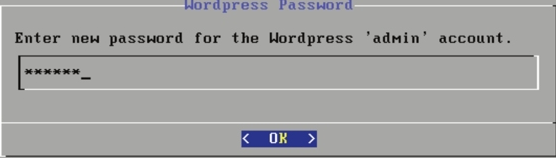
（12）该界面要求再次为Root用户输入相同的密码，单击OK按钮，将显示如图所示的界面。



（13）在该界面为MySQL服务的Root用户设置一个密码，设置完后单击OK按钮，将显示如图所示的界面。



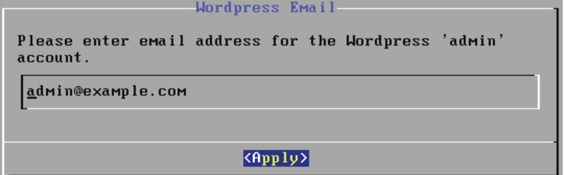
（14）在该界面再次为MySQL服务的Root用户输入相同的密码，然后单击OK按钮，将显示如图所示的界面。



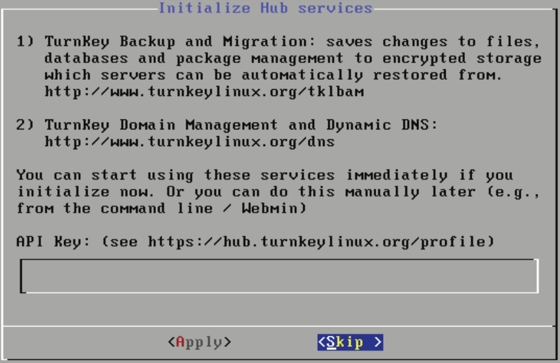
（15）在该界面要求为Wordpress的用户admin设置一个密码，输入密码后，单击OK按钮，将显示如图所示的界面。



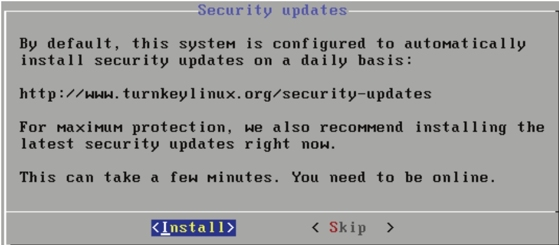
（16）在该界面再次为Wordpress用户admin输入相同的密码，然后单击OK按钮，将显示如图所示的界面。



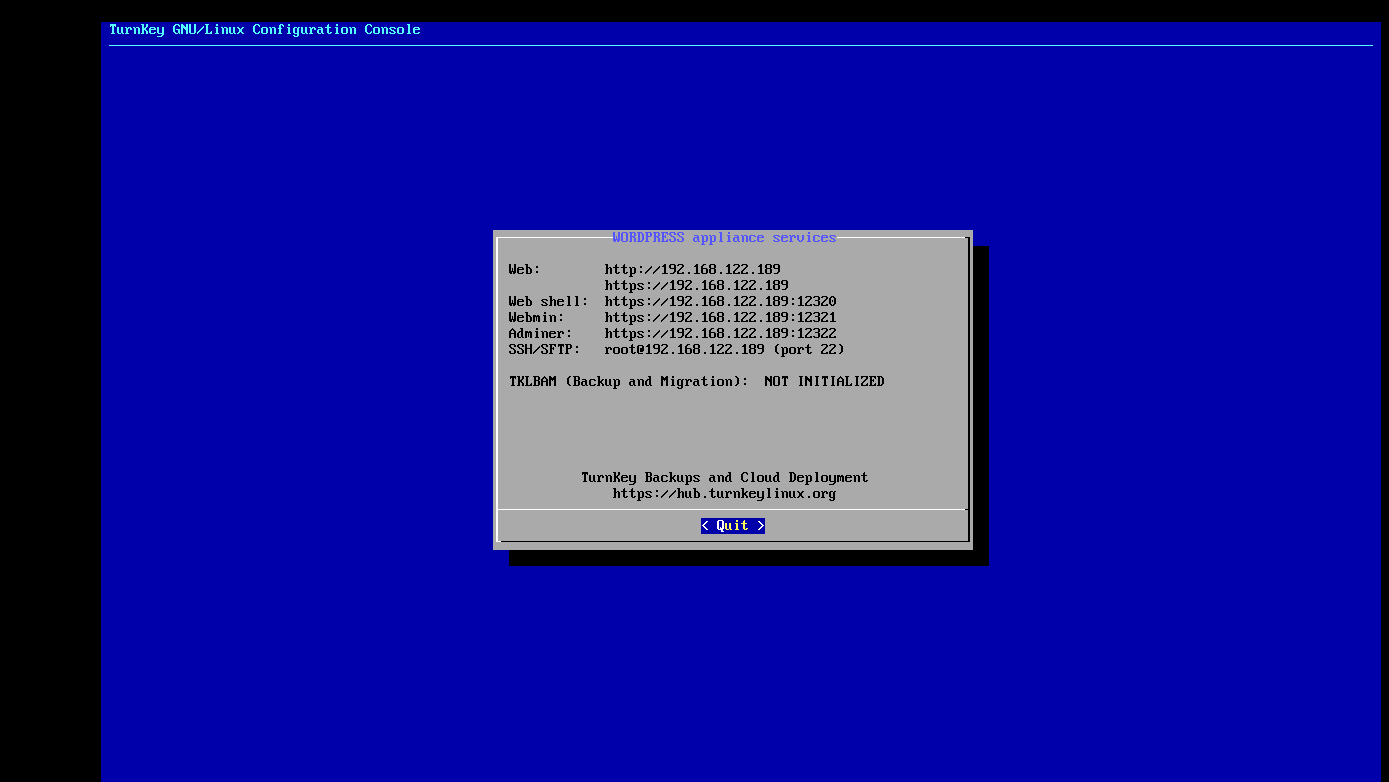
（17）该界面提示为Wordpress用户admin设置一个邮件地址，这里使用默认的[email protected]。然后单击Apply按钮，将显示如图所示的界面。



（18）该界面显示了初始化Hub服务信息，在该界面单击Skip按钮，将显示如图所示的界面。



（19）该界面提示是否现在安装安全更新，这里单击Install按钮，将显示如图所示的界面。

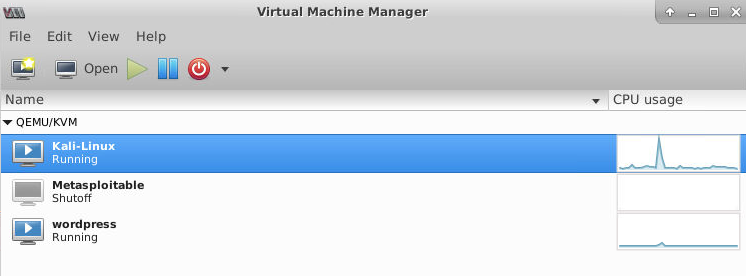


（20）该界面显示了WordPress应用服务的详细信息，如Web地址、Web shell地址和端口、Webmin地址、PHPMyAdmin地址和端口及SSH/SFTP地址和端口等。此时，表明WordPress Turnkey Linux就可以使用了。

**3. 攻击WordPress应用程序**

上一小节介绍了WordPress虚拟机的安装。现在就可以启动WordPress虚拟机，在Kali Linux下使用WPScan攻击它。WPScan是一个黑盒安全扫描器，它允许用户查找Word Press安装版的一些已知的安全漏洞。本小节将介绍使用WPScan工具攻击WordPress应用程序。

(1) 首先打开Kali和wordpress



(2) 使用wpscan -h可以查看各种参数以及定义



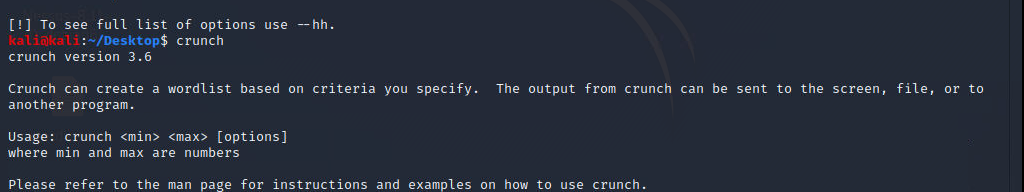
(3) Kali-linux创建密码字典

所谓的密码字典主要是配合密码破解软件所使用，密码字典里包括许多人们习惯性设置的密码。这样可以提高密码破解软件的密码破解成功率和命中率，缩短密码破解的时间。当然，如果一个人密码设置没有规律或很复杂，未包含在密码字典里，这个字典就没有用了，甚至会延长密码破解所需要的时间。在Linux中有Crunch和rtgen两个工具，可以来创建密码字典。为方便用户的使用，本节将介绍Crunch的使用方法。

Crunch是一种创建密码字典工具，该字典通常用于暴力破解。使用Crunch工具生成的密码可以发送到终端、文件或另一个程序。下面将介绍使用Crunch工具创建密码字典。

使用Crunch生成字典。具体操作步骤如下所示。

a. 启动crunch命令。执行命令如下所示。

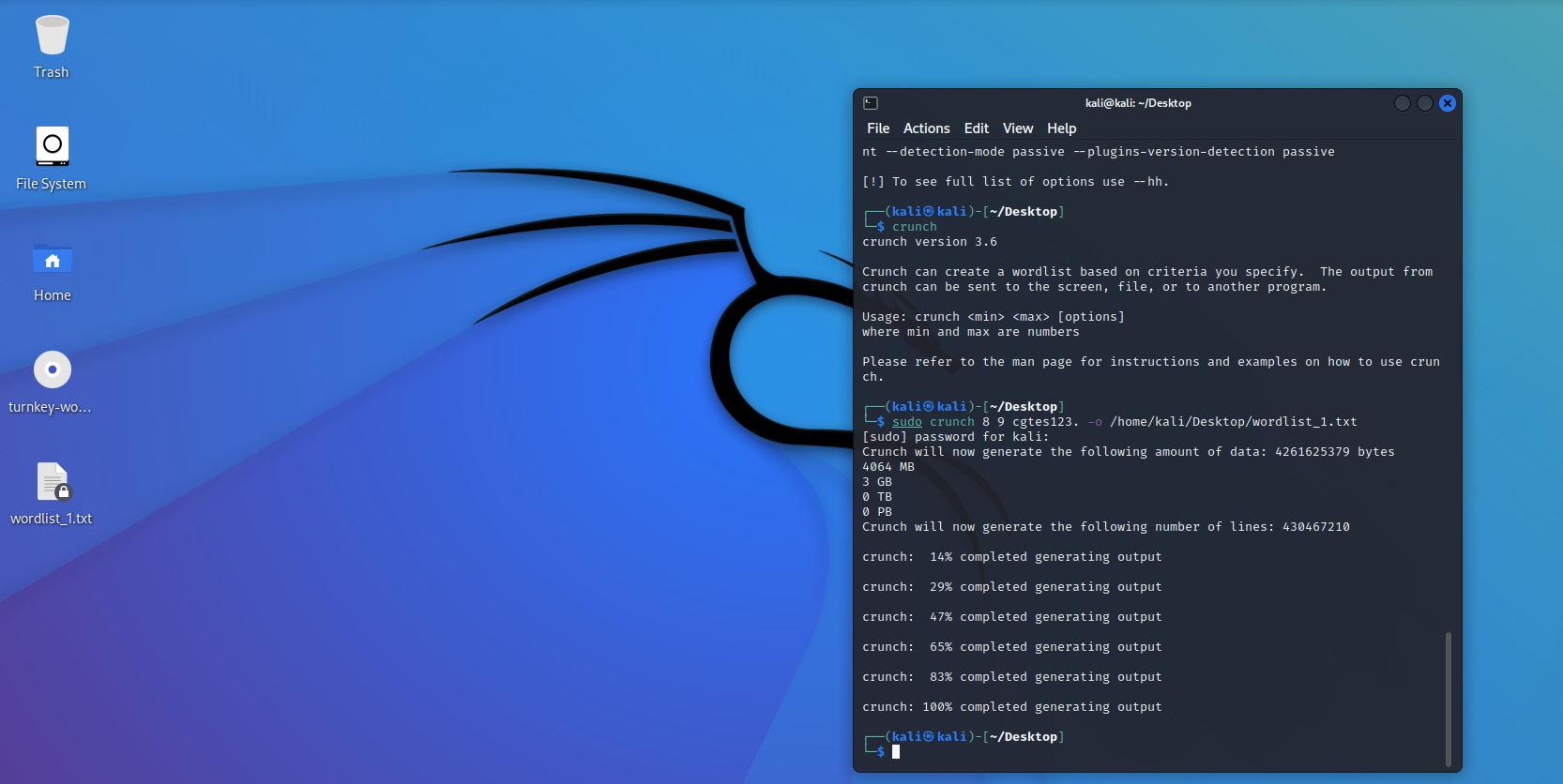


输出的信息显示了crunch命令的版本及语法格式。其中，使用crunch命令生成密码的语法格式如下所示：

sudo crunch [minimum length] [maximum length] [character set] [options]

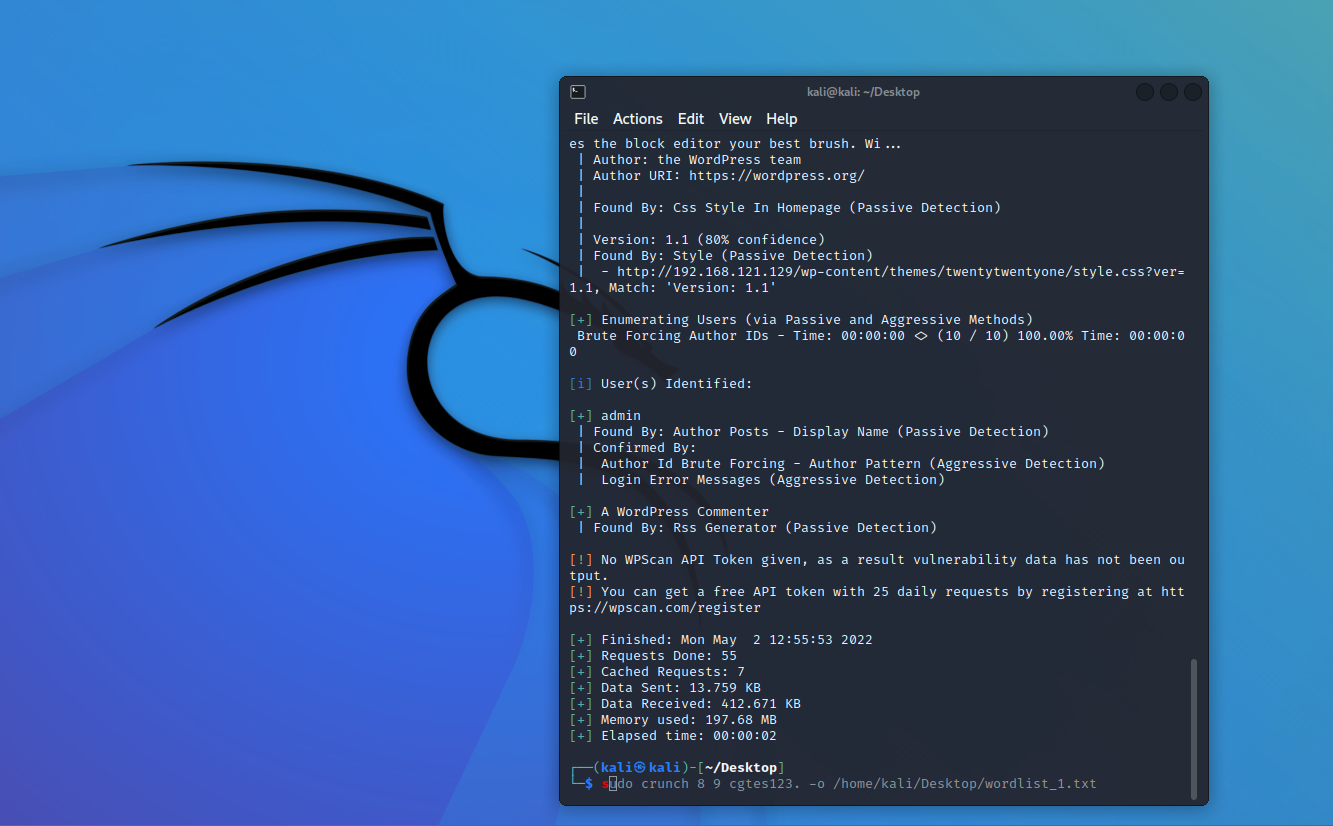
b. 创建一个密码列表文件，并保存在桌面上。其中，生成密码列表的最小长度为8，最大长度为9，并使用cgtest.1为字符集。执行命令如下所示：

sudo crunch 8 9 cgtes123. -o /home/kali/Desktop/wordlist\_1.txt



(4) 扫描wordpress用户

wpscan --url 192.168.121.129 --enumerate u

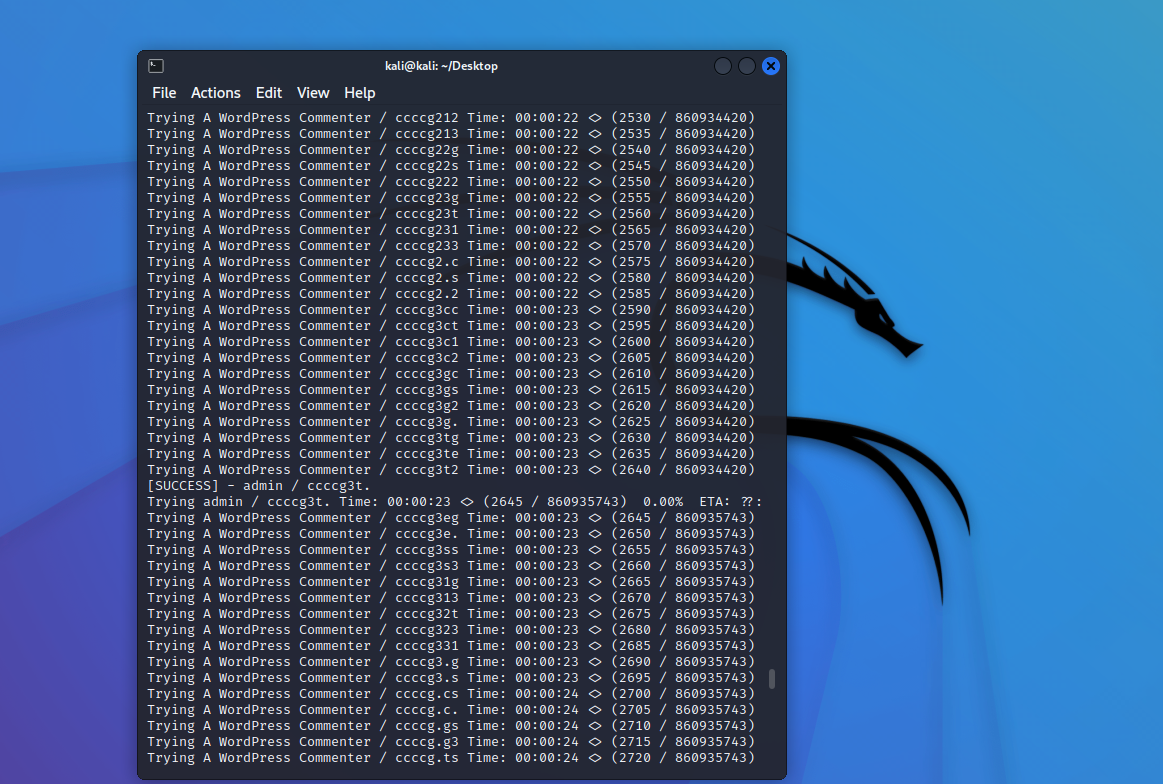


(5) 使用crunch 工具生成的密码表暴力破解wordpress用户密码

wpscan --url 192.168.121.129 -e u --passwords /home/kali/Desktop/wordlist\_1.txt



以下是暴力循环获取的密码：



## 实验数据

见上图

## 实验数据处理

无

## 实验结果与分析

WordPress是使用PHP语言开发的博客平台，用户可以在支持PHP和MySQL数据库的服务器上架设属于自己的网站。也可以把 WordPress当作一个内容管理系统（CMS）来使用。

WordPress是一款个人博客系统，并逐步演化成一款内容管理系统软件，它是使用PHP语言和MySQL数据库开发的，用户可以在支持 PHP 和 MySQL数据库的服务器上使用自己的博客。

WordPress有许多第三方开发的免费模板，安装方式简单易用。不过要做一个自己的模板，则需要你有一定的专业知识。比如你至少要懂的标准通用标记语言下的一个应用HTML代码、CSS、PHP等相关知识。

WordPress官方支持中文版，同时有爱好者开发的第三方中文语言包，如wopus中文语言包。WordPress拥有成千上万个各式插件和不计其数的主题模板样式。

不仅是WordPress，互联网上所有具有内容管理系统(CMS)的网站都容易受到黑客攻击。WordPress网站成为通用目标的原因是因为WordPress是世界上最受欢迎的网站CMS。它为全球超过33%的网站提供支持，这种巨大的流行度使黑客可以轻松地找到许多安全性较低的网站，以便他们可以利用它们及其共享漏洞，无论它是什么。有一个普遍的误解，认为黑客正在滥用个人数据或将网站劫为人质。虽然这可能发生，但根据我们的经验，超过95%的攻击希望仅散布垃圾邮件!他们访问服务器并劫持它以共享一些不法链接等。另一个常见的情况是初学者正在学习仅出于刺激目的而利用不太安全的网站。 这不会减少威胁的严重性。

对于密码的设置，不要所有账号都用同一个密码，如果密码很多，可以考虑使用第三方密码管理工具，比如 Last Pass 等。如果您使用弱密码，那么黑客可以通过一些黑客工具轻松获取密码。