**WEB漏洞扫描软件调研**

**警告：一切扫描渗透行为需经过委托方的授权，否则一切后果自负！**

**警告：一切扫描渗透行为需经过委托方的授权，否则一切后果自负！**

**警告：一切扫描渗透行为需经过委托方的授权，否则一切后果自负！**

**1.xray（官网：https://xray.cool/）:**

准备xray安装包：xray\_linux\_amd64.zip

创建xray文件夹：sudo mkdir /home/ubuntu/xray

解压zip文件：unzip xray\_linux\_amd64.zip -d /home/ubuntu/xray

安装xray: ./xray\_linux\_amd64 (可能需要执行，第一次因为没有xray.yaml文件会报错，需再执行一次)

使用说明: ./xray\_linux\_amd64 --help

Example:

扫描公司官网： https://www.nullmax.cn/

先生成ca证书： ./xray\_linux\_amd64 genca

扫描： ./xray\_linux\_amd64 webscan --url https://www.nullmax.cn/ --html-output outcome.html

\*如果没有扫到漏洞是不会生成html文件的

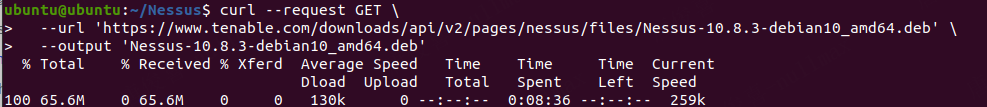
**2.nessus（官网： https://www.tenablecloud.cn/products/nessus）:**

参考文档：https://blog.csdn.net/qq\_50247813/article/details/144314168

1.访问官网下载nessus：

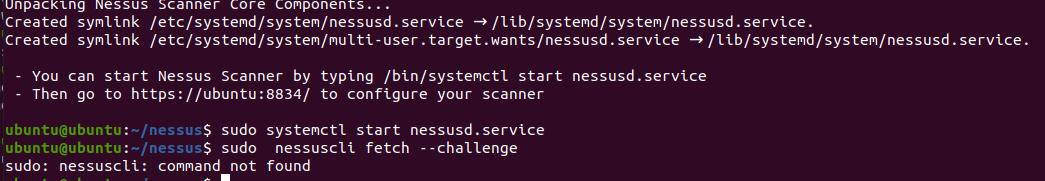
https://www.tenablecloud.cn/products/nessus?utm\_source=baidu&utm\_medium=CPC&utm\_campaign=Nessus\_PC&utm\_content=nessus&utm\_term=nessus%20%E5%AE%98%E7%BD%91

|  |
| --- |
| Bash  curl --request GET \ > --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.8.3-debian10\_amd64.deb' \ > --output 'Nessus-10.8.3-debian10\_amd64.deb' |



2.安装nessus，去到安装包文件夹下，使用dpkg -i Nessus-10.8.3-ubuntu1604\_amd64.deb

1.）根据提示启动nessusd服务： systemctl start nessusd.service

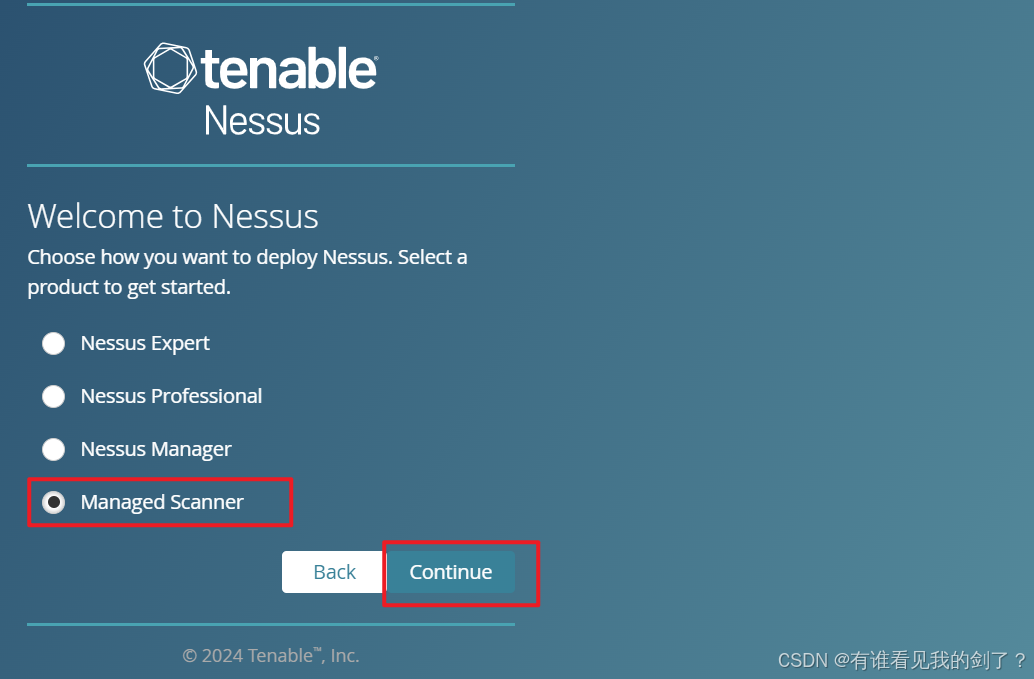


2.）访问提示的网站： https://ubuntu:8834/

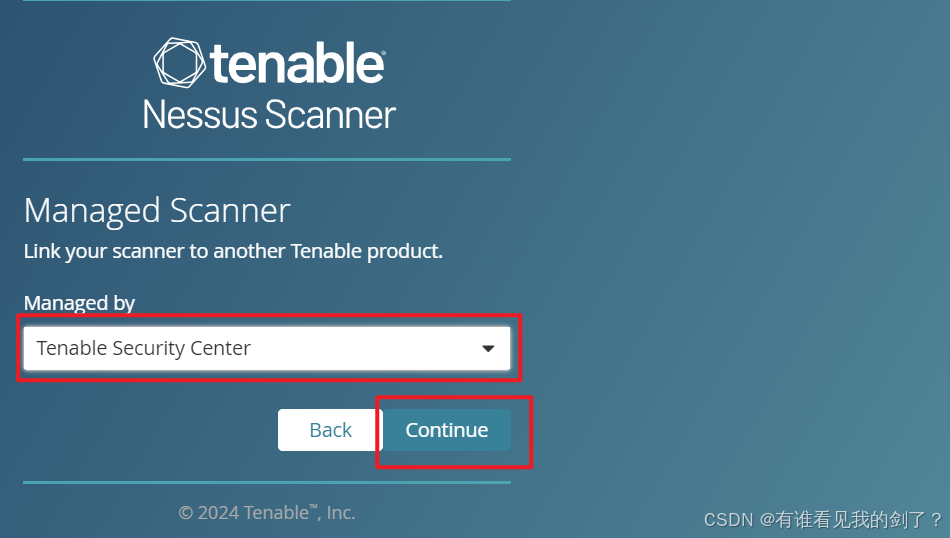




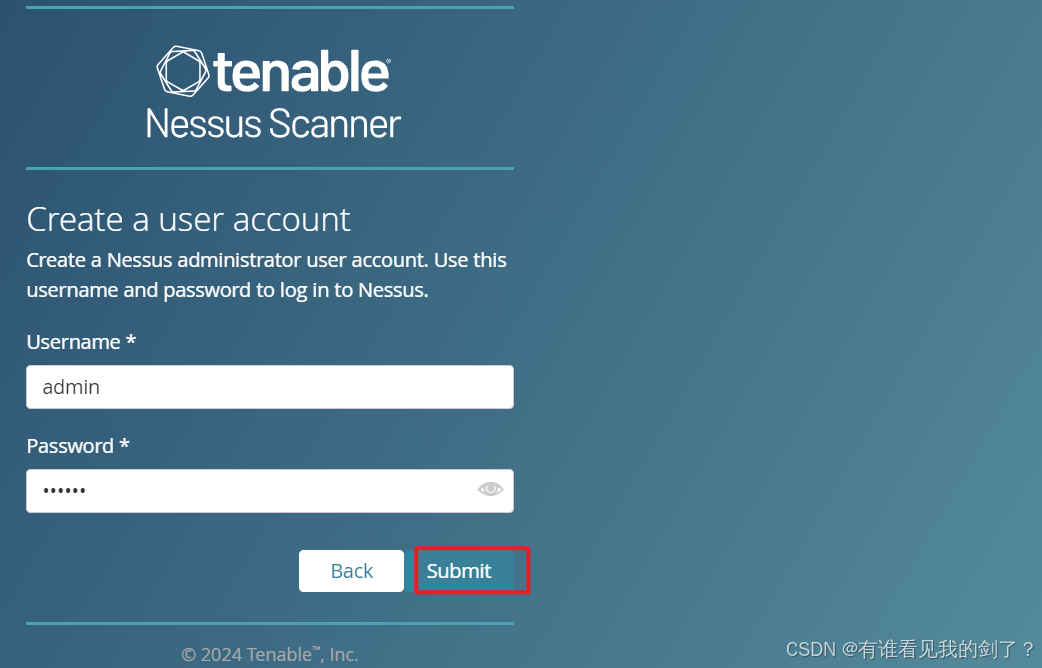
选最后一个Managed Scanner：



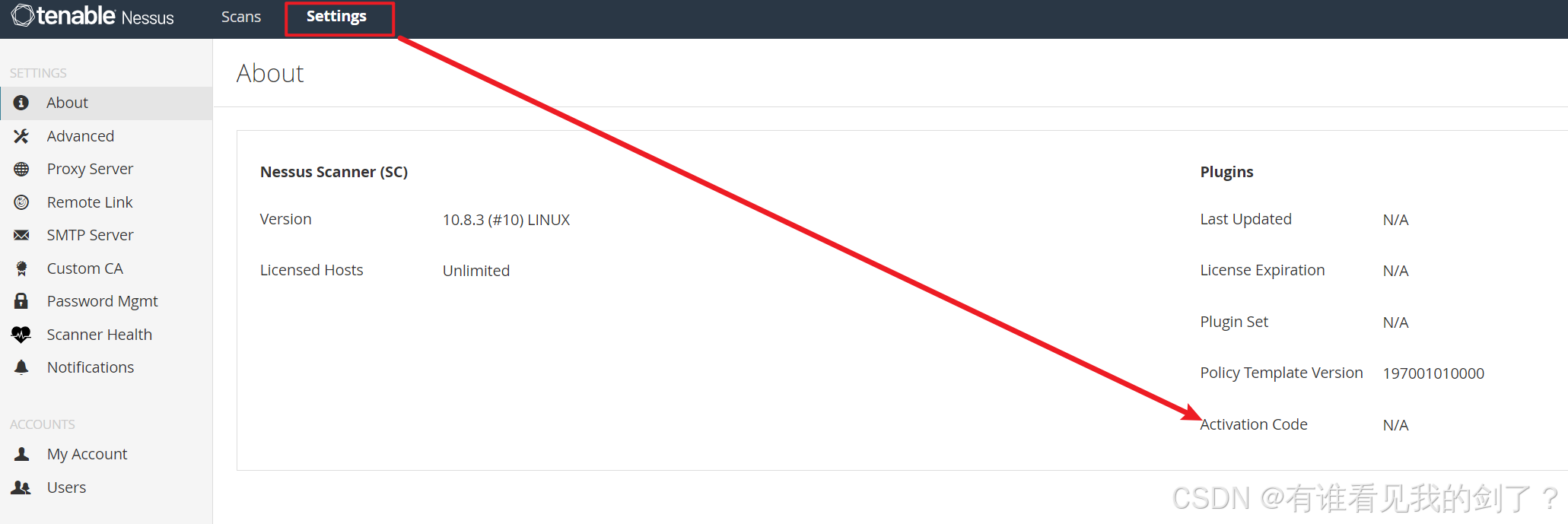
然后选择Tenable Security Center



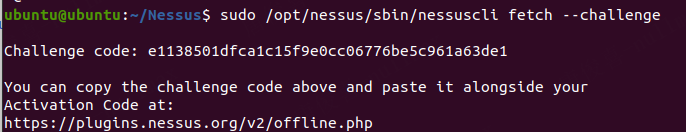
注册账号



激活Nessus:



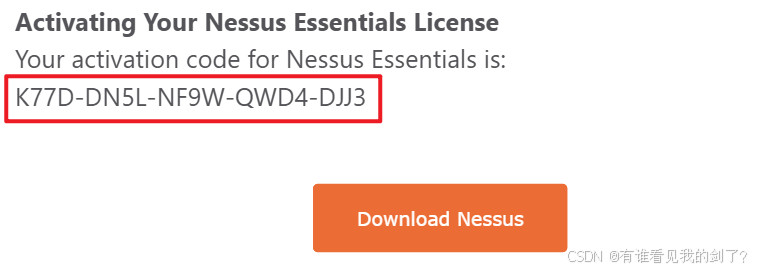
|  |
| --- |
| Bash root@localhost:~# sudo /opt/nessus/sbin/nessuscli fetch --challenge  Challenge code: f45689d2a6ed72661729d67ab7536c2de092fb56  You can copy the challenge code above and paste it alongside your Activation Code at: https://plugins.nessus.org/v2/offline.php |



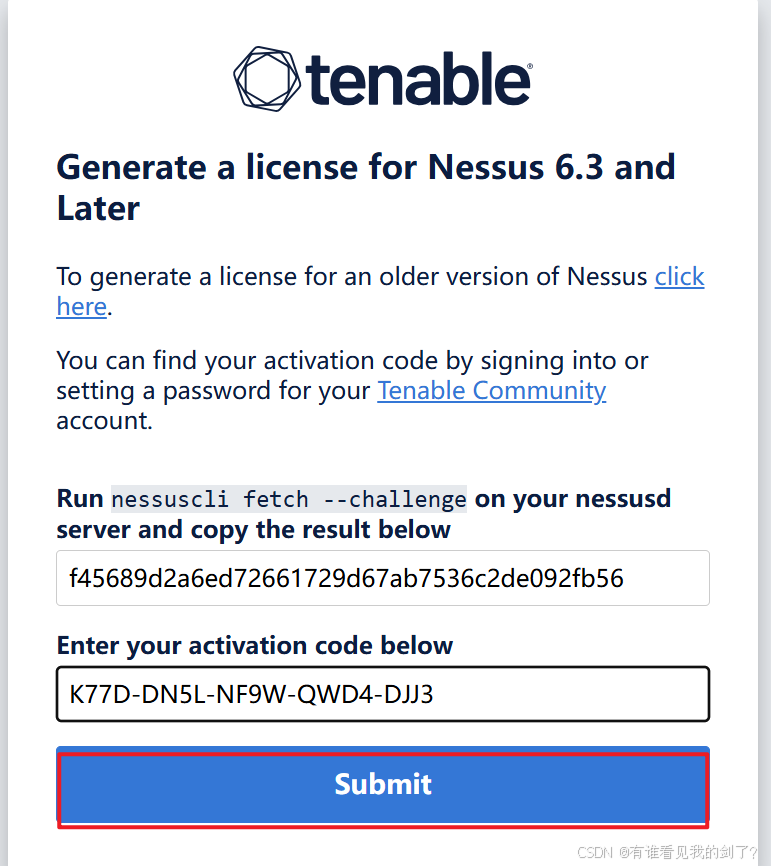
获取activation code

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





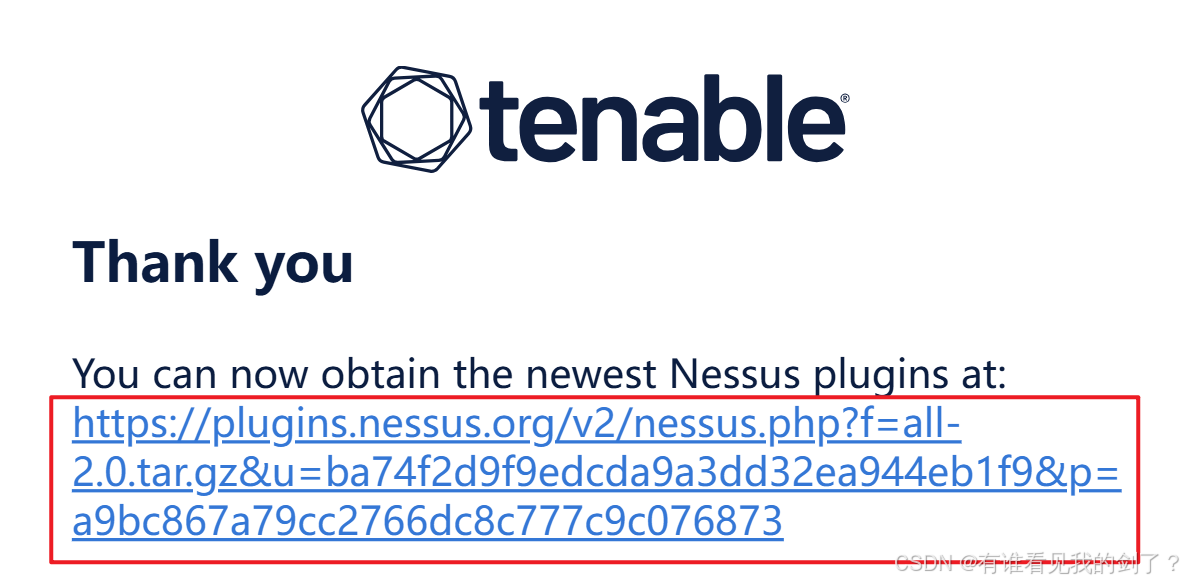
1. 获取 LICENSE 和 插件压缩包  
   https://plugins.nessus.org/v2/offline.php



nessus.license: 创建license文件把下面的code粘贴进去

|  |
| --- |
| Bash -----BEGIN TENABLE LICENSE----- Z1NPZXE4blAyQXIyblp4MUIvSjJvMmFJbHY5UlJna0h1bGxrTk93N1FaU1pjQXhvMDAvbVdna1dB SDRIOWFBQ2U5QlQra3NuQnNDOXJTQTA1b3NvVFhlb3BMTzZBUHFxVlVxQ3JVRjV2TWQzSVR3bVU2 RnErYmxqK1Y3Y2VFMEJyRFpyRW9QUTJOcUhVM0ZqRzRYMkFrQ2NVdXFUcUxrSGxQcFplUWNoOHBu ZW5vV3VvL0c4L2NyWmtMV1JRVXBnRmpGTzVaWFl4U2Z4WEc1aGJZZm5jR0FPUk05U1pQYkdlL08z Q2psSmMrSFV1NVIvZ3Jpd2plZmxPZ0hqb05GYzMycldwVWo3U3ptSTN2cVR5alJadk1qTEFIcjNK SXRyYVdqQ1VzZ0k2dmJIYkJUQndPM3NKZ0ZicC96eFZVeGRwYTZyQUJTRmkvbS9TYlBoYzNYcmNi V1Jsa01GMWVaYXhLbUtuL3dTbEp6TXFhaWtSbllJeC9DNEJkc09BVkVTUCs5SGRZd2RvRzdTbWdT UzhXbTNLcDZkdkZROXpFZmNkUGI5QmdtanBhalg4R3JaNjBJN2ZxeDBKVldaMFRGZktmYW41NVZw UjBYS0NBS0RiK3pCdGwzZ1ppQXFHa1pWMFByVVM4MCs0ZGJaQThGZnZXTGdNQkE4cERHcUliUWhW amxhSVpkeWc3N01yeVk5TTZXbWVaVGZYbk85SzYrdHBwbVRya0Rqc2h0RzZvTDE0Qnk3VHIzeEpl YnB0aUNrNUxUS051amN6Q0RBVnUrMHF2Rjk2MEtKYjVkWGc4QTNsMXF1dll5KzhQeENSRXVmQ2pC MURmTG5aUVhVSFZ2Tm1mLyt5VWZtWlpLWXRUNEdFd2h3eWNoOFhDaFh4TmtSaGFJQ1pVWDZUd009 DQp7ImFjdGl2YXRpb25fY29kZSI6IkQ4WjktOEFUNy1GUDVILTU0M1otVTdEOSIsInVwZGF0ZV9w YXNzd29yZCI6ImE1OWNhMGZmODFjOTZiNmVjYjY0ZTgzNzBlOTEwN2M5IiwicGVuZG9fYXBpX2tl eSI6ImE3YzhkNWM0LWI2YWUtNDg2Ny03ZGFiLTY5YTkyYTA4NDdlMSIsIm5hbWUiOiJOZXNzdXMg SG9tZSIsInR5cGUiOiJob21lIiwiZXhwaXJhdGlvbl9kYXRlIjoxODk4MTI4ODA5LCJjdXN0b21l cl9pZCI6MCwiaXBzIjoxNiwidXBkYXRlX2xvZ2luIjoiM2Y0ZDU0MjRhMTA1Y2Q5YzA1OWYwMDcy YmEyNWE2YmMiLCJkcm0iOiI1NTgzNmNiNDZjODFmOWE5NjQwZWYzNzgzNGVmODk2NiJ9 -----END TENABLE LICENSE----- |

4.获取插件压缩包  
丢到浏览器里面下载

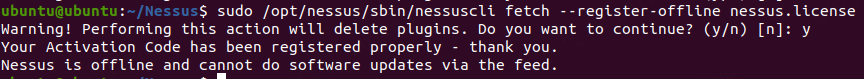


下载LICENSE证书，将 LICENSE 和 插件压缩包上传到服务器

|  |
| --- |
| Bash root@localhost:~# ls -1 Nessus-10.8.3-ubuntu1604\_amd64.deb all-2.0.tar.gz nessus.license |

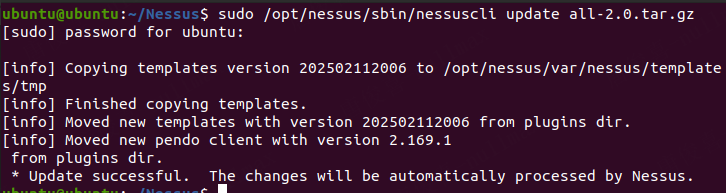
使用LICENSE 离线激活 Nessus

|  |
| --- |
| Bash root@localhost:~# sudo /opt/nessus/sbin/nessuscli fetch --register-offline nessus.license Warning! Performing this action will delete plugins. Do you want to continue? (y/n) [n]: y Your Activation Code has been registered properly - thank you. Nessus is offline and cannot do software updates via the feed. |



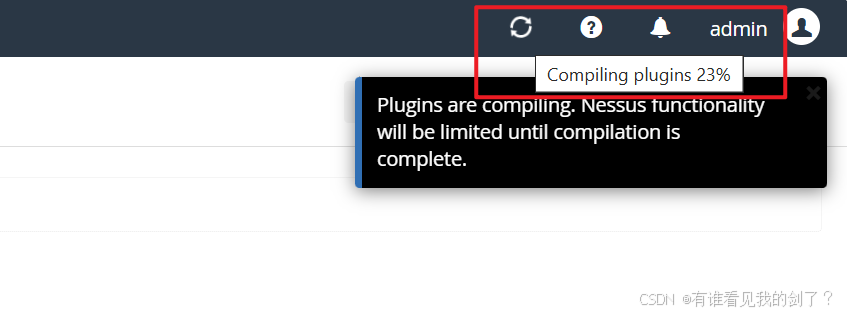
导入插件

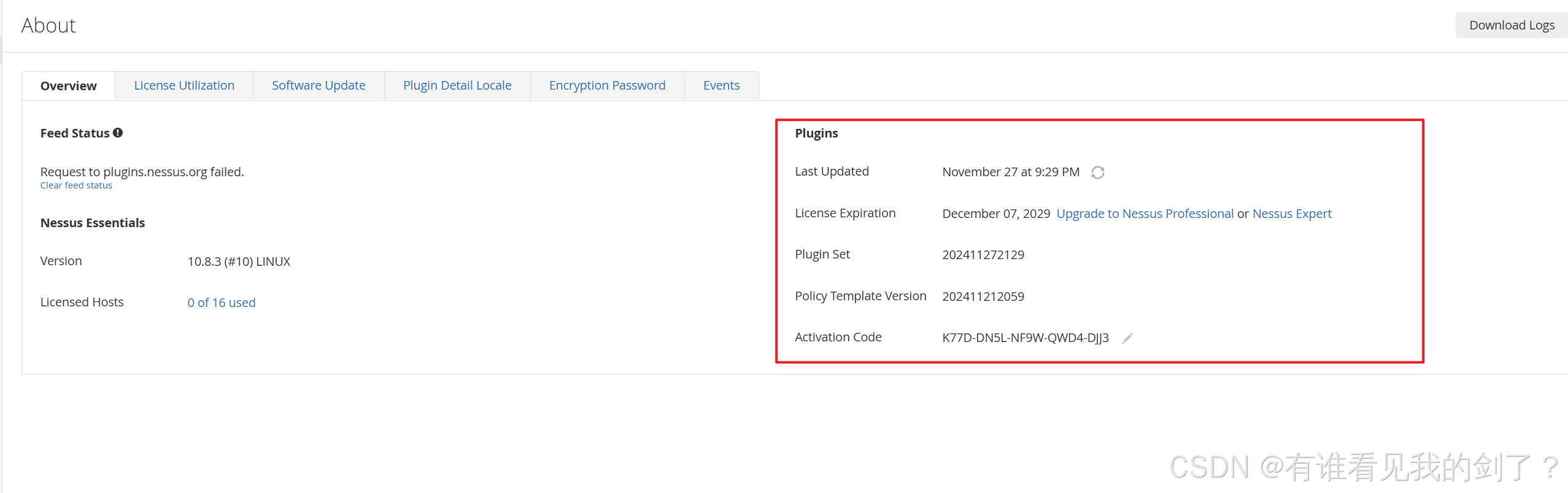
|  |
| --- |
| Bash root@localhost:~# sudo /opt/nessus/sbin/nessuscli update all-2.0.tar.gz  [info] Copying templates version 202411212059 to /opt/nessus/var/nessus/templates/tmp [info] Finished copying templates. [info] Moved new templates with version 202411212059 from plugins dir. [info] Moved new pendo client with version 2.169.1  from plugins dir.  \* Update successful. The changes will be automatically processed by Nessus. |



|  |
| --- |
| Bash #重启nessus服务 root@localhost:~# systemctl restart nessusd |

登入Nessus





FFUV-VQYQ-MXTA-UGSF-TRCH

**3.EZ（官网-绿盟：https://msec.nsfocus.com/）**

1.官网注册，然后申请证书（免费30天），然后下载证书

2.下载EZ

3. sudo mkdir /home/ubuntu/ez 创建ez文件夹

4. unzip ez\_linux\_amd64.zip 解压zip文件

5. 将下载好的证书移到ez文件夹中

6. 运行EZ: ./ez\_linux\_amd64 webscan 生成.yaml配置文件

7. 使用./ez\_linux\_amd64 web 开启web服务

8. 输入http://10.10.6.204:8888,之后报错invalid request，再按下面提示的url访问： pleases visit....



9. 官方使用文档： https://docs.ezreal.cool/docs/intro/

10. 渗透测试需要可控：

1. 选择测试范围：网络地址、域名范围、端口

2. 不要选择测试内外主机

3. 枚举尽量不选