

信息安全
技术大讲堂

从实践中学习

Metasploit 5 渗透测试

机械工业出版社
China Machine Press



信息安全
技术大讲堂

从实践中学习 Metasploit 5 渗透测试

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解网络扫描的相关知识
通过128个操作实例手把手带领读者从实践中学习网络扫描
从协议工作原理到应用方式，再到扫描策略，逐步讲解

机械工业出版社
China Machine Press

从实践中学习 Metasploit 5 渗透测试

大学霸 IT 达人 编著

书号：978-7-111-63085-2

本书涉及的工具和软件需要读者自行下载。下载途径有以下几种：

- (1) 根据图书对应章节给出网址，自行下载。
- (2) 加入技术讨论 QQ 群（343867787），获取工具。

2.1.1 安装并激活 Nessus


Nessus 工具默认没有安装在任何系统中。所以，如果要使用该工具，则需要先安装才可以。在安装 Nessus 工具之前，首先要获取该工具的安装包。而且，Nessus 工具安装后，必须要激活才可使用。所以，下面将分别介绍安装并激活 Nessus 的方法。

1. 获取 Nessus 安装包

在大部分系统中，都没有自带 Nessus 的安装包。所以，如果要安装该工具，则需要先到其官方网站获取软件包。其中，Nessus 的官方下载地址是：

<http://www.tenable.com/products/nessus/select-your-operating-system>

在浏览器中输入以上地址，将打开如图 2.1 所示的界面。

Nessus - 8.5.1 

Release Date
07/02/2019

Release Notes:
Nessus 8.5.1













Name	Description	Details
 Nessus-8.5.1-Win32.msi	Windows 7, 8, 10 (32-bit)	Checksum
 Nessus-8.5.1.dmg	macOS (10.8 - 10.14)	Checksum
 Nessus-8.5.1-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	Checksum
 Nessus-8.5.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	Checksum
 Nessus-8.5.1-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	Checksum
 Nessus-8.5.1-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
 Nessus-8.5.1-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
 Nessus-8.5.1-es6.i386.rpm	Red Hat ES 6 i386(32-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	Checksum
 Nessus-8.5.1-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	Checksum
 Nessus-8.5.1-fc20.x86_64.rpm	Fedora 20, 21, 25, 26, 27 (64-bit)	Checksum
 Nessus-8.5.1-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	Checksum
 Nessus-8.5.1-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	Checksum

图 2.1 下载 Nessus 软件包

从该界面可以看到，官网提供了 Nessus 工具各种平台的安装包，如 Windows、Mac OS X、Linux、FreeBSD 等。用户可以根据自己的操作系统及架构，选择对应的安装包。例如，选择下载 Debian x64 架构的安装包。在 Name 列单击对应的包，即 Nessus-8.5.1-debian6_amd64.deb 包，将显示接受许可协议界面，如图 2.2 所示。

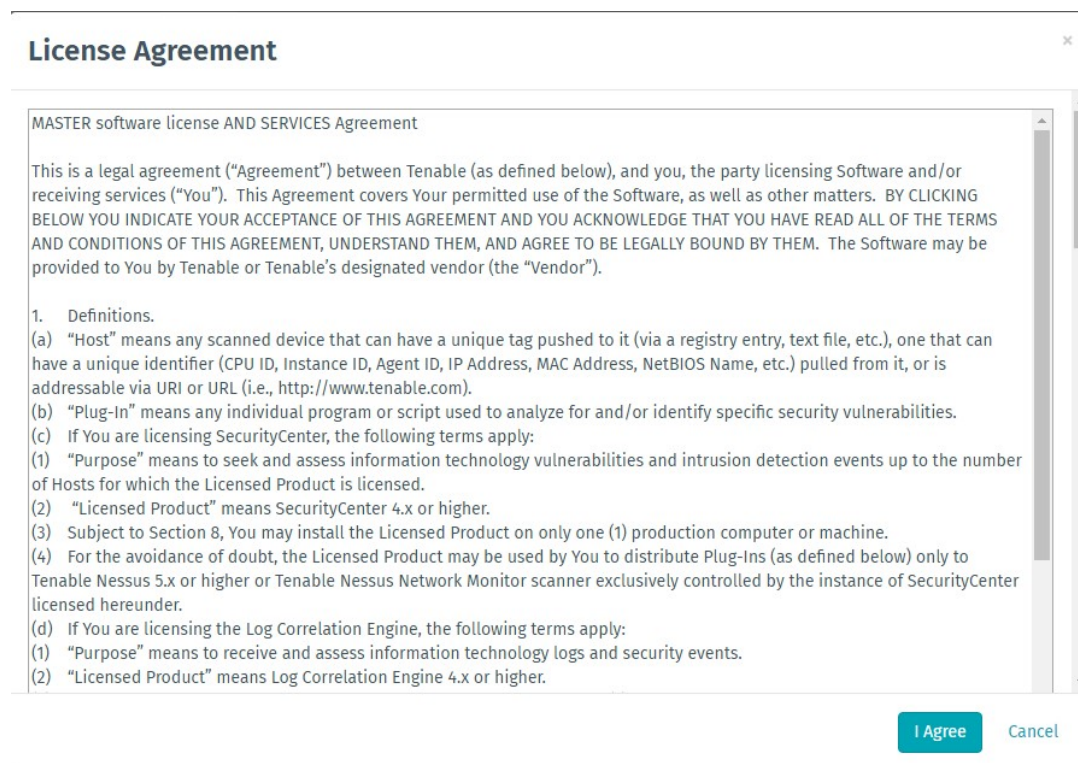


图 2.2 许可证协议对话框

该界面显示了下载 Nessus 软件包的许可证协议信息。这里单击 I Agree 按钮，将开始下载。

2. 安装 Nessus

【示例 2-1】下面将以 Kali Linux 为例，介绍在 Linux 下安装 Nessus 工具的方法。具体操作步骤如下所示：

(1) 从官网下载安装包。本例中下载的安装包文件名为 Nessus-8.5.1-debian6_amd64.deb。

(2) 将下载的安装包复制到 Kali 中，本例中复制到/root 下。接下来，就可以安装 Nessus 工具了。

执行命令如下所示：

```
root@daxueba:~# dpkg -i Nessus-8.5.1-debian6_amd64.deb
正在选中未选择的软件包 nessus。
(正在读取数据库 ... 系统当前共安装有 327450 个文件和目录。)
```

```
正准备解包 Nessus-8.5.1-debian6_amd64.deb ...
正在解包 nessus (8.5.1) ...
正在设置 nessus (8.5.1) ...
Unpacking Nessus Core Components...
- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://daxueba:8834/ to configure your scanner
正在处理用于 systemd (232-22) 的触发器 ..
```

看到输出以上类似信息，则表示 Nessus 工具安装完成。接下来，用户在浏览器的地址栏中输入 https://daxueba:8834/ 或 https://IP:8834，即可访问 Nessus 服务。

提示：在 Linux 系统中，Nessus 工具默认安装在 /opt/nessus 目录中。

3. 激活 Nessus

在使用 Nessus 之前，必须先激活该服务才可使用。如果要激活 Nessus 服务，则需要到官网获取一个激活码。下面将介绍获取激活码的方法。具体操作步骤如下所示：

(1) 在浏览器中输入以下地址：

<http://www.nessus.org/products/nessus/nessus-plugins/obtain-an-activation-code>

成功访问以上链接后，将打开如图 2.3 所示的界面。

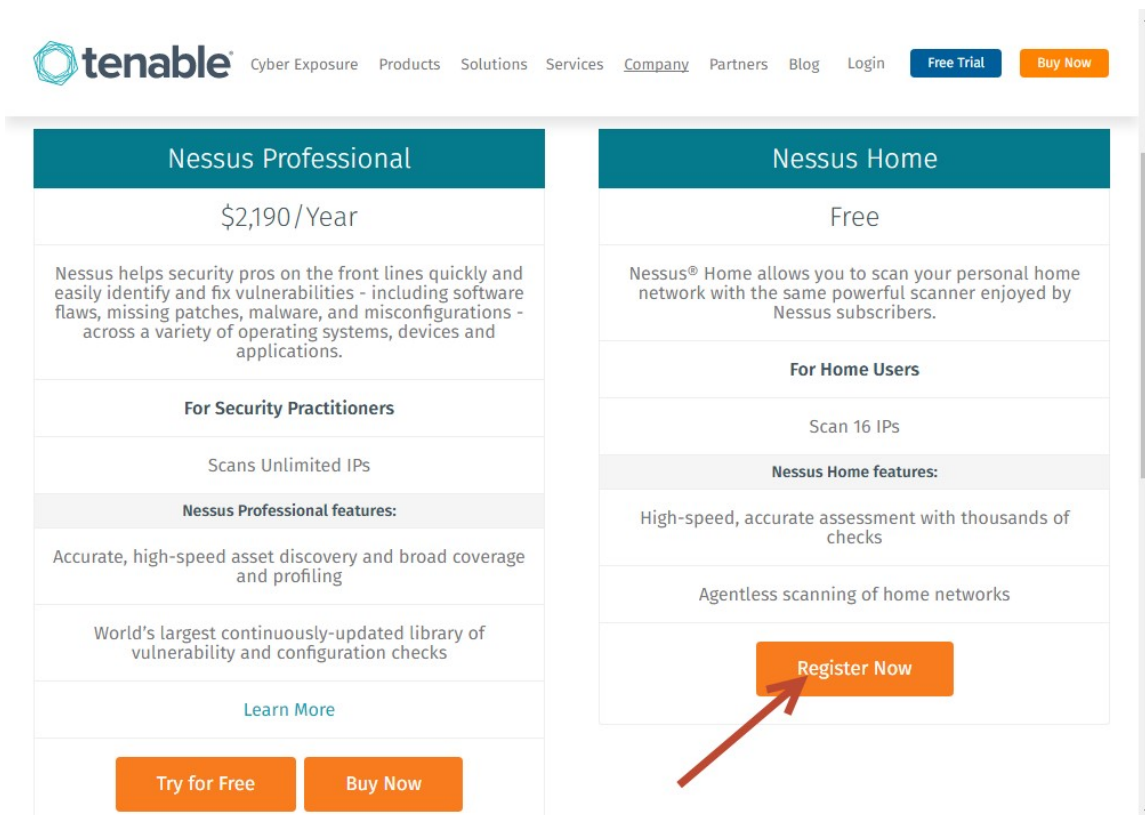


图 2.3 获取激活码

(2) 在该界面单击 Nessus Home Free 下面的 Register Now 按钮，将显示如图 2.4 所示的界面。

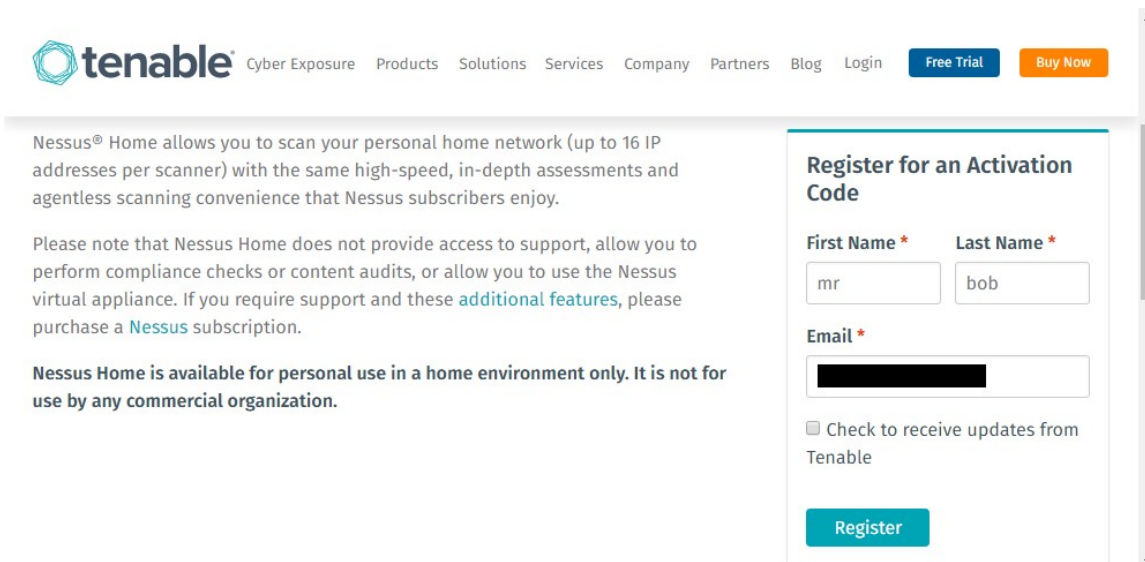


图 2.4 注册信息

(3) 在该界面填写一些信息，为了获取激活码。在该界面 First Name 和 Last Name 文本框中，用

户可以任意填写。但是，Email 下的文本框必须填写一个合法的邮件地址，用来获取邮件。当以上信息设置完成后，单击 Register 按钮。接下来，将会在注册的邮箱中收到一份关于 Nessus 的邮件。进入邮箱打开收到的邮件，将会看到一串数字，类似 XXXX-XXXX-XXXX-XXXX，即激活码。

(4) 当成功安装 Nessus 工具后，就可以使用以上获取到的激活码来激活该服务了。

提示：从 Nessus 8.5.0 开始，用户在配置 Nessus 时，可以直接对该服务进行激活。所以，用户不提前获取激活码也可以。

2.1.2 登录及配置 Nessus

当安装成功 Nessus 工具后，即可远程登录该服务，并且使用它实施漏洞扫描。但是，在实施漏洞扫描之前，还需要进行简单的配置，如创建策略和扫描任务等。下面将介绍登录及配置 Nessus 的方法。

1. 登录 Nessus 服务

在登录 Nessus 服务之前，首先需要确定该服务已经启动。否则，无法连接到该服务。默认情况下，安装该服务后是没有启动的。所以，用户需要先启动该服务。执行命令如下所示：

```
root@daxueba:~# /etc/init.d/nessusd start
```

Starting Nessus services:

[确定]

从输出的信息中，可以看到 Nessus 服务已经启动。接下来，用户就可以连接该服务了。

【实例 2-1】登录 Nessus 服务。具体操作步骤如下所示：

(1) 在浏览器的地址栏中输入 `https://IP:8834`，访问 Nessus 服务。在浏览器地址栏中输入对应地址后，将打开如图 2.5 所示的界面。

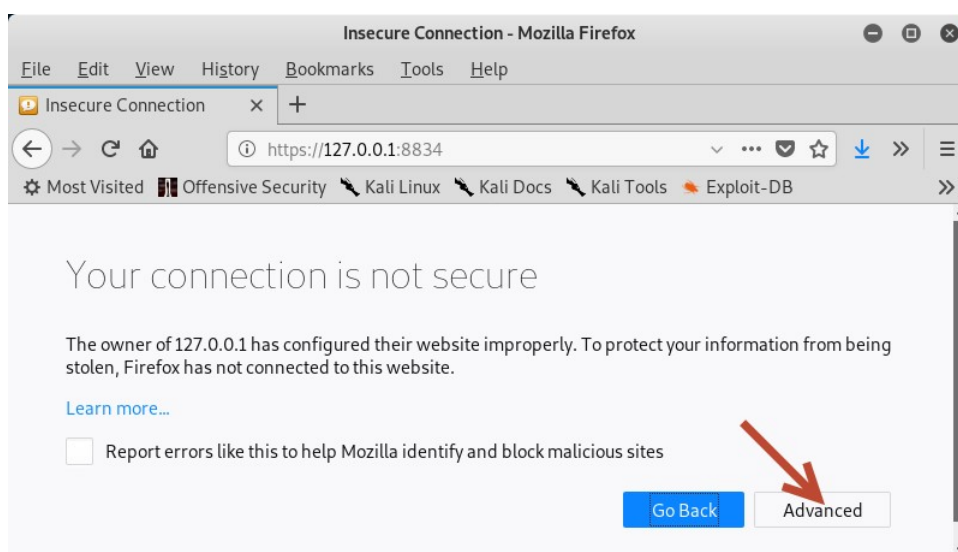


图 2.5 连接不受信任

注意：Nessus 服务使用的是 https 协议，而不是 http 协议。

(2) 在该界面显示该连接不受信任。这是因为 Nessus 是一个安全连接（HTTPS 协议），所以需要被信任后才允许登录。此时，在该界面单击 Advanced 按钮，将显示如图 2.6 所示的界面。

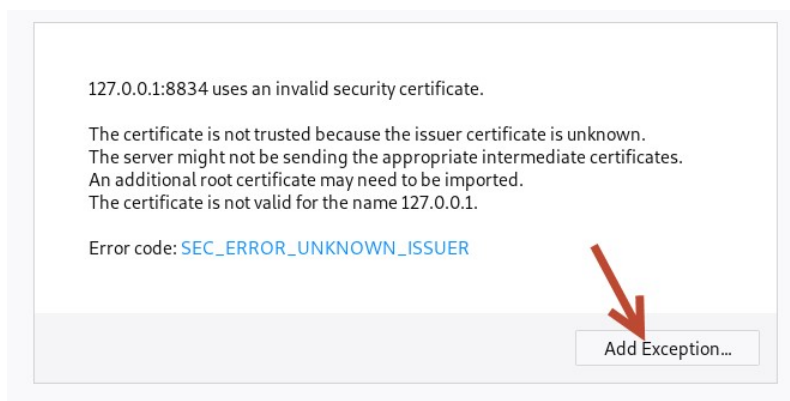


图 2.6 了解风险

(3) 该界面显示了该连接可能存在的风险。此时，单击 Add Exception...按钮，将显示如图 2.7 所示的界面。

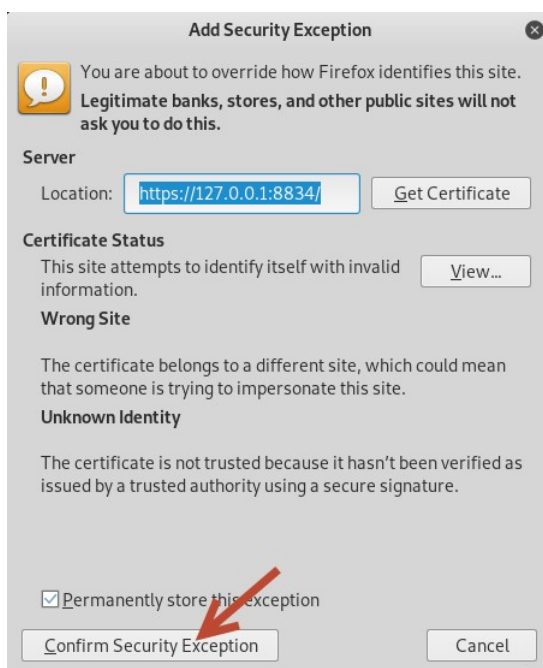


图 2.7 添加安全例外

(4) 在该界面单击 Confirm Security Exception 按钮，将显示如图 2.8 所示的界面。

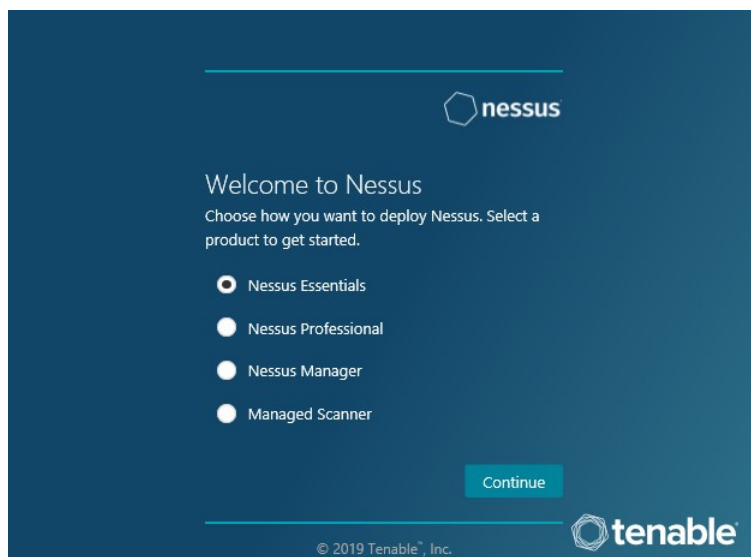


图 选择产品

(5) 该界面显示了 Nessus 的所有版本, 包括 Nessus Essentials (Nessus 免费版)、Nessus Professional (Nessus 专业版)、Nessus Manager (Nessus 管理台) 和 Managed Scanner (被管理的扫描者器)。这里将选择免费版, 即 Nessus Essentials, 并单击 Continue 按钮, 将显示如图所示的界面。

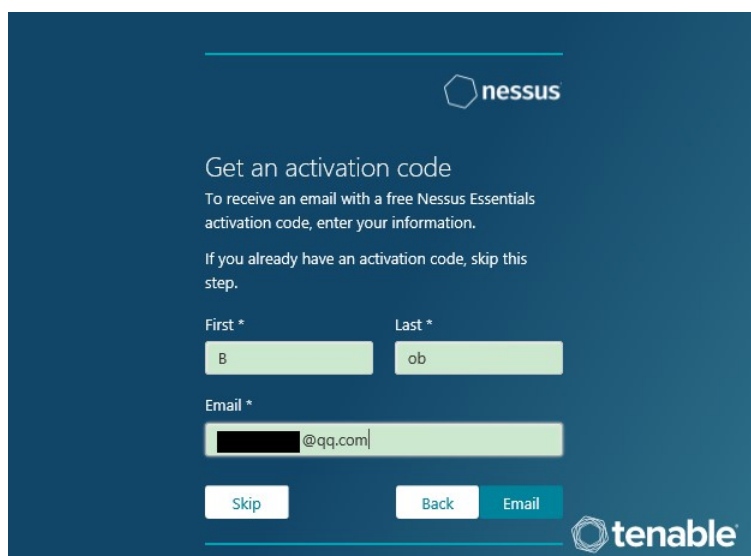


图 获取激活码

(6) 该界面用来获取激活码, 输入注册的信息。其中, 这里输入的 Email 地址必须是一个真实的邮件地址, 用来接收激活码。然后, 单击 Email 按钮, 将显示如图所示的界面。此时, 即可在指定的邮箱地址中收到获取的激活码。如果用户使用前面的方法已经获取到激活码的话, 直接单击 Skip 按钮, 跳过该步骤即可。

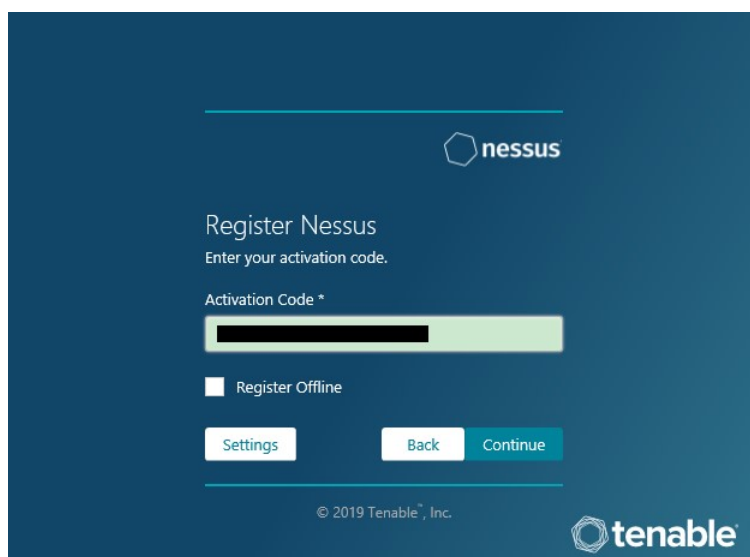


图 输入激活码

提示：在该界面用户可以提前进行一些高级设置，如代理服务器、提供插件的主机和主密码。单击 Settings 按钮，将显示高级设置界面，如图所示。

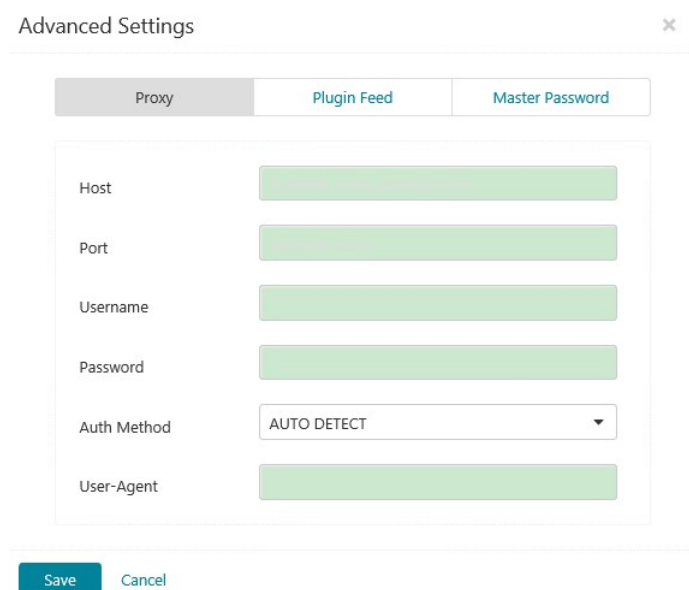


图 高级设置

从该界面可以看到包括三个选项卡，分别为 Proxy（代理服务器）、Plugin Feed（提供插件主机）和 Master Password（主密码）。用户通过选择不同的选项卡，即可进行对应的设置。设置完成后，单击 Save 按钮保存，将返回到图 1.18 所示的界面。其中，这些高级设置，成功登录 Nessus 服务器后也可以设置，将在后面讲解。

（7）在该界面输入前面获取到的激活码，并单击 Continue 按钮，将显示如图 7 所示的界面。

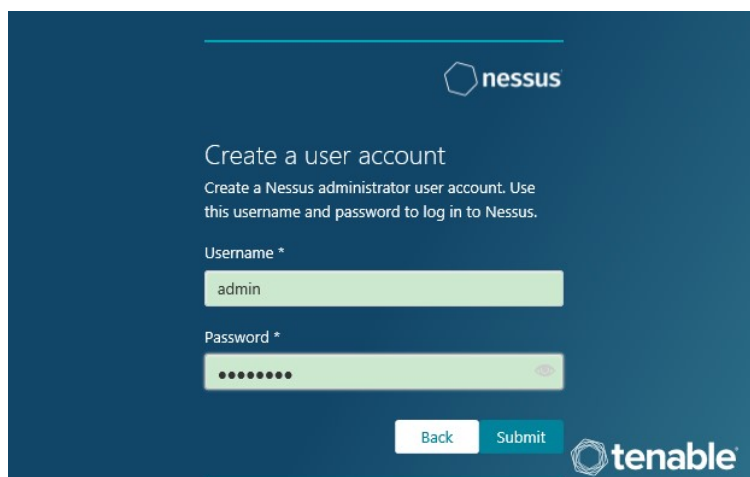


图 创建一个账户

（8）该界面要求创建一个账号，用于管理 Nessus 服务。这是因为第一次使用，目前还没有创建任何账号。在该界面创建一个用户账号，并设置密码。然后单击 **Submit** 按钮，将显示如图所示的界面。

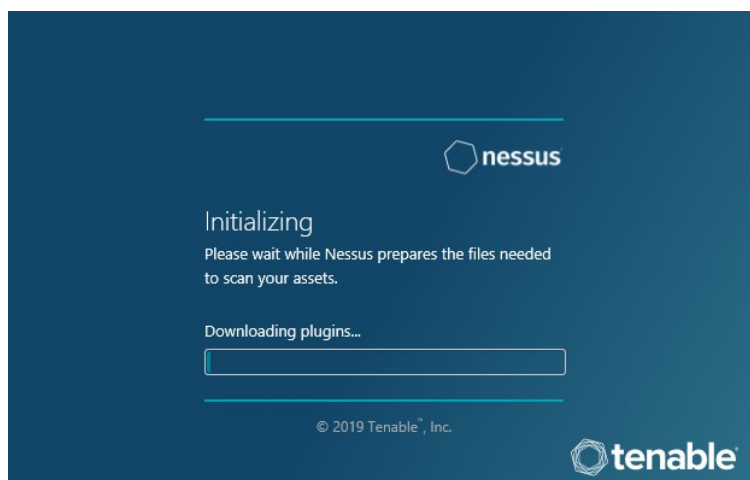


图 下载 Nessus 插件

（9）从该界面可以看到正在下载插件，并进行初始化。此过程，大概需要十分钟的时间。当初始化完成后，自动打开 Nessus 的主界面，如图 1.23 所示。

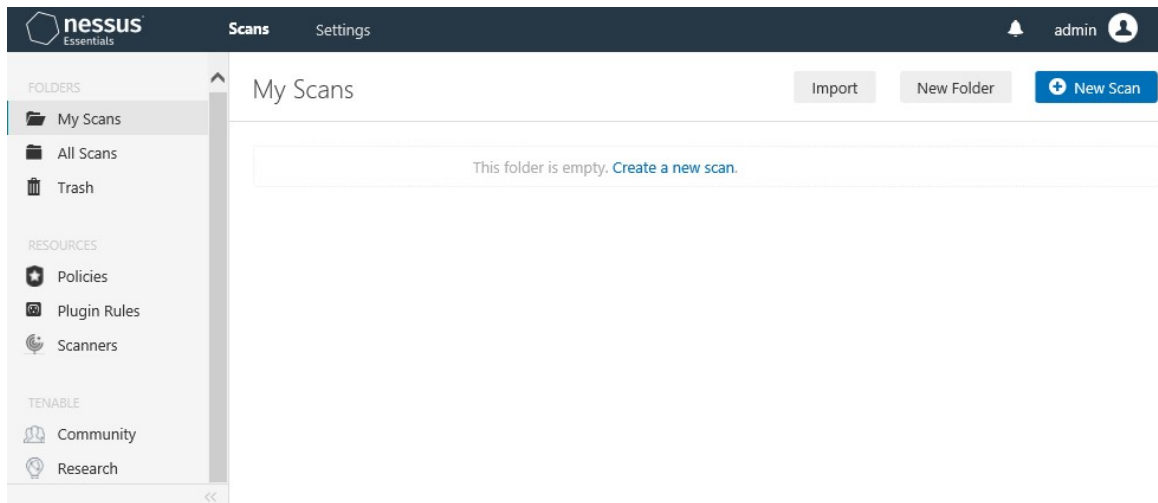


图 Nessus 的主界面

(10) 看到该界面，则表示已成功登录到 Nessus 服务。接下来，创建对应的策略和扫描任务即可对目标实施漏洞扫描。

2. 创建策略

策略简单的说就是使 Nessus 工具使用最佳化的配置，对目标主机进行扫描。所以，在实施扫描之前，创建策略也是非常重要的。Nessus 工具默认提供了 22 个扫描策略模板。如果用户希望重新定制的话，则可以创建新的策略。下面将介绍新建策略的方法。

【实例 2-2】创建策略。具体操作步骤如下所示：

(1) 在 Nessus 主界面的左侧栏中单击 Policies 命令，将显示如图 2.13 所示的界面。

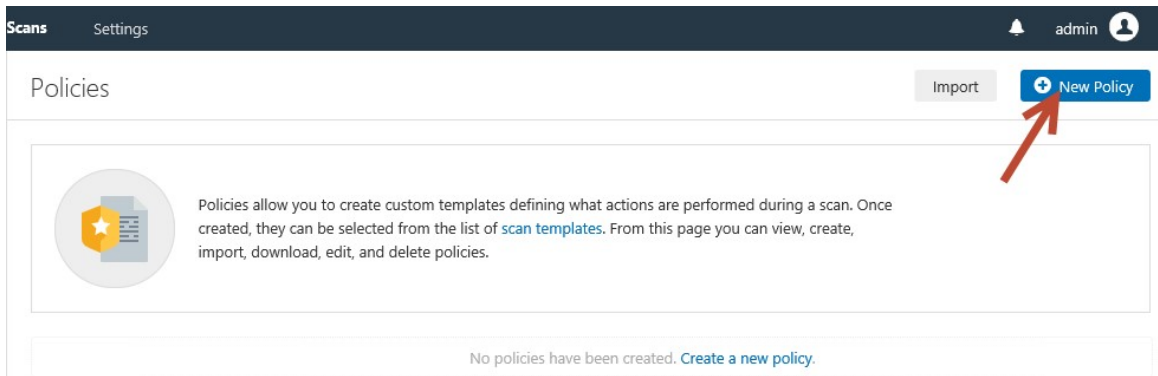


图 2.13 策略界面

(4) 在该界面单击右上角的 New Policy 按钮，将显示如图 2.14 所示的界面。

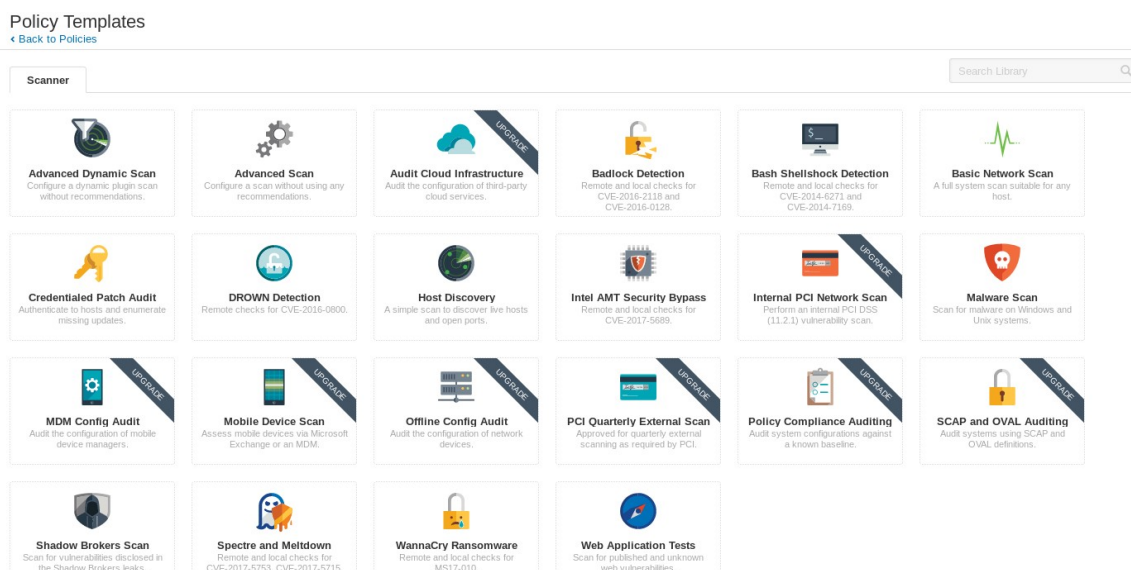


图 2.14 策略模板

(5) 从该界面可以看到所有的策略模板，用户可以选择任意一个模板类型来创建新的策略。其中，在图标中显示有 UPGRADE 信息的，表示家庭版不可以使用。这里选择 Advanced Scan 类型。单击该图标后，将显示如图 2.15 所示的界面。

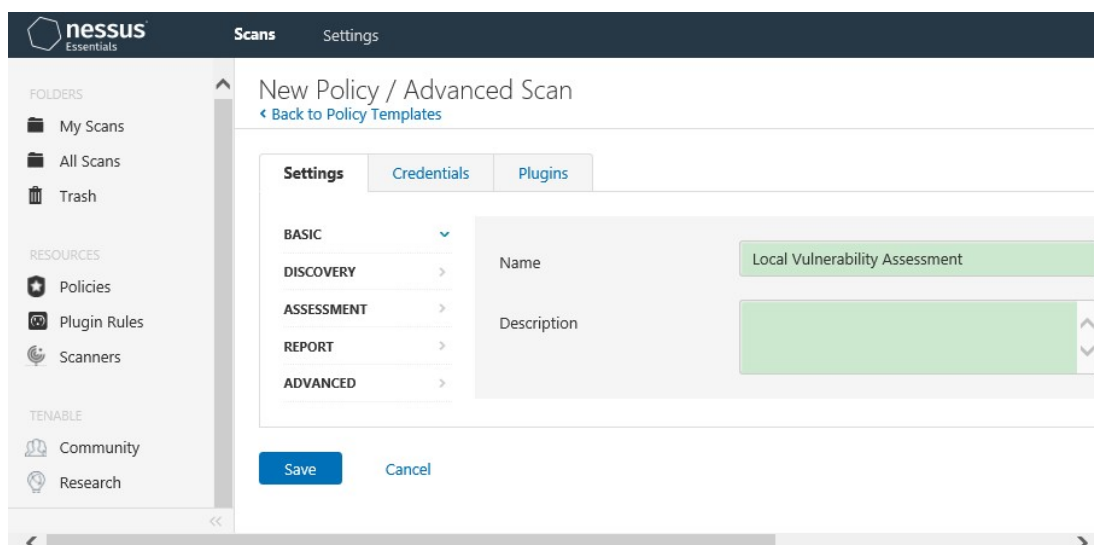


图 2.15 新建策略

(6) 在该界面设置策略名和描述信息（可选项）。这里设置策略名为 Local Vulnerability Assessment。然后单击 Plugins 标签，将显示如图 2.16 所示的界面。

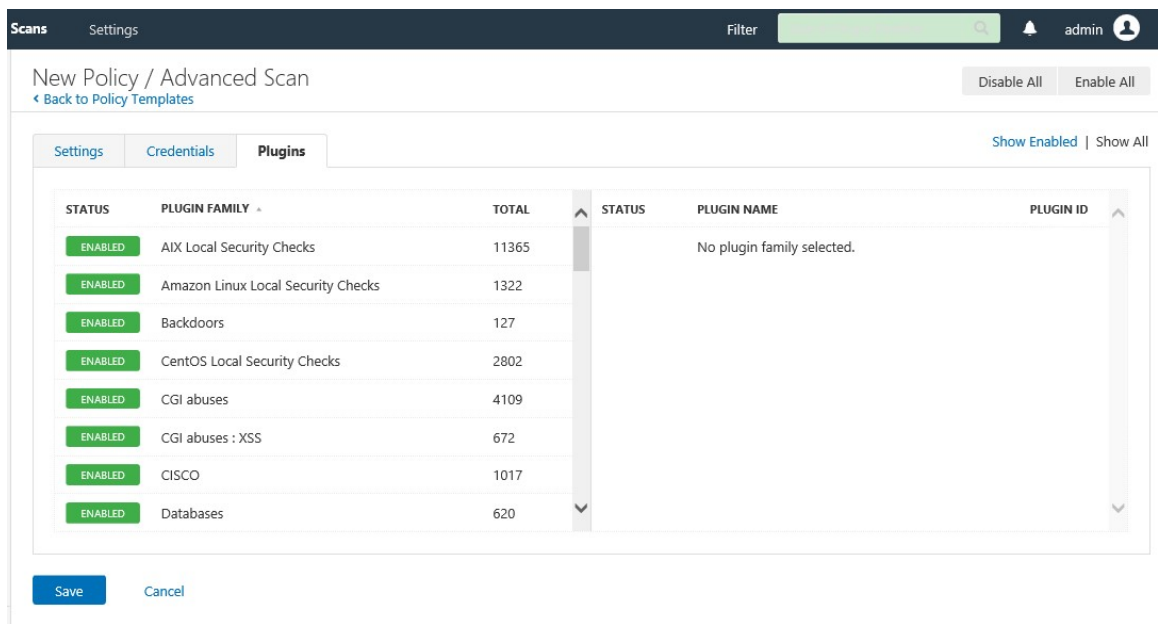


图 2.16 插件程序

(7) 该界面显示了所有插件程序，从该界面可以看到默认全部是启动的。在该界面可以单击 **Disable All** 按钮，禁用所有启动的插件程序。然后指定需要启动的插件程序，如启动 **Debian Local Security Checks** 和 **Default Unix Accounts** 插件程序，启动后显示效果如图 2.17 所示。

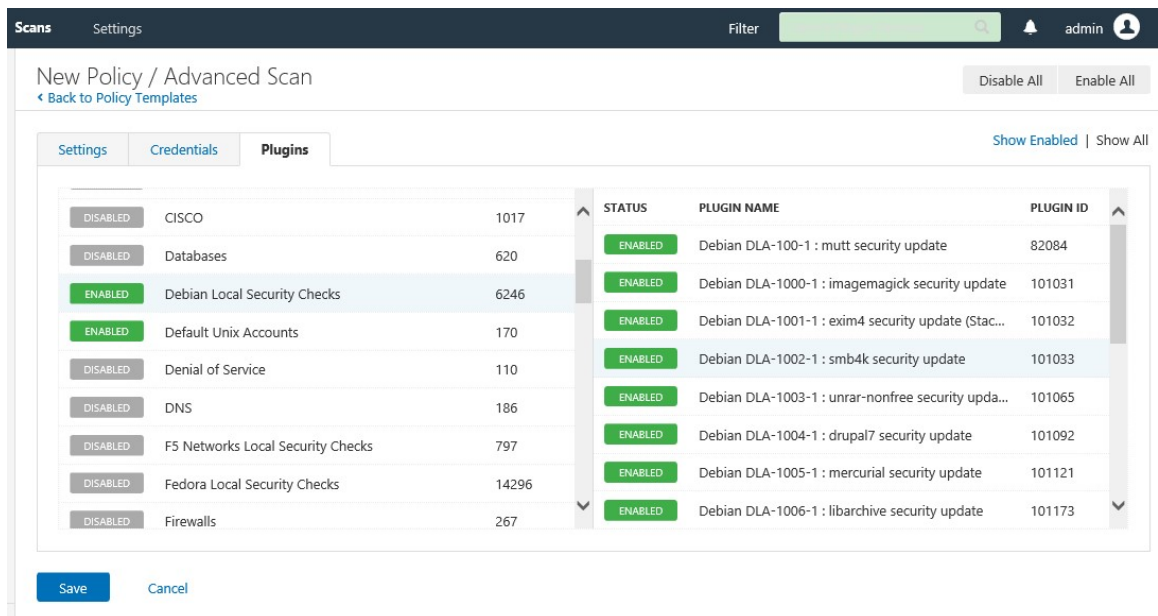


图 2.17 启动的插件程序

提示：用户可以根据自己的需要，添加各种类型的漏洞插件。

(8) 在该界面单击 **Save** 按钮，将显示如图 2.18 所示的界面。

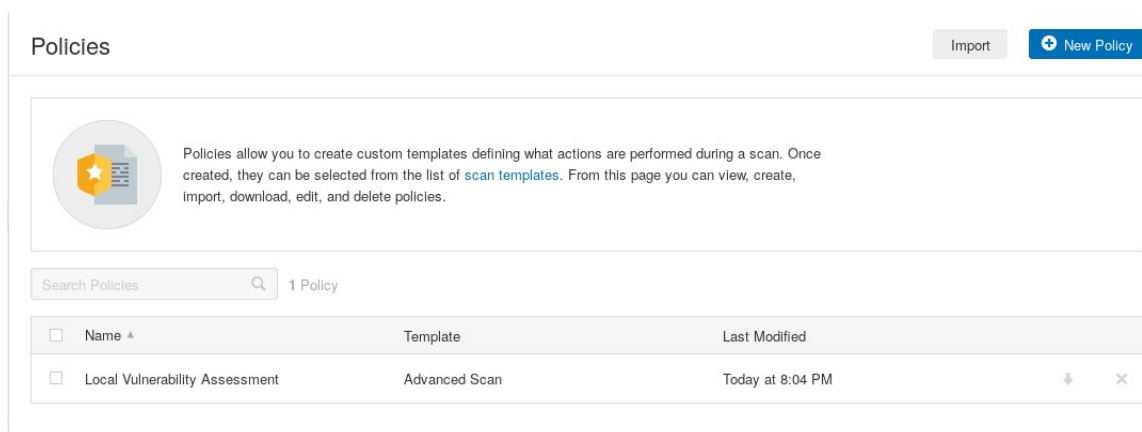


图 2.18 新建的策略

(9) 从该界面可以看到新建的策略 Local Vulnerability Assessment，表示该策略已创建成功。

3. 创建扫描任务

策略创建成功后，必须要新建扫描任务才能实施漏洞扫描。下面将介绍新建扫描任务的具体操作步骤。

(1) 在 Nessus 的主界面单击 Scans 选项卡，打开扫描任务界面，如图 2.19 所示。

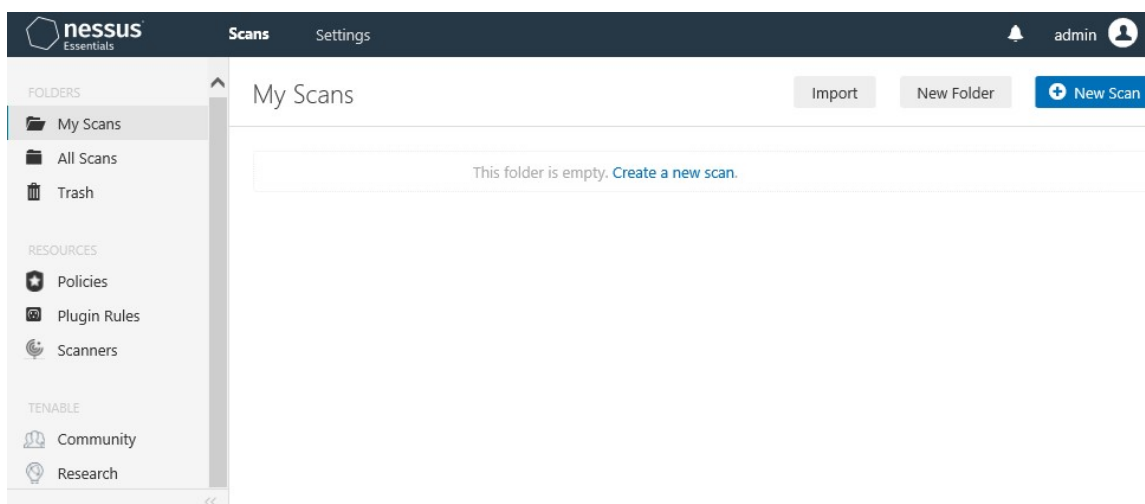


图 2.19 扫描任务界面

(2) 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。在该界面单击右上角的 New Scan 按钮，将显示如图 2.20 所示

Scan Templates

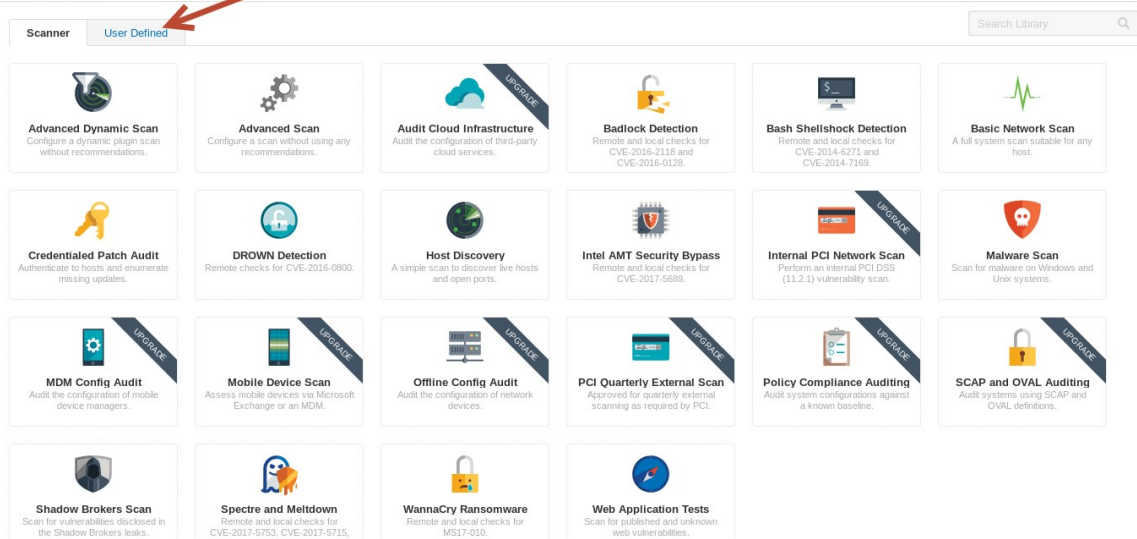
[Back to Scans](#)

图 2.20 新建扫描任务

(3) 该界面显示了一些可创建的扫描任务模板。而且，在 User Defined 选项卡下可以看到用户手动创建的策略模板。这里选择 Advanced Scan 模板类型，将显示如图 2.21 所示的界面。

图 2.21 新建扫描任务

(4) 在该界面设置扫描任务名称、描述、文件夹及扫描目标，如图 2.21 所示。设置完以上信息后，可以单击 Plugins 标签，设置启用不同的漏洞扫描插件。然后单击 Save 按钮，即可看到新建的扫描任务，如图 2.22 所示。

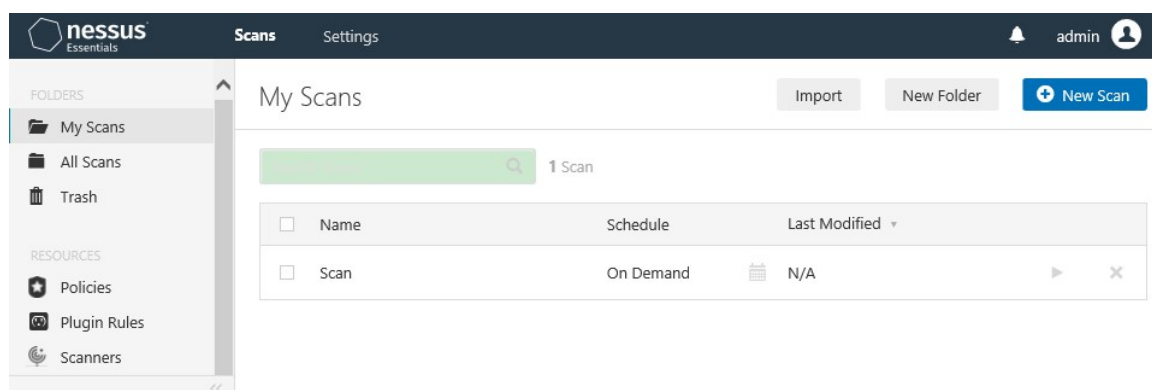



图 2.22 新建的扫描任务

(5) 此时，在该界面单击  图标，将开始对目标进行扫描。

2.1.4 分析并导出漏洞扫描报告

2.生成扫描报告

为了方便用户对其它漏洞进行分析，下面将介绍将扫描结果生成报告的方法。

【实例 2-5】将扫描结果导出为 HTML 格式的报告。具体操作步骤如下所示：

(1) 在扫描结果界面单击 **Report** 按钮，将弹出一个菜单栏，如图 2.29 所示。

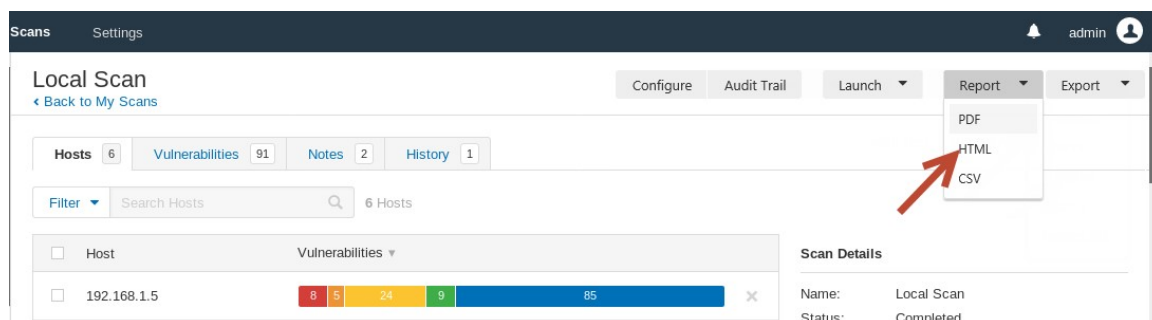


图 2.29 菜单栏

(2) 该菜单栏中显示了可以生成的扫描漏洞报告格式。这里选择导出文件格式为 **HTML**。所以，单击 **HTML** 选项，将弹出如图 2.30 所示的对话框。

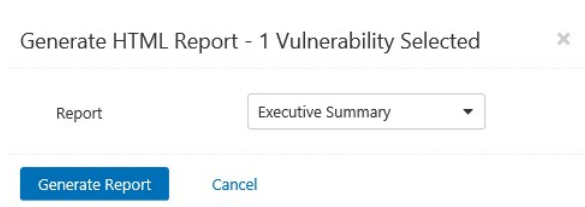


图 导出报告

(3) 从该界面可以看到，默认导出的报告内容为综合摘要信息。Nessus 还支持自定义导出的内容，单击 **Report** 对应文本框中的小三角，选择 **Custom** 选项，将显示如图所示的界面。

Generate HTML Report - 1 Vulnerability Selected

Report: Custom

Data: ☒ Vulnerabilities

Group Vulnerabilities By: Host

☒ Scan Information

☒ Host Information

Vulnerabilities Details: Select All | Clear

<input checked="" type="checkbox"/> Synopsis	<input checked="" type="checkbox"/> CVSS Base Score
<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> CVSS Temporal Score
<input checked="" type="checkbox"/> See Also	<input checked="" type="checkbox"/> STIG Severity
<input checked="" type="checkbox"/> Solution	<input checked="" type="checkbox"/> References
<input checked="" type="checkbox"/> Risk Factor	<input checked="" type="checkbox"/> Exploitable With
<input checked="" type="checkbox"/> CVSS v3.0 Base Score	<input checked="" type="checkbox"/> Plugin Information
<input checked="" type="checkbox"/> CVSS v3.0 Temporal Score	<input checked="" type="checkbox"/> Plugin Output

Some vulnerability details do not exist in all results

Generate Report Cancel ☐ Save as default

图 自定义导出内容

(4) 从该界面可以看到，增加了三部分选项，分别是 **Data**、**Group Vulnerabilities by** 和 **Vulnerabilities Details**。其中，**Data** 表示导出的内容。**Group Vulnerabilities by** 意思是漏洞分组依据，即导出的文件内容按照哪种方式显示，这里可选择的方式有 **Host**（主机）和 **Plugin**（插件）两种；**Vulnerabilities Details** 表示选择导出的漏洞相关信息，如 **Synopsis**、**Description**、**See Also** 等。默认，将导出所有的漏洞信息。如果用户不希望导出某个漏洞相关信息的话，将复选框中的对勾去掉即可。所以，用户可以根据自己的需要导出相应的内容。例如，这里设置导出的所有内容按照 **Host** 方式分组。设置完成后，单击 **Generate Report** 按钮将开始下载生成的报告。

提示：用户可以使用以上的方法，生成其它格式的扫描报告。

附录 D sqlmap 远程插件 sqlmap

sqlmap 是一款开源的数据库渗透测试工具，可以用来进行自动化检测。并且，还可以利用 **SQL** 注入漏洞，获取数据库服务器的权限。**Metasploit** 提供了 **sqlmap** 插件，可以直接调用 **sqlmap** 工具，并实施 **SQL** 注入漏洞扫描。本章将介绍 **sqlmap** 插件的使用方法。

D.1 配置 sqlmap 服务

当用户加载 **sqlmap** 插件后，即可连接 **sqlmap** 服务器。但是，如果要连接 **sqlmap** 服务器，则必须先配置该服务器。本节将介绍具体配置 **sqlmap** 服务的方法。

D.1.1 启动 sqlmap 服务

Kali Linux 中提供了一款名为 sqlmapapi 工具，可以用来启动 sqlmap 服务。其中，该工具的语法格式如下所示：

sqlmapapi [options]

该工具支持的选项及含义如下所示：

- ❑ -h,--help: 显示帮助信息。
- ❑ -s,--server: 以服务端模式运行。
- ❑ -c,--client: 以客户端模式运行。
- ❑ -H HOST,--host=HOST: 指定服务端监听的 IP 地址，默认是 127.0.0.1。
- ❑ -p PORT,--port=PORT: 指定服务端监听的端口号，默认是 8775。
- ❑ --adapter=ADAPTER: 指定服务端使用的适配器，默认是 wsgiref。
- ❑ --username=USERNAME: 指定基础认证用户名。
- ❑ --password=PASSWORD: 指定基础认证密码。

【实例 D-1】使用 sqlmapapi 工具启动 sqlmap 服务。执行命令如下所示：

```
root@daxueba:~# sqlmapapi -s -H 192.168.80.129 -p 8775
[12:36:55] [INFO] Running REST-JSON API server at '192.168.80.129:8775'..      #监听的地址
[12:36:55] [INFO] Admin (secret) token: b05a75467b13f99822972f02f02d97c8      #Admin 密钥
[12:36:55] [DEBUG] IPC database: '/tmp/sqlmapipc-9hgni1'                      #IPC 数据库
[12:36:55] [DEBUG] REST-JSON API server connected to IPC database
[12:36:55] [DEBUG] Using adapter 'wsgiref' to run bottle                      #使用的适配器
```

看到以上类似信息输出，则表示成功建立了服务端。其中，该服务器监听的地址为 192.168.80.129，端口为 8775。接下来，用户在客户端即可连接该服务器了。

D.1.2 连接 sqlmap 服务

当用户成功启动 sqlmap 服务后，即可连接该服务了。其中，用来连接 sqlmap 服务的语法格式如下所示：

sqlmap_connect host port

以上语法中，参数 host 表示 sqlmap 服务的主机地址；port 表示 sqlmap 服务监听的端口。

【实例 D-2】使用 sqlmap_connect 命令连接到 sqlmap 服务。具体操作步骤如下所示：

(1) 加载 sqlmap 插件。执行命令如下所示：

```
msf5 > load sqlmap
[*] Sqlmap plugin loaded
[*] Successfully loaded plugin: Sqlmap
```

从输出的信息可以看到，成功加载了 sqlmap 插件。

(2) 使用 sqlmap_connect 命令连接到 sqlmap 服务器。执行命令如下所示：

```
msf5 > sqlmap_connect 192.168.80.129 8875
[+] Set connection settings for host 192.168.80.129 on port 8875
```

看到以上输出信息，则表示成功连接到 sqlmap 服务器。

D.2 管理任务

当用户使用 `sqlmap` 插件远程连接到 `sqlmap` 服务后，则可以创建对应的扫描任务，并实施扫描。本节将介绍对扫描任务进行管理，如查看扫描任务列表、新建扫描任务、配置扫描任务选项等。

D.2.1 查看扫描任务

当用户在管理任务之前，可以先查看下当前扫描任务列表。其中，查看扫描任务列表的语法格式如下所示：

```
sqlmap_list_tasks
```

【实例 D-3】查看当前的扫描任务。执行命令如下所示：

```
msf5 > sqlmap_list_tasks
```

执行以上命令后，没有输出任何信息，则说明目前没有任何扫描任务。

D.2.2 新建扫描任务

如果用户还没有创建扫描任务的话，则需要新建扫描任务。其中，新建扫描任务的语法格式如下所示：

```
sqlmap_new_task
```

【实例 D-4】新建扫描任务。执行命令如下所示：

```
msf5 > sqlmap_new_task
```

```
[+] Created task: 1
```

看到以上输出信息，则表示创建了一个扫描任务。其中，该扫描任务 ID 为 1。此时，用户再次查看扫描任务列表，即可看到新建的扫描任务。如下所示：

```
msf5 > sqlmap_list_tasks
```

```
[+] Task ID: 1
```

从输出的信息可以看到，目前有一个扫描任务，其任务 ID 为 1。由此可以说明，成功创建了扫描任务。

D.2.3 设置选项

当用户创建一个扫描任务后，可以设置一些选项，以提高扫描效率。其中，这里的选项是 `sqlmap` 工具运行时候的选项，可以使用 `sqlmap -hh` 命令查看支持的所有选项。其中，用于设置选项的语法格式如下所示：

```
sqlmap_set_option <taskid> <option_name> <option_value>
```

以上语法中，参数 `taskid` 表示任务 ID；`option_name` 表示选项名称；`option_value` 表示选项值。

【实例 D-5】为新建的扫描任务设置 `cookie` 选项。执行命令如下所示：

```
msf5 > sqlmap_set_option 1 cookie "security=low; PHPSESSID=887a3f0479a89c8b9bd7309f3fd3bade"
```

```
[*] Success: true
```

看到以上输出信息，则表示成功设置了 `cookie` 选项值。如果想要查看设置的选项值，可以使用 `sqlmap_get_option` 命令实现。

用户使用同样的方法，还可以设置其它选项。如下所示：

```
msf5 > sqlmap_set_option 1 risk 3
```

```
#设置风险级别
```

```
[*] Success: true
msf5 > sqlmap_set_option 1 level 5           #设置探测级别
[*] Success: true
```

D.2.4 获取选项

当用户设置选项后，可以使用 `sqlmap_get_option` 命令查看获取的选项值。其中，使用该命令获取选项值的语法格式如下所示：

```
sqlmap_get_option <taskid> <option_name>
```

以上语法中，参数 `taskid` 表示任务 ID；`option_name` 表示选项名。这里的 `option_name` 和 `sqlmap_set_option` 命令中的 `option_name` 含义一样。

【实例 D-6】获取 cookie 选项值。执行命令如下所示：

```
msf5 > sqlmap_get_option 1 cookie
[+] cookie : security=low; PHPSESSID=887a3f0479a89c8b9bd7309f3fd3bade
```

从输出的信息可以看到，成功获取到了 cookie 选项值。其中，该选项值为 `security=low; PHPSESSID=887a3f0479a89c8b9bd7309f3fd3bade`。

D.2.5 执行扫描任务

当用户将创建的任务选项设置完成后，则可以执行该扫描任务。其中，执行扫描任务的语法格式如下所示：

```
sqlmap_start_task <taskid> [<url>]
```

以上语法中，参数 `taskid` 表示任务 ID；`url` 表示指定扫描目标的 URI。

【实例 D-7】执行扫描任务。执行命令如下所示：

```
msf5 > sqlmap_start_task 1 http://192.168.80.134/dvwa/vulnerabilities/sqli/?id=1&Submit=y
[*] Started task: true
```

看到以上输出信息，则表示成功执行了扫描任务。

D.2.6 获取任务状态

当用户执行扫描任务后，可以使用 `sqlmap_get_status` 命令获取任务状态，以确定是否执行完成。其中，获取任务状态的语法格式如下所示：

```
sqlmap_get_status <taskid>
```

以上语法中，参数 `taskid` 表示任务 ID。

【实例 D-8】使用 `sqlmap_get_status` 命令获取任务状态。执行命令如下所示：

```
msf5 > sqlmap_get_status 1
[*] Status: running
```

从输出的信息可以看到，状态值为 `running`（运行），则表示正在实施扫描。当扫描完成后，状态值为 `terminated`。如下所示：

```
msf5 > sqlmap_get_status 1
[*] Status: terminated
```

从输出的信息可以看到，当前状态值为 `terminated`（终止），则表示扫描完成。

D.3 管理扫描结果

当用户实施扫描完成后，即可管理扫描结果，如获取日志信息、扫描结果及导入扫描结果。本节将介绍对扫描结果进行管理。

D.3.1 获取日志信息

当实施扫描完成后，可以使用 `sqlmap_get_log` 命令获取日志信息。其中，用于获取日志信息的语法格式如下所示：

```
sqlmap_get_log <taskid>
```

以上语法中，参数 `taskid` 表示任务 ID。

【实例 D-9】获取扫描任务 ID 为 1 的日志信息。执行命令如下所示：

```
msf5 > sqlmap_get_log 1
[*] [10:35:34] INFO: resuming back-end DBMS 'mysql'
[*] [10:35:34] INFO: testing connection to the target URL
[*] [10:35:35] INFO: the back-end DBMS is MySQL
```

从输出的信息可以看到，成功连接到目标 URL。而且，检测到目标服务器使用的数据库为 MySQL。

D.3.2 获取扫描结果

当实施扫描完成后，可以使用 `sqlmap_get_data` 命令扫描结果。其中，用于获取扫描结果的语法格式如下所示：

```
sqlmap_get_data <taskid>
```

以上语法中，参数 `taskid` 表示任务 ID。

【实例 D-10】获取扫描结果。执行命令如下所示：

```
msf5 > sqlmap_get_data 1
[*] URL: http://192.168.80.134/dvwa/vulnerabilities/sqli/?id=1&Submit=y
Title   Payload
-----
```

从输出的信息可以看到共显示了两列，分别是 `Title`（标题）和 `Payload`（攻击载荷）。这里没有获取到任何结果，所以每列值为空。

D.3.3 导入扫描结果

当用户实施扫描完成后，可以将扫描结果导入到 Metasploit 数据库中。其中，导入扫描结果的语法格式如下所示：

```
sqlmap_save_data <taskid>
```

以上语法中，参数 `taskid` 表示任务 ID。

【实例 D-11】导入扫描结果到 Metasploit 数据库。执行命令如下所示：

```
msf5 > sqlmap_save_data 1
[*] URL: http://192.168.80.134/dvwa/vulnerabilities/sqli/?id=1&Submit=y
[+] Saved vulnerabilities to database.
```

从输出的信息可以看到，成功保存漏洞到数据库。

