**Tenable Nessus**

**功能操作手册**

版本： 1.0

日期： 2017-12-27

客户名称:

目录

[一、概述 3](#_Toc502153893)

[二、环境需求 3](#_Toc502153894)

[2.1 硬件需求 3](#_Toc502153895)

[2.2 操作系统需求 3](#_Toc502153896)

[2.3 防火墙需求 3](#_Toc502153897)

[三、软件安装 4](#_Toc502153898)

[3.1 安装暴力猜解组件（可选） 4](#_Toc502153899)

[3.2 安装Nessus组件 4](#_Toc502153900)

[3.3 Nessus组件的初始化调试 4](#_Toc502153901)

[四、漏洞扫描测试项 7](#_Toc502153902)

[4.1 针对Windows/Linux主机进行网络扫描测试 7](#_Toc502153903)

[4.2针对Linux主机进行“弱密码”或“暴力猜解”测试 11](#_Toc502153904)

[4.3 针对Web网站进行Web App漏洞扫描 17](#_Toc502153905)

[4.4 漏洞风险等级自定义测试 19](#_Toc502153906)

[4.5 漏洞信息关联性测试 22](#_Toc502153907)

[五、扫描任务计划与时间管理测试项 23](#_Toc502153908)

[5.1 设置任务计划 23](#_Toc502153909)

[六、配置合规审计测试项 26](#_Toc502153910)

# 一、概述

Tenable Nessus

Nessus为业界部署最广泛的漏洞扫描、系统配置与合规性验证产品。全球已超过2万4千家企业使用，在信息安全和法规遵循产品中，获得众多专业人士认可。Nessus 可以进行高速扫描、系统配置稽核、资产发现、恶意软件发现、敏感性资料探索、补丁程序管理整合和漏洞分析。Tenable 的漏洞研究团队准确的依据环境需求，提供不断更新的数据库(plugins)，目前已支持超过 90000多 个漏洞和系统配置检查，涵盖35000条CVE ID。Nessus 能扩展并适用于最大型的企业 环 境，而且部署十分容易。

# 二、环境需求

## 2.1 硬件需求

|  |  |  |
| --- | --- | --- |
| Nessus | CPU: 4 核  内存: 4 GB及以上  磁盘空间: 30 GB及以上 | 支持在虚拟化平台部署。 |

## 2.2 操作系统需求

CentOS/Redhat操作系统注意项：

* Tenable Nessus只占用/opt目录空间，请划分足够的空间至/opt目录或根目录。
* 需关闭selinux，编辑/etc/selinux/config ,设置为SELINUX=disabled

## 2.3 防火墙需求

需确保Nessus向被检查对象（主机系统及网络设备)有完全访问权限，无防火墙限制。

确保Nessus有向外网访问权限，用于激活license和更新plugin。

# 三、软件安装

## 3.1 安装暴力猜解组件（可选）

Nessus支持暴力猜解扫描，暴力猜解扫描时调用的是第三方hydra组件，如果需要测试暴力猜解扫描(章节4.2)，请先按如下步骤安装hydra.

安装命令: yum install epel-release -y && yum install -y hydra

安装完后，通过执行这些空命令，验证hydra是否安装成功。成功的结束语含finished at字段。

/usr/bin/hydra -l pp -p pp smb://127.0.0.1

/usr/bin/hydra -l pp -p pp ssh://127.0.0.1

## 3.2 安装Nessus组件

使用scp将Nessus的RPM安装包copy到Centos的／root目录

安装Nessus RPM包

rpm -Uvh Nessus-6.5.6-es6.x86\_64.rpm

当Nessus安装完成后按照提示输入/sbin/service nessusd start ，启动Nessus服务

[root@Nessus ~]# rpm -Uvh Nessus-6.5.6-es6.x86\_64.rpm

warning: Nessus-6.5.6-es6.x86\_64.rpm: Header V4 RSA/SHA1 Signature, key ID 1c0c4a5d: NOKEY

Preparing... ########################################### [100%]

1:Nessus ########################################### [100%]

Unpacking Nessus Core Components...

nessusd (Nessus) 6.5.6 [build M20049] for Linux

Processing the Nessus plugins...

[##################################################]

All plugins loaded (1sec)

- You can start Nessus by typing /sbin/service nessusd start

- Then go to https://SC:8834/ to configure your scanner

[root@ Nessus ~]# /sbin/service nessusd start

Starting Nessus services: [ OK ]

[root@ Nessus ~]#

## 3.3 Nessus组件的初始化调试

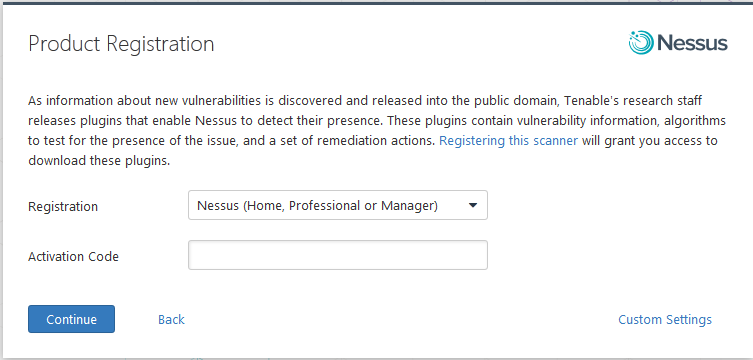
1.打开浏览器新窗口输入 <https://nessus-server-ip:8834> ,进入Nessus的管理界面，选continue



设定管理员账户和口令。 Username：admin Password：Admin@tenable123 密码可按客户要求设定成其他。



继续后会出现注册页面，在Activation Code这一栏输入激活码。



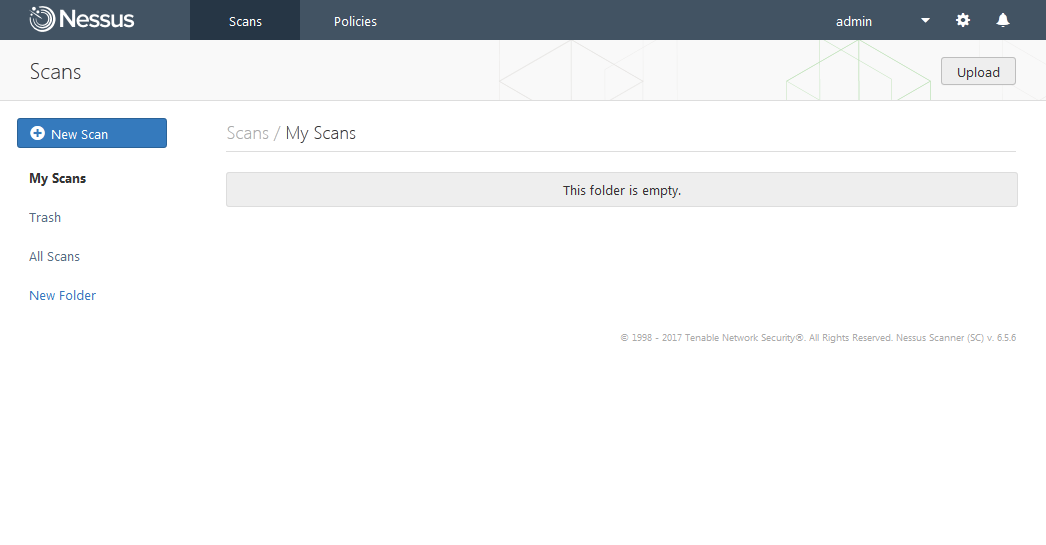
填入激活码后开始激活Nessus并自动下载Plugin。

Tips:如果页面下载plugin失败错误，请尝试在系统命令行使用如下命令

/opt/nessus/sbin/nessuscli update --plugins-only

按命令下载后会自动加载plugin，会花一些时间，请耐心等待。

加载完plugin后Nessus的登录页面出现了登录提示框，输入之间设置的账号密码，即可进入Nessus平台操作页面。



# 四、漏洞扫描测试项

## 4.1 针对Windows/Linux主机进行网络扫描测试

|  |  |
| --- | --- |
| 测试项目 | 针对Windows / Linux主机进行网络扫描测试 |
| 测试说明 | 授权扫描的检测会带入具有权限的系统帐号来进行检测，相对于一般的网络扫描更能精准发现到漏洞——授权扫描将进行全面深层的检测，并以系统注册表、已安装的软件、档案版本等更准确的方法去寻找已有风险，授权扫描亦可检查系统合规情况，以及有没有被病毒感染等情况，有助企业全面得知内部信息安全问题。 |
| 测试步骤 | 1. 在Nessus中新增扫描任务——登入Nessus管理界面后，在『Scans』下，请点选『New Scan』新增扫描任务。      1. Nessus上已经内建多项策略范本，例如主机探索、网页漏洞测试、Windows恶意程序扫描、法规合规性检测、以及特定重大漏洞检测等等可套用。同时也提供『Advanced Scan』让管理者自行定义策略。本次测试选择『Advanced Scan』，命名为“网络扫描任务”。        1. 在『Targets』里，通过写入IP或DNS方式设定受测主机。      1. 手动开始扫描任务——说明：到目前步骤为止，尚未加入登陆授权，所以此处的扫描结果均以“网络扫描”方式获得。     网络扫描结果演示如下：     1. 在扫描任务中新增主机授权——按照步骤1~3操作，将扫描任务命名为“登陆扫描”；      1. 在『Credentical』里，输入授权扫描需使用的帐号密码，在此新增一个Windows或Linux的授权项目，类型分别选择“Windows”或“SSH”。这里测试的是一台linux主机，所以选择SSH，并输入账号密码。然后保存扫描任务。      1. 然后手动开始扫描登录任务。     登录扫描任务结果演示： |
| 成功标准 | 漏洞扫描能成功完成，并且对比步骤7与步骤4的扫描结果，后者得到相对更多的漏洞。 |
| 测试结果 |  |

## 4.2针对Linux主机进行“弱密码”或“暴力猜解”测试

|  |  |
| --- | --- |
| 测试项目 | 针对 Linux主机OS及相关服务程序（如基于linux的mysql、apache等）进行弱密码、暴力猜解（Brute Force）扫描测试 |
| 测试说明 | 通过基于网络端口的主动式扫描，发现主机弱密码（弱密码定义：默认密码、简单密码、空口令等统称为“弱密码”），或利用自定义的密码字典实施暴力猜解。  \*注意：在测试开始前请确保已关闭了密码错误锁定策略。 |
| 测试步骤 | 1. 准备一台Linux主机，也可视情况配置需要测试的服务程序。 2. 2a、弱密码测试项准备——为主机OS或服务程序的管理员配置为默认密码，如 root/root 、root/mysql、admin/admin等，组合规则将根据不同的应用而不同。   2b、暴力猜解测试项准备—— 为主机OS或服务程序管理员账号修改成相对复杂的密码，并将其正确的username、password分别记录到两个txt文本文件中；同时在相关文件内，掺入若干数量的无效用户名或密码。   1. 在Nessus中新增扫描任务——登入Nessus管理界面后，在『Scans』下，请点选『New Scan』新增扫描任务。本项测试选择『Advanced Scan』，命名为“弱密码扫描任务”。      1. 在『Advanced』-->『General Setting』 选项中，关闭“Enable safe Check”选项；在『Assessment』-->『Accuracy』选项中，开启“Perform thorough tests”选项。        1. 在『Brute Force』-->『General Setting』选项中，关闭“Only use credentials provided by the user”选项      1. 保存后启动扫描任务     扫描结果演示：       1. 创建暴力猜解扫描任务   其它步骤同1~5，暴力猜解还需要在『Hydra』选项中，开启“Always enable Hydra”选项，并分别上传用户名、密码文件(txt格式)，至“Logins file”与“Passwords file”。    用户名/密码字典演示如下    注意：密码字典库最后一行按下回车，保持为一个空行，如上图。  如果想加快扫描速度，可以使扫描任务只开启ssh的plugin。在Plugins栏里，先Disable ALL所有plugin，然后再Brute force attacks里只开启hydra:SSH2     1. 保存扫描任务后，开始执行扫描。(被扫描主机的root密码已经被我改为Admin@tenable123了)。     暴力猜解扫描任务结果演示如下： |
| 成功标准 | 漏洞扫描能成功完成，并分别在不同扫描任务中，检测出弱密码或密码字典中的密码。 |
| 测试结果 |  |

## 4.3 针对Web网站进行Web App漏洞扫描

|  |  |
| --- | --- |
| 测试项目 | 针对Web网站进行Web App漏洞扫描测试 |
| 测试说明 | 通过网络远程扫描方式检查Web网站漏洞，用以发现由于Web代码编译不当或固件版本原因，而潜在的各类注入攻击、各类跨站攻击、各类劫持攻击…等等相关漏洞或风险点。 |
| 测试步骤 | 1. 在Nessus中新增扫描任务——登入Nessus管理界面后，在『Scans』下， 请点选『New Scan』新增扫描任务。 2. 本项测试选择『Web App Test』策略模板，命名为“Web扫描任务”。        1. 保存后手动开始扫描任务     说明：受制于网络延迟、Web服务器性能、代码爬虫的起始路径、页面层级数量等等多方面因素，Web App漏洞扫描参数的设定会具有多样性，扫描过程与结果也会因此而不同。视具体测试情况，需要时可以选用『Advanced Scan』模板，以利用更多可调参数进行相对更具针对性的Web app漏扫测试。 |
| 成功标准 | 漏洞扫描能成功完成，并检测出相应Web App漏洞。 |
| 测试结果 |  |

## 4.4 漏洞风险等级自定义测试

|  |  |
| --- | --- |
| 测试项目 | 漏洞风险等级自定义测试 |
| 测试说明 | 出于业务需求或某种原因，组织有时需要针对特定主机+特定漏洞风险等级做出自定义修改，甚至是采取临时性忽略或永久性忽略的措施。 |
| 测试步骤 | 1. 手动开始一项扫描任务，目标至少包含2台主机，并检查扫描结果。 2. 选择其中一项漏洞（漏洞1），点击漏洞右侧的编辑符号        1. 可以直接修改漏洞风险等级，或者直接将该漏洞隐藏掉。隐藏就代表接受该漏洞风险，如果同时勾选“Apply this rule to all future scans”，将来的扫描任务这台主机不会再出现此漏洞。     Expire默认值为空，代表本规则永久有效，可以手动调节Expire至指定日期。     1. 隐藏后可以立即看到效果，plugin id为95332的Python漏洞已经不存在了。 |
| 成功标准 | 漏洞能被“可接受”，也能修改风险等级。 |
| 测试结果 |  |

## 4.5 漏洞信息关联性测试

|  |  |
| --- | --- |
| 测试项目 | 针对单个主机漏洞信息在不同安全组织、制造商的信息关联性测试 |
| 测试说明 | 目前漏洞普遍存在多个组织同时收入其编号的情况，为避免重复记录及报告，厂商的漏洞描述必须包括不同漏洞组织的信息关联性信息 |
| 测试步骤 | 1. 检查任意扫描结果中的漏洞信息。 |
| 成功标准 | 在检测出的同一项漏洞插件内（Plugin），显示多个组织的编号，如MS 、RHEL、CVE、RHSA |
| 测试结果 | 得到类似以上信息 |

# 五、扫描任务计划与时间管理测试项

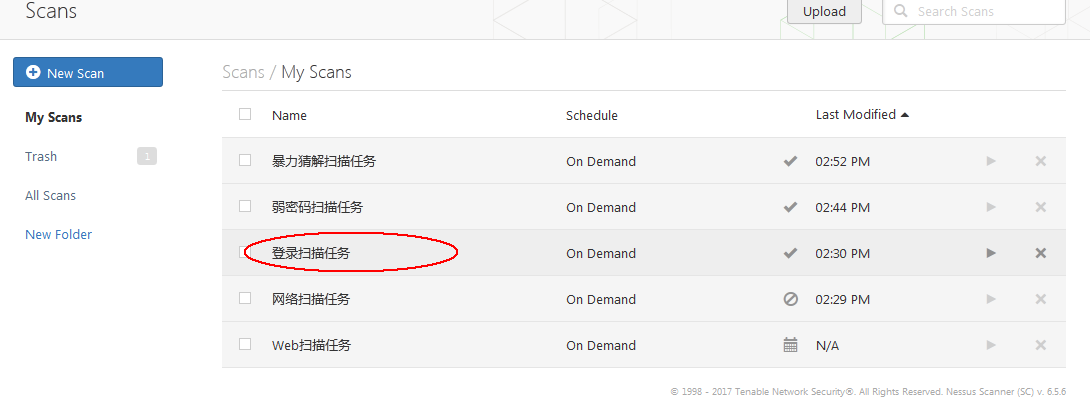
## 5.1 设置任务计划

针对服务器的扫描时间大多建议在凌晨访问量很少的时候进行。为了方便自动化管理，可以自行设定扫描作业开始时间，以及扫描动作的周期性间隔。

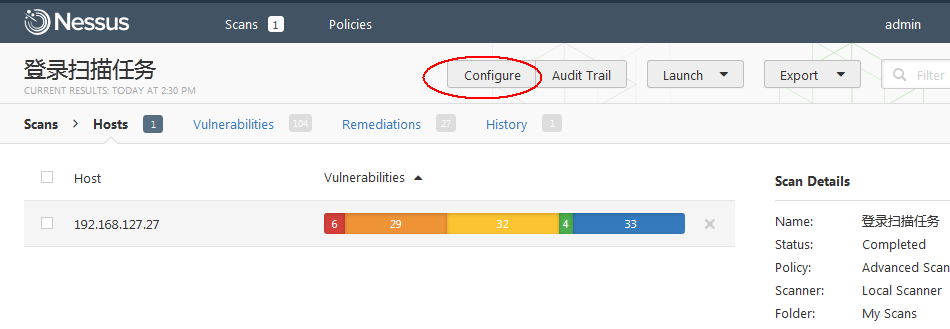
例如：设定每周六凌晨1点至5点为允许扫描时间，任务计划从1点开始自动扫描。

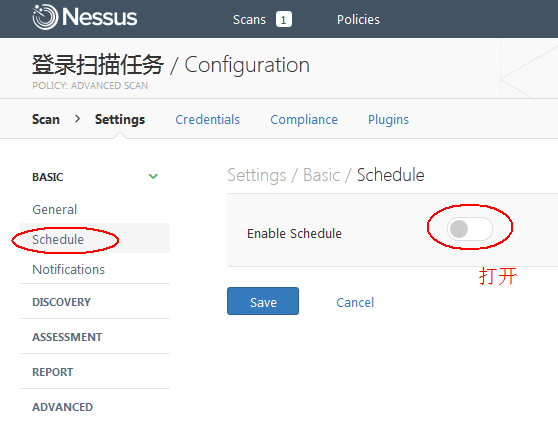
请参考以下步骤：

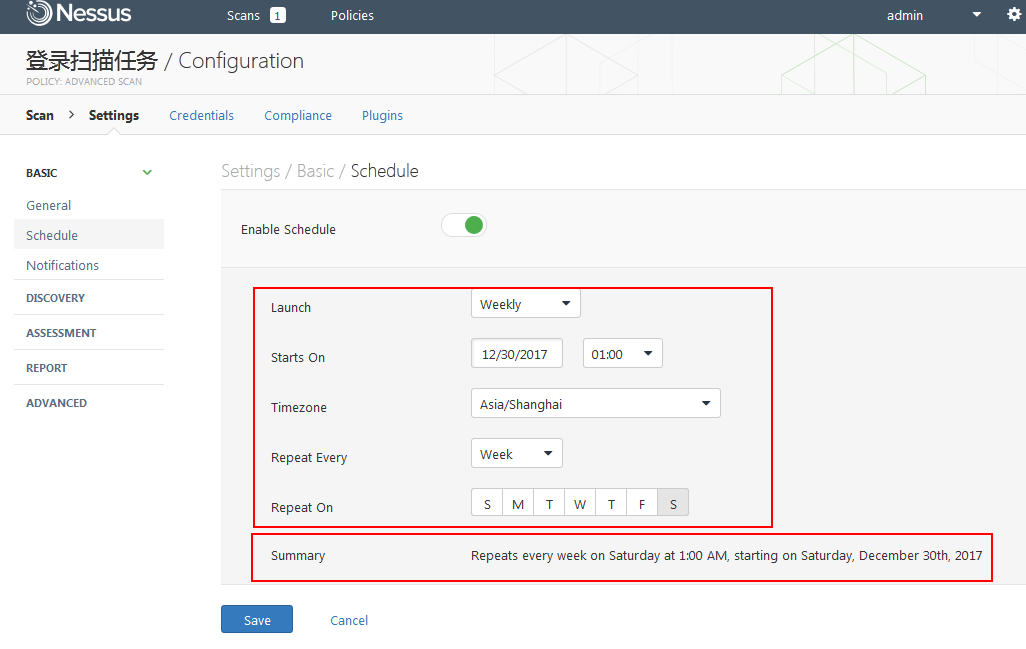
1. 登录Nessus，点击进入某个扫描任务下。



点击页面上方的Configure，进入扫描任务的配置页面

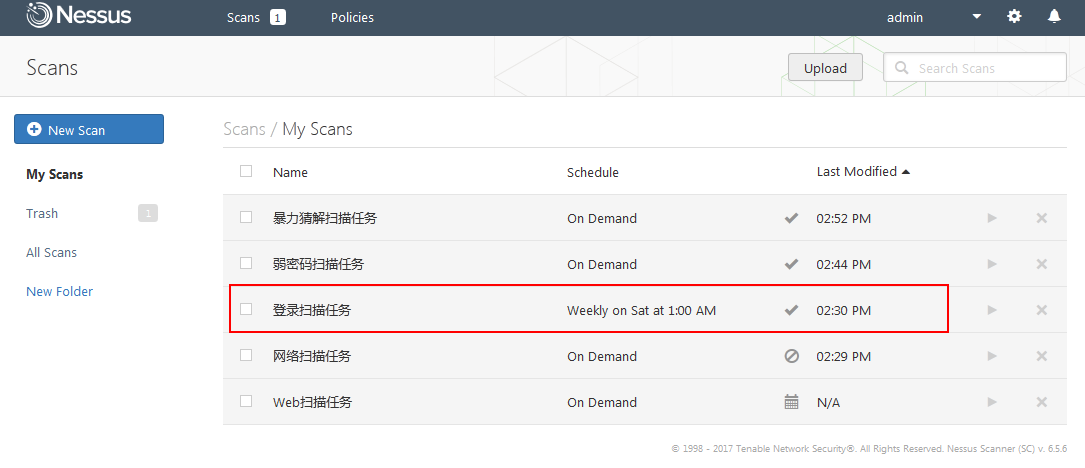


1. 在Setting –> Schedule下，打开Enable Schedule开关 
2. 参考下图将扫描计划设置为每周六的早上1点整。



设置后可以看到Summary栏里任务计划设置结果。

1. 保存后也能看到这个任务的Schedule也详细描述了自动任务计划的时间。



# 六、配置合规审计测试项

Tenable Nessus除了漏洞扫描，本身提供非常大量的法规可供比对，如PCI DSS、DISA STIG、SIS等，以及网络设备、资料库、系统等配置合规审计范本，管理者无须在自己写规则，直接套用内建范本即可使用。

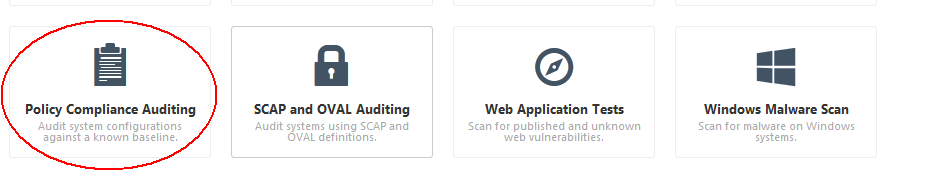
方案特色：Tenable提供丰富的合规审计范本种类供选用，同时此类范本支持自定义修改和快捷导出/导入，以灵活满足企业特定的审计需求，具备很高的易用性与适用性。

本次配置合规审计测试，共涉及xx种不同类型的系统或服务

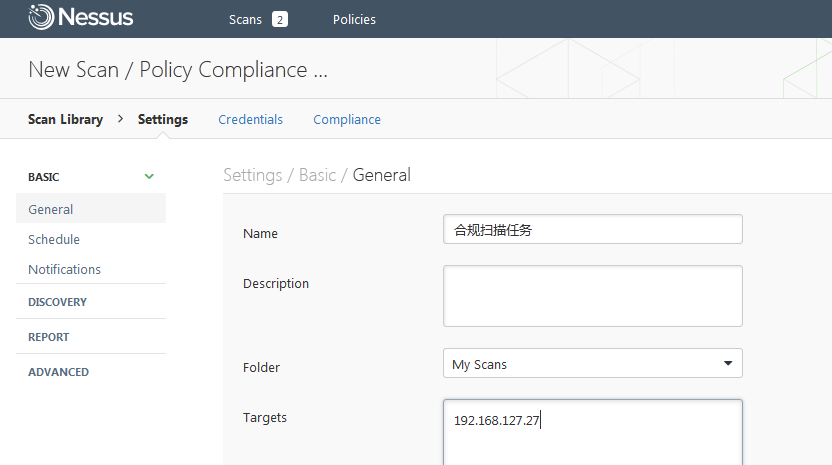
* + Windows Server 2008
  + Redhat Linux 6
  + ……

以其中的Linux Server为例，操作步骤如下：

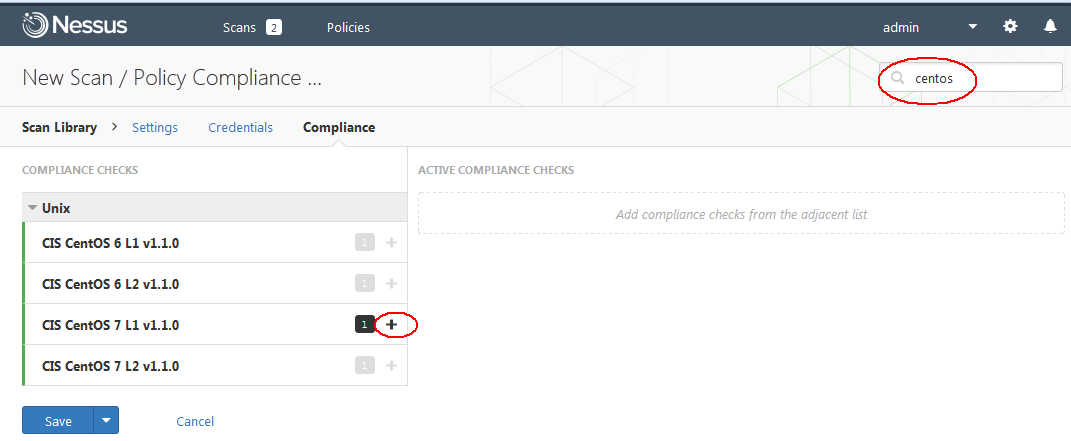
1. 新增合规性扫描任务，在『Scans』下，点击『New Scan』，本次使用Policy Compliance Auditing策略模板



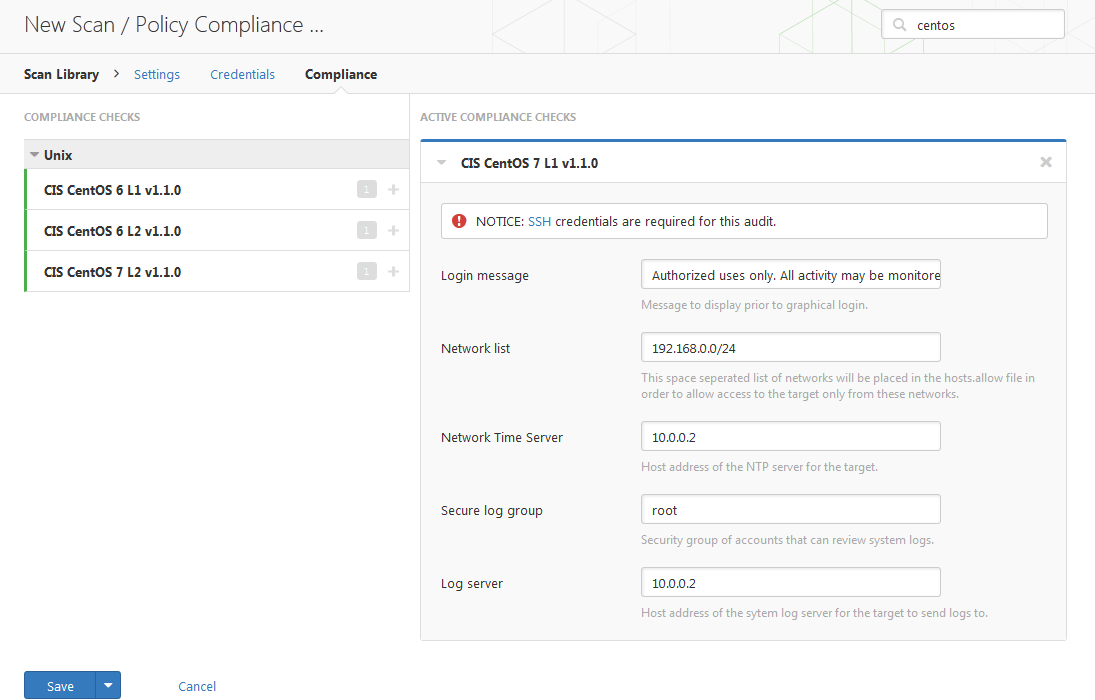
1. 定义扫描名称和目标主机IP。



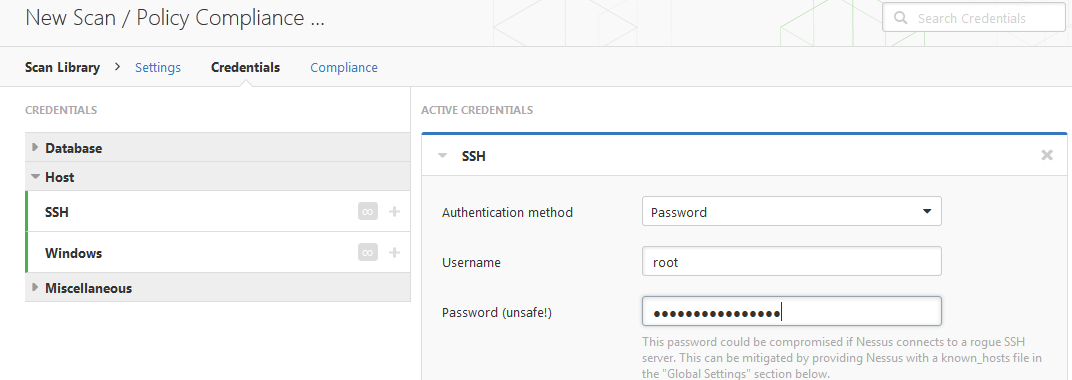
1. 在Compliance页面里，开始设置合规脚本。这里演示系统自带的合规模板。在右上角搜索centos,在搜索结果里选择CIS CentOS7中的一个。点击右侧的符号“+”



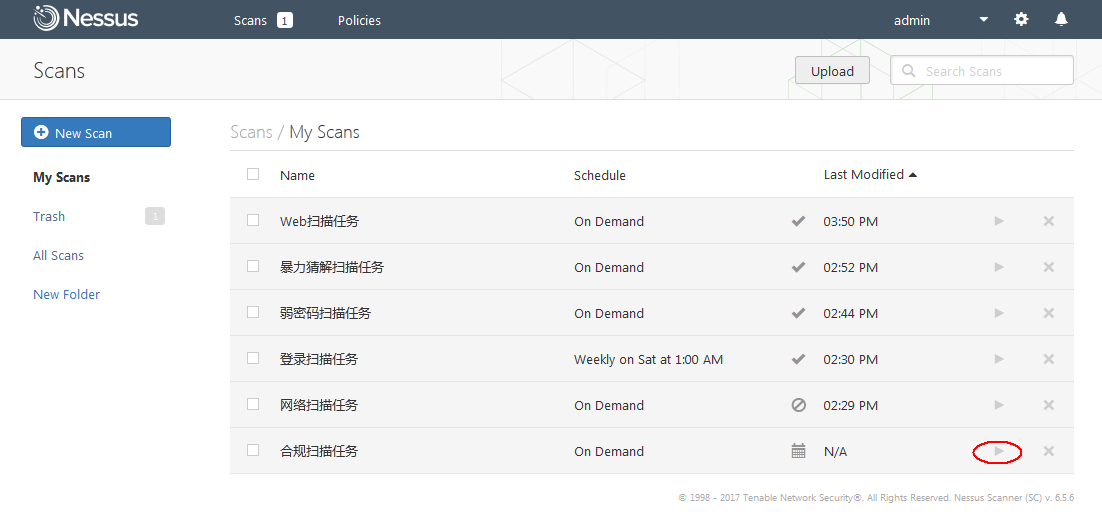
按提示，还需要设置登录到目标主机的Credentical



1. 随即在Credentical项里设置目标主机SSH的登录账号和密码。



1. 其他设定项目皆与一般扫描无异，然后保存，并执行合规扫描任务。



扫描结果演示如下：

通过点击下方的符号切换漏洞和合规的结果，如下图，有82项未通过，133项通过

