Nessus 8.12.0 最新版破解方法

Author: ze7o

Date: 2020/10/15

发布至www.blueprintf.com社区

0x1 准备阶段：

1. 通过[Nessus官方](#)下载安装包

⊕ Nessus-8.12.0-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit)	77.1 MB	Oct 8, 2020

2. 通过[Nessus官方渠道](#)提交试用信息，之后邮箱会收到激活码(activation code)
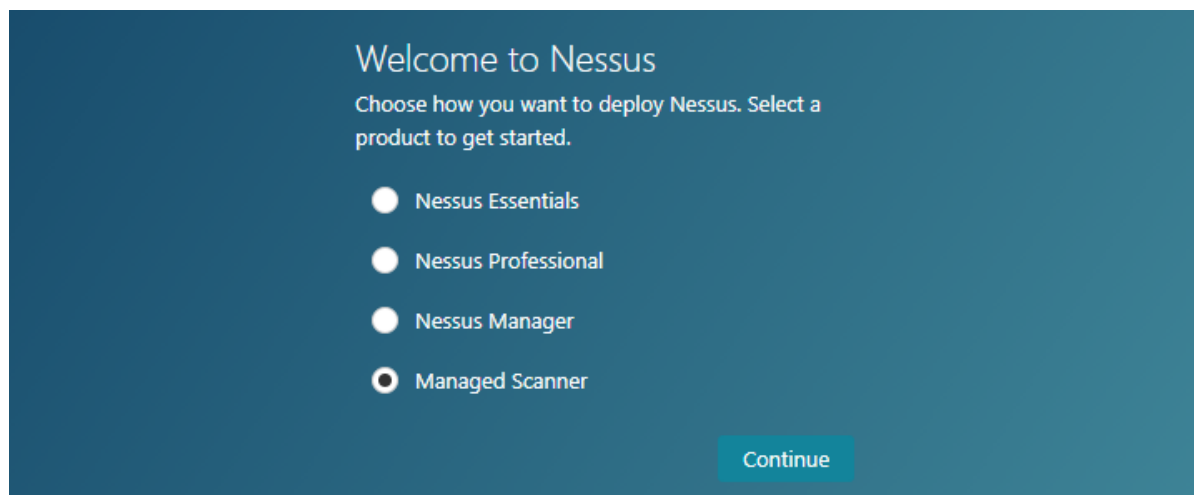

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

725C-1431-8DBE-C   5
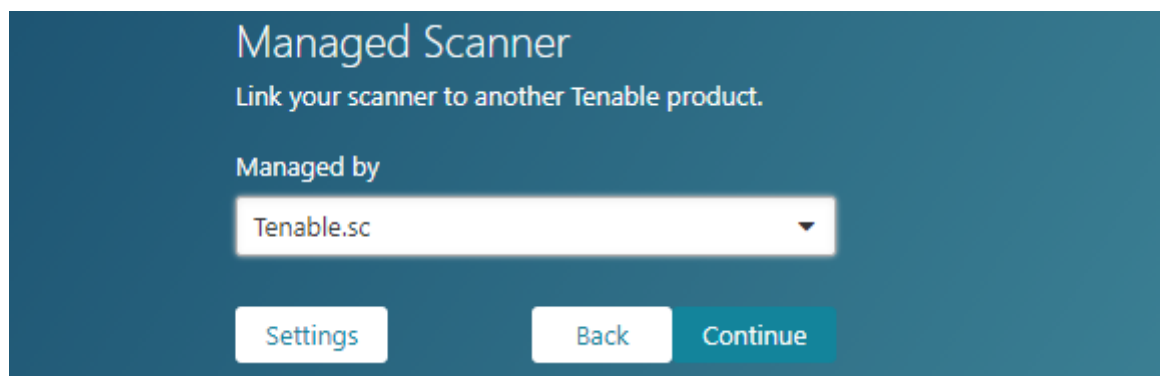
3. 双击安装包Nessus-8.12.0-x64.msi进行安装
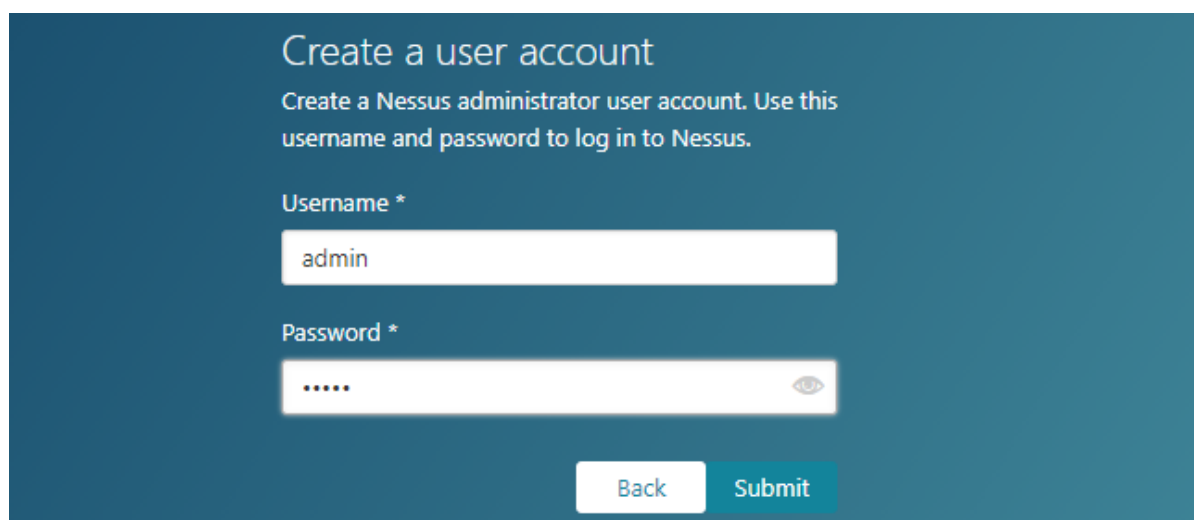
0x2 安装配置

1. 安装成功后，Nessus会自动打开浏览器，进入欢迎配置页，选择Managed Scanner并点击 Continue

2. 选择Tenable.sc并点击Continue

3. 设置账户密码并点击Submit

4. 完成配置后，将进入Nessus设置页

0x3 离线激活

1. 获得询问码(challenge code)

使用管理员权限运行命令行，进入到Nessus安装目录后，使用该命令获得询问码

```
.\nessuscli.exe fetch --challenge
```


2. 进入离线激活页面，输入最开始邮件得到的激活码和询问码，点击Submit获得**离线插件包和激活证书**

Generate a license for Nessus 6.3 and Later

To generate a license for an older version of Nessus click here.

On your nessusd server, run 'nessuscli fetch --challenge' and copy the result here:

```
26e2f48bfe9f5985eb6cc498a3449f
```

Enter your activation code here:

```
725C-1431-8DBE-64   -51
```

Submit

Thank you. You can now obtain the newest Nessus plugins at :

https://plugins.nessus.org/v2/nessus.php?f=all-2.0.tar.gz&u=aa3ae49f3399ddbe8356d0038aa410d1&p=d6390a632aa2

You can copy the following license and paste it into the Nessus console to proceed:

```
-----BEGIN TENABLE LICENSE-----
c3JCKzUwanZBeDQ5UnFuVXBrVytWTWZJU1JEVi9PU0xvdXkzUGE5R11OT00yT2djdjQrNkFzRW9S
OEFvZWhxZHoyb3NkRDNmVkR0YmtCTjhiNm5TVWxtY0RZUTddPM2R1K2FpNnBmUnJJYmdsL0RPTWFP
L1MvVXRtdXdqamJYa3hGNFpyR31DZ0dwbU99jMkRHYkVvM21Va21JY1BQTDdrTEczNWxRV2Qzdk03
T3k2aXE3eG1yTTVGb2hReDB1dGtIY1hyMECrNOJ6ZX1aWXBRT1FLUj1aWGFhROZGMWdxZ296UHBH
VG5ZRnNmMkpWcDZmYWYVXdmxKb2pFVGFuKzhaZm94WG85eEJtT0U3MWxYUm5vSitjZ212Wk10REdR
TUQ2dDRFQkwrY3Qydk5pdkxypcnpvRUtwcUNXczZobmlUZEFian14Ym43eW5mSkY4SUxBTnI2MnZV
NjNCYjMrZ1dna1g4e1dnZG4wcmsrNUVoeGw3aXdLLc0I3QWtjYXpFWGtPL31rbHV4cnB5TWRsT1Vt
SDZ6amNHc3F1a3hhRFVdFB0dkpqGQjRvYmJZc1TwQU1De11RSWVvdW26M27WZ31pS111SF11d3Nw
```

3. 点击页面上的链接下载得到all-2.0.tar.gz插件包，接着获取询问码的命令行，安装插件包
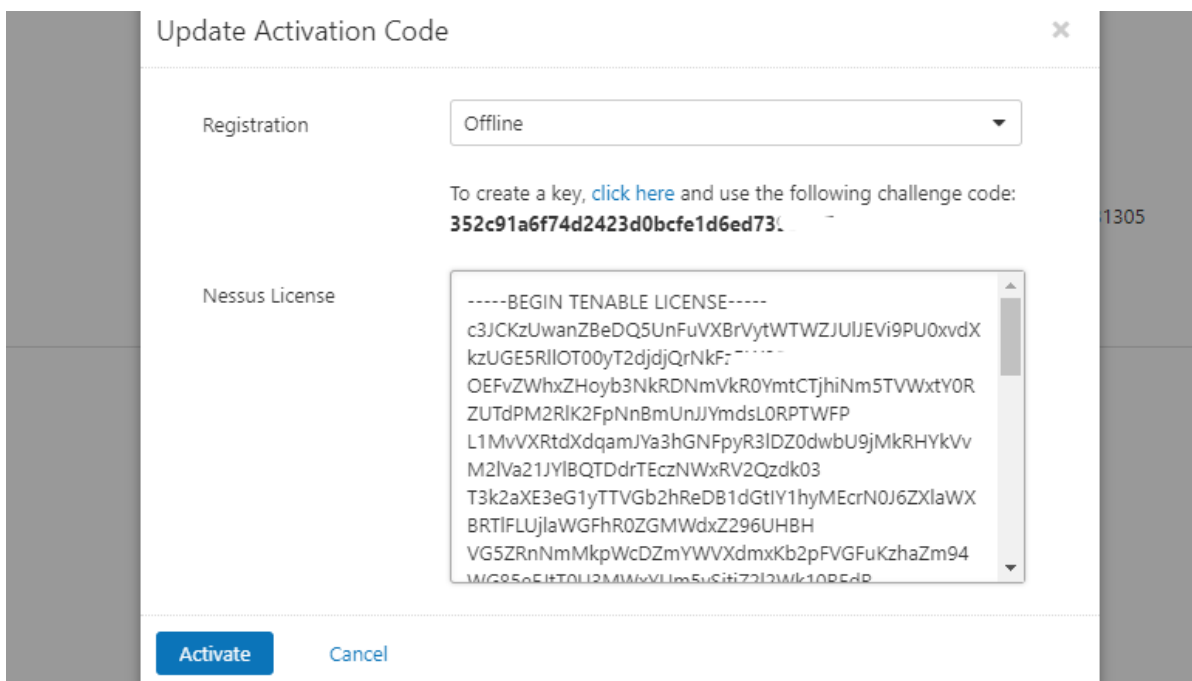
```
.\nessuscli.exe update .\all-2.0.tar.gz
```

```
PS D:\Tools\Nessus> .\nessuscli.exe update .\all-2.0.tar.gz
[info] Copying templates version 202009231305 to D:\Tools\Nessus\nessus\templates\tmp
[info] Finished copying templates.
[info] Moved new templates with version 202009231305 from plugins dir.
* Update successful.  The changes will be automatically processed by Nessus.
PS D:\Tools\Nessus>
```

4. **保存结果中的数字串202009231305**，后面会用到

###

5. 回到Nessus设置页，Activation Code 还是 N/A，没关系，点击旁边的小笔🖊进行手动激活

选择Offline，输入**激活证书**点击Activate激活（激活证书在0x3 第2步骤获得）

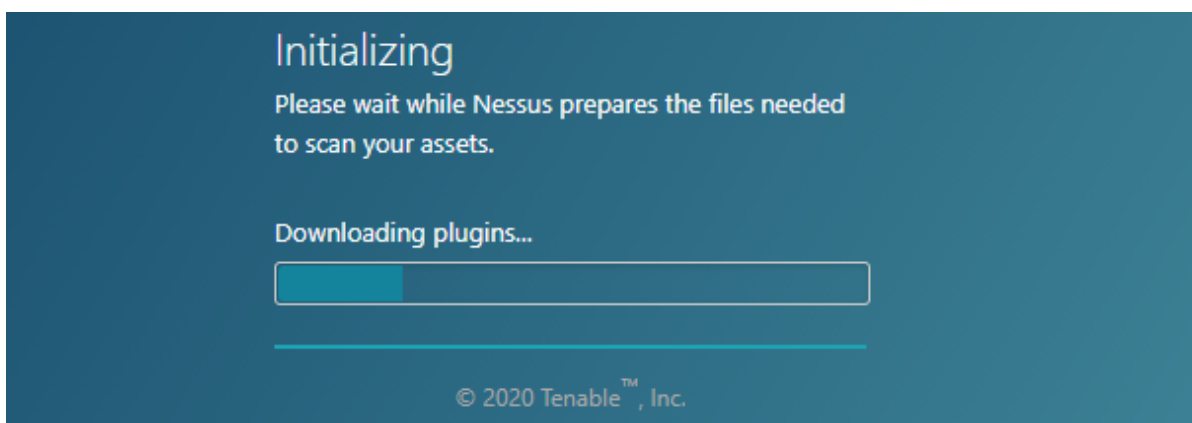接着会初始化一段时间（显示在Download，但没发现有新插件，猜测可能是在校对本地插件）


完成后进入设置页，激活成功，显示仅允许扫描16个IP
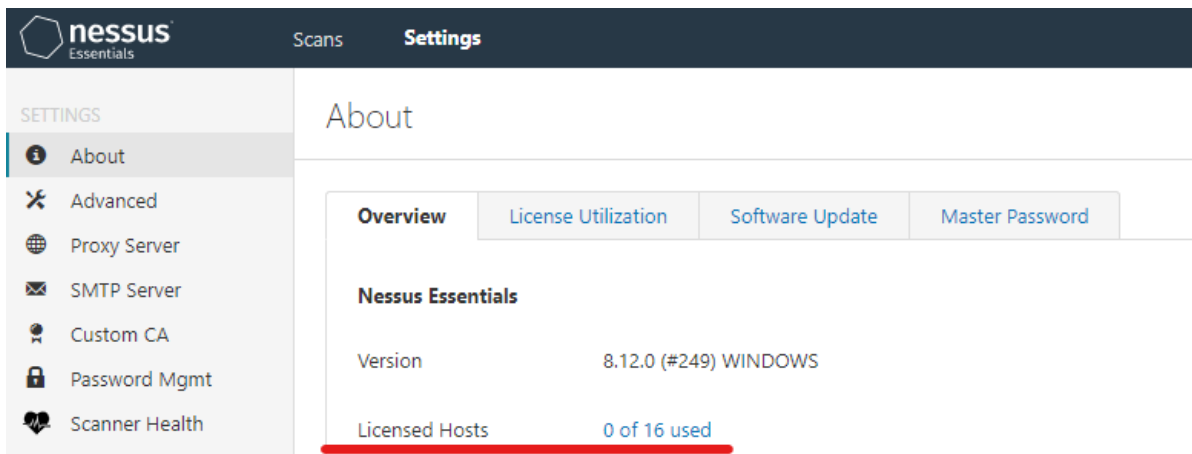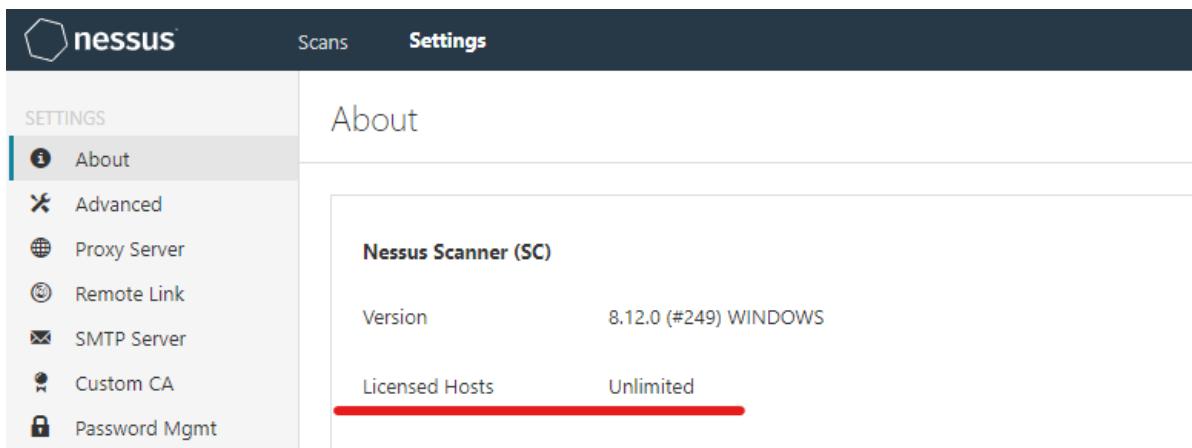
0x4 破解数量限制

接下来进入关键步骤了

1. 将0x3 第4步骤**获得的数字串，替换到下面的数字串中**，并保存到文件plugin_feed_info.inc

```
PLUGIN_SET = "202009231305";
PLUGIN_FEED = "ProfessionalFeed (Direct)";

PLUGIN_FEED_TRANSPORT = "Tenable Network Security Lightning";
```

2. **将plugin_feed_info.inc替换到Nessus安装目录的nessus目录下（覆盖原有文件）**
3. 将Nessus安装目录**nessus/plugins/目录下的plugin_feed_info.inc文件删除**
4. 进入Windows服务管理，重新启动Nessus服务
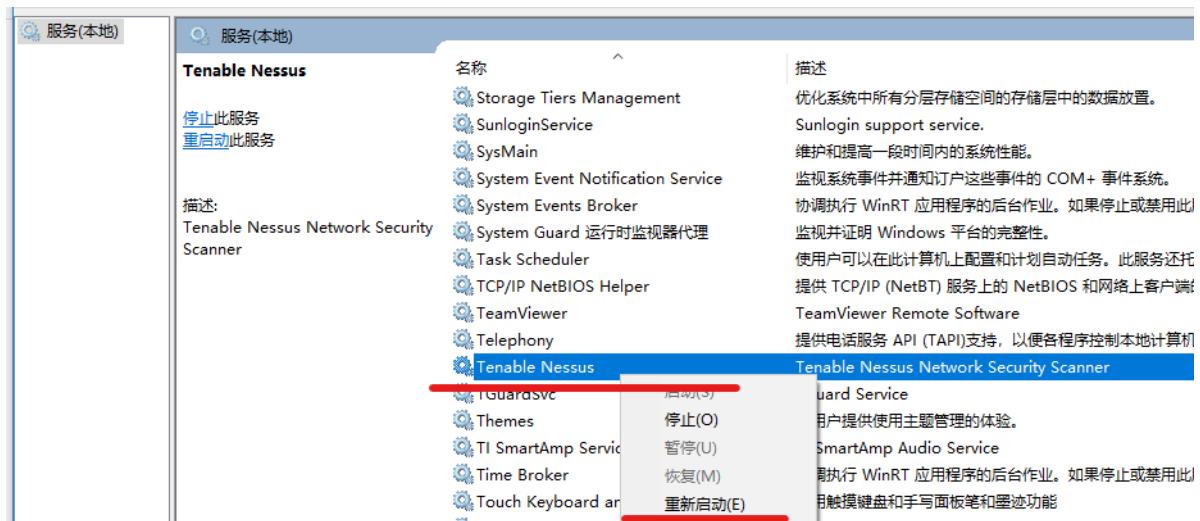
重启后的Nessus在初始化成功后，设置页面将变成下面的样子，表示激活成功。

Author: ze7o

Date: 2020/10/15