1. VIT相关
2. VIT测试定义

VIT（Vulnerability Identification Testing）漏洞扫描测试，通过工具对DUT（device under test测试设备）进行扫描，挖掘DUT是否有已知漏洞，查看测试DUT在漏洞扫描过程中是否可以充分地保持essential function。

1. VIT测试目的

保证嵌入式设备不存在已知的漏洞。有些已知的漏洞对于设备的风险较低，在测试不通过时应予以解释是否需要减缓其影响。

1. VIT测试方法

漏洞扫描器一般基于漏洞数据库来检查远程主机，漏洞数据库包含了检查安全问题的所有信息（服务、端口、包类型、潜在的攻击路径，等等）。它可以扫描网络和网站上的上千个漏洞，提供一个风险列表，以及补救的建议。

Nessus：Nessus是最流行的漏洞扫描器之一。它可以用于认证和非认证的漏洞扫描。除了可以进行网络漏洞扫描外，它还支持外部和内部PCI扫描、恶意软件扫描、移动设备扫描、策略合规性扫描、web应用程序测试、补丁审计等。它使用超过70,000个插件来扫描一个目标机。

1. 注意事项
2. DUT中的任何内部防火墙应保持使用时的状态；
3. 下行essential function监视时的配置

最大负载

在线实时或离线监视DUT控制输出的时间特性抖动

1. DUT有多个可访问网络接口时，应每次一个进行VIT；
2. VIT中，如果DUT不能充分保持essential function，问题必须可复现，才能判定为不通过；
3. 测试中使用的漏洞列表日期不应早于证书日期前一个月（31天）。
4. 测试通过准则

Req. ERT.R54: VIT中，DUT充分地保持essential function；无”critical”和”high”漏洞；所有发现的”medium”漏洞（如有）应被减缓；所有发现的”low”漏洞（如有）应针对EDSA-311中相应SL的FSA-E要求进行分析，如果漏洞与对应SL的FSA-E要求不冲突，则DUT必须通过VIT

Req. ERT.R55: VIT中，如果DUT不能充分保持essential function，问题必须可复现，才能判定为不通过。

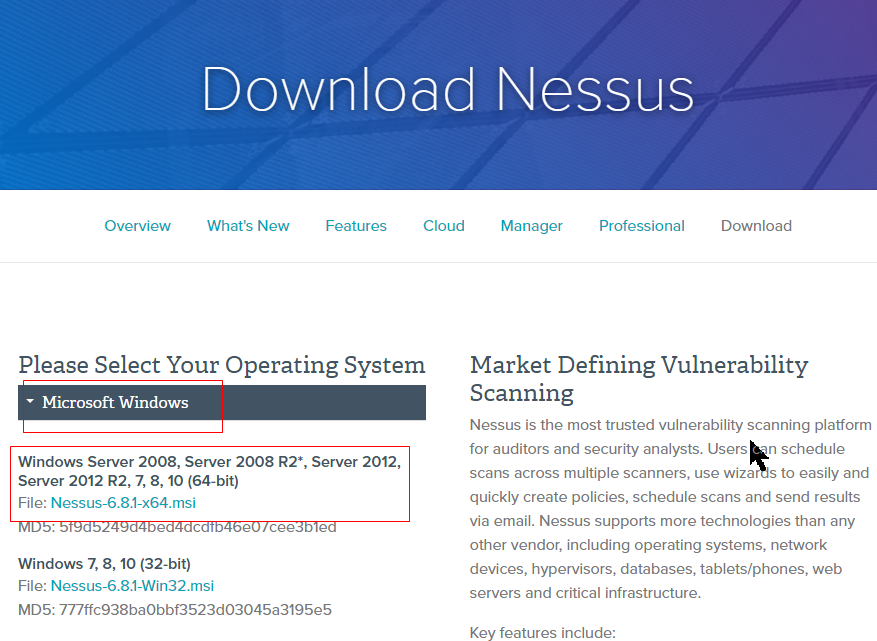
1. Nessus的下载与安装

在官网的下载中只有家庭版是免费的，鉴于现在对工具并不了解，所以先使用家庭版了解熟悉工具。

1. 下载安装包

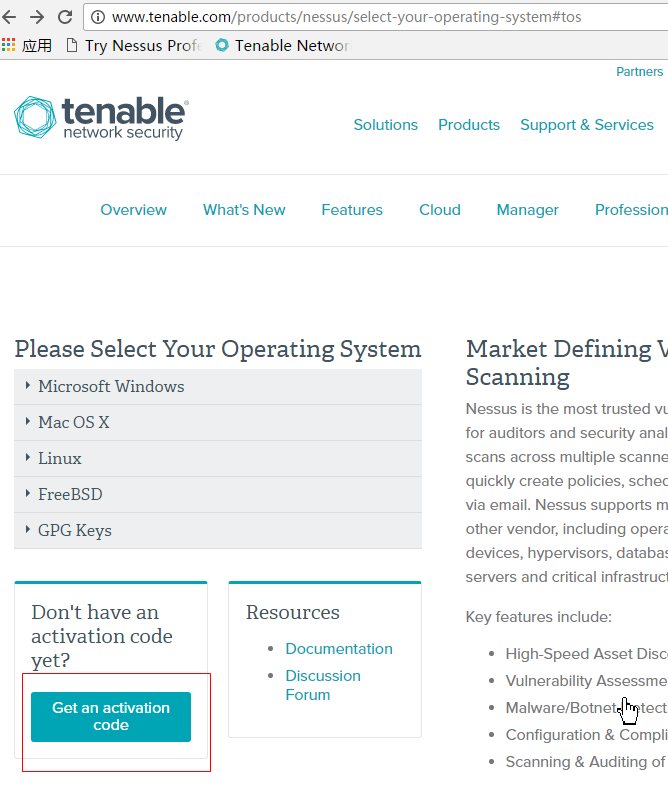
在Nessus官网找到下载页面

http://www.tenable.com/products/nessus/select-your-operating-system，根据电脑配置我下载的是windows系统64位版本。

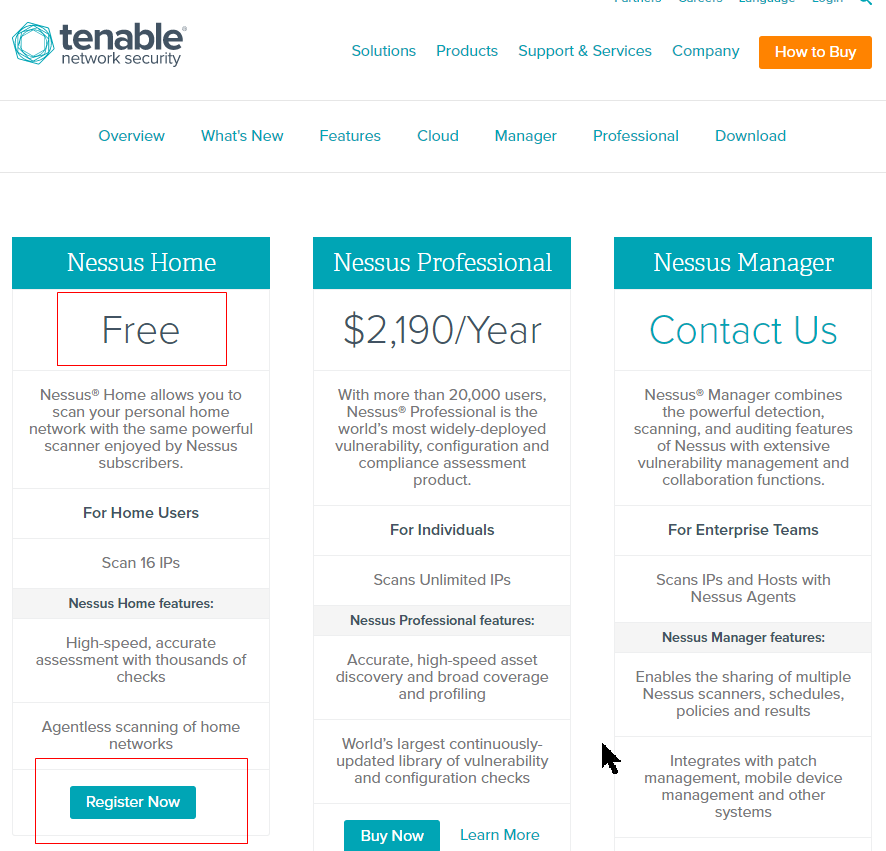


1. 获取激活码

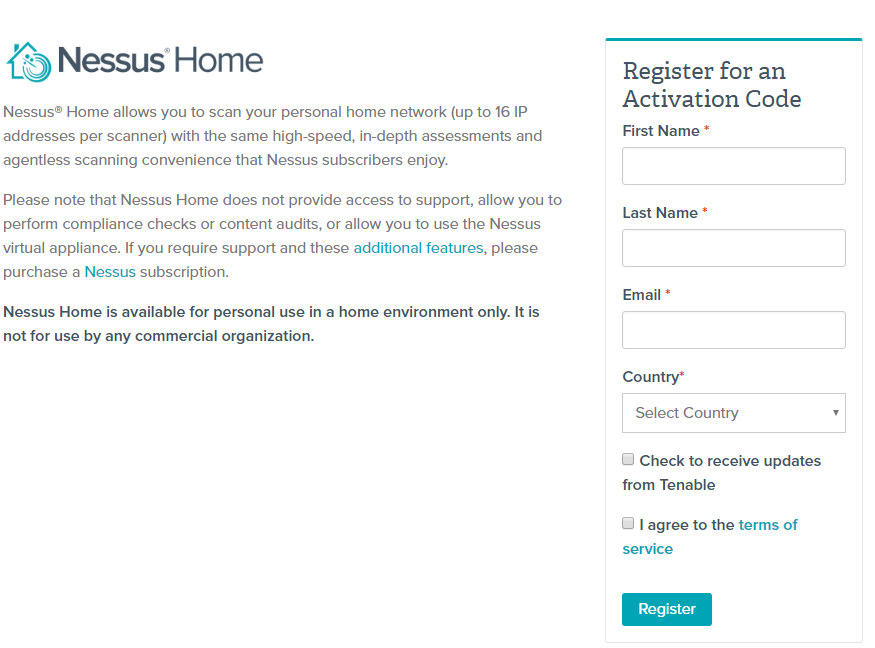
在下载页面的下方可以看到一个Get an activation code的按钮，点击进入获取激活码页面。



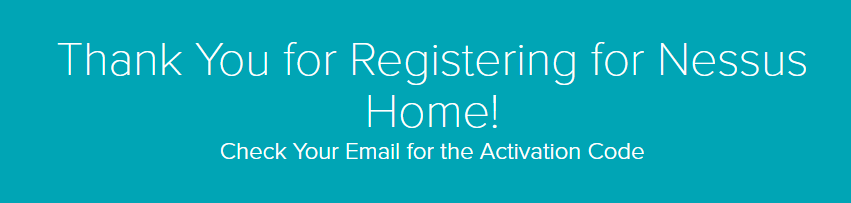
进入页面后只有家庭版免费，先获取家庭版使用权已了解Nessus使用方式



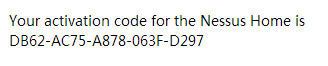
点击注册，First Name和LastName可以随便填写，邮箱要确保真实有效用于接收激活码。



信息填写完成后，点击注册，会弹出如下界面，接下来等待邮件。



会收到标题为“Tenable Nessus Home Activation Code”的邮件，激活码如下，邮件中声明激活码仅一次使用有效。

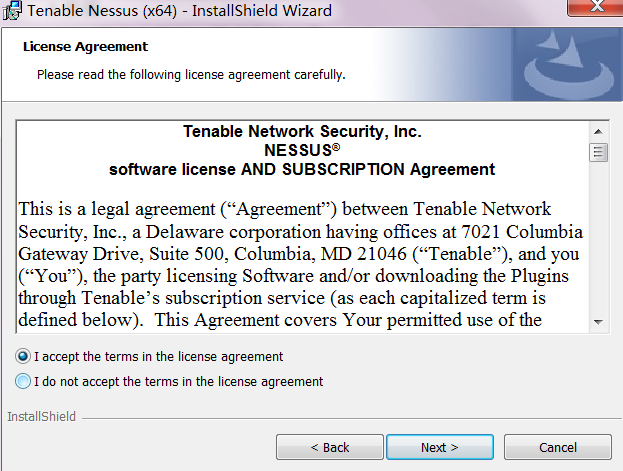


1. 安装

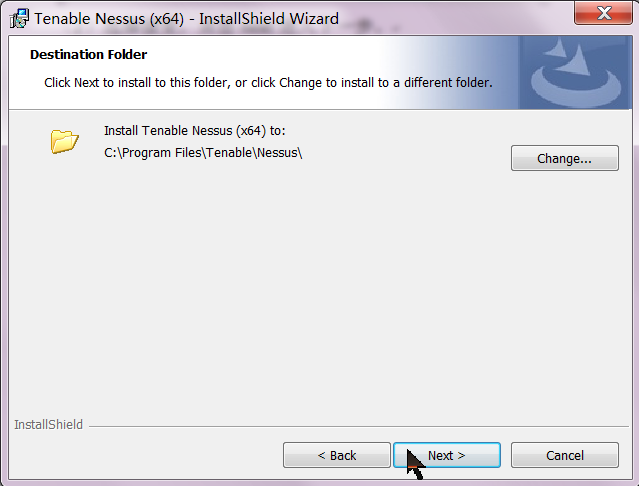
（1）双击安装包，弹出安装向导，点击next进入下一步。



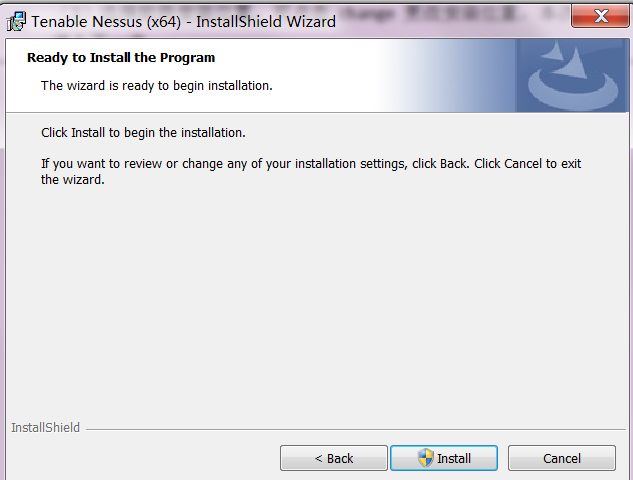
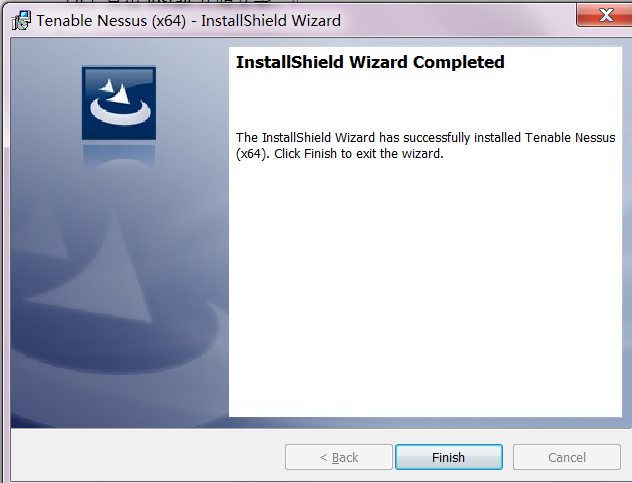
（2）选择接受，点击next进入下一步。



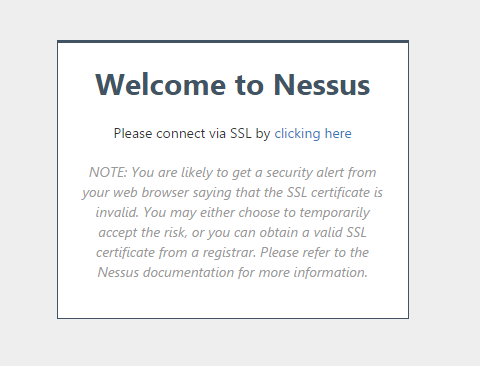
（3）选择软件安装位置，可点击change更改安装位置，本次选默认安装路径，点击next进入下一步。



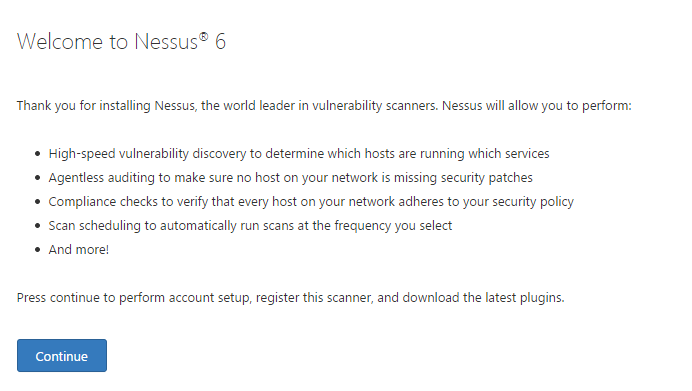
（4）点击install开始安装，安装成功后提示如下右图所示。

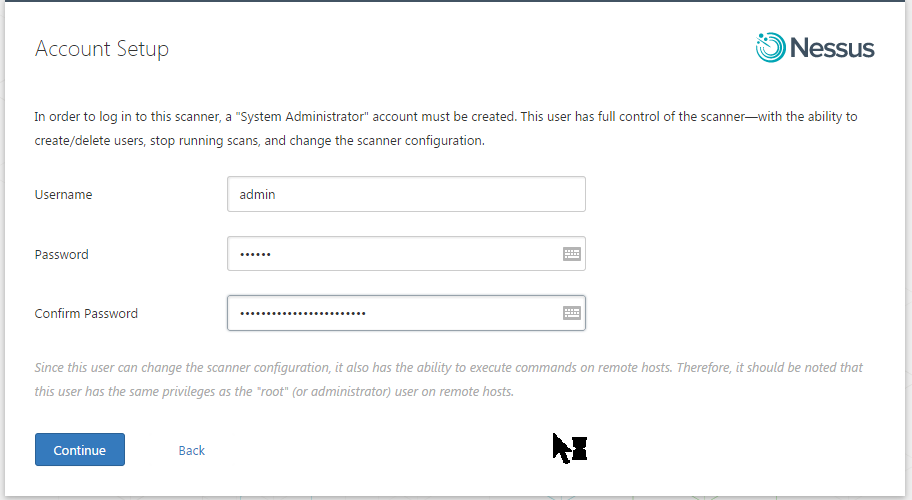
（5）安装成功后，点击finish，会自动在电脑的默认浏览器弹出如下界面。



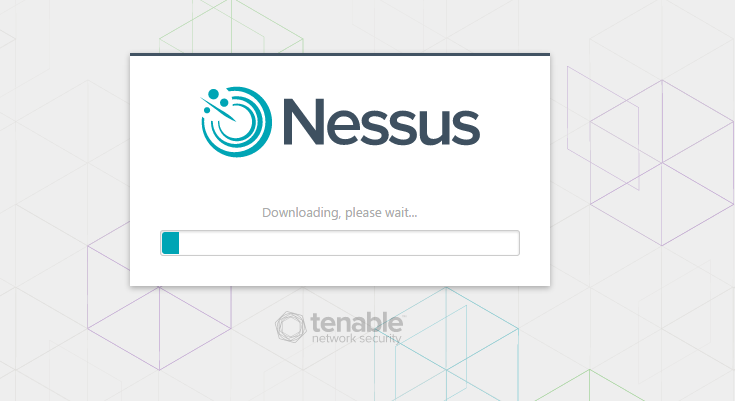
（6）单击clicking here，弹出如下界面。



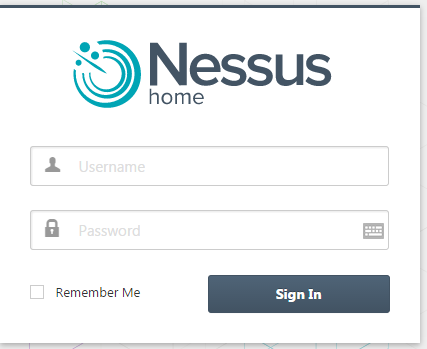
（7）单击continue，出现如下界面，填写用户名和密码单击continue，在新弹出页面填入刚获得的激活码，单击continue。



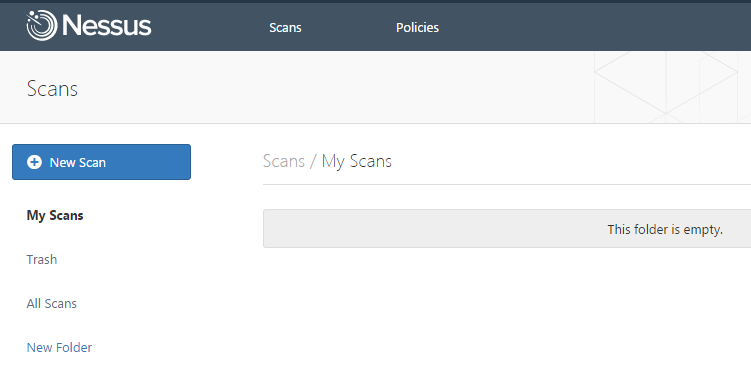
（8）之后进入插件下载初始化过程，时间较久。



下载过程结束后，出现如下界面，输入之前设置的账号密码登录。

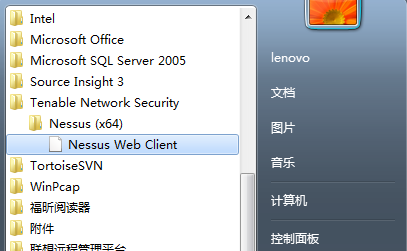


登陆后，出现如下界面，至此安装过程结束。



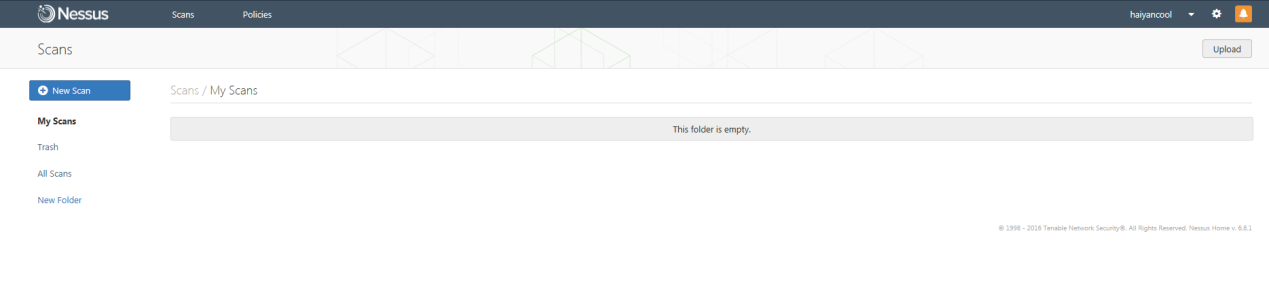
1. Nessus使用说明
2. 打开Nessus

点击所有程序，通过下图方式可打开软件。



1. 主界面

正式版主界面有四个按钮，分别是：Reports（报表）、Scans（扫描）、Policies（策略）、User（用户），但试用版只有Scans（扫描）和Policies（策略）。



User（用户）：进行用户的管理，增加、修改、删除账号；

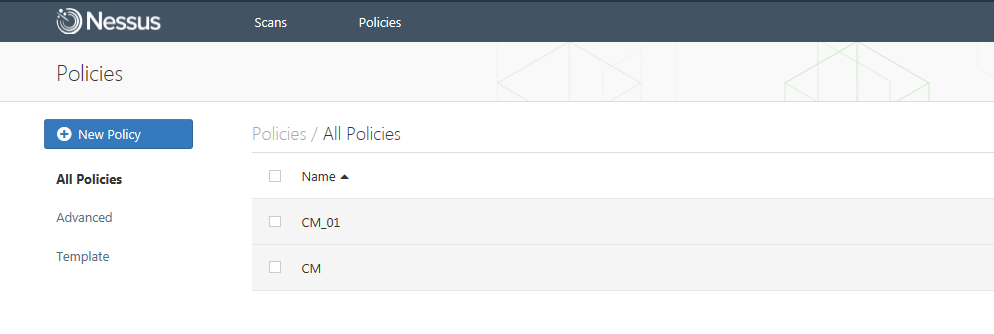
Policies（策略）：设置扫描的策略、方式等参数；

Scans（扫描）：进行扫描工作，匹配上步设置的策略即可；

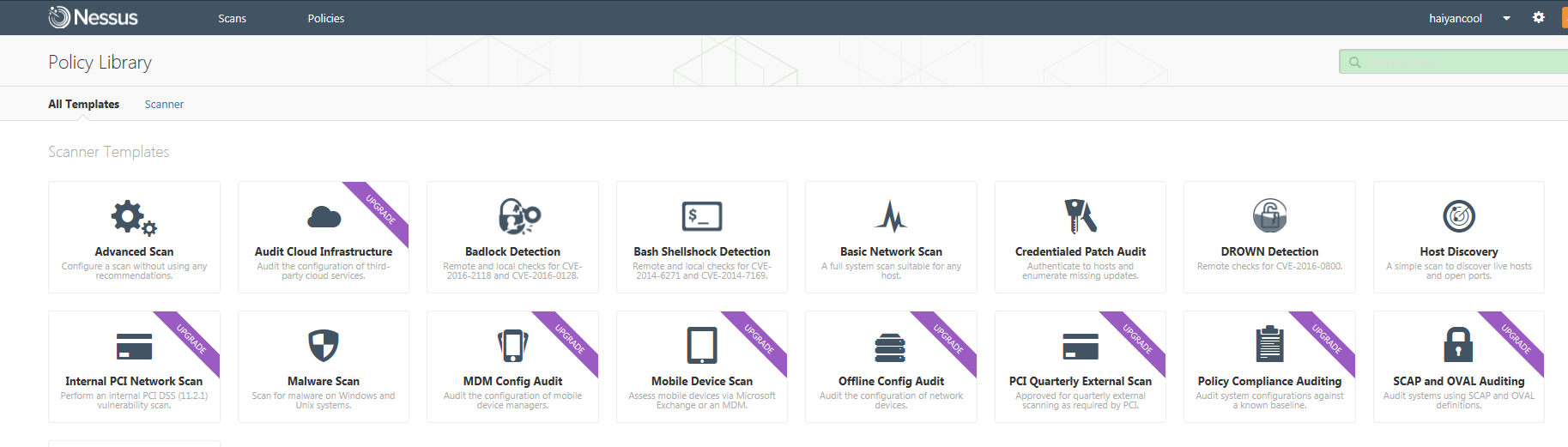
Reports（报表）：导出报告，进行软件评估。

可以直接通过模板新建扫描任务，然后进行相应的配置，保持配置后开启扫描任务；也可以先新建一个策略，然后在新建一个扫描任务选择使用刚刚新建的策略（此时扫描任务只需填写任务名称和扫描目标），保持配置后开启扫描任务。下面详细介绍Policies（策略）和Scans（扫描）。

1. 策略
2. 进入Policies页面



点击New Policy，看到下图所有模板

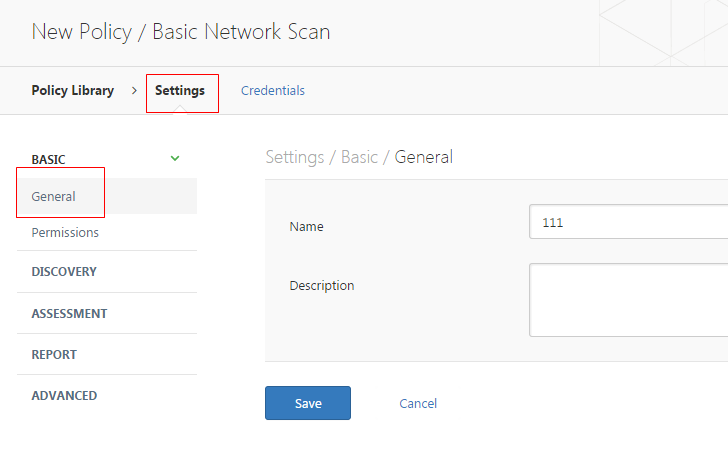


1. 策略名称与描述对照表

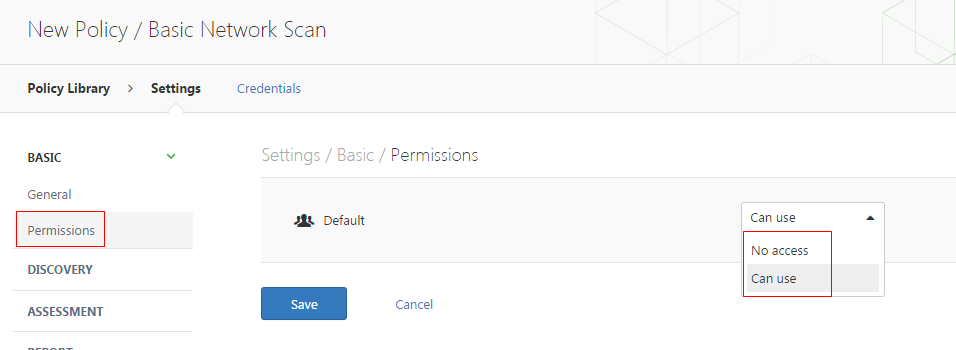
|  |  |
| --- | --- |
| **策略名称** | **描述** |
| Advanced Scan 高级扫描 | 需要完全控制策略配置的用户的扫描模板 |
| Audit Cloud Infrastructure 审计云基础架构 | 要审计基于云的服务配置的用户 |
| Bash Shellshock Detection | Bash Shellshock漏洞的远程和受信任检查 |
| Basic Network Scan 基础网络扫描 | 用于用户扫描内部或外部主机 |
| Credentialed Patch Audit 审计认证补丁 | 登录到系统中，并列举缺少的软件更新 |
| GHOST Detection | 认证检查GHOST漏洞 |
| Host Discoverry | 实时确定主机和开放的端口 |
| Internal PCI NEtwork Scan 内部PCI网络扫描 | 用于管理员为支付卡行业数据安全标准内部网络的合规性审计而准备 |
| Mobile Device Scan 移动设备扫描 | 用于用户的苹果的配置文件管理器、ADSI、MobileIron或Good MDM。 |
| Offline Config Audit 离线配置审计 | 上传和审计网络设备的配置文件 |
| PCI Quarterly External Scan PCI季度外部扫描 | 季度外部扫描PCI要求批准的策略。 |
| Policy Compliance Auditing 策略合规审计 | 审计用户提供的一个一直的及准系统配置 |
| SCAP Compliance Audit SCAP合规审计 | 审计系统使用的是安全内容自动化协议（SCAP）的内容 |
| Web Application Tests Web应用程序测试 | 用于用户执行一般的Web应用程序扫描 |
| Windows Malware Scan Windows恶意软件扫描 | 用于用户搜索Windows系统中的恶意软件 |

以Basic Network Scan为例

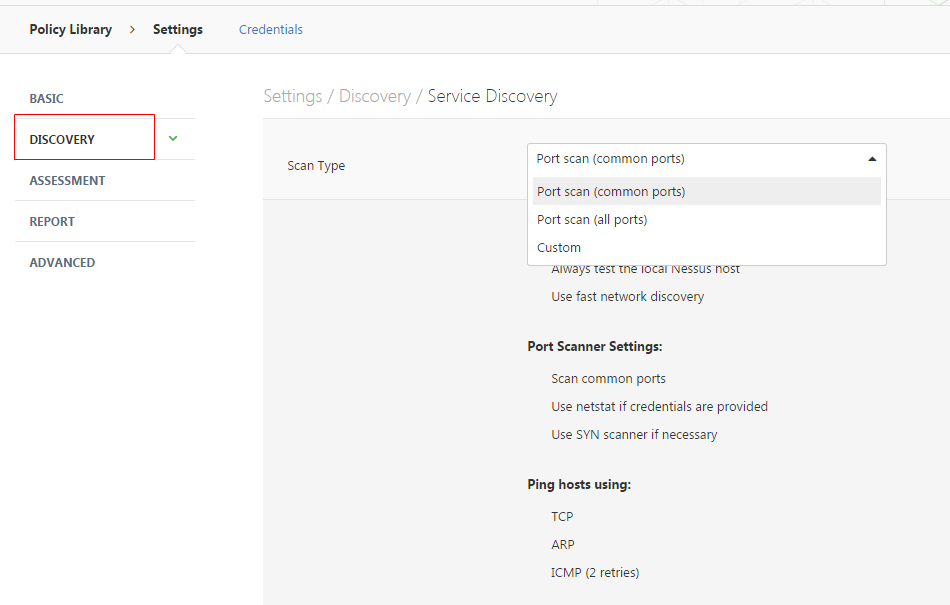
1. 填写策略名称



permissions选项有2种，No access仅限于创建策略的用户使用，Can use则其他用户也可使用该策略



Discovery部分可以根据使用的策略设置主机发现、端口扫描、服务发现方法等

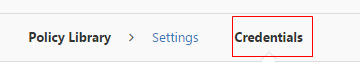


1. 策略认证凭据

通过使用凭证，Nessus可以不需要代理获得本地访问扫描目标系统的权限。

Nessus支持有几种形式的身份验证，包括但不限于数据库、SSH、网络设备、补丁管理服务器和各种明文验证协议。

菜单位置如下：



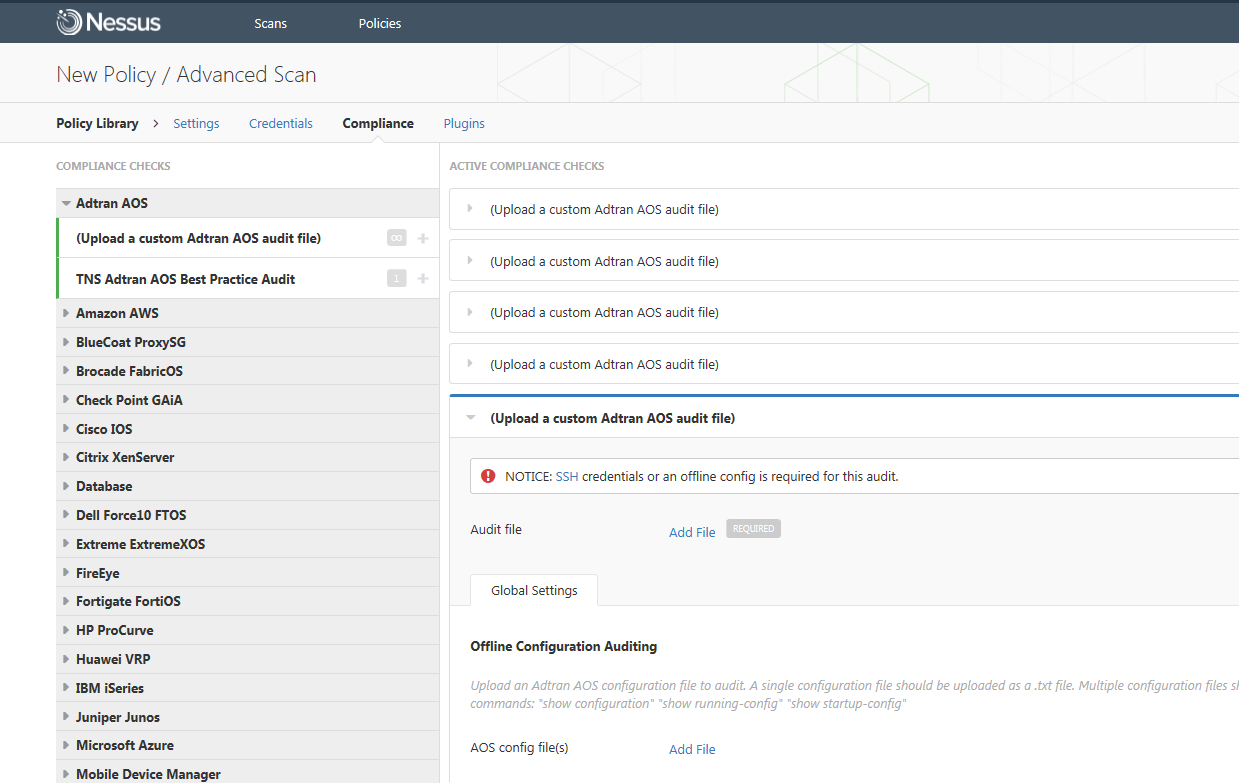
允许多个凭证相同的策略，对于无限制某些类型的凭证，图标标识如下：

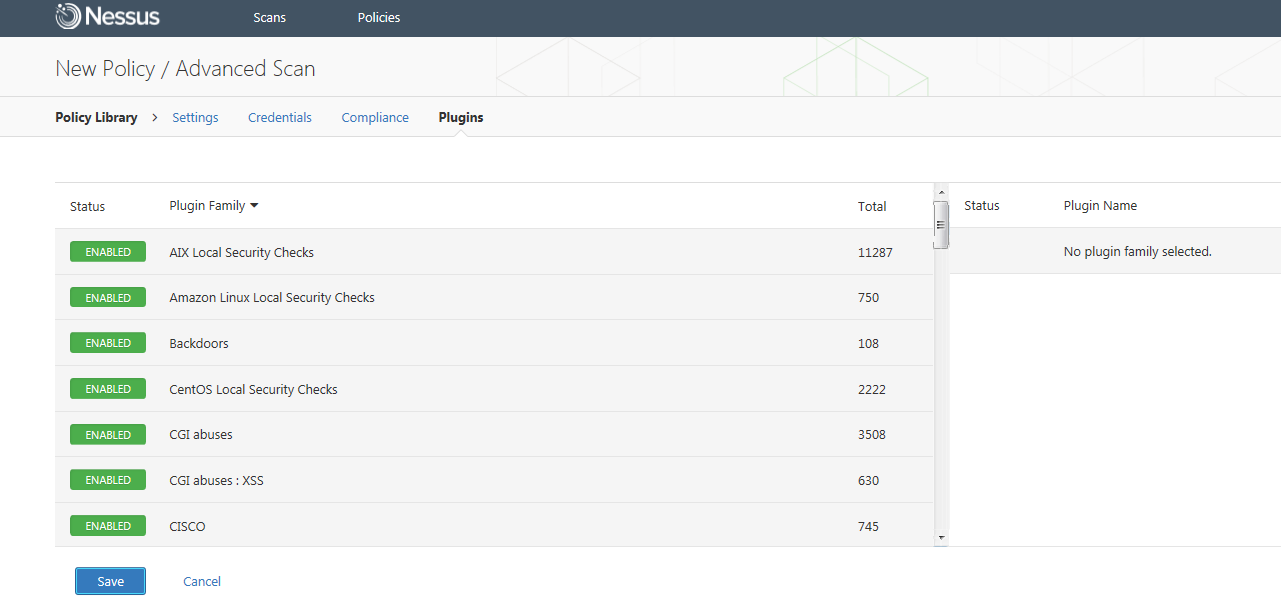


而限制数量的凭证类型，会显示剩余可用的数量：



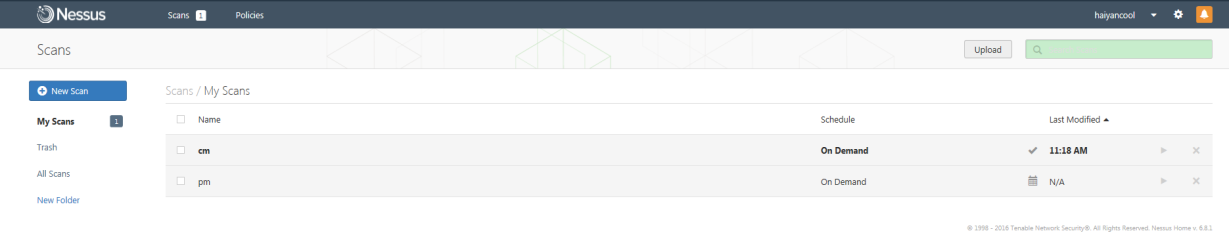
1. Nessus策略创建完成后，依次点击Scans--NewScan--User，利用已有的策略创建扫描项。这里只需要填写名称及目标地址即可。保存后即可运行。
2. Advanced Scan，若选择高级策略，除了要配置Setting和Credentials（方法和Basic Network Scan相同）之外，还要配置Compliance和Plugins。



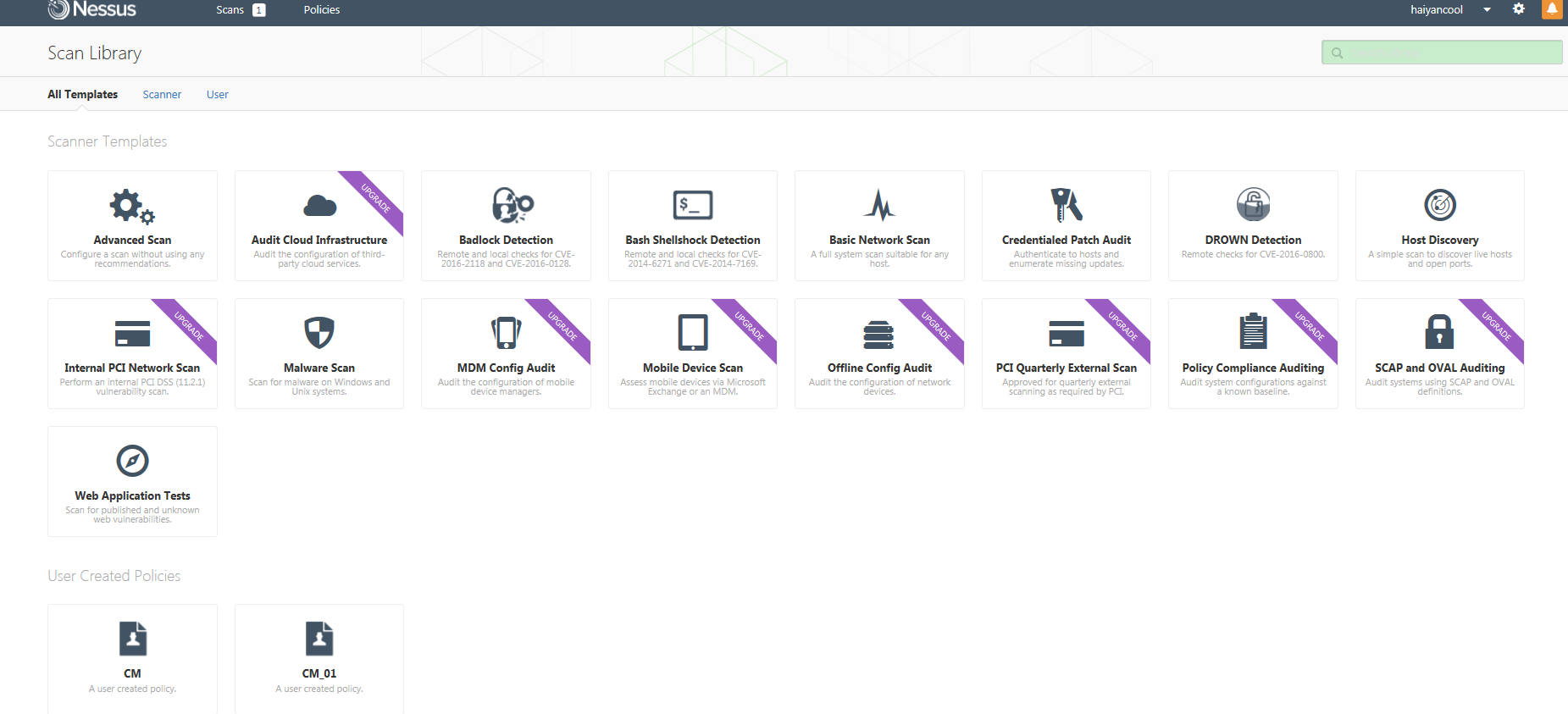


1. 扫描

点击Scans / My Scans页面

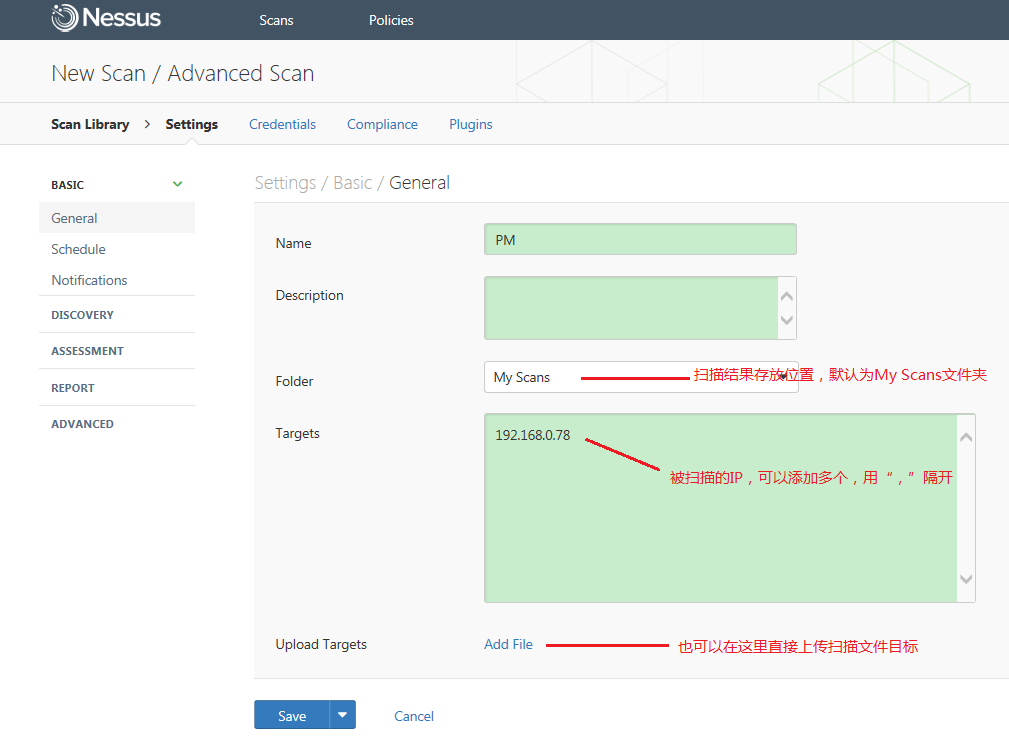


点击New Scan，进入模板界面，扫描也同样可以选择Basic Network Scan、Advanced Scan、或用已创建的策略

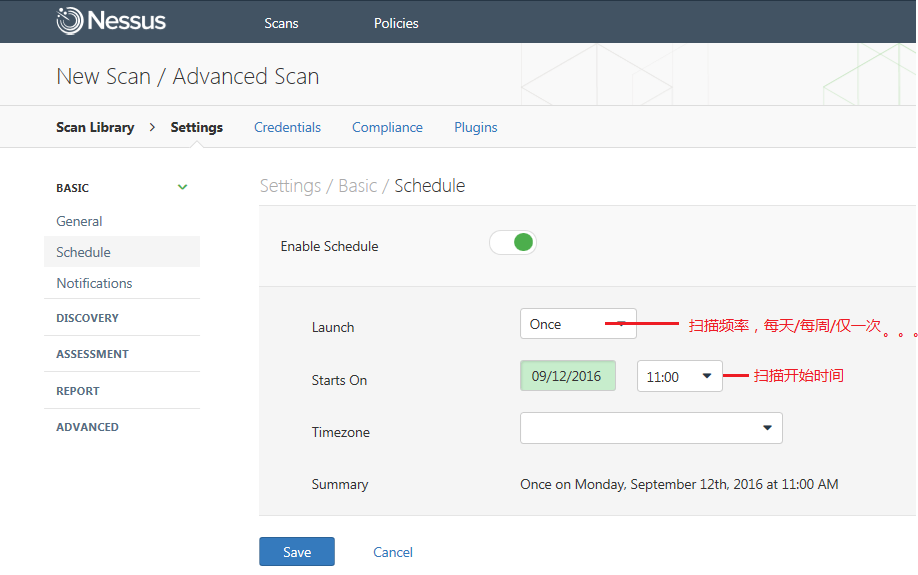


以下以Advanced Scan为例介绍每个功能按钮代表意义，Basic Network Scan同理略。

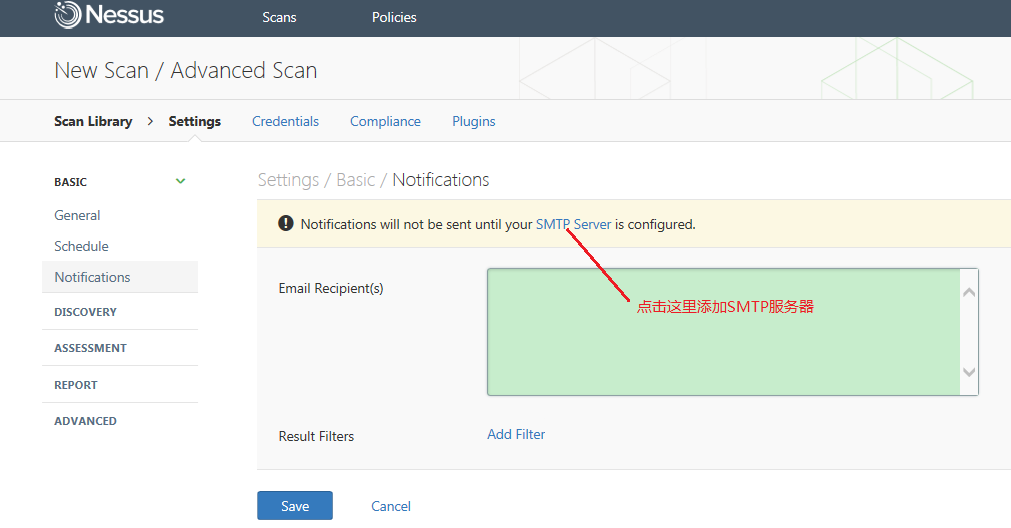
Settings / basic / General添加基本信息

 在弹出的界面中设置任务名称、任务存放位置（默认只能选择My scan 和Trash这两个文件夹）及需要扫描的目标，target中可以输入一个目标或者多个目标，用逗号隔开即可，也可以点击add file直接上传文件，加载扫描目标。一般targets填写需要扫描的ip或者主机名，需要ip可以ping通。

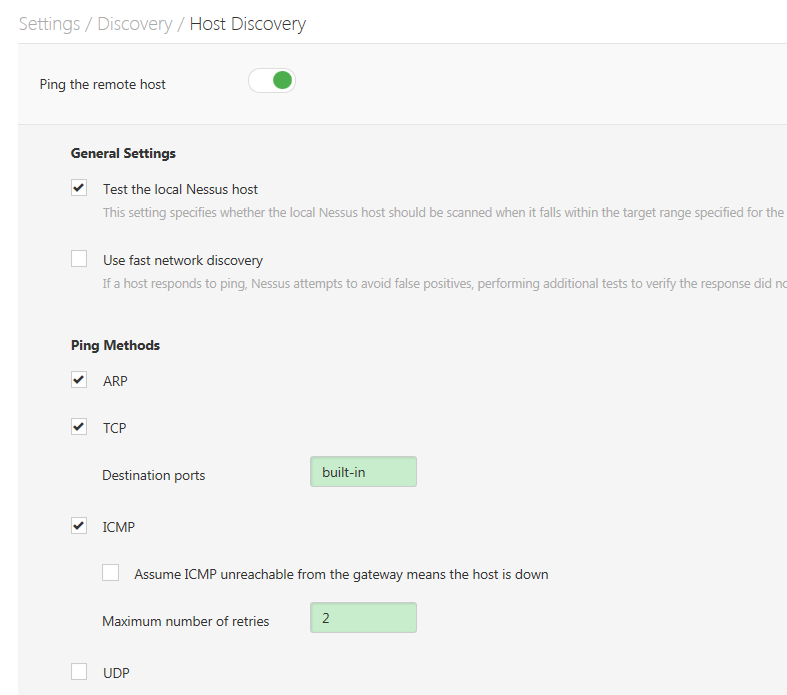
Settings / basic / Schedule设置扫描是否建立时间表



Settings / basic / Schedule扫描结果通知[SMTP](https://localhost:8834/" \l "/settings/communication/network/smtp) 服务器



Settings / discovery / Host Discovery

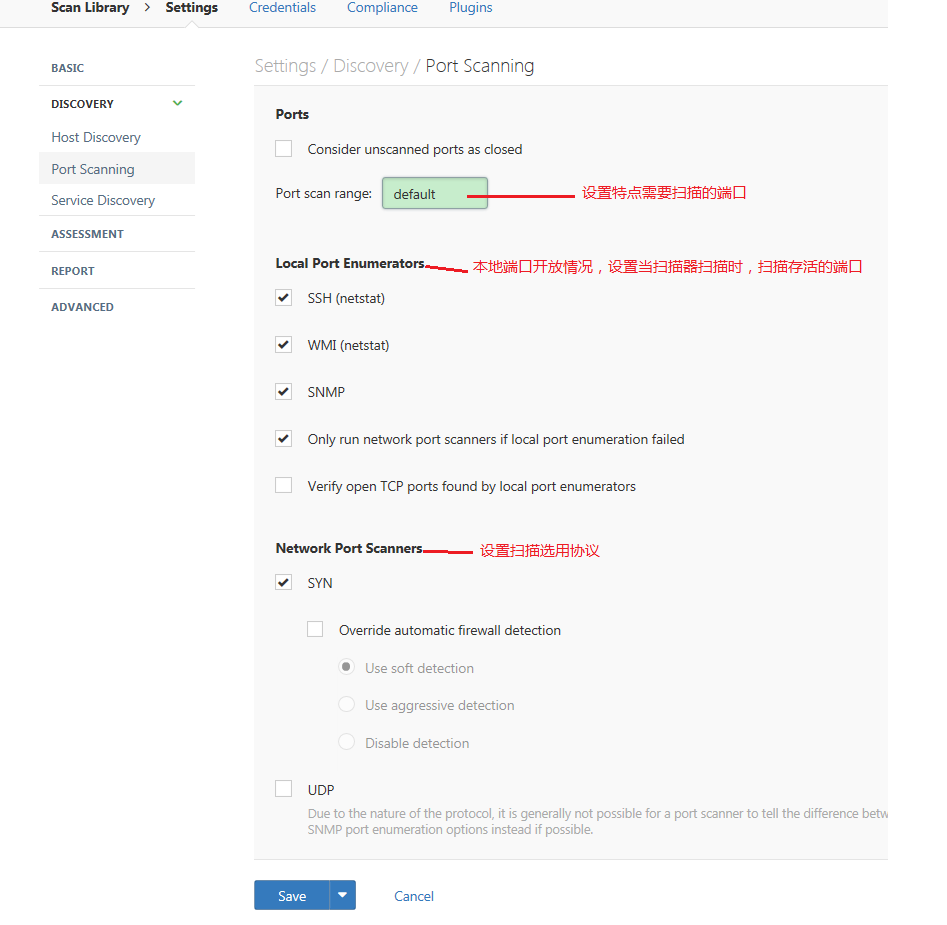


Test the local Nessus host：指定本地Nessus主机是否应该被扫描时落在目标范围指定的扫描

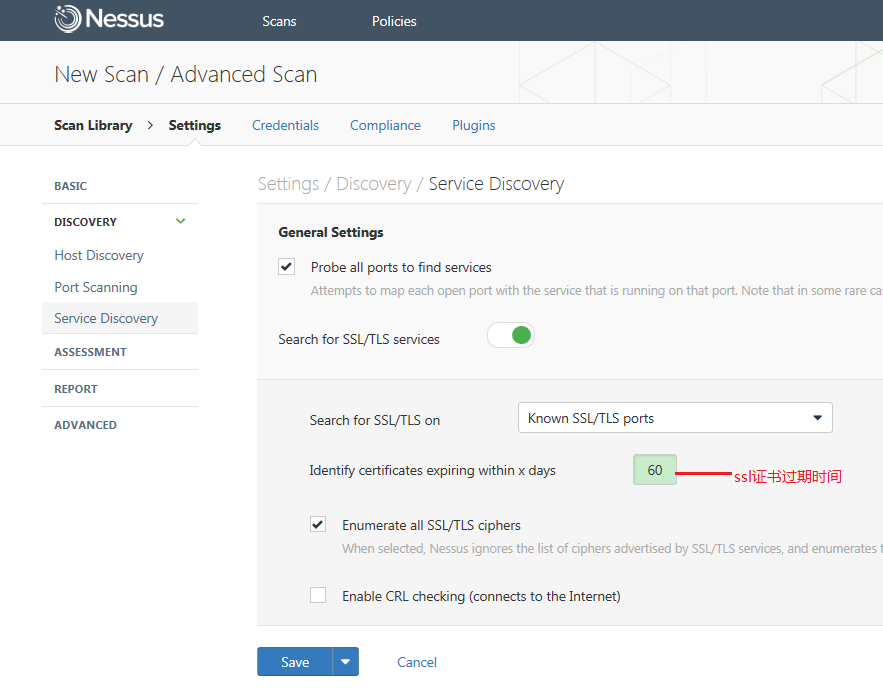
Use fast network discovery：在一个扫描器扫描时，为了避免扫描目标返回的数据有误，导致扫描器判断错误，额外添加一个扫描器，通过不同的网络状况来验证响应，

Ping Methods：修改ping包的发送类型，选默认即可

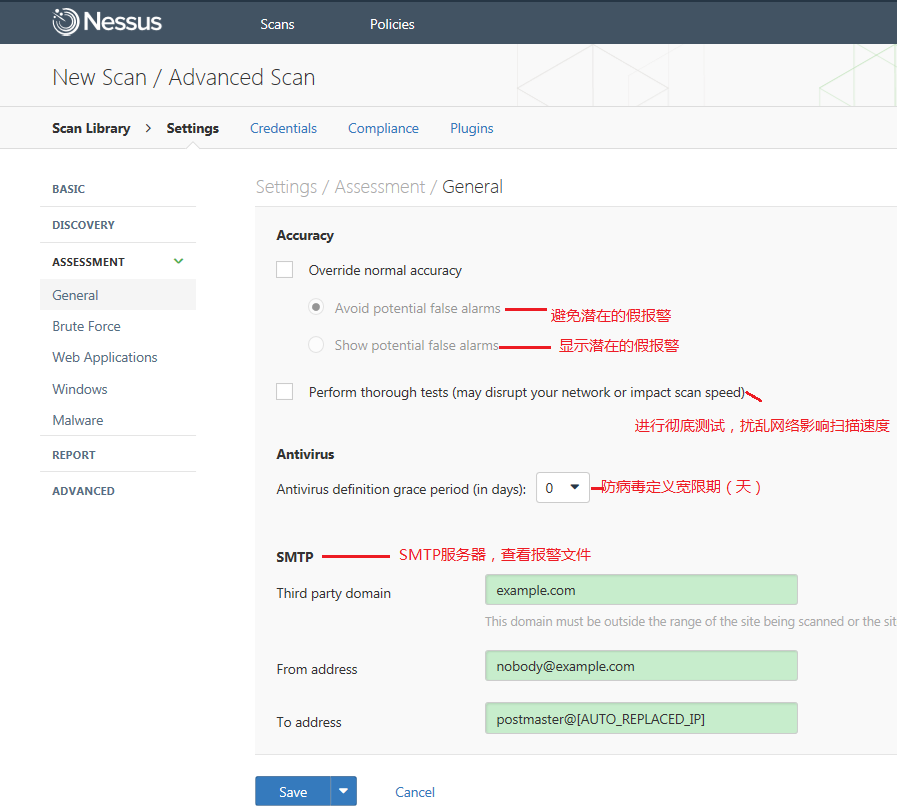
Settings / discovery / Port Scanning端口扫描



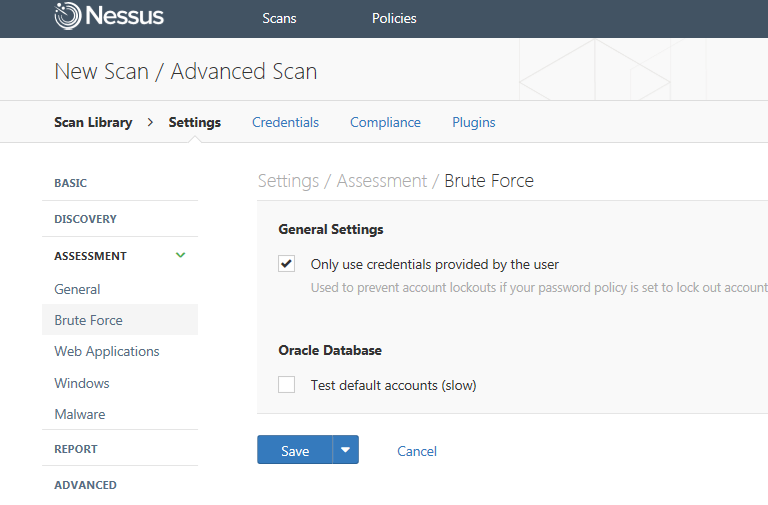
Settings / discovery / Service Discovery：扫描服务器的登录SSL设置



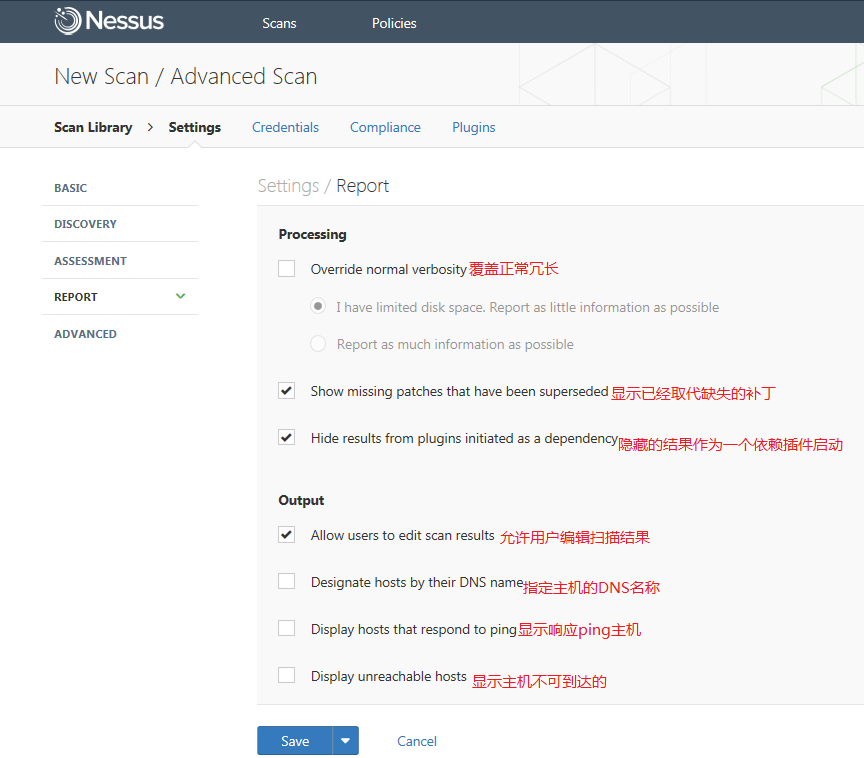
Settings / assessment / General：



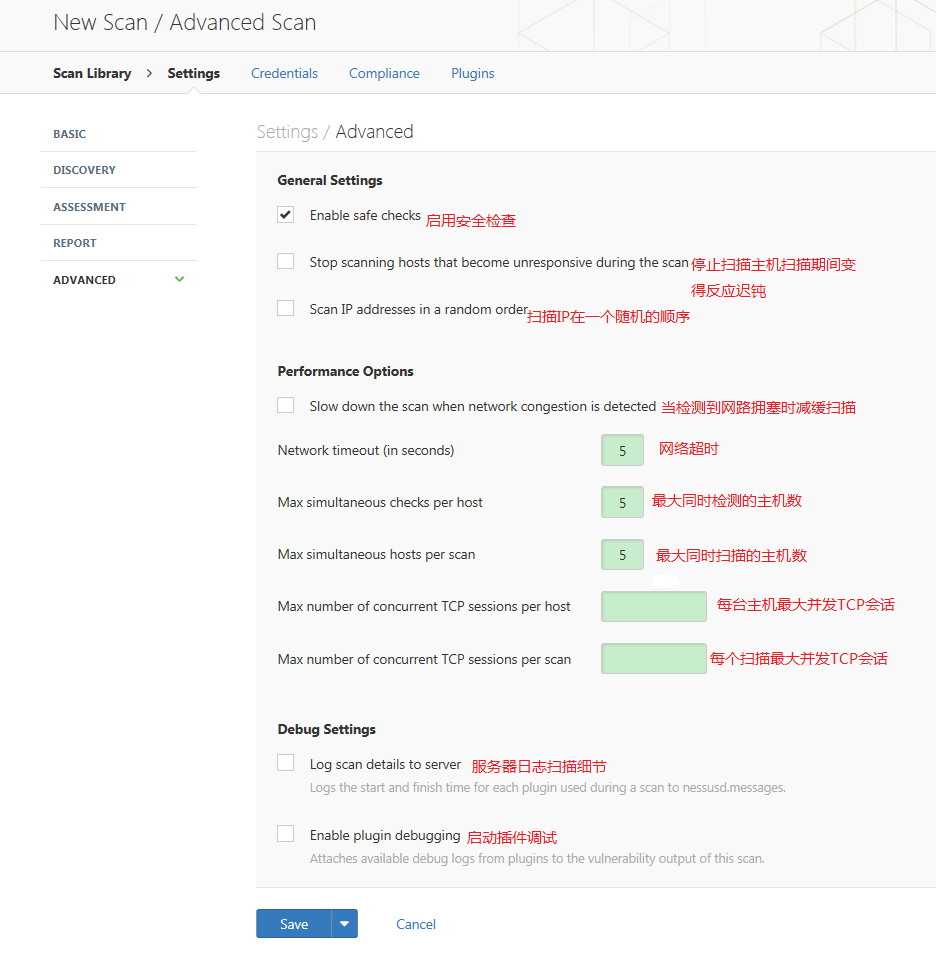
Settings / assessment / Brute Force：强力设置，默认如图（用户只使用所提供的凭证），若选Oracle数据库速度慢



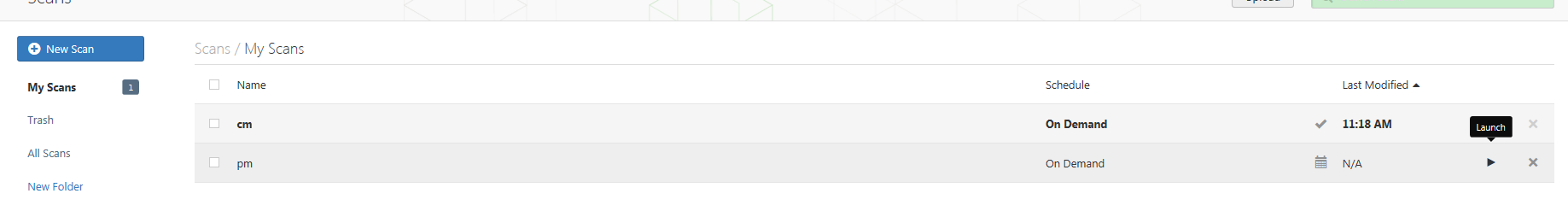
Settings / report：报告，按以下默认即可



Settings / advanced：

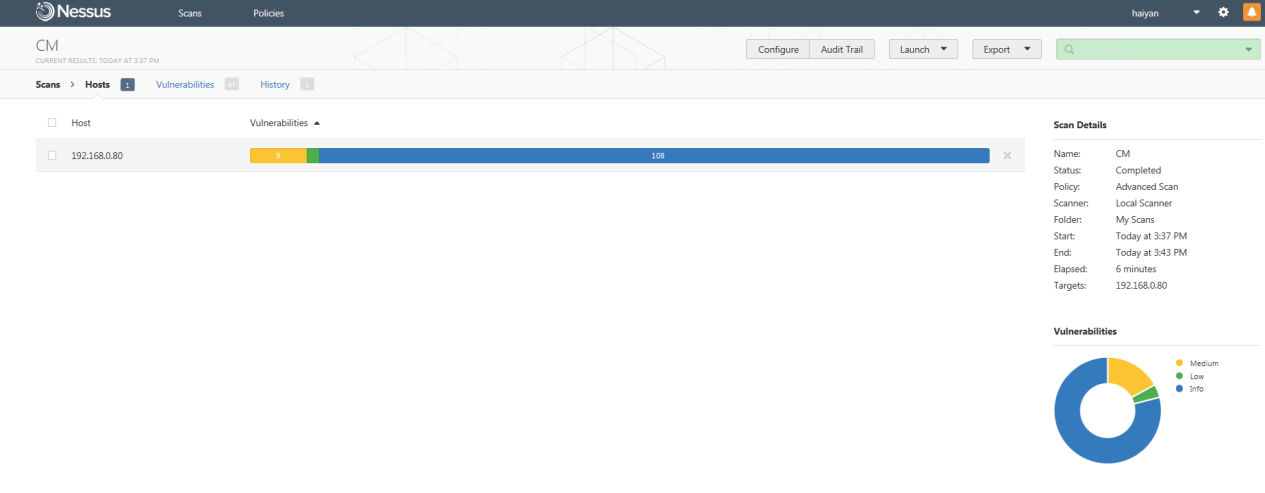


设置好后可以先点Save保存待运行，也可以点Launch直接扫描，保存后状态为On Demand

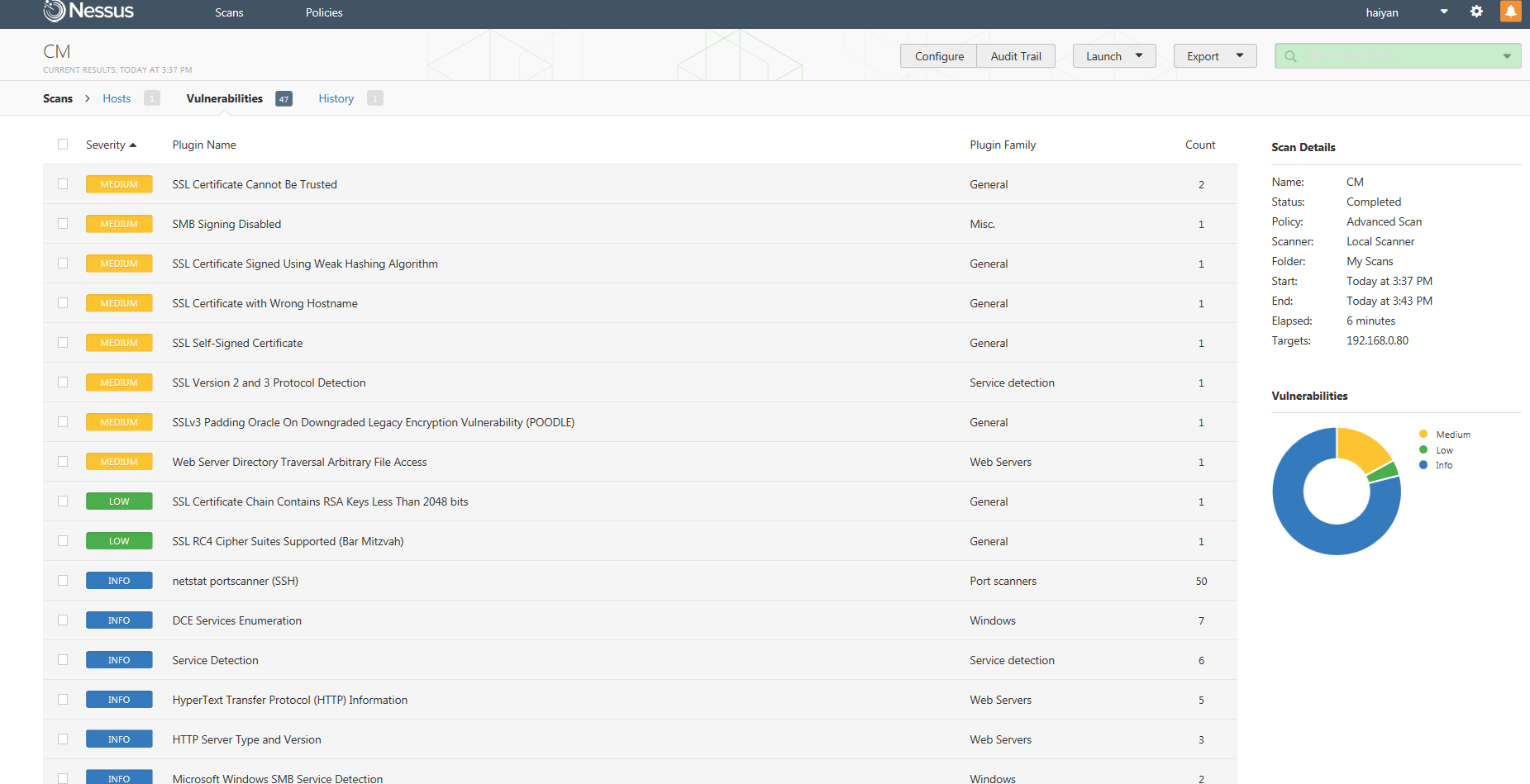


1. 报告

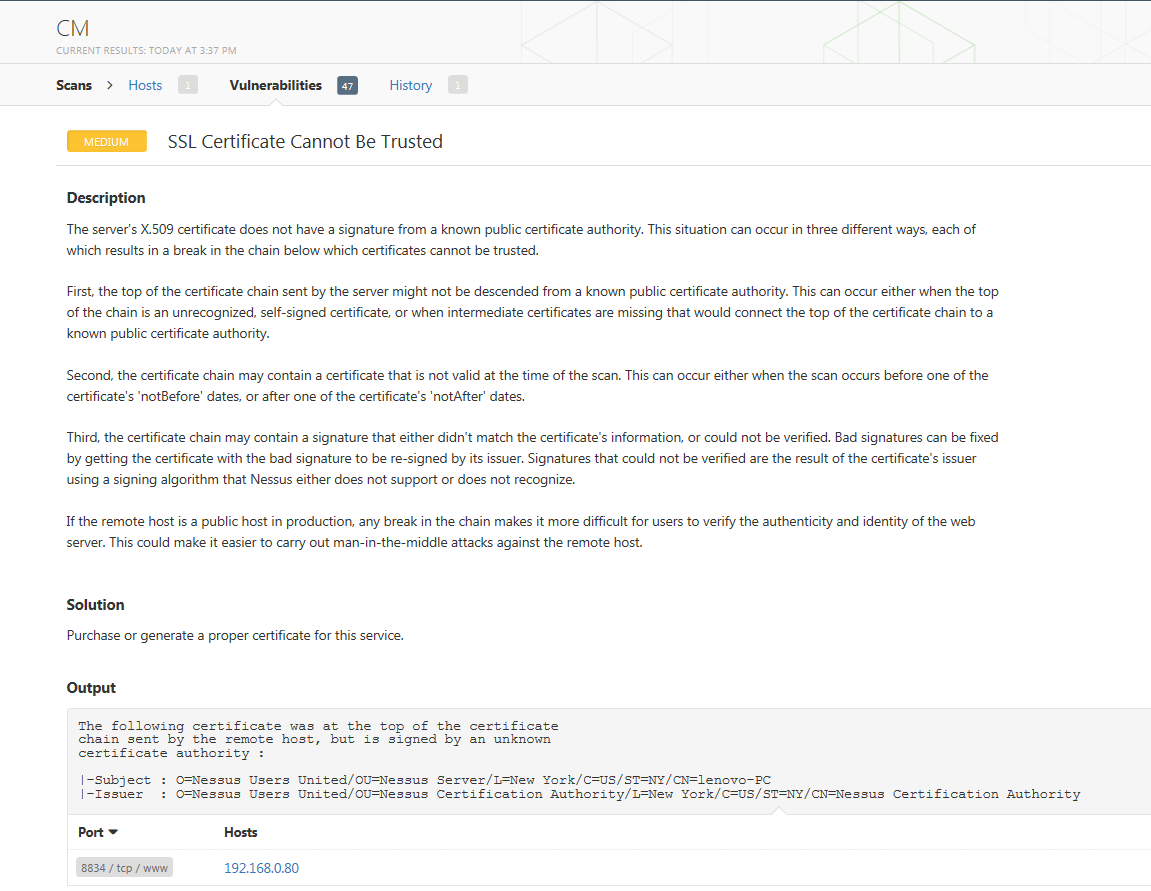
按照以上配置好，等待扫描器完成扫描后，就可以查看报告了，生成下图的报告



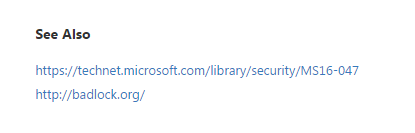
点击Vulnerabilities（脆弱性），可以查看本次扫描得出的所有漏洞概要，一共分为三种，严重，中危，低危，下图只有中危和低危的



点击单个漏洞可以看到详细信息，根据相应提示进行修复。



在see also中可以看到相关厂商的链接，可通过这些链接找到相应的补丁程序



扫描结束，点击右上角Export可将扫描结果导出为HTML文件。

