**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：漏洞扫描**

## 实验目的

使用Nessus来扫描系统

## 实验仪器

希冀平台

Linux kali 5.4.0-kali3-amd54

Metasploitable2 虚拟机

## 实验原理

漏洞扫描器是一种能够自动在计算机、信息系统、网络及应用软件中寻找和发现安全弱点的程序。它通过网络对目标系统进行探测，向目标系统发生数据，并将反馈数据与自带的漏洞特征库进行匹配，进而列举目标系统上存在的安全漏洞。漏洞扫描是保证系统和网络安全必不可少的手段，面对互联网入侵，如果用户能够根据具体的应用环境，尽可能早的通过网络扫描来发现安全漏洞，并及时采取适当的处理措施进行修补，就可以有效地阻止入侵事件的发生。由于该工作相对枯燥，所以我们可以借助一些便捷的工具来实施，如Nessus和OpenVAS。本章将详细讲解这两个工具的使用。

扫描和识别目标的漏洞通常被渗透测试者看做无聊的任务之一。但是，它也是最重要的任务之一。这也应该被当做为你的家庭作业。就像在学校那样，家庭作业和小测验的设计目的是让你熟练通过考试。

漏洞识别需要你做一些作业。你会了解到目标上什么漏洞更易于利用，便于你发送威力更大的攻击。本质上，如果攻击者本身就是考试，那么漏洞识别就是你准备的机会。

Nessus 和 OpenVAS 都可以扫描出目标上相似的漏洞。这些漏洞包括：

Linux 漏洞

Windows 漏洞

本地安全检查

网络服务漏洞

## 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。

Nessus号称是世界上最流行的漏洞扫描程序，全世界有超过75000个组织在使用它。该工具提供完整的电脑漏洞扫描服务，并随时更新其漏洞数据库。Nessus不同于传统的漏洞扫描软件，Nessus可同时在本机或远端上遥控，进行系统的漏洞分析扫描。Nessus也是渗透测试重要工具之一。所以，本章将介绍安装、配置并启动Nessus。

**1. Nessus的安装**

Nessus 的安装在实验《网络攻击\_Exp2\_定制Kali Linux》中的实验步骤5中已经讲解，本次实验主要讲解如何使用Nussus。

通过以上步骤的详细介绍，Nessus就配置好了，现在就可以使用Nessus扫描各种的漏洞。使用Nessus扫描漏洞之前需要新建扫描策略和扫描任务，为了后面能顺利的扫描各种漏洞，接下来将介绍新建策略和扫描任务的方法。

**2. 添加策略**

1） 首先输入命令，启动Nessus。

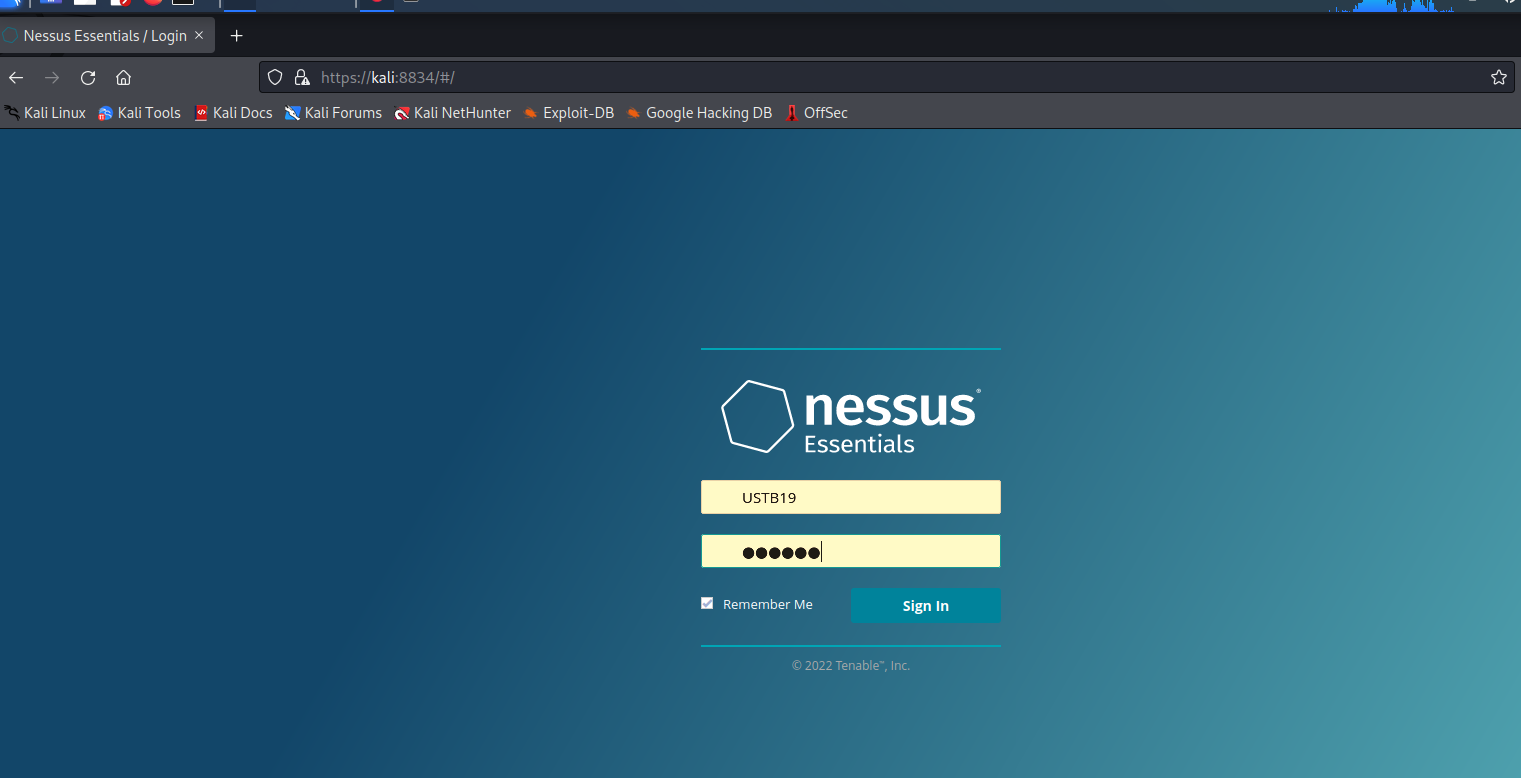
使用命令行启动Nessus服务

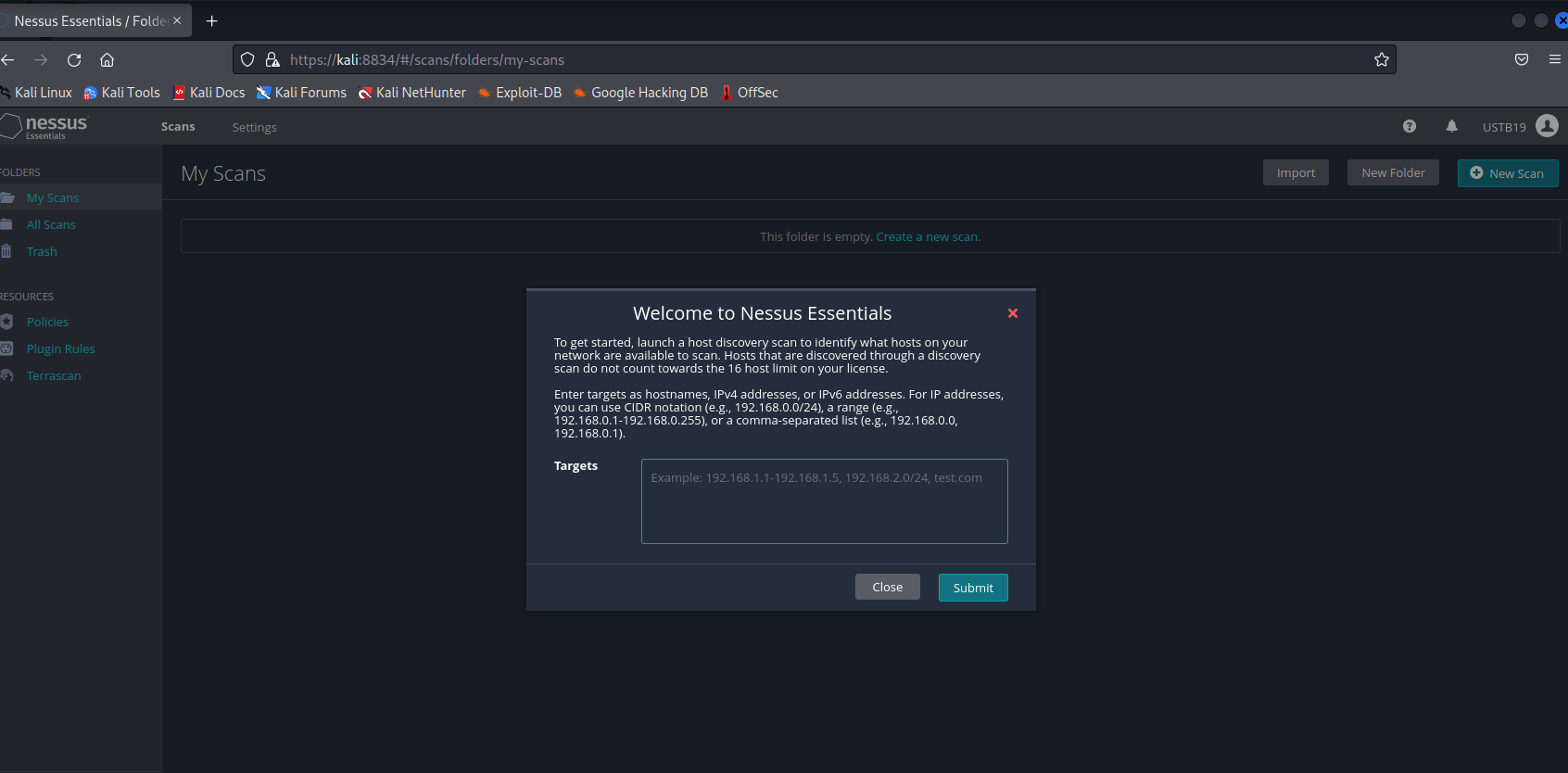
/bin/systemctl start nessusd.service



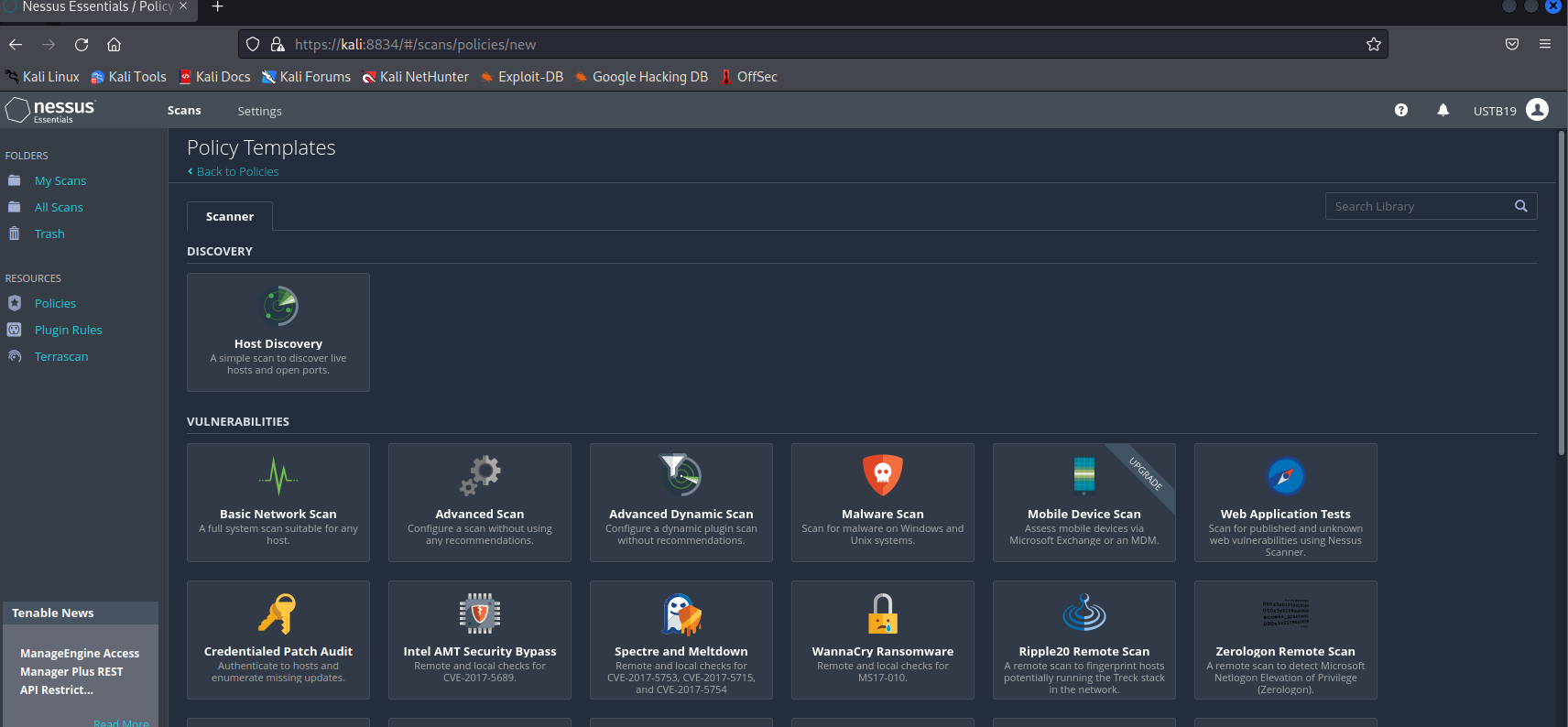
2） 打开浏览器，输入[https://kali:8834](https://kali:8834/) 登陆Nessus。

以下是账号密码：

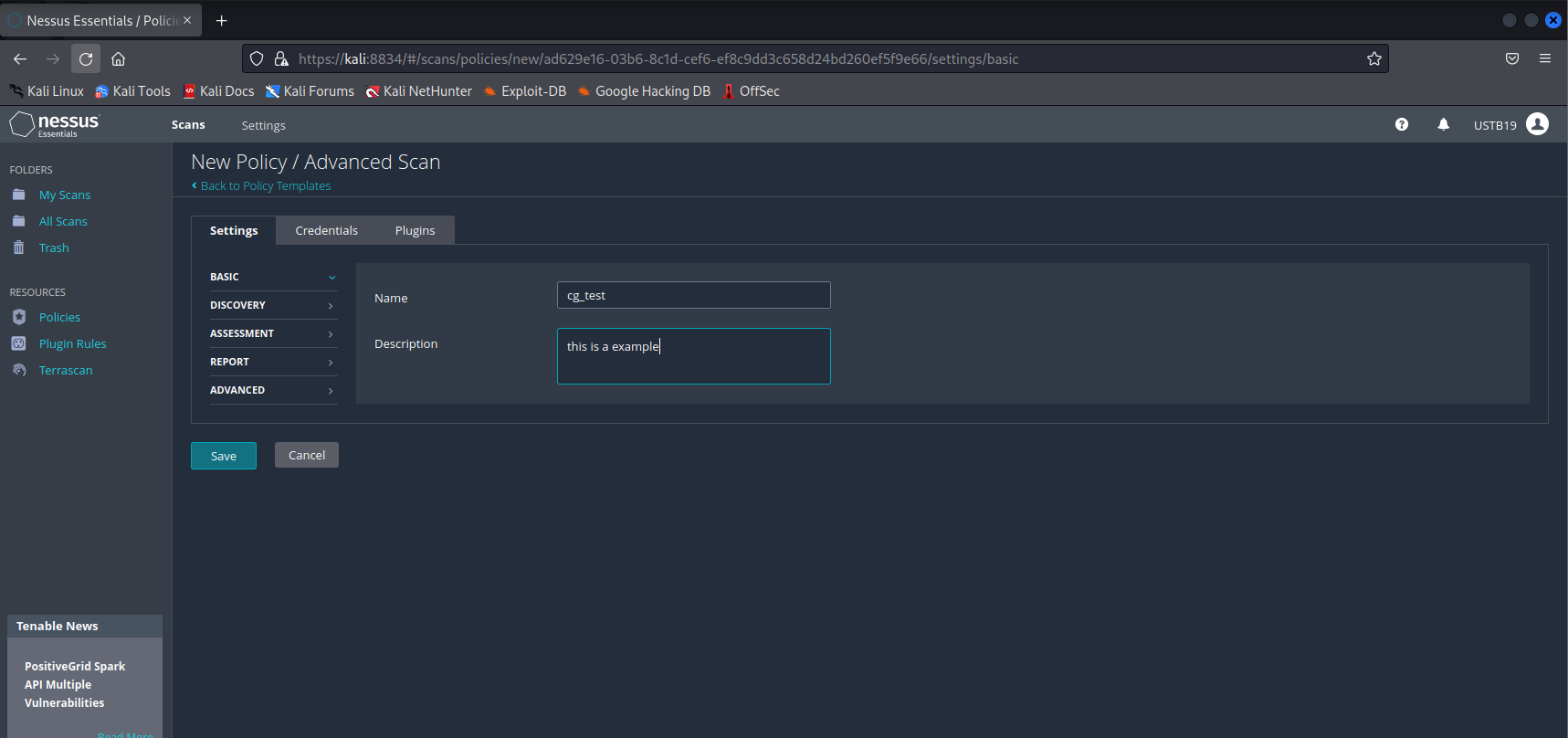




3）在该界面使用鼠标切换到Policies选项卡上，在该界面单击Create a New Policy按钮

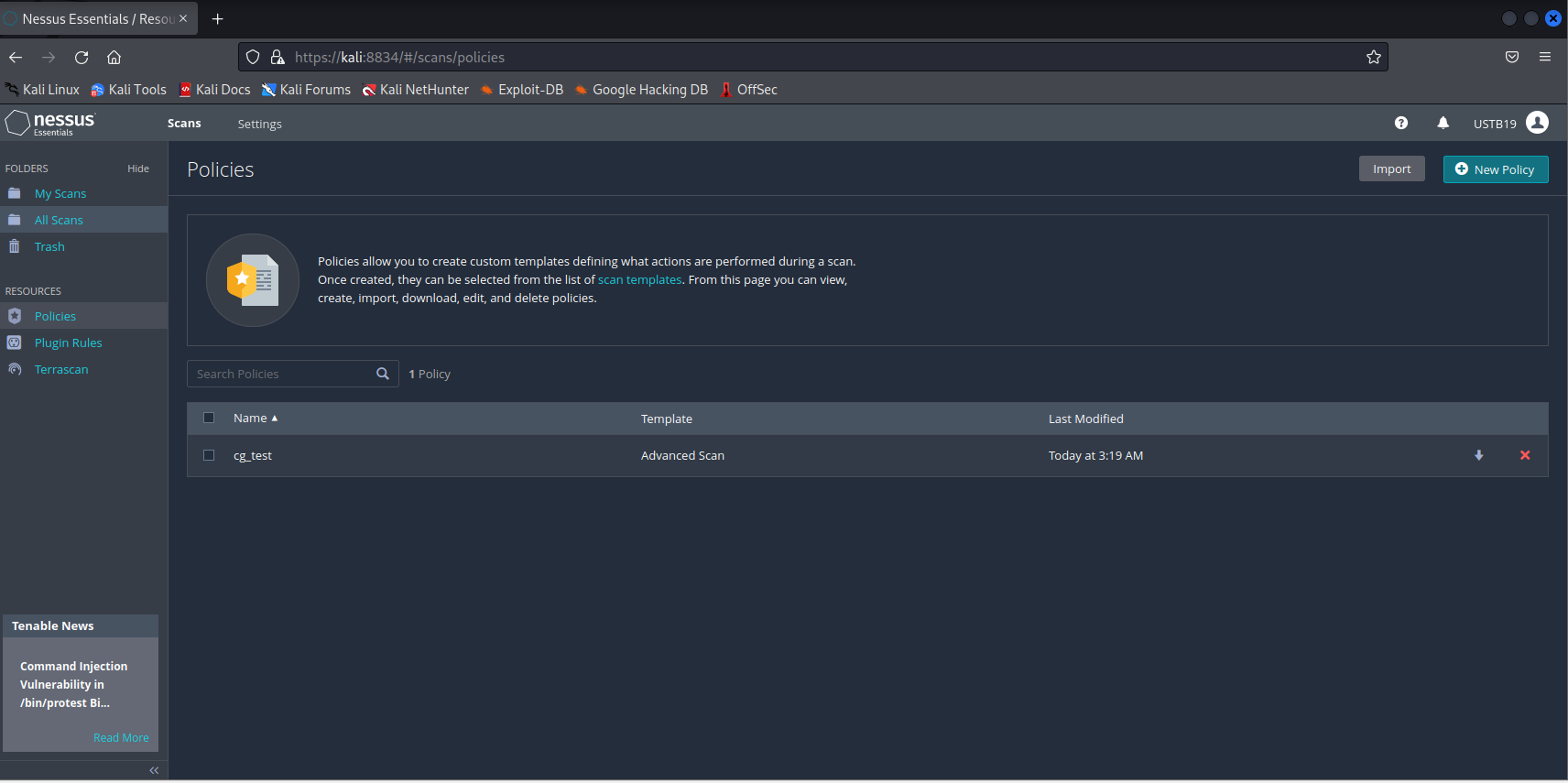


我们选择advanced scan 在该界面设置策略名、描述信息（可选项）。

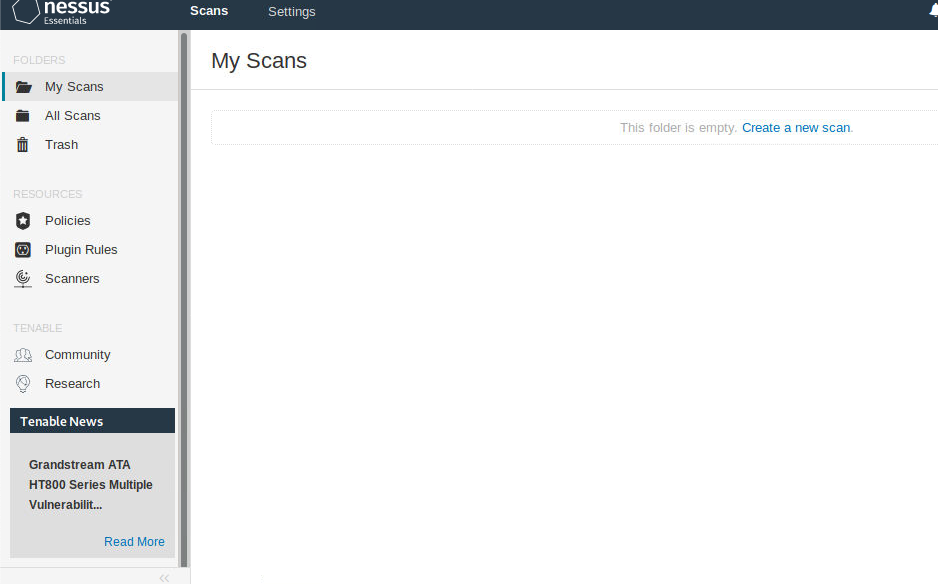


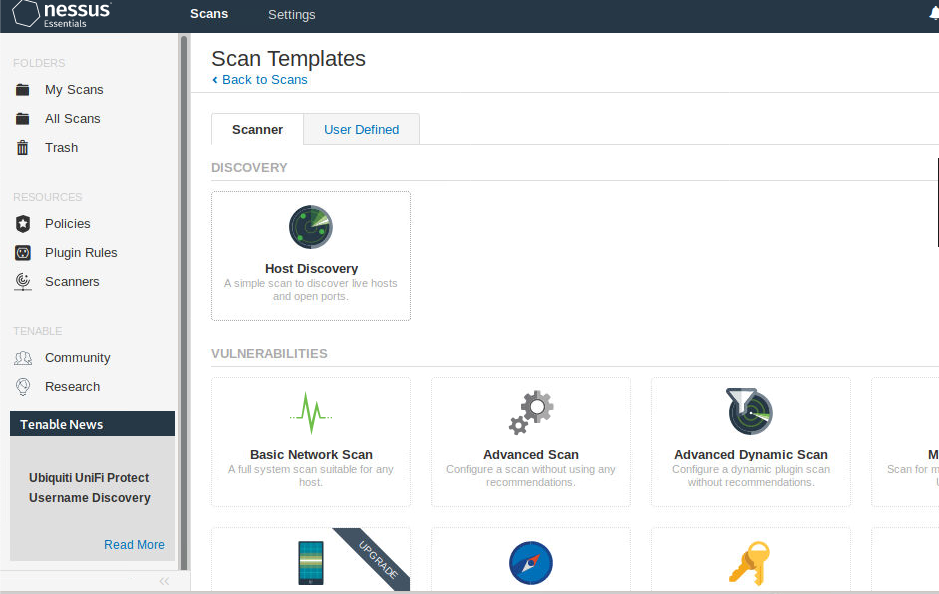
在该界面单击Save按钮

从该界面可以看到新建的策略cg\_test,表示该策略已创建成功

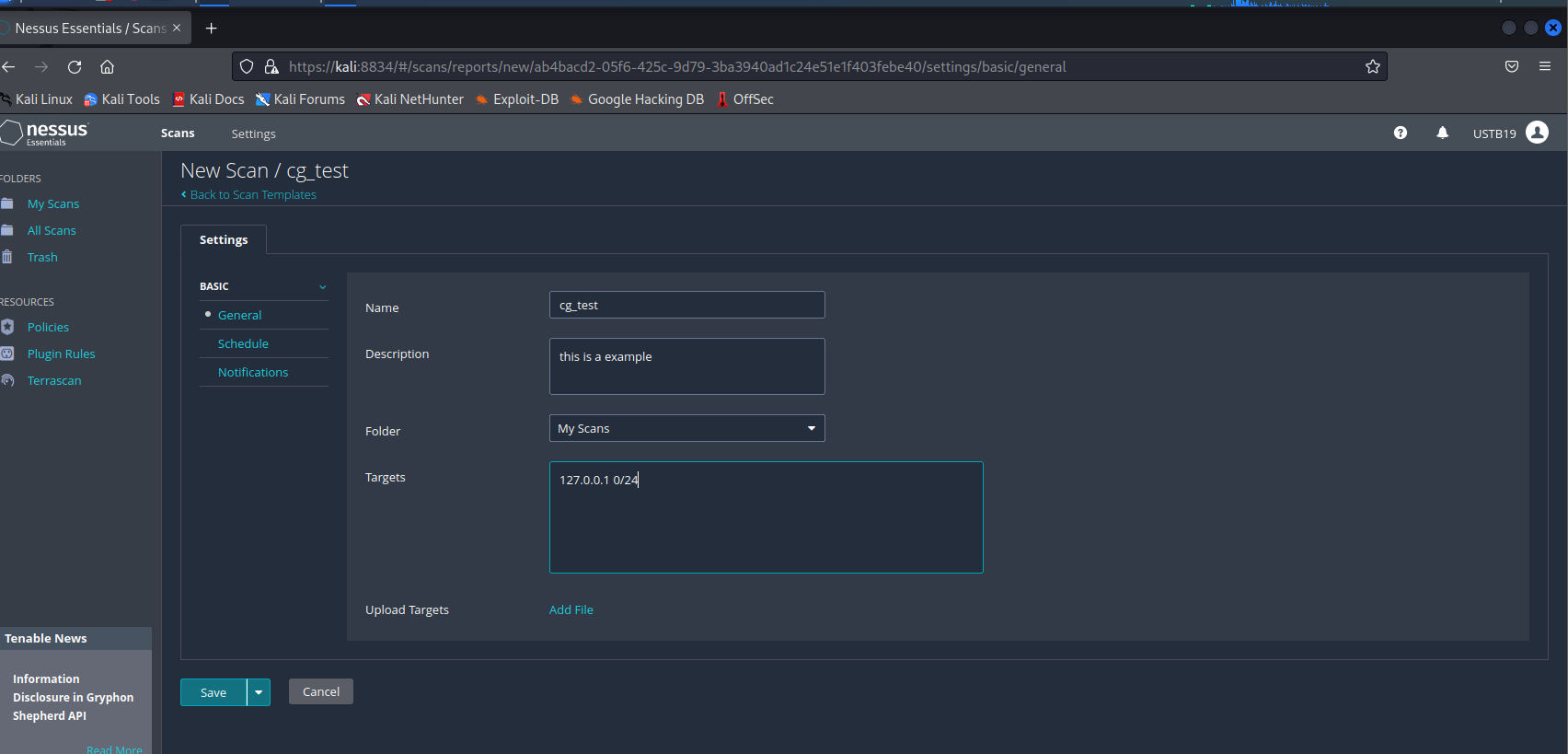


**3. 新建扫描任务**

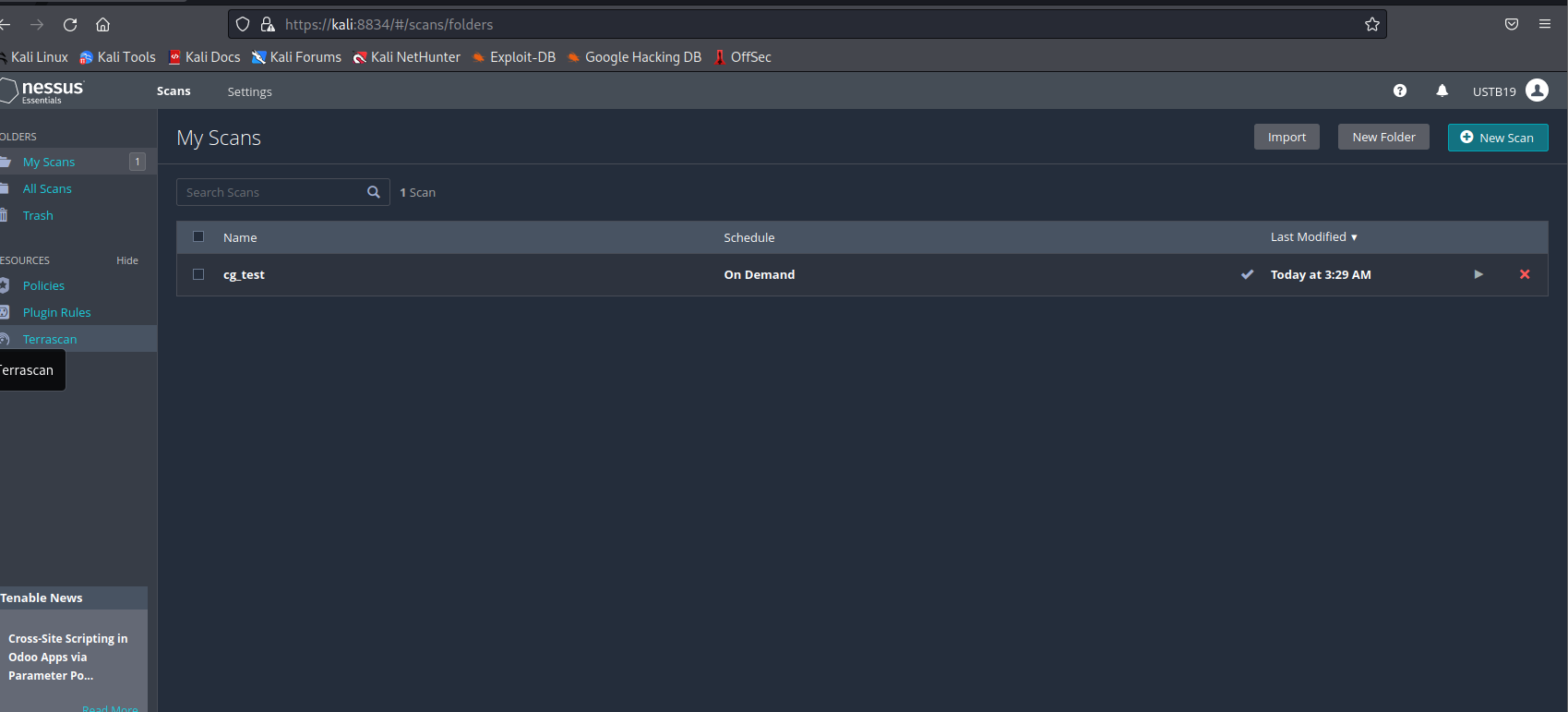
从该界面可以看到当前没有任何扫描任务，所以需要添加扫描任务后才能扫描。在该界面单击New Scan按钮 



我们选择用户自定义的cg\_test，也就是上个步骤我们定义的策略。



点击运行我们的扫描任务



**4. 扫描本地漏洞**

在前面介绍了Nessus的安装、配置、登录及新建策略和扫描任务，现在可以开始第一次测试组的安全漏洞。对于新建策略和扫描任务这里就不再赘述，本小节中只列出扫描本地漏洞所需添加的插件程序及分析扫描信息。

【实例】扫描本地漏洞具体操作步骤如下所示。

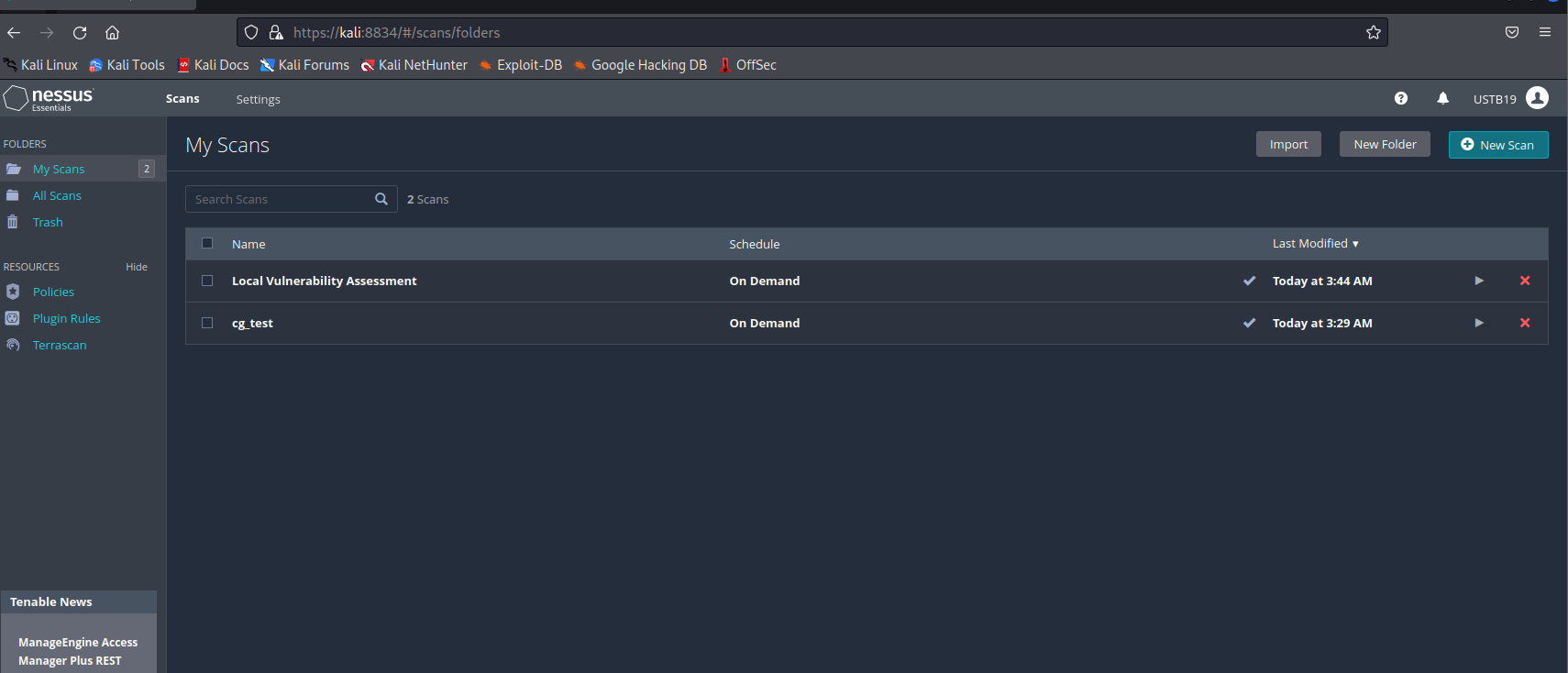
1）新建名为Local Vulnerability Assessment策略。

2）添加所需的插件程序。

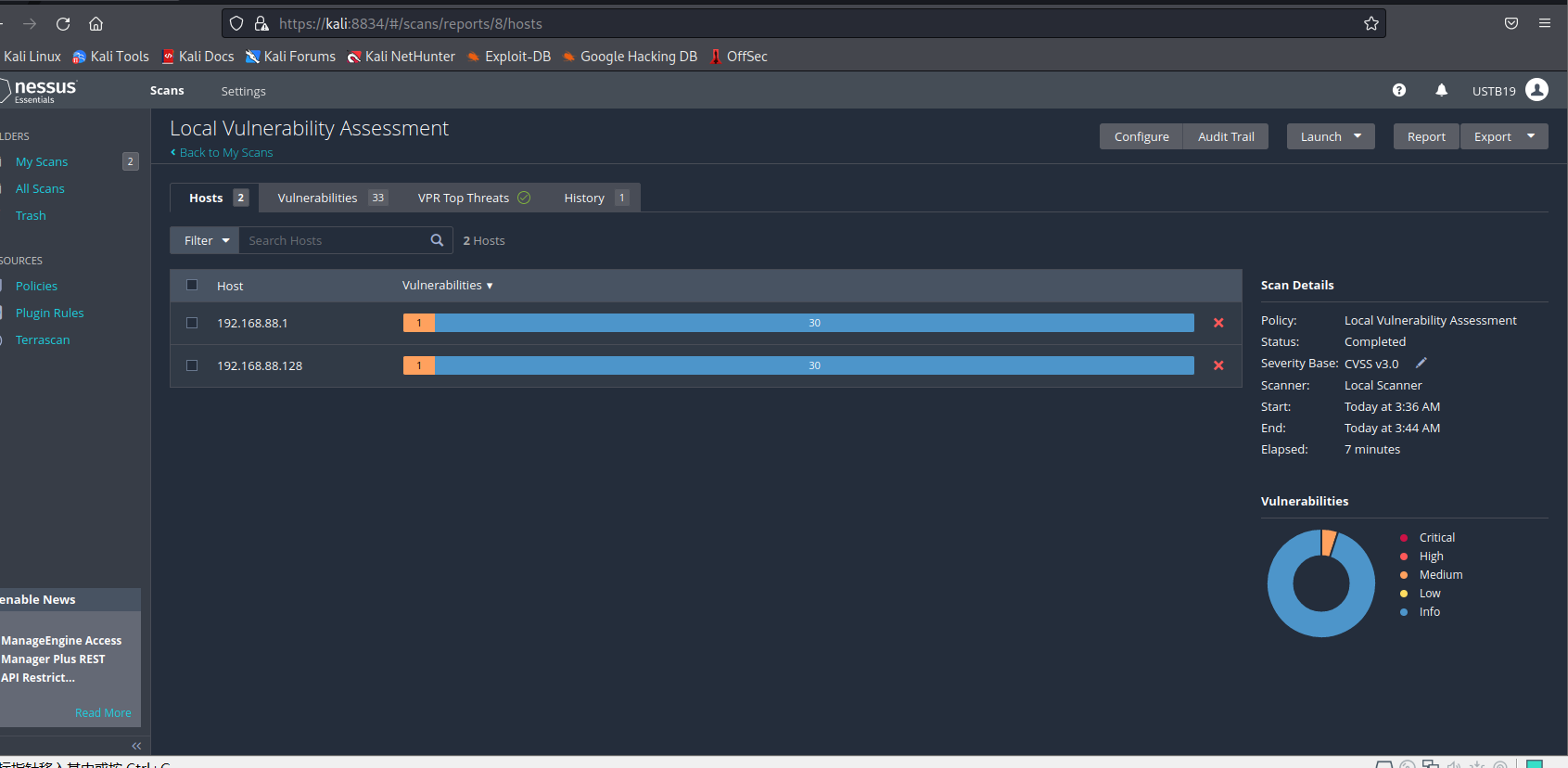
* Ubuntu Local Security Checks：扫描本地Ubuntu安全检查。
* Default Unix Accounts：扫描默认Unix账户。

3）新建名为Sample Scan扫描任务。

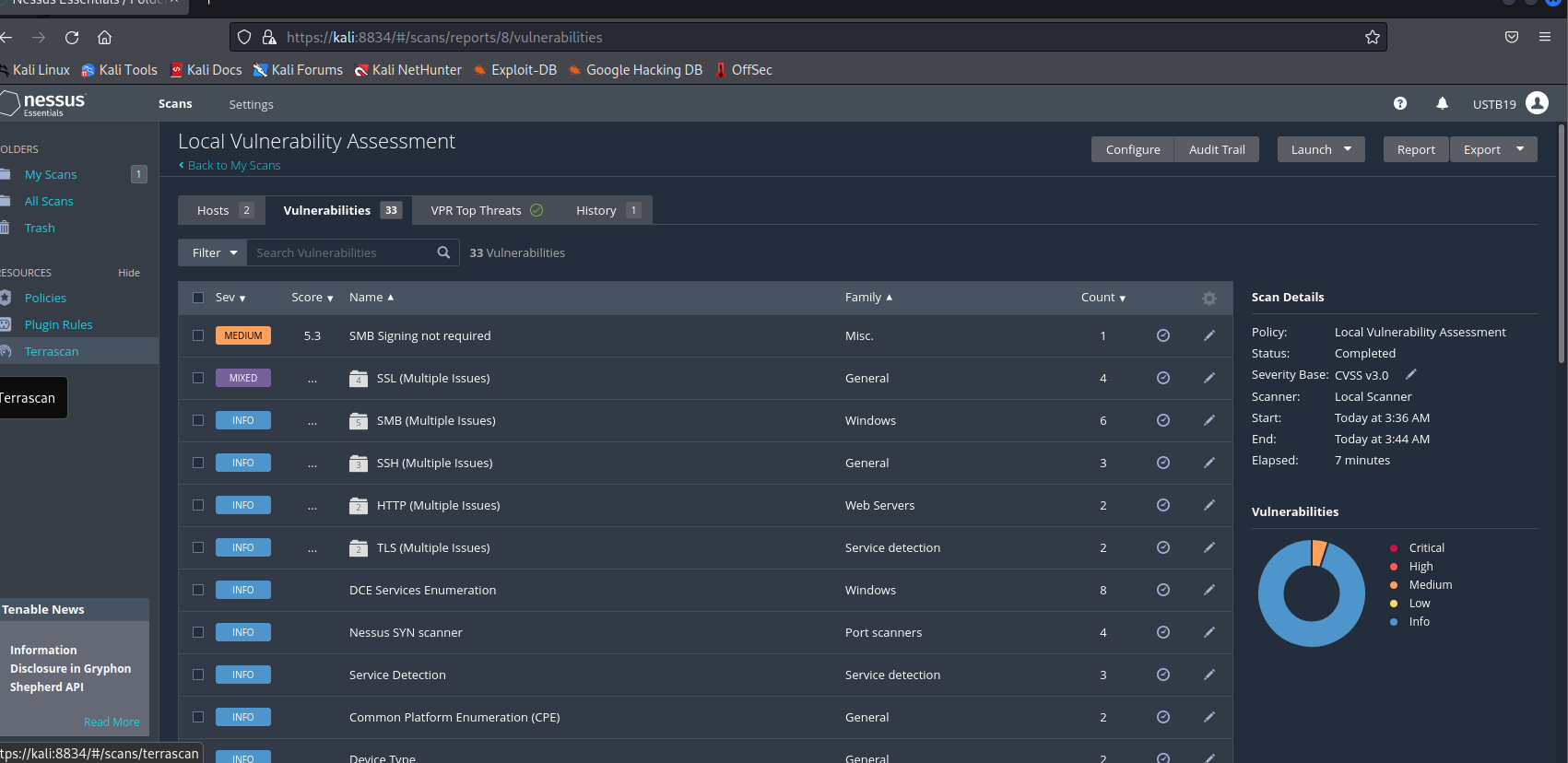
4）扫描漏洞。扫描任务执行完成后，将显示如图所示的界面。



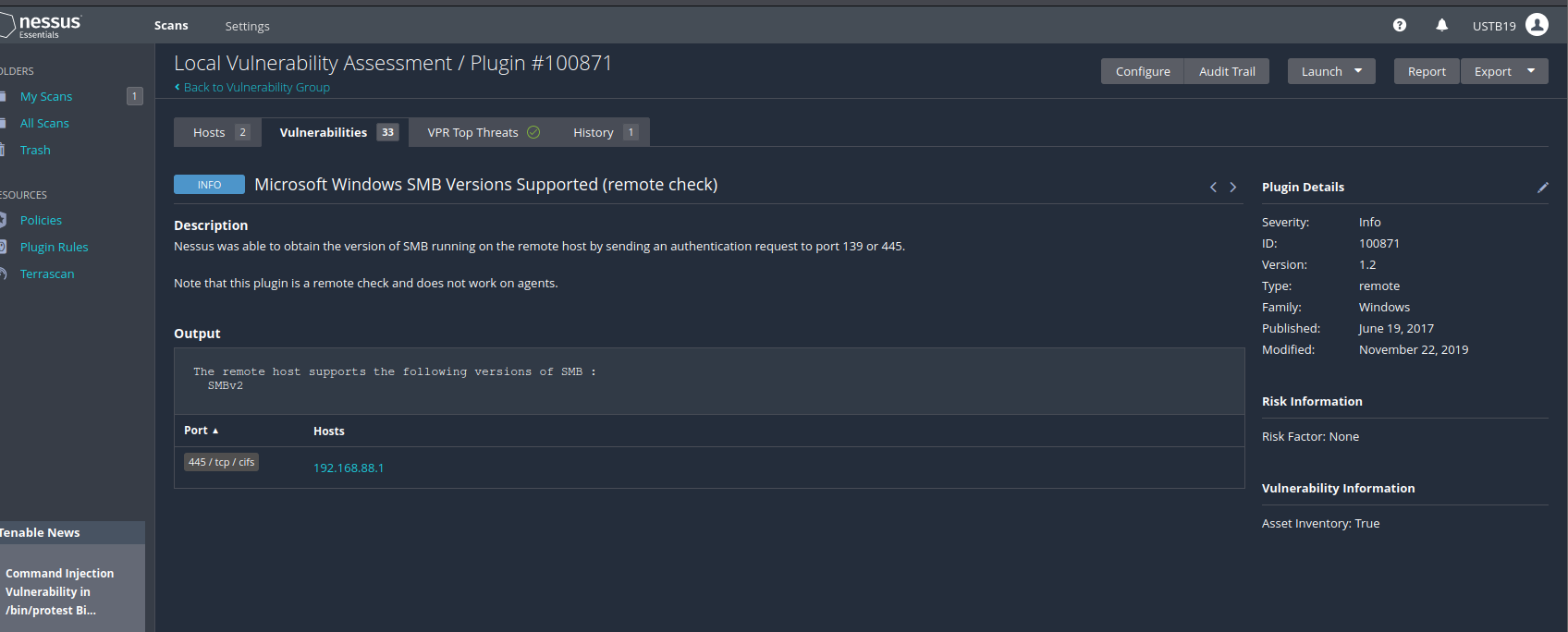
5）在该界面双击扫描任务名称，将显示扫描的详细信息，如图所示。



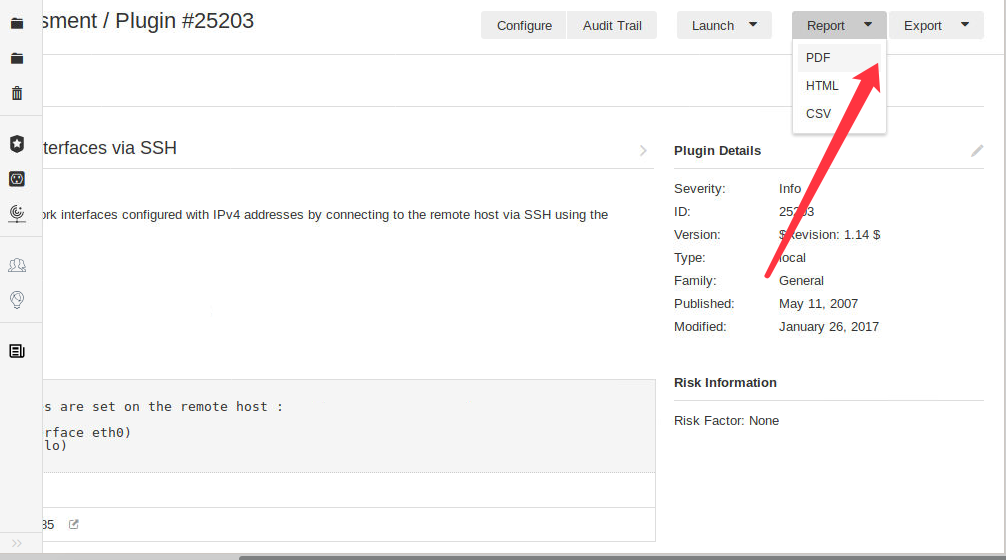
6）从该界面可以看到总共扫描了两台主机。扫描主机的漏洞情况，可以查看Vulnerability列，该列中的数字表示扫描到的信息数。右侧显示了扫描的详细信息，如扫描任务名称、状态、策略、目标主机和时间等。右下角以圆形图显示了漏洞的危险情况，分别使用不同颜色显示漏洞的严重性。本机几乎没任何漏洞，所以显示是蓝色（Info）。关于漏洞的信息使用在该界面可以单击Host列中的任何一个地址，显示该主机的详细信息，包括IP地址、操作系统类型、扫描的起始时间和结束时间等。



7）在该界面单击INFO按钮，将显示具体的漏洞信息。



8） 右上角还可以将信息导出。



**5. 扫描网络漏洞**

如果用户想要使用Nessus攻击一个大范围的漏洞，需要配置评估漏洞列表并指定获取信息的评估列表。本小节将介绍配置Nessus在目标主机寻找网络漏洞，这些漏洞指目标主机或其他网络协议。

【实例】扫描网络漏洞的具体操作步骤如下所示。

1）新建名为Internal Network Scan策略。

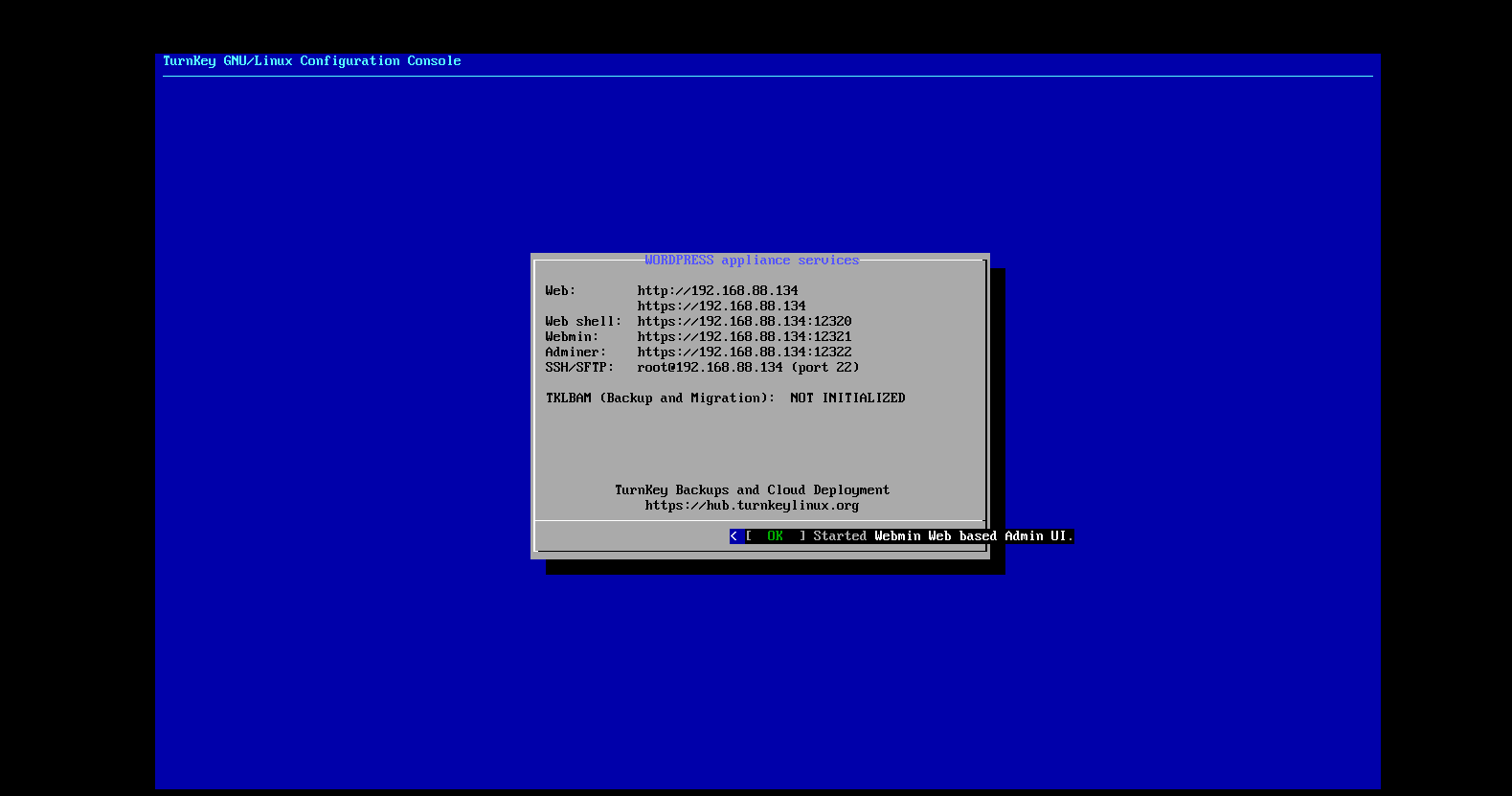
2）添加所需的插件程序，如表所示。

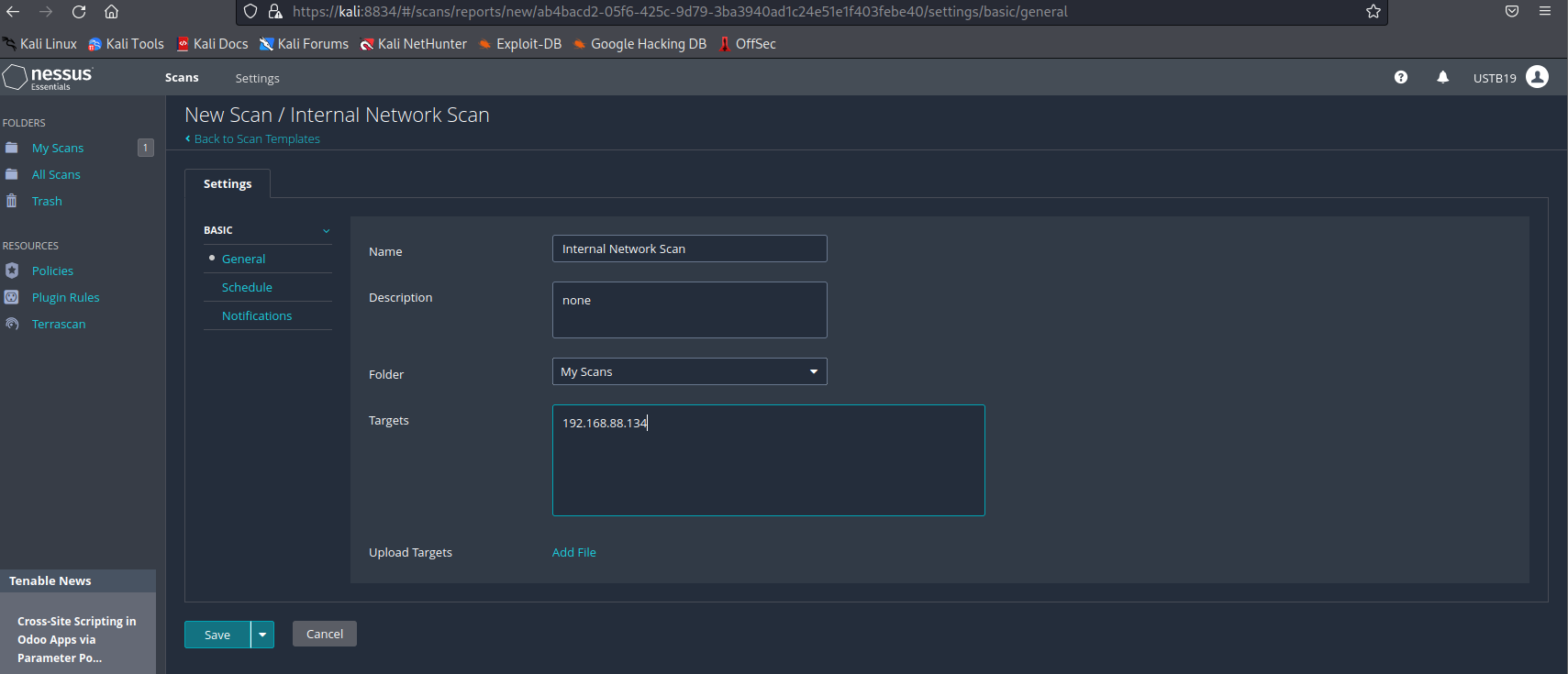
| **名称** | **描述** |
| --- | --- |
| CISCO | 扫描CISCO系统 |
| DNS 扫描 | DNS服务器 |
| Default Unix | Accounts 扫描本地默认用户账户和密码 |
| FTP | 扫描FTP服务器 |
| Firewalls | 扫描代理防火墙 |
| Gain a shell remotely | 扫描远程获取的Shell |
| Geeral | 扫描常用的服务 |
| Netware | 扫描网络操作系统 |
| Peer-To-Peer File Sharing | 扫描共享文件检测 |
| Policy Compliance | 扫描PCI DSS和SCAP信息 |
| SCADA | 扫描设置管理工具 |
| SMTP Problems | 扫描SMTP问题 |
| SNMP | 扫描SNMP相关信息 |
| Service Detection | 扫描服务侦察 |
| Settings | 扫描基本设置 |

3）选择Basic Network Scan。



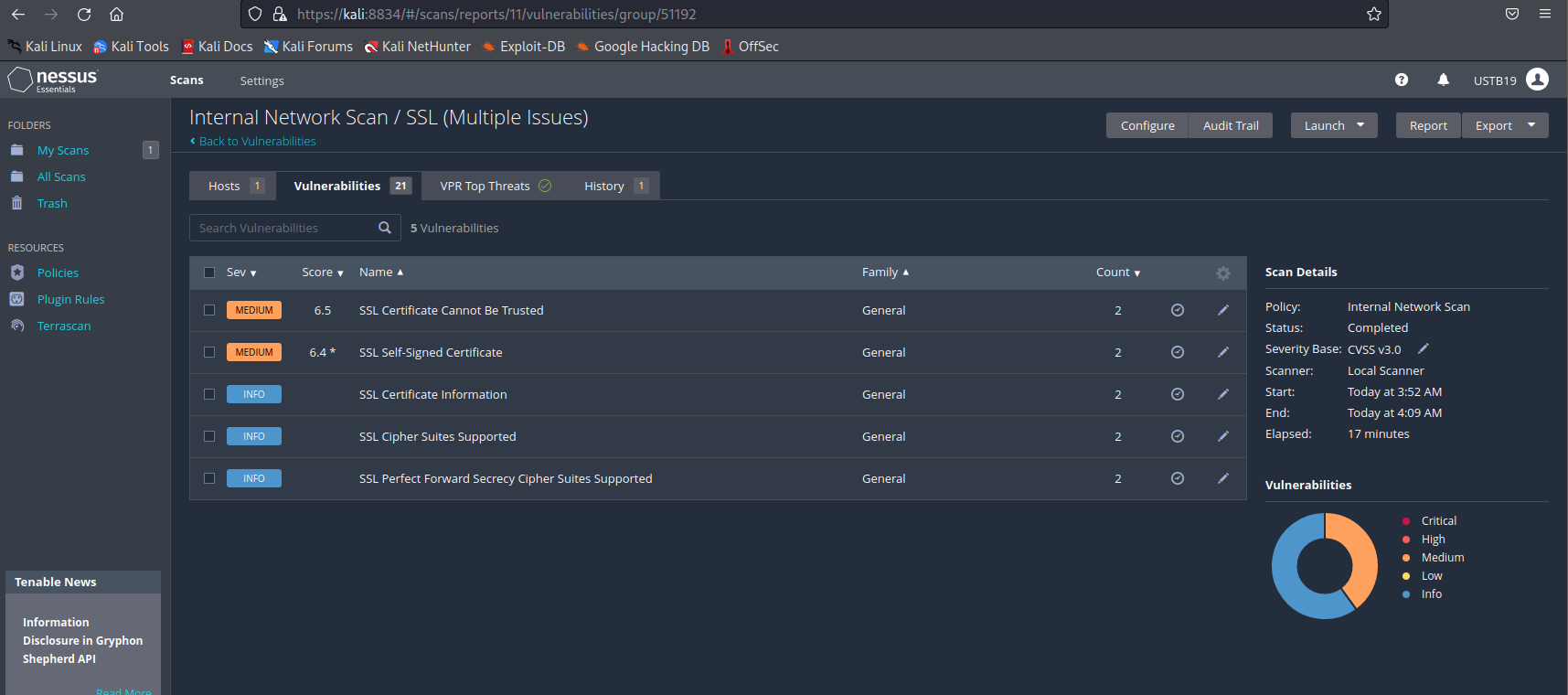
4）这里我们直接运行了我们的Scan，正在运行，扫描的是我们的wordpress主机。 192.168.122.189.(这一步学生也可以选择扫描我们当前环境另外一个虚拟机Metasploitable 2.0虚拟机，当前镜像没有保存wordpress镜像)







5）扫描结果如图所示。



6）从该界面可以看到有两个比较严重的漏洞。如果想要详细地分析该漏洞，建议将该信息使用文件的形式导出。

**6. 扫描指定Linux的系统漏洞**

本小节将介绍使用Nessus扫描指定Linux系统上的漏洞。

【实例】扫描指定Linux系统漏洞的具体操作步骤如下所示。

1）使用Metasploitable 2.0作为目标主机。用户也可以使用其他版本的Linux系统。

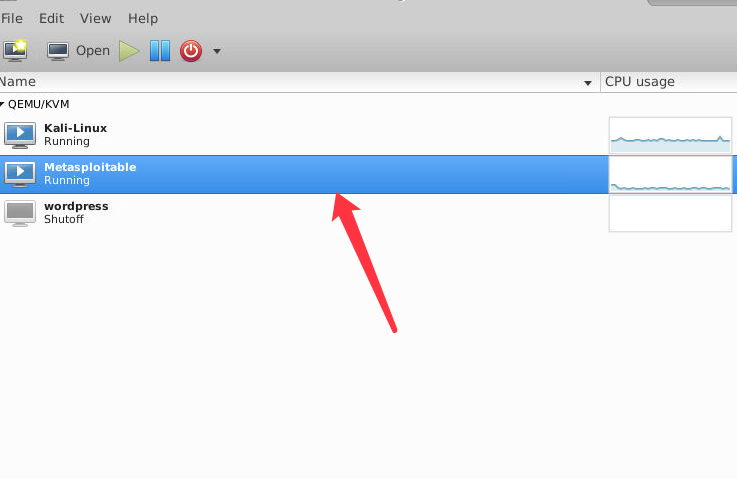
2）新建名为Linux Vulnerability Scan策略。

3）添加所需的插件程序，如表所示。

|  |  |
| --- | --- |
| Backdoors | 扫描秘密信息 |
| Brute Force Attacks | 暴力攻击 |
| CentOSo Local Security Checks | 扫描CentOS系统的本地安全漏洞 |
| DNS | 扫描DNS服务器 |
| Debian Local Security Checks | 扫描Debian系统的本地安全漏洞 |
| Default Unix Accounts | 扫描默认Unix用户账号 |
| Denial of Service | 扫描拒绝的服务 |
| FTP | 扫描FTP服务器 |
| Fedora Local Security Checks | 扫描Fedora系统的本地安全漏洞 |
| Firewalls | 扫描防火墙 |
| FreeBSD Local Security Checks | 扫描FreeBSD系统的本地安全漏洞 |
| Gain a shell remotely | 扫描远程获得的Shell |
| General | 扫描漏洞 |
| Gentoo Local Security Checks | 扫描Gentoo系统的本地安全漏洞 |
| HP-UX Local Security Checks | 扫描HP-UX系统的本地安全漏洞 |
| Mandriva Local Security Checks | 扫描Mandriva系统的本地安全漏洞 |
| Misc | 扫描复杂的漏洞 |
| Red Hat Local Security Checks | 扫描Red Hat系统的本地安全漏洞 |
| SMTP Porblems | 扫描SMTP问题 |
| SNMP | 扫描SNMP漏洞 |
| Scientific Linux Local Security Checks | 扫描Scientific Linux系统的本地安全漏洞 |
| Slackware Local Security Checks | 扫描Slackware系统的本地安全漏洞 |
| Solaris Local Security Checks | 扫描Solaris系统的本地安全漏洞 |
| SuSE Local Security Checks | 扫描SuSE系统的本地安全漏洞 |
| Ubuntu Local Security Checks | 扫描Ubuntu系统的本地安全漏洞 |
| Web Servers | 扫描Web服务器 |

4）新建名为Linux Vulnerability Scan扫描任务。

这里我们事先打开我们准备好的Ubuntu虚拟机。

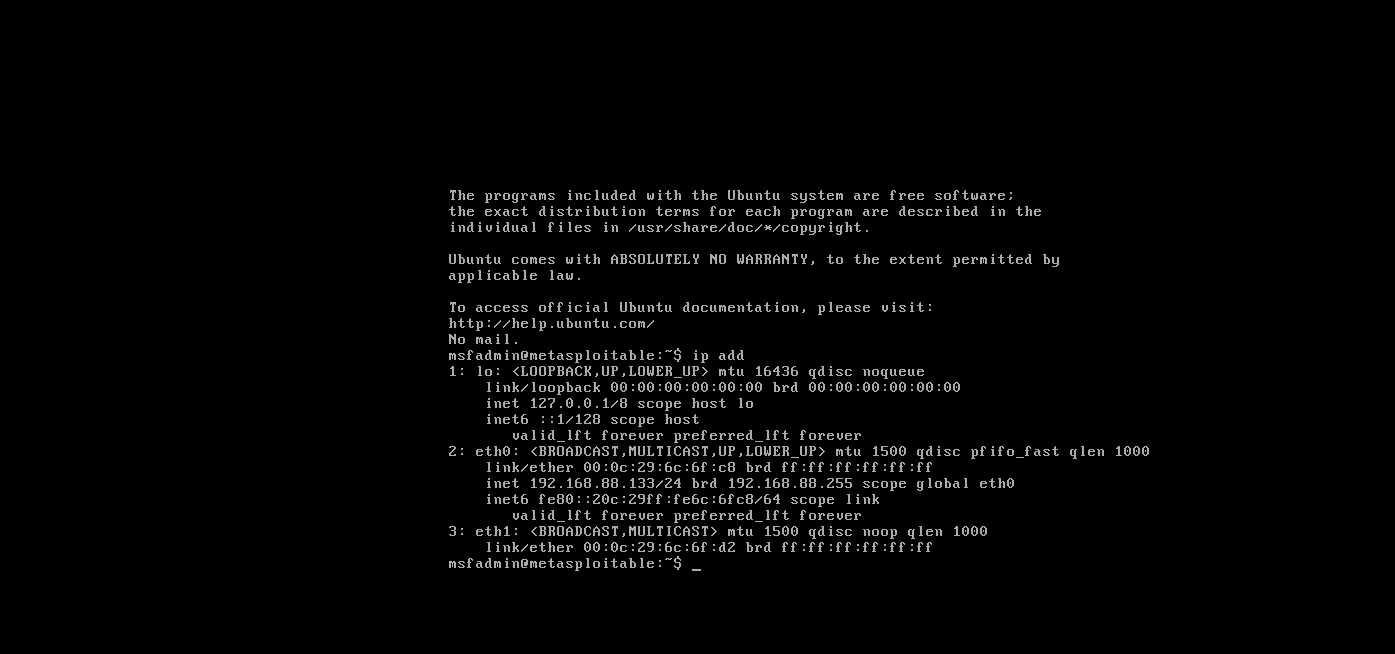


metasplotable的账号和密码都是msfadmin

在metasplotable输入ip addr查看IP地址。

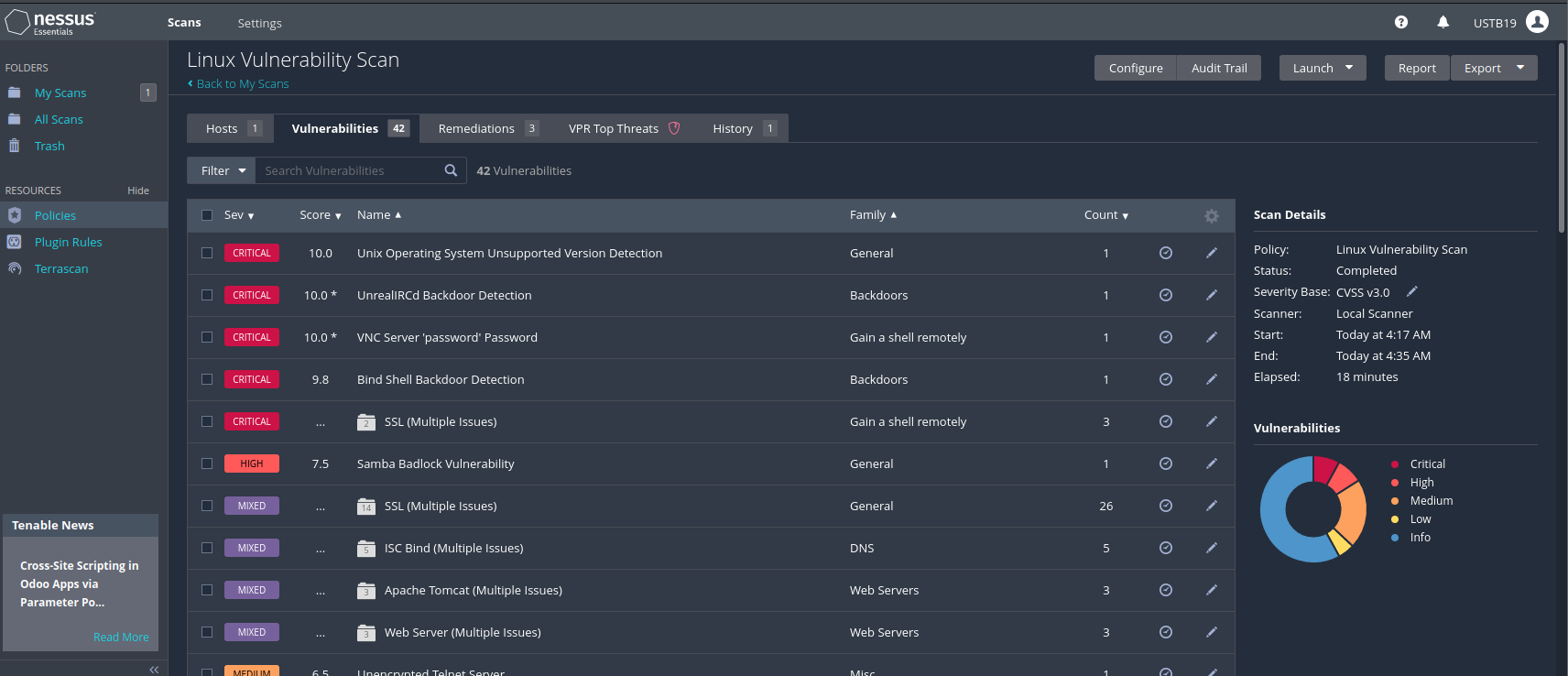
您还可以使用以下命令显示内部 IP 地址：

hostname -I



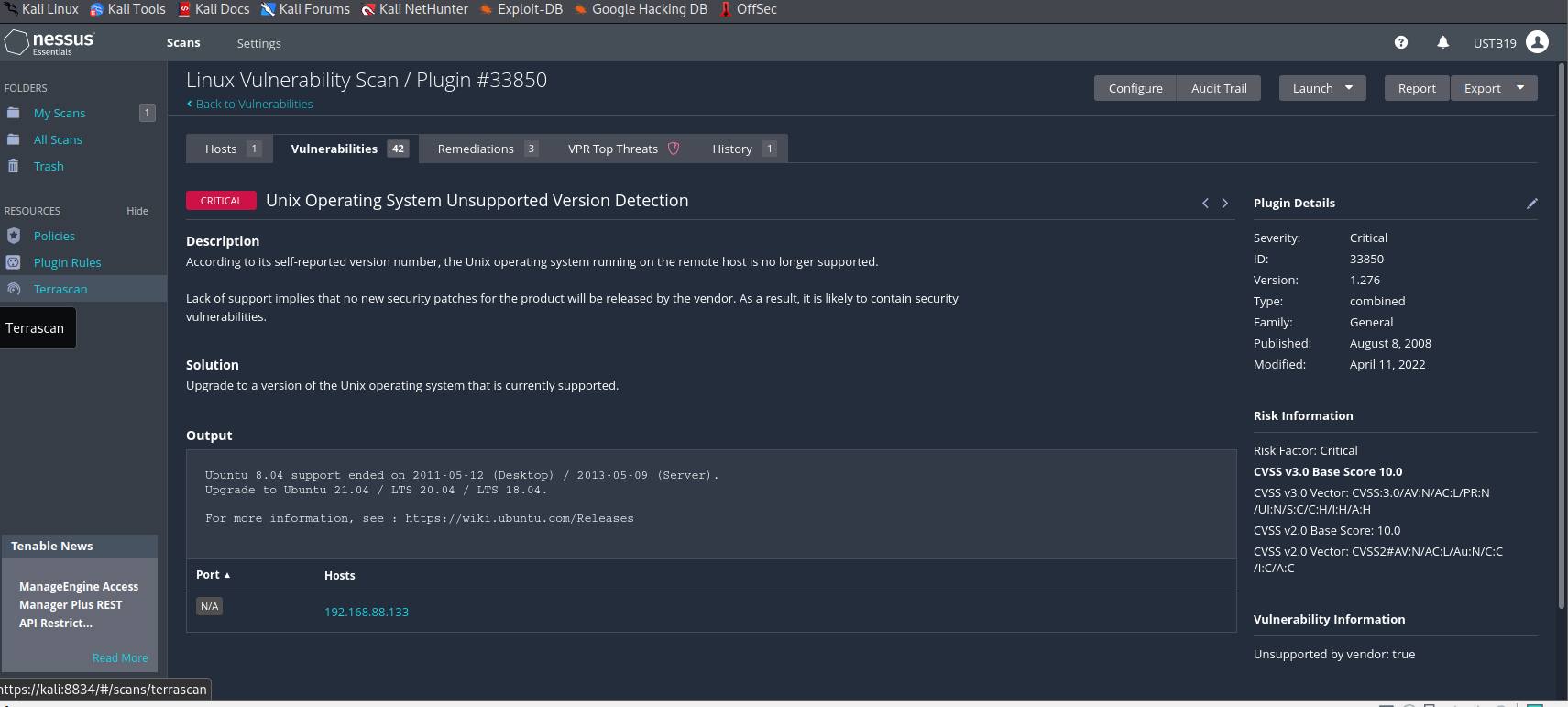
5）扫描漏洞，扫描结果如图所示。

查看列表页。



可以看到 Metasploitable 2.0的严重的漏洞有很多。

查看错误详情，给出了漏洞解决方案



OpenVAS（开放式漏洞评估系统）是一个客户端/服务器架构，它常用来评估目标主机上的漏洞。OpenVAS是Nessus项目的一个分支，它提供的产品是完全地免费。本节将介绍配置及启动OpenVAS。

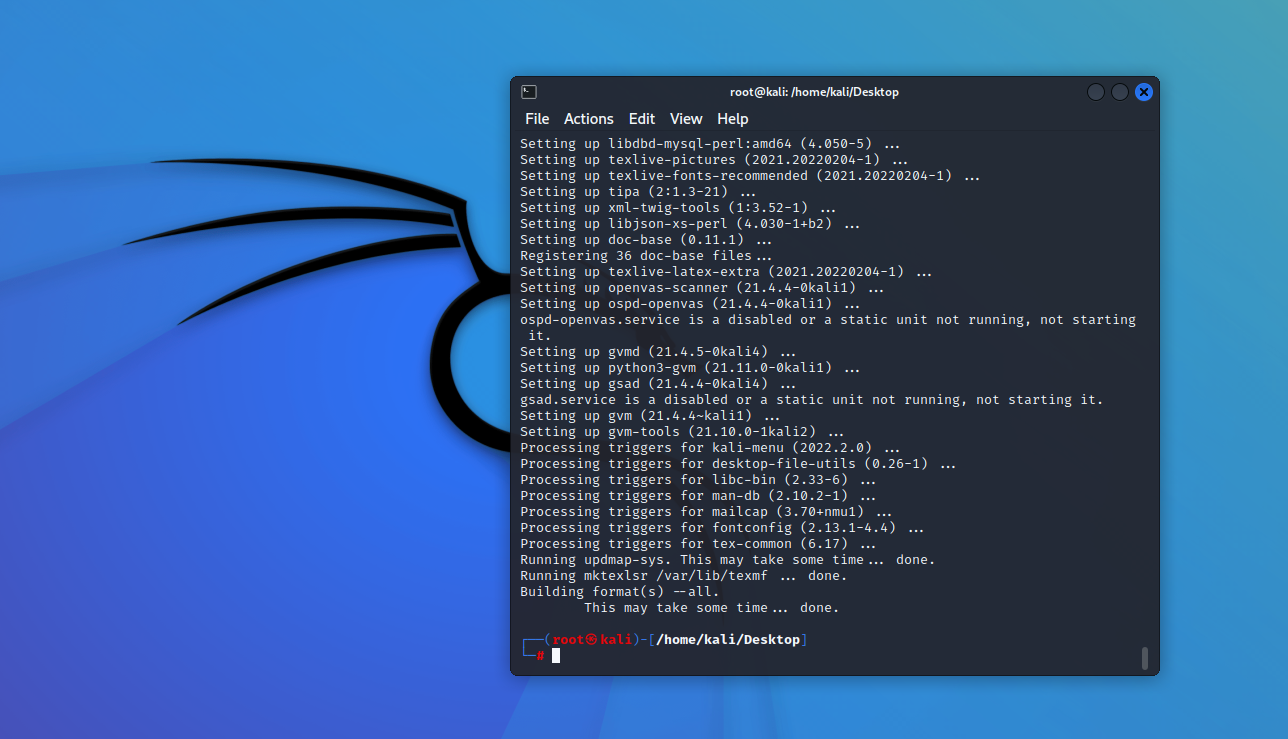
**0. 安装OpenVAS**

注意：从Kali Rolling（2020.2a）开始，OpenVAS现在称为GVM。因此，命令也将有所不同。（Kali将OpenVAS 9更新为GVM 11）

sudo apt install openvas -y

or

sudo apt install gvm -y



1. 启动终端，然后运行OpenVAS的安装程序

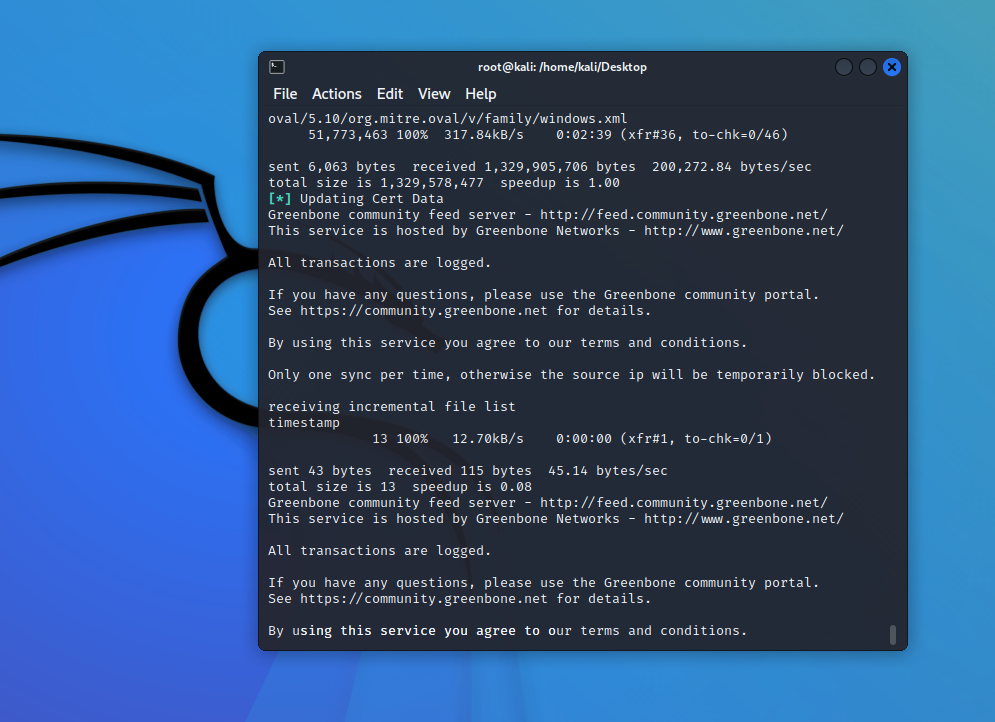
sudo openvas-setup

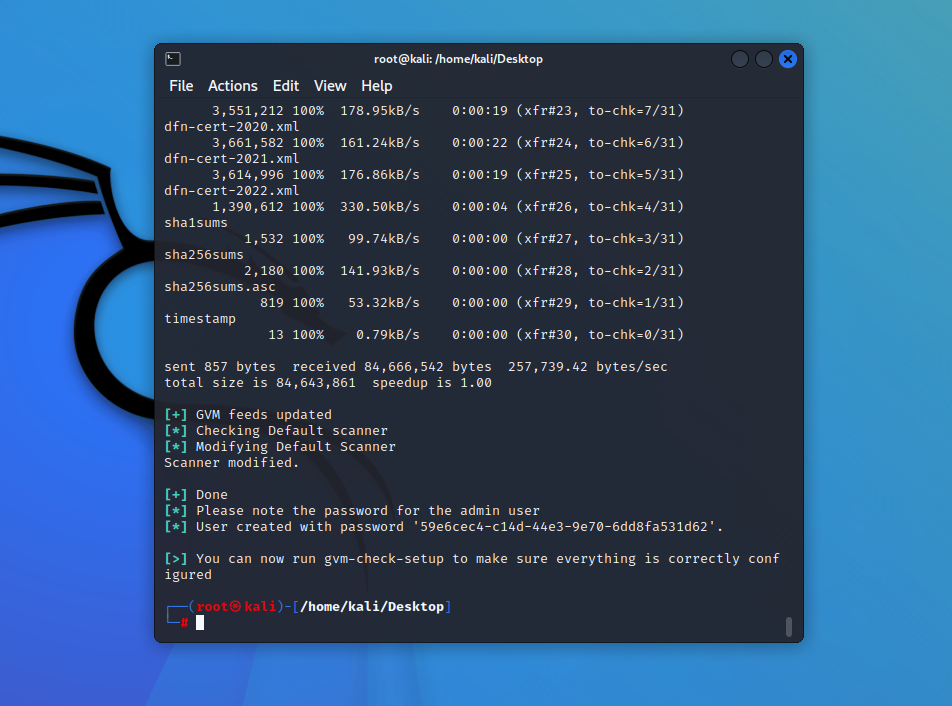
or

sudo gvm-setup

等待下载和更新完成，需要一段时间









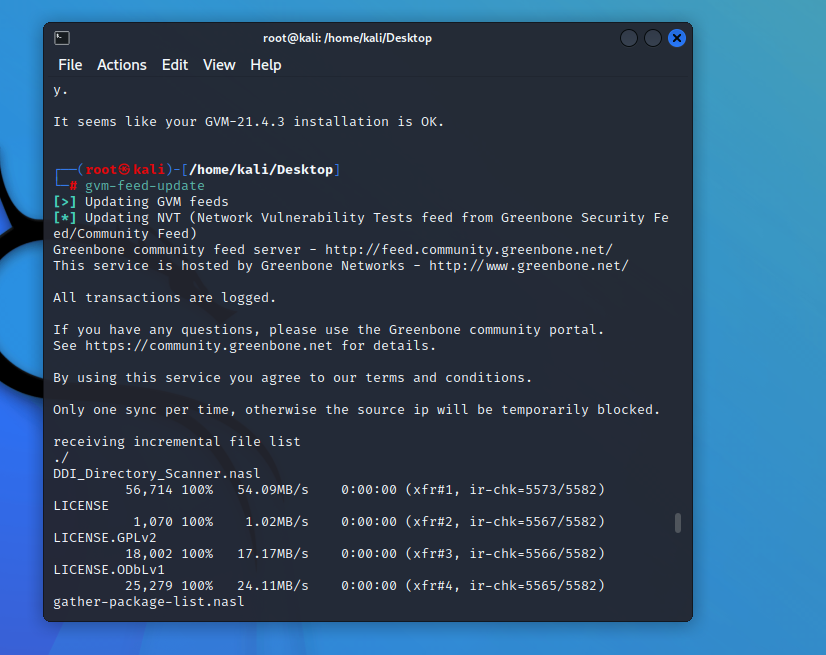


1. 完成后，将显示管理员登录用户名和管理员登录密码，记下它们，每次尝试登录OpenVAS时我们都将需要它们
2. OpenVAS的更新feed（只有新更新才需要），在初始化时，此步骤已经完成一次。

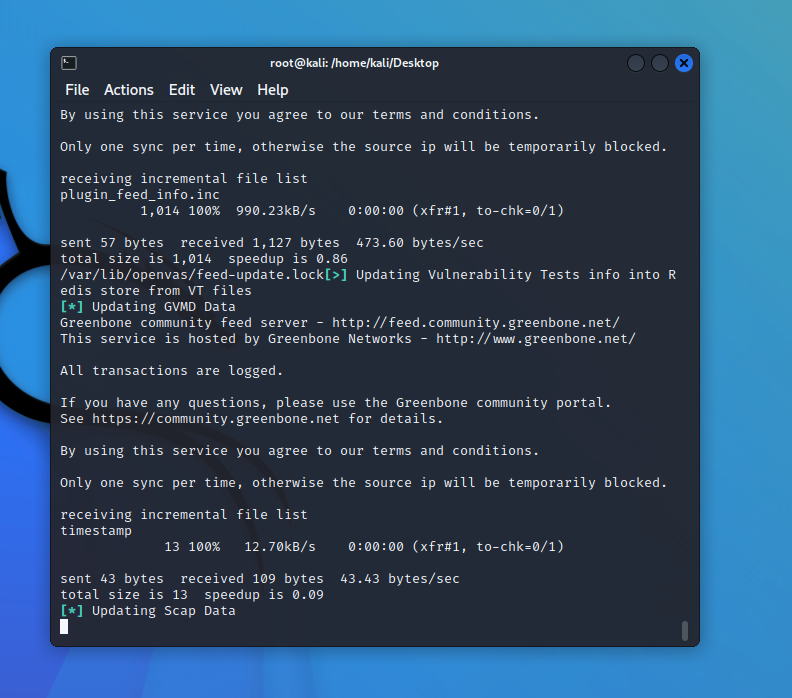
sudo openvas-feed-update

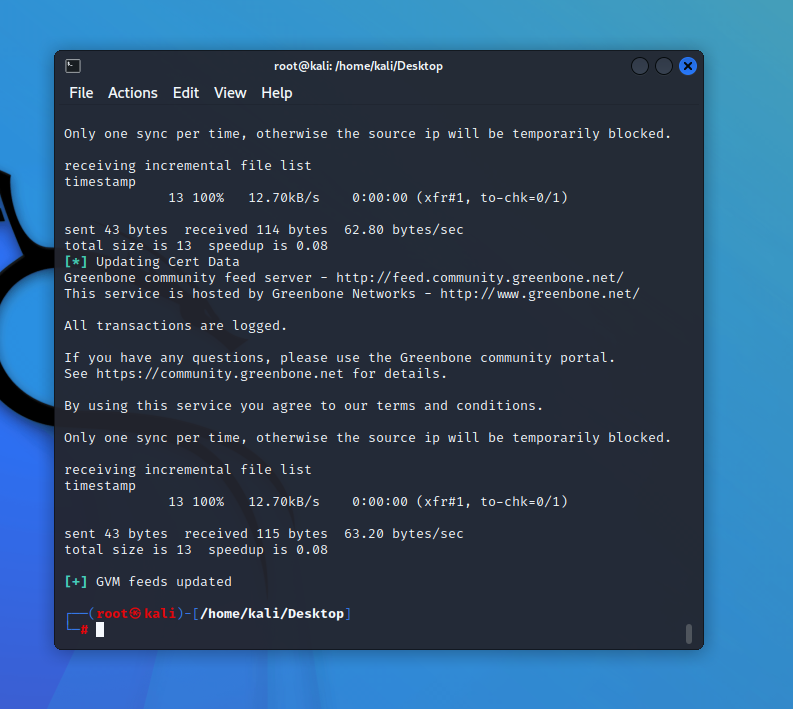
or

sudo gvm-feed-update









如果失败（您可能会遇到此错误）：

rsync: failed to connect to feed.openvas.org (xx.xx.xx.xx): Connection refused (111)

rsync: failed to connect to feed.openvas.org (xx:xx:xx:xx::xx): Connection timed out (110)

rsync error: error in socket IO (code 10) at clientserver.c(127) [Receiver=3.1.3]

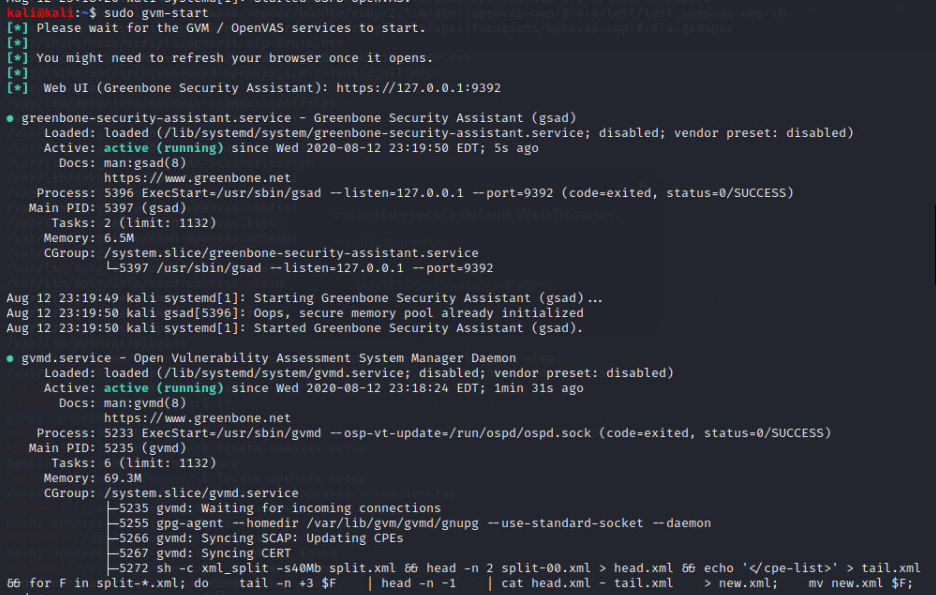
只需使用相同的命令再试一次，它应该可以通过。

1. 启动OpenVAS

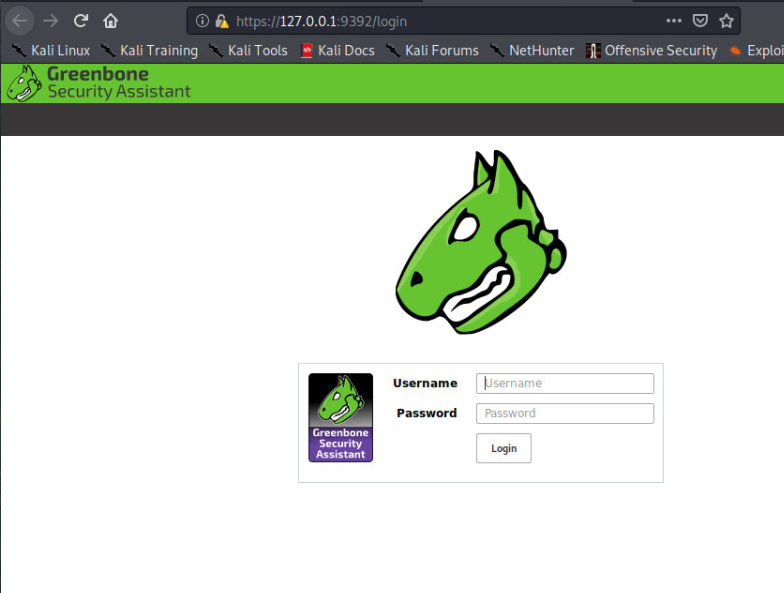
sudo openvas-start

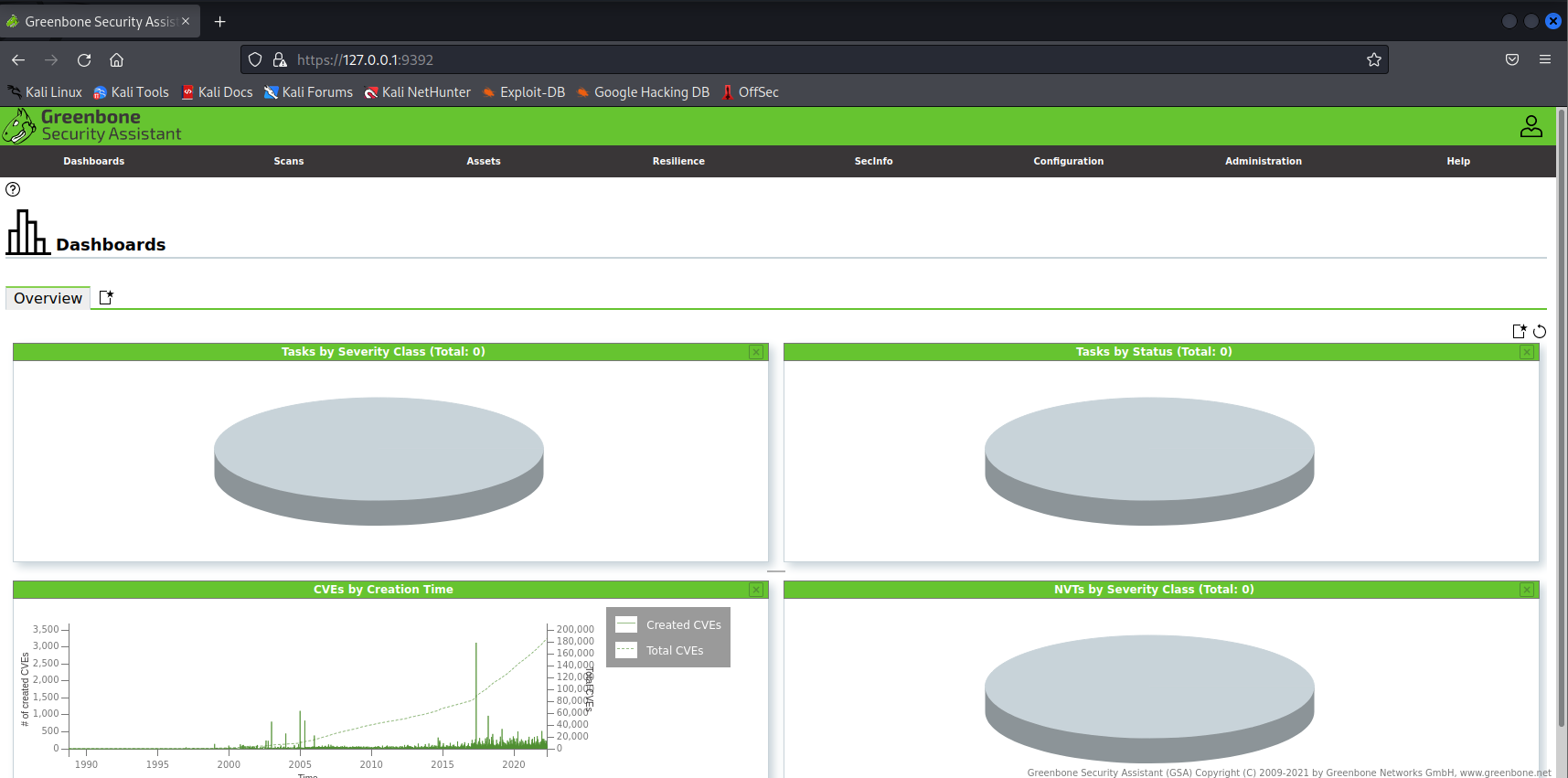
or

sudo gvm-start



通过浏览器访问 https://127.0.0.1:9392 进入登陆页面





## 实验数据

见上图

## 实验数据处理

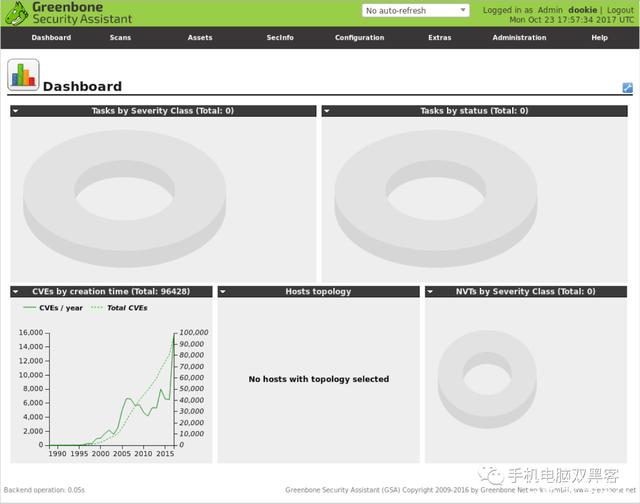
无

## 实验结果与分析

本次实验学习了漏洞扫描工具以及靶机Metasploit，深刻强化了计算机网络的知识。

**2020年10种最佳漏洞扫描工具**

**1.OpenVAS漏洞扫描工具**



OpenVAS漏洞扫描器是一种漏洞分析工具，由于其全面的特性，IT部门可以使用它来扫描服务器和网络设备。

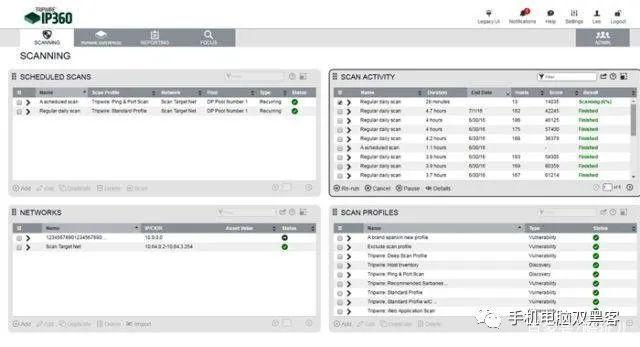
这些扫描器将通过扫描现有设施中的开放端口、错误配置和漏洞来查找IP地址并检查任何开放服务。

扫描完成后，将自动生成报告并以电子邮件形式发送，以供进一步研究和更正。

OpenVAS也可以从外部服务器进行操作，从黑客的角度出发，从而确定暴露的端口或服务并及时进行处理。

如果您已经拥有一个内部事件响应或检测系统，则OpenVAS将帮助您使用网络渗透测试工具和整个警报来改进网络监控。

**2.Tripwire IP360**

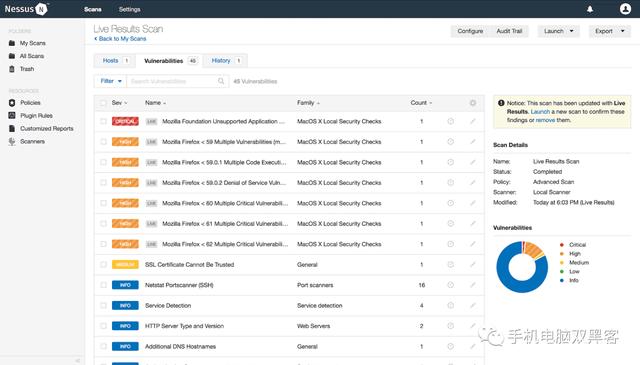


Tripwire IP360是市场上领先的漏洞管理解决方案之一，它使用户能够识别其网络上的所有内容，包括内部部署，云和容器资产。

Tripwire将允许IT部门使用代理访问他们的资产，并减少代理扫描。

它还与漏洞管理和风险管理集成在一起，使IT管理员和安全专业人员可以对安全管理采取更全面的方法。

**3.Nessus漏洞扫描工具**



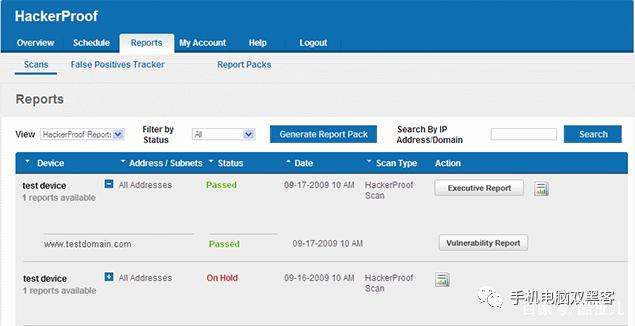
Tenable的Nessus Professional是一款面向安全专业人士的工具，负责修补程序、软件问题、恶意软件和广告软件删除工具，以及各种操作系统和应用程序的错误配置。

Nessus提供了一个主动的安全程序，在黑客利用漏洞入侵网络之前及时识别漏洞，同时还处理远程代码执行漏洞。

它关心大多数网络设备，包括虚拟，物理和云基础架构。

Tenable还被认为是Gartner Peer Insights在2020年3月之前进行危险性评估的首选方案。

**4，Comodo HackerProof**

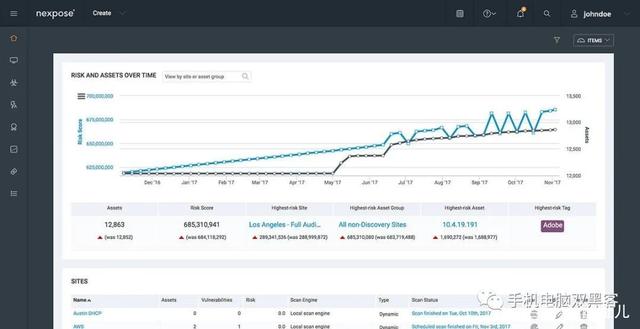


Comodo HackerProof是另一款优秀的漏洞扫描程序，它具有强大的功能，可让IT部门每天扫描其漏洞。

PCI扫描选项，防止驱动攻击和站点检查器技术，有助于下一代网站扫描。

除了这些特权，Comodo还提供了一个指标，让用户在与其互动时感到安全。

**5，Nexpose community**



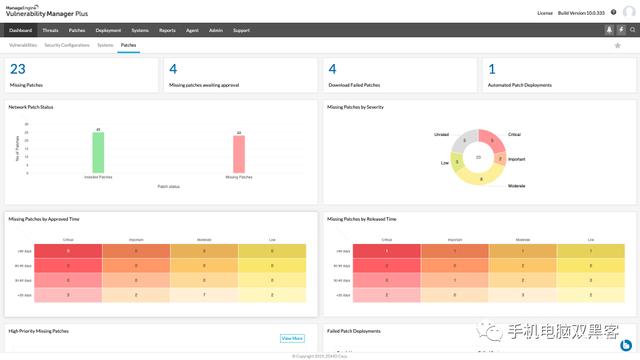
Nexpose community是由Rapid7开发的漏洞扫描工具，它是涵盖大多数网络检查的开源解决方案。

这个解决方案的多功能性是IT管理员的一个优势，它可以被整合到一个Metaspoit框架中，能够在任何新设备访问网络时检测和扫描设备。

它还可以监控真实世界中的漏洞暴露，最重要的是，它可以进行相应的修复。

此外，漏洞扫描程序还可以对威胁进行风险评分，范围在1-1000之间，从而为安全专家在漏洞被利用之前修复漏洞提供了便利。Nexpose目前可免费试用一年。

**6，Vulnerability Manager Plus**



Vulnerability Manager Plus是由ManageEngine开发的针对目前市场的新解决方案。

它提供基于攻击者的分析，使网络管理员可以从黑客的角度检查现有漏洞。

除此之外，还可以进行自动扫描、影响评估、软件风险评估、安全性配置错误、修补程序、0 day漏洞缓解扫描程序， Web服务器渗透测试和强化是Vulnerability Manager Plus的其他亮点。

**7，Nikto**

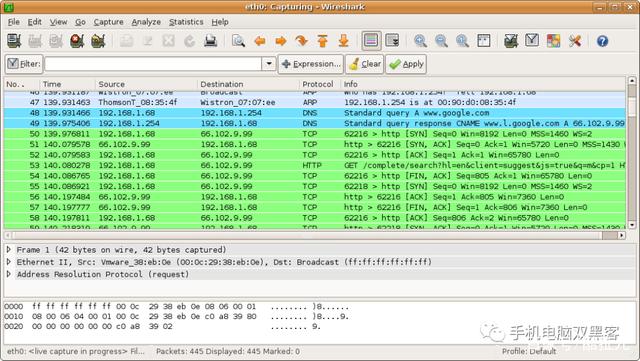


Nikto是另一个免费的在线漏洞扫描工具，如Nexpose community。

Nikto可帮助您了解服务器功能，检查其版本，在网络服务器上进行测试以识别威胁和恶意软件的存在，并扫描不同的协议，如https、httpd、HTTP等。

还有助于在短时间内扫描服务器的多个端口。Nikto因其效率和服务器强化功能而受到青睐。

**8，Wireshark**



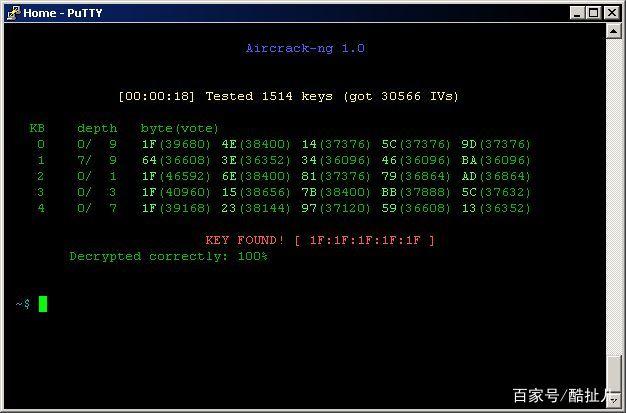
Wireshark被认为是市场上功能强大的网络协议分析器之一。

许多政府机构，企业，医疗保健和其他行业都使用它来分析非常敏感的网络。一旦Wireshark识别出威胁，便将其脱机以进行检查。

Wireshark可在Linux，macOS和Windows设备上成功运行。

Wireshark的其他亮点还包括标准的三窗格数据包浏览器，可以使用GUI浏览网络数据，强大的显示过滤器，VoIP分析，对Kerberos，WEP，SSL / TLS等协议的解密支持。

**9，Aircrack-ng**

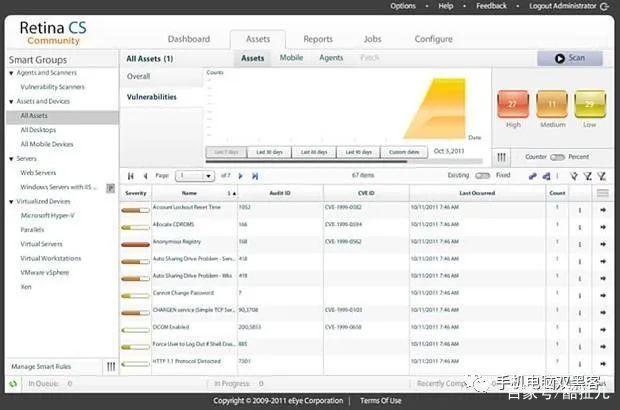


Aircrack-ng将帮助IT部门处理WiFi网络安全问题。

它被用于网络审计，并提供WiFi安全和控制，还可以作为具有驱动程序和显卡，重放攻击的最佳wifi黑客应用程序之一。

通过捕获数据包来处理丢失的密钥。支持的操作系统包括NetBSD，Windows，OS X，Linux和Solaris。

**10.Retina**



Retina漏洞扫描工具是基于Web的开源软件，从中心位置负责漏洞管理。

它的功能包括修补、合规性、配置和报告。

负责数据库、工作站、服务器分析和web应用程序，完全支持VCenter集成和应用程序扫描虚拟环境。

它负责多个平台，提供完整的跨平台漏洞评估和安全性。

资料来源：[用于渗透测试的10种漏洞扫描工具 (baidu.com)](https://baijiahao.baidu.com/s?id=1677428914826977630&wfr=spider&for=pc)