

漏洞扫描利器之 Nessus 实验指导书

一、 实验说明

【实验目的】

- 理解漏洞扫描的原理
- 掌握漏洞扫描的基本方法
- 了解漏洞信息分析的基本方法

【实验内容】

- Nessus 安装及配置
- Nessus 漏洞扫描
- Nessus 扫描结果初步分析

【实验环境】

- 学生机：Windows 系统
- 扫描目标：自选适当目标系统

【下载地址】

Nessus 的官方地址为：

<https://www.tenable.com/downloads/nessus>

可以根据运行环境选择适当的版本下载。

下载 Nessus 需要一定的时间，建议提前做好准备。

二、 Nessus 简介

Nessus 是一款得到全球超过 30000 余家企业信赖的信息系统漏洞扫描产品，在全球得到最为广泛的部署，是漏洞评估行业的黄金标准。

Nessus 采用插件技术，可以快速的将新发现的漏洞信息加入到

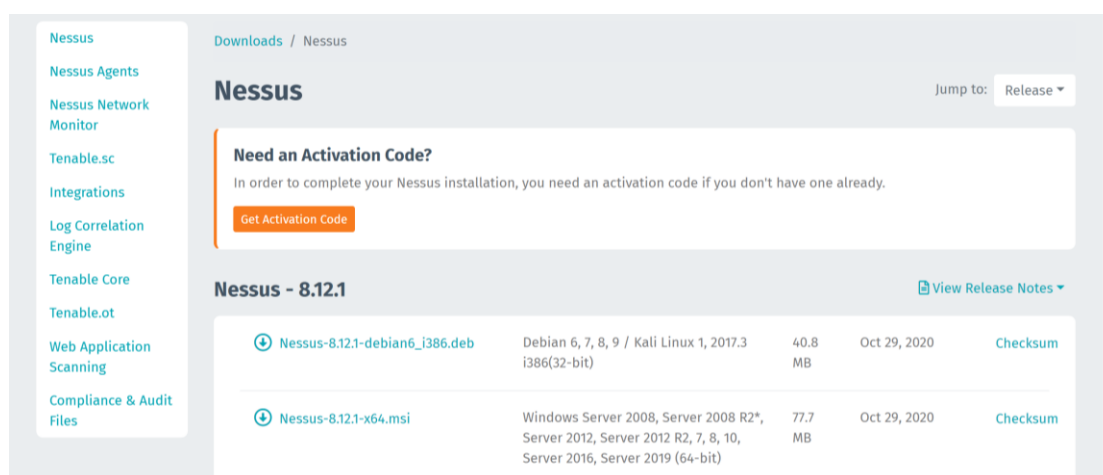
漏洞数据库中,从而减少“零日攻击”可能带来的威胁和造成的损失。

Nessus 分为基础版 (Nessus Essentials) 和专业版 (Nessus Professional)。其中,基础版主要面向教育领域的免费版本,拥有专业版绝大部分的扫描功能,但在一个周期(90 天)内只能最多扫描 16 个不同的 IP 地址。

三、 实验过程

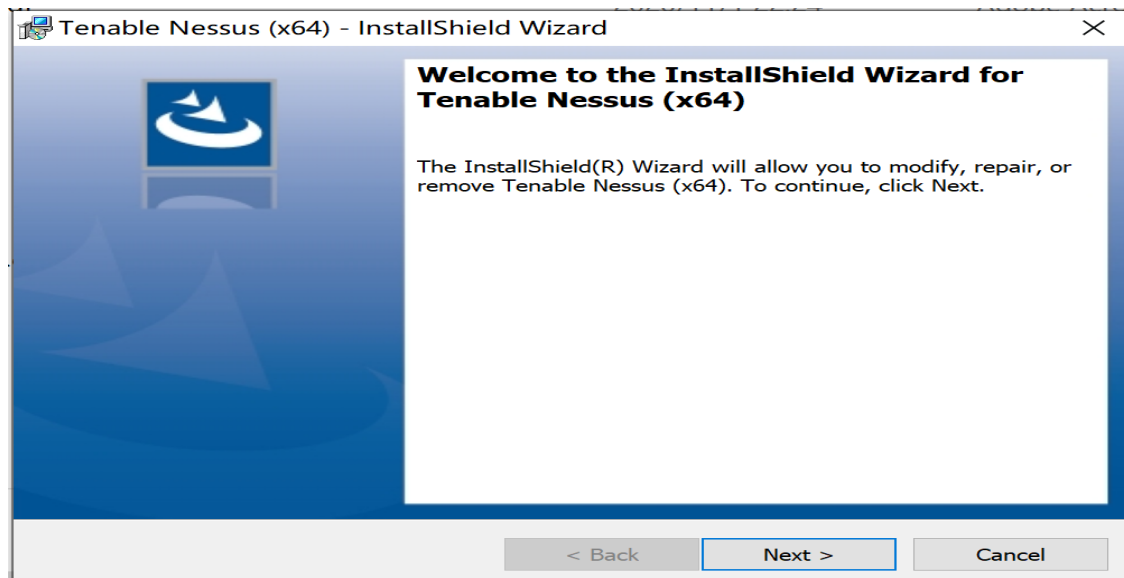
1、 Nessus 安装和初始化

下图为获取激活码和选择适应版本的页面。

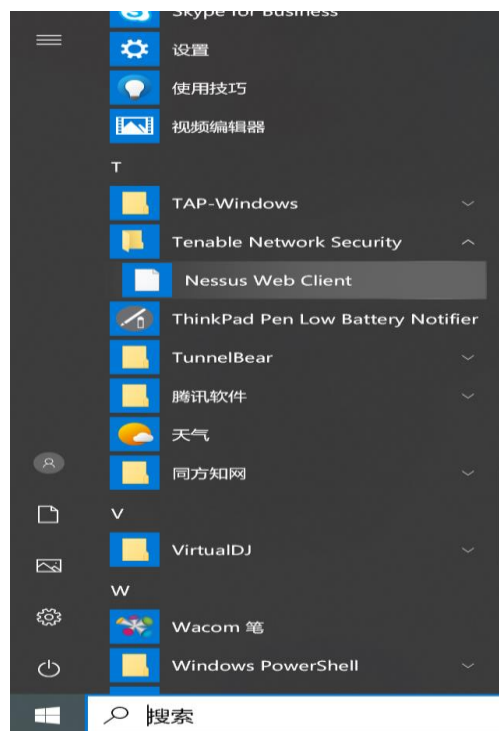


激活码可以在这里获取或者在安装完成后再获取。

安装过程非常简单,基本只要点击“下一步”即可。



安装完成后在开始菜单中就会出现一个“Tenable Network Security”的项目，并且在其下有一个称为”Nessus WEB Client“的子项目。



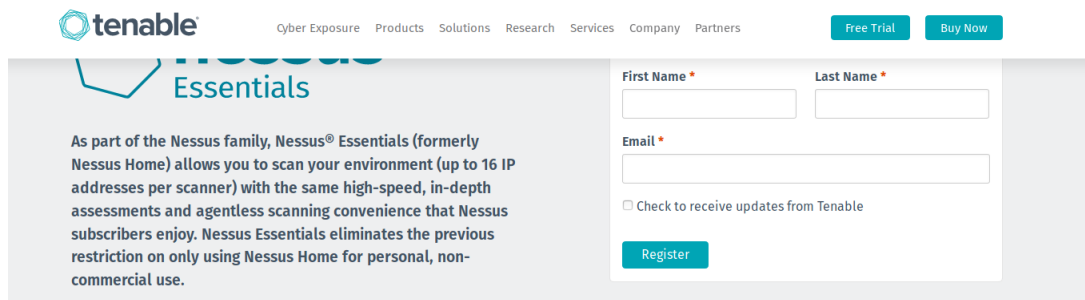
点击“Nessus Web Client”即可启动 Nessus 的界面。

首次登录，将进入用户名和密码创建过程。然后，需要输入激活码。

获取激活码需要一个真实邮箱地址

获取激活码的地址：

<https://www.tenable.com/products/nessus/nessus-essentials>



tenable Cyber Exposure Products Solutions Research Services Company Partners [Free Trial](#) [Buy Now](#)

Essentials

As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy. Nessus Essentials eliminates the previous restriction on only using Nessus Home for personal, non-commercial use.

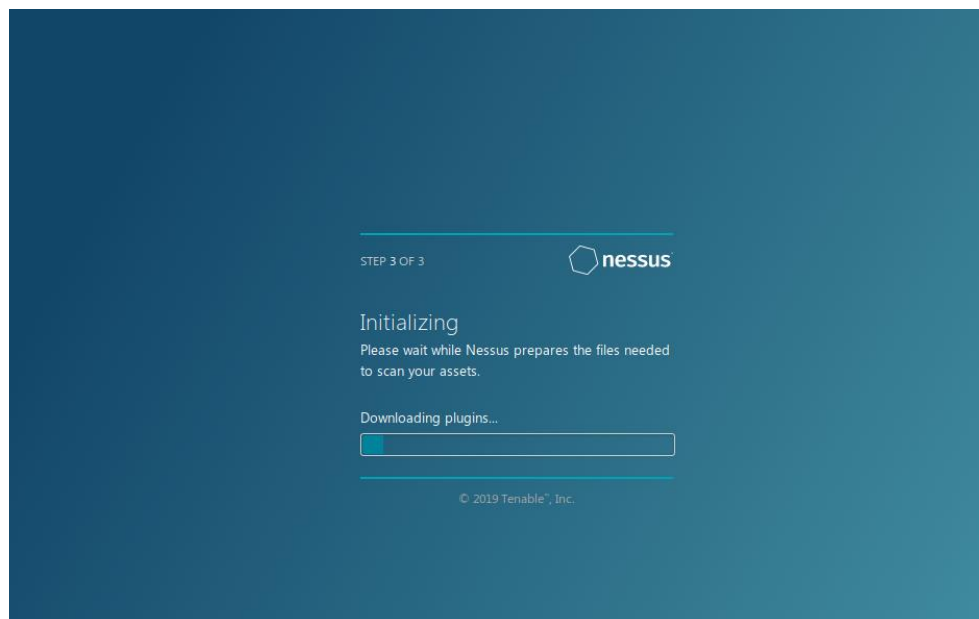
First Name * Last Name *

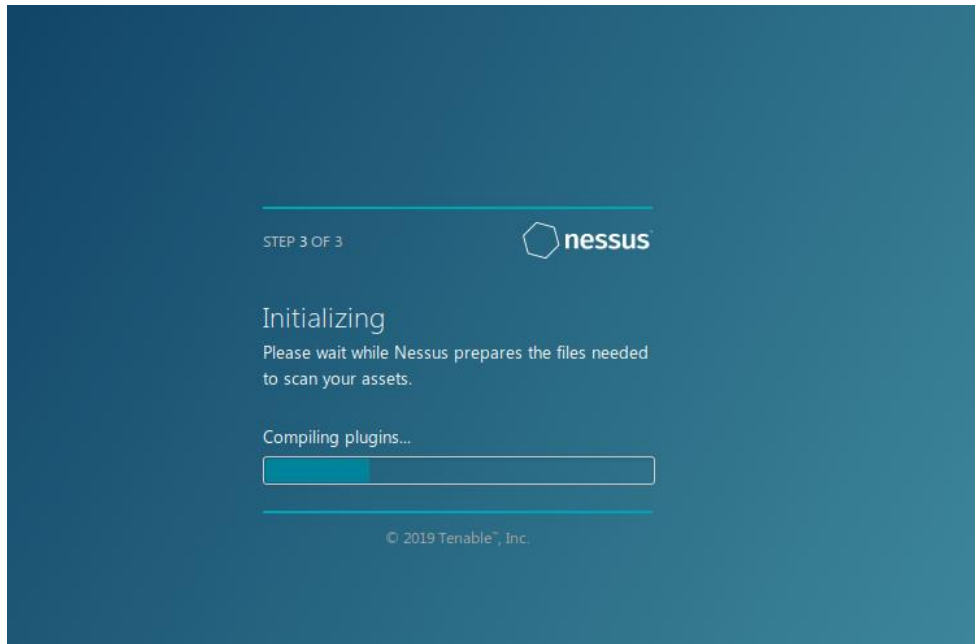
Email *

☐ Check to receive updates from Tenable

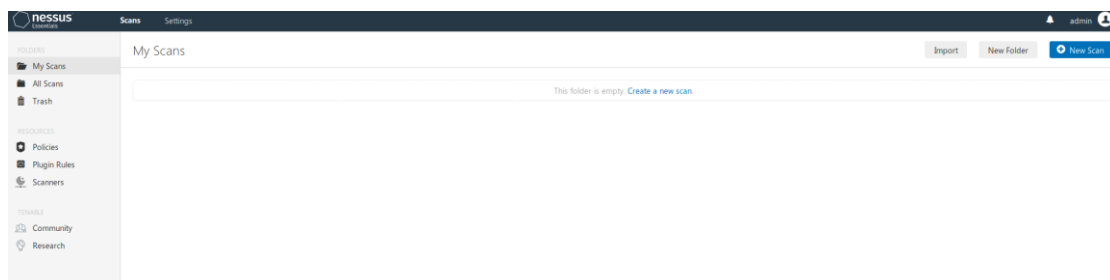
[Register](#)

从邮件中得到激活码激活, 然后下一步, 进入插件下载和进一步安装过程。

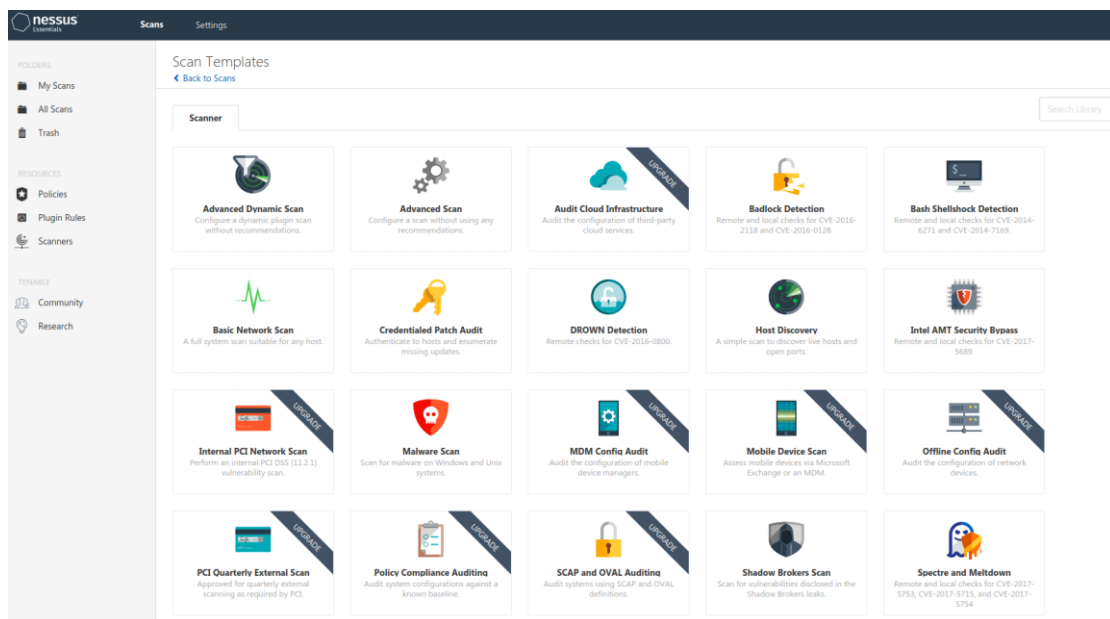




全部安装完成后，即可进入 Nessus 界面。



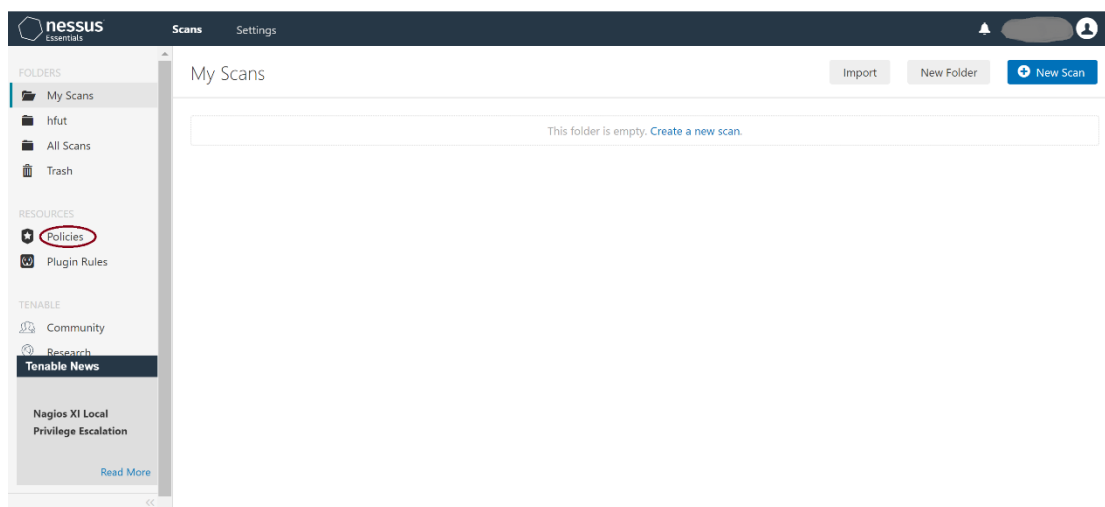
点击“New Scan”即进入新扫描模板。



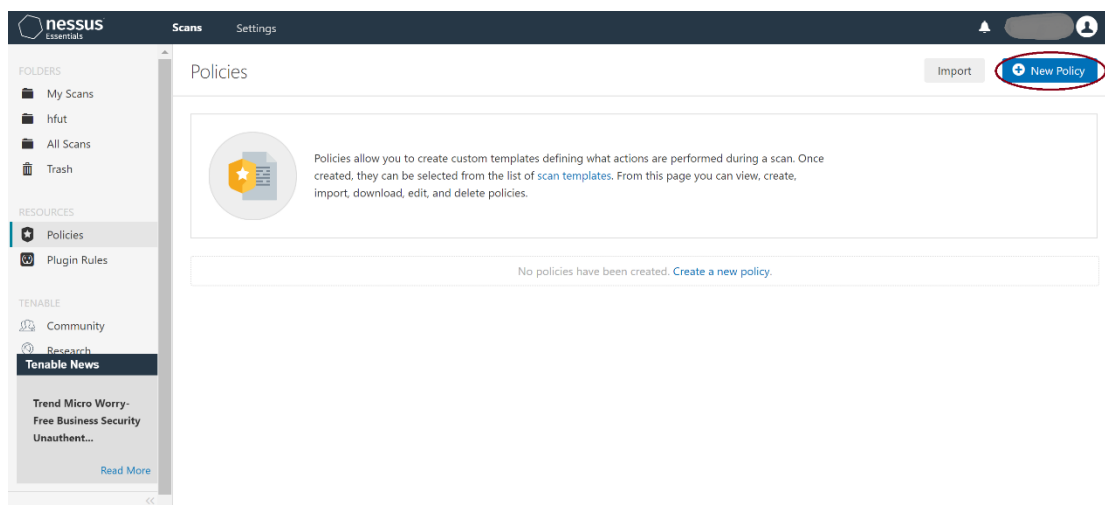
至此，Nessus 的安装和初始化过程全部完成。

2、 制定扫描策略

(1) 选择页面左边菜单栏中的 Policies



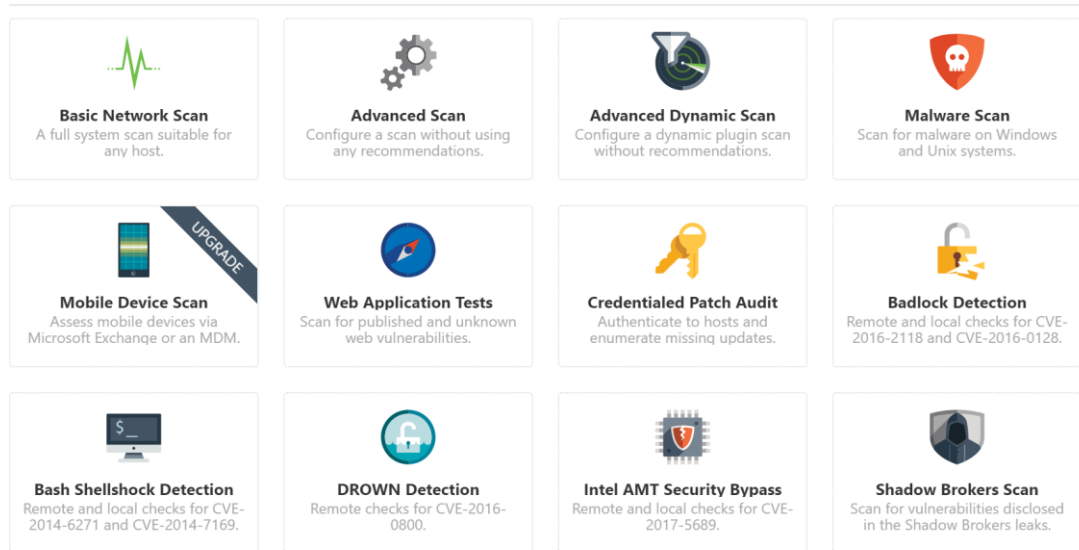
(2) 选择新的扫描策略—New Policy



(3) 选择策略模板

Nessus 有多种不同的模板,如扫描活跃主机的 Discovery 模板、扫描漏洞的 Vulnerabilities 模板等。本次实验针对的是漏洞扫描,所以就在 Vulnerability 模板中选择。

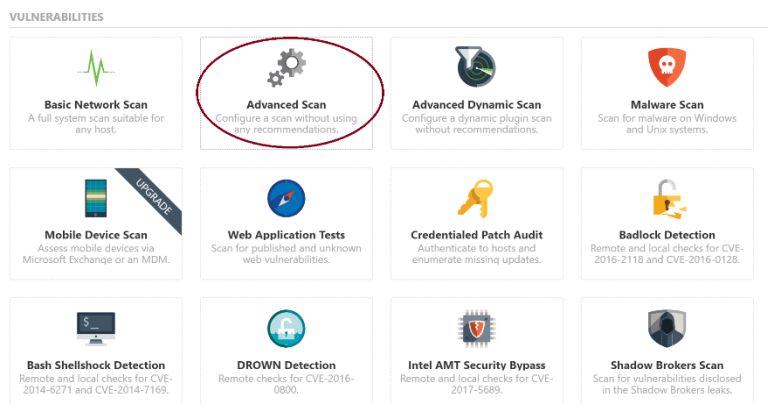
VULNERABILITIES



其中，Basic Network Scan 模板的策略，Advanced Scan 是高级扫描策略，Malware 是恶意代码扫描，Web Application Tests 是 WEB 应用安全扫描等。

可以根据需要分别对不同模板的扫描策略进行编辑，使扫描更具针对性。下面以 Advanced Scan 模板为例，说明扫描策略的配置过程。此配置过程也可以从 Basic Network Scan 模板的用户自定义入口进入。

● 选择 Advance scan



● 给策略起名并设定目标

New Policy / Advanced Scan

[Back to Policy Templates](#)

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

My policy

find Vulnerability

Save

Cancel

在 BASIC 中需要填写策略的名字，一般用英文。Description 可以省略；Discovery 里面有主机发现、端口扫描和服务发现等功能，可以在其中选择不同的发现方法；Assessment 里面有一些攻击性的设定；Report 里面是报告的一些设定；Advanced 里面是一些超时、每秒扫描多少项等基础设定，一般来说这里默认就好。本实验主要来设定“plugins”。

New Policy / Advanced Scan

Disable All

Enable All

[Back to Policy Templates](#)

Settings

Credentials

Plugins

Show Enabled

Show All

STATUS	PLUGIN FAMILY	TOTAL
ENABLED	AIX Local Security Checks	11381
ENABLED	Amazon Linux Local Security Checks	1806
ENABLED	Backdoors	121
ENABLED	CentOS Local Security Checks	3185
ENABLED	CGI abuses	4408
ENABLED	CGI abuses : XSS	687
ENABLED	CISCO	1715
ENABLED	Databases	711

STATUS	PLUGIN NAME	PLUGIN ID
	No plugin family selected.	

Save

Cancel

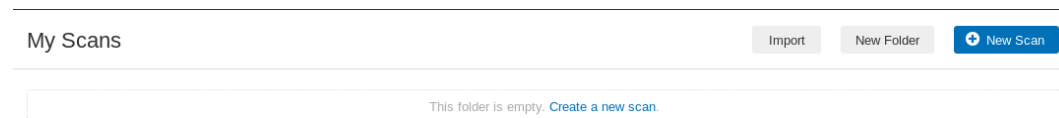
Plugins 里面就是具体的策略，里面有父策略，具体的父策略下面还有子策略，把这些策略制定得体的话，使用者可以更加有针对性

的进行扫描。

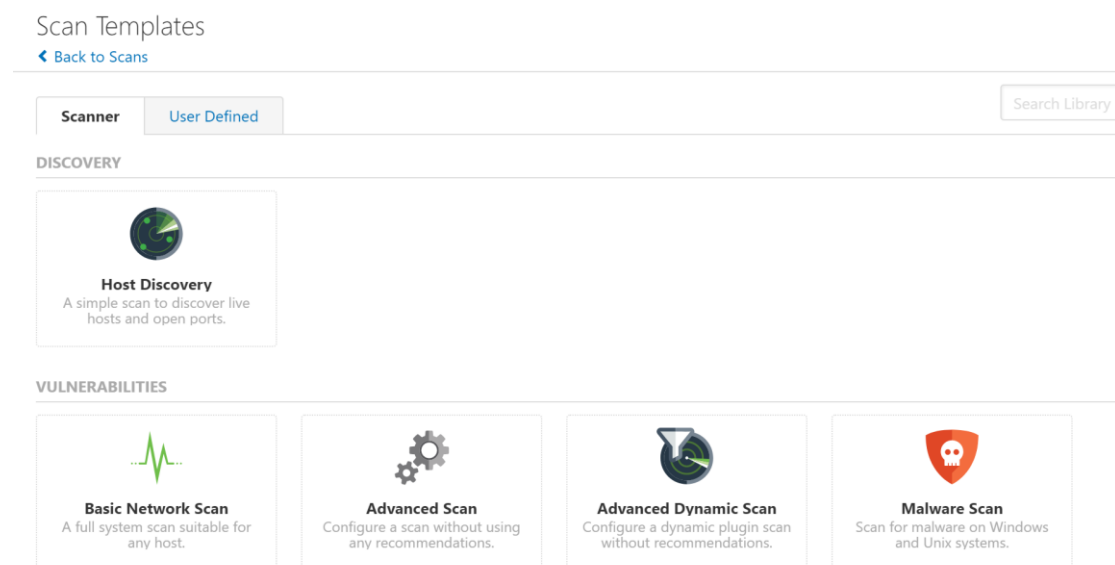
策略很多，我们需要有针对性的进行筛选，筛选后“save”，策略制定完成。

3、 制定任务

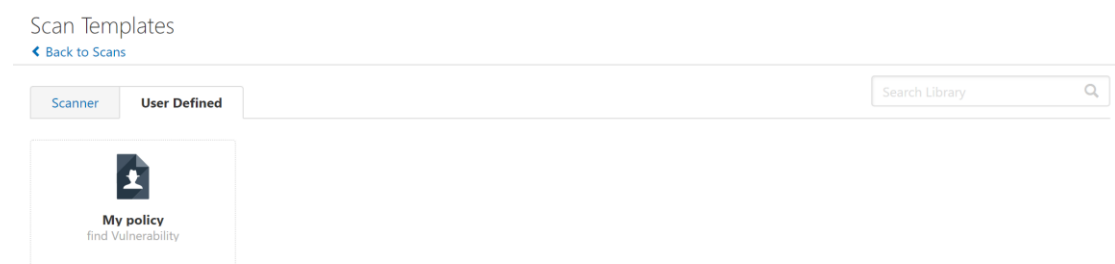
(1) 选择 My scan 中的 new scan



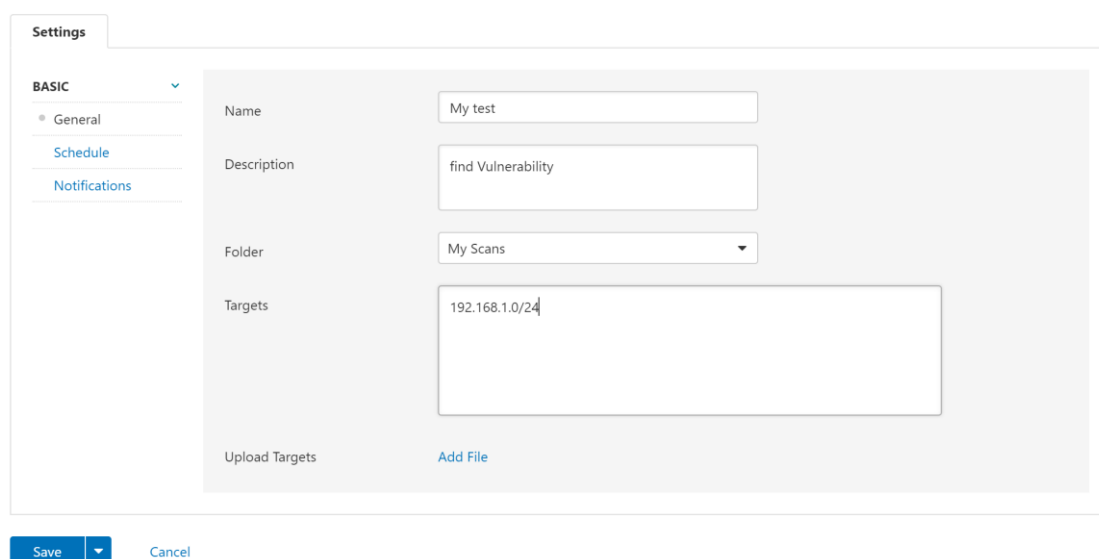
(2) 选择 User Defined



(3) 选择 user defined 之后可看到之前制定好的策略就在其中，选择即可。



(4) 打开进入任务配置页面，如图



名字为 My test，目标为寻找漏洞，目标网络为内网 ip 网段：
192.168.1.0/24

然后点击 save

4、 执行任务



My Scans			Import	New Folder	New Scan
Search Scans			1 Scans		
<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	My test	On Demand	N/A	▶	×

点击任务上的三角形符号，任务开始执行。



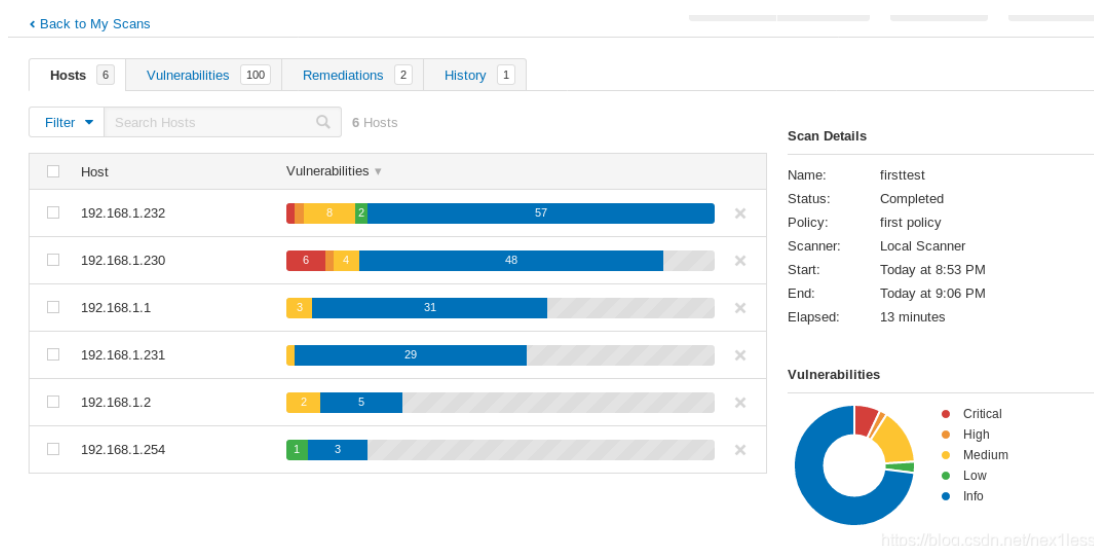
My Scans			Import	New Folder	New Scan
Search Scans			1 Scans		
<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	My test	On Demand	Today at 10:05 PM		■

扫描的时间长度取决于制定的策略。

5、 扫描结束，记录与分析漏洞

扫描完成后会有类似如下图所示的报告输出。其中：

- IP 地址是属于扫描范围内的在线的主机，并且按照发现漏洞的数量和严重程度的综合排序。Nessus 用不同颜色代表漏洞的危险程度，颜色中的数字代表发现了几个相同威胁等级的漏洞。
- 红色代表为发现致命漏洞
- 橙色代表高危等级漏洞
- 黄色代表中等威胁等级漏洞
- 绿色代表低威胁等级漏洞
- 蓝色代表有警告信息



由上图可见，在这个网络中的各个设备中存在大量漏洞，并按漏洞级别做出了分类，我们还可以点击上方的“vulnerabilities”，去查看漏洞详细信息等，也可以做成报告，方便下一步计划的实施。

四、 实验要求

1、 扫描目标

自主选择非敏感目标，如学校、商业机构等，严禁对党政军及司

法机构进行扫描。

选择时需注意目标不宜过大，否则会消耗很多时间。

2、 扫描策略

分别用两个不同策略对同一目标进行扫描，其中 Advanced Scan 为必选，另外一个从 Malware Scan 和 Web Application Tests 中任选。多选不限。

3、 结果分析

对扫描结果中的中等以上等级危险漏洞试着进行初步分析，包括出现漏洞的位置、造成漏洞的原因、漏洞利用途径、补救措施等。