

# THM-Nessus(基础)-学习

本文相关的TryHackMe实验房间链接: <https://tryhackme.com/room/rpnessusredux>

## H2 简介

**注意：本文中安装的是免费版的Nessus。**

Nessus 是一款 C/S 架构的漏洞扫描系统，作为一款漏洞扫描软件，不仅功能全面，而且还可以实时更新漏洞库，据统计有超过 75,000 个机构在使用它。

Nessus 使用类似于 Nmap 的技术来查找和报告漏洞，然后将这些漏洞呈现在一个GUI 中供我们查看，Nessus 与其他扫描软件不同，因为它在扫描时不做假设，例如，假设 Web 应用程序在端口 80 上运行。

Nessus有付费版和免费版，免费版的功能相对于付费版受到一定限制。



## H2 Nessus安装

官方安装指南：<https://docs.tenable.com/nessus/Content/GettingStarted.htm>



在Kali虚拟机上安装Nessus

步骤一：

访问网址 <https://www.tenable.com/products/nessus/nessus-essentials> 注册一个账户（输入用户名称+电子邮箱即可），获取激活码

### Register for an Activation Code

First Name \*

Last Name \*

Email \*

☐ Check to receive updates from Tenable

Register

# 感谢您注册 Nessus Essentials!

检查您的电子邮件以获取激活码

感谢您注册 Nessus® Essentials。包含您的激活码的电子邮件已通过您提供的电子邮件地址发送给您。

## 下载 Nessus

要下载 Nessus，请访问 Nessus 下载页面。

下载

步骤二：

下载对应版本的Nessus（这里选择Linux-Debian-amd64平台，此平台对于比较新的Kali版本都适用），保存到/Downloads/文件夹（或者其他文件夹）

## 下载

下载 / 内苏斯

## 内苏斯

### 1 下载并安装 Nessus

#### 选择下载

版本

Nessus - 10.3.0



平台

Linux - Debian - amd64



📄 下载

校验和

[通过 curl 下载 >](#)

[Docker & 虚拟机 >](#)

### 2 启动和设置 Nessus

打开Nessus并按照设置向导完成Nessus设置

### 3 入门

查看我们 的Nessus文档

## 概括

发布日期：2022 年 7 月 11 日

发行说明：

[Nessus 10.3.0 发行说明](#)

签名密钥：

[RPM-GPG-KEY-Tenable-1024](#)

[RPM-GPG-KEY-Tenable-2048](#)

步骤三：

在终端中，我们将导航到包含刚才所下载文件的文件夹并运行以下命令：

```
#sudo dpkg -i package_file.deb
```

```
sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb    #请记住用你下载的文件名称替换  
package_file.deb
```

```
(root@hekeats)-[/home/hekeats/下载]  
# sudo dpkg -i Nessus-10.3.0-debian9_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 379115 个文件和目录。)
```

```
准备解压 Nessus-10.3.0-debian9_amd64.deb ...
```

```
正在解压 nessus (10.3.0) ...
```

```
正在设置 nessus (10.3.0) ...
```

```
Unpacking Nessus Scanner Core Components...
```

```
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service  
- Then go to https://hekeats:8834/ to configure your scanner
```

记录信息备用：

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to <https://hekeats:8834/> to configure your scanner

步骤四：

现在我们将用以下命令启动 Nessus 服务：

```
sudo /bin/systemctl start nessusd.service
```

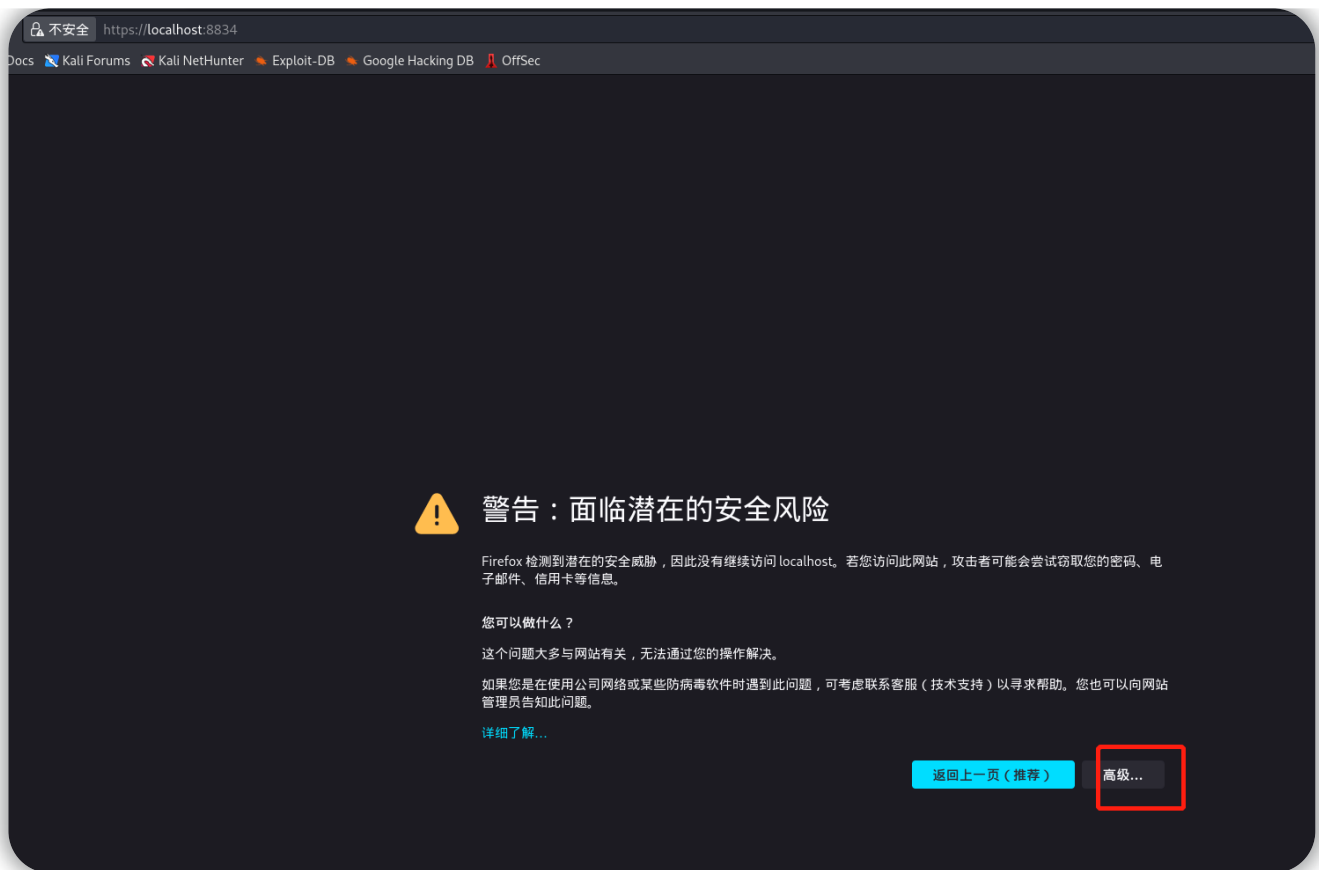
步骤五：

打开网站访问本地8834端口：

```
#在浏览器url中输入
```

```
https://localhost:8834/    #也可以使用自己的kali账户名：https://hekeats:8834/
```

你可能会收到安全风险警报提示，单击“高级...” -> 接受风险并继续：



步骤六：

接下来，我们将设置扫描器，选择Nessus Essentials选项：



## Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ☒ Nessus Essentials
- ☐ Nessus Professional
- ☐ Nessus Expert
- ☐ Nessus Manager
- ☐ Managed Scanner

Continue

© 2022 Tenable™, Inc.

接下来选择skip，因为我们之前已经注册了账户，并在自己的邮箱里面收到了激活码：



## Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First \*

Last \*

Email \*

Skip

Back

Email

© 2022 Tenable™, Inc.

填入之前在邮箱中收到的激活码即可：



## Register Nessus

Enter your activation code.

Activation Code \*

☐ Register Offline

[Settings](#)

[Back](#)

[Continue](#)

© 2022 Tenable™, Inc.

创建Nessus使用时进行登陆的账户和密码：





**nessus**<sup>®</sup>  
Essentials

## Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username \*

Password \*

Back

Submit

© 2022 Tenable<sup>™</sup>, Inc.

步骤八：

Nessus 现在将安装运行所需的插件（如果进度条看起来没有移动，这意味着 VM 上没有足够的空间来安装）。



## Initializing

Please wait while Nessus prepares the files needed to scan your assets.

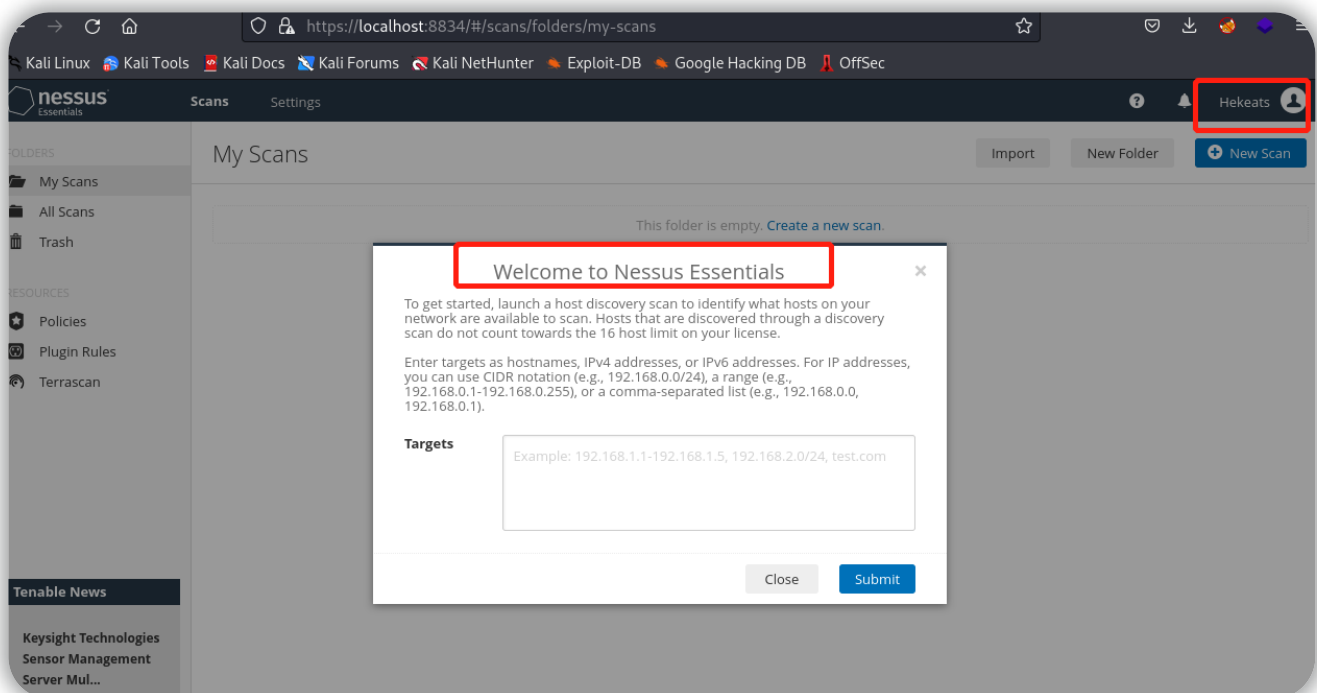
Downloading plugins...



© 2022 Tenable™, Inc.

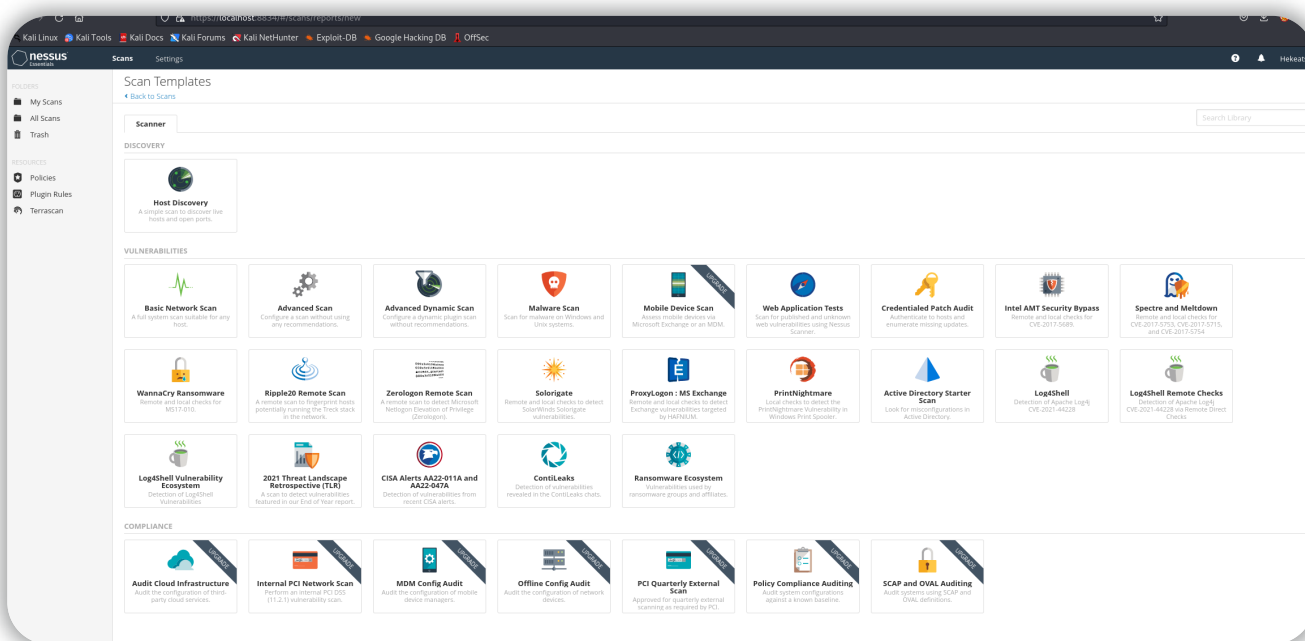
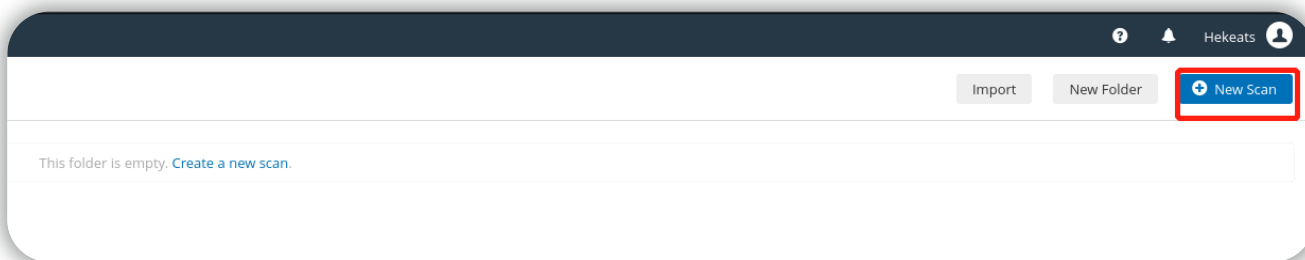
步骤九：

使用之前设置的账户密码--登陆即可。

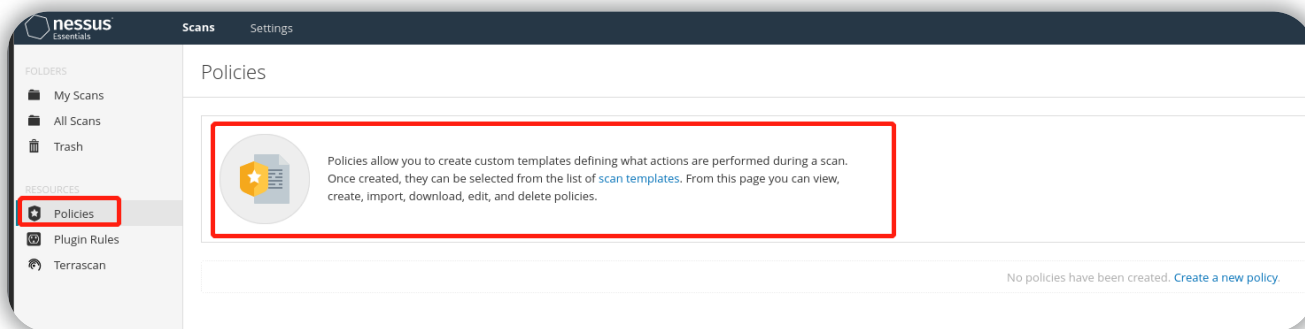


## H2 Nessus 导航和扫描

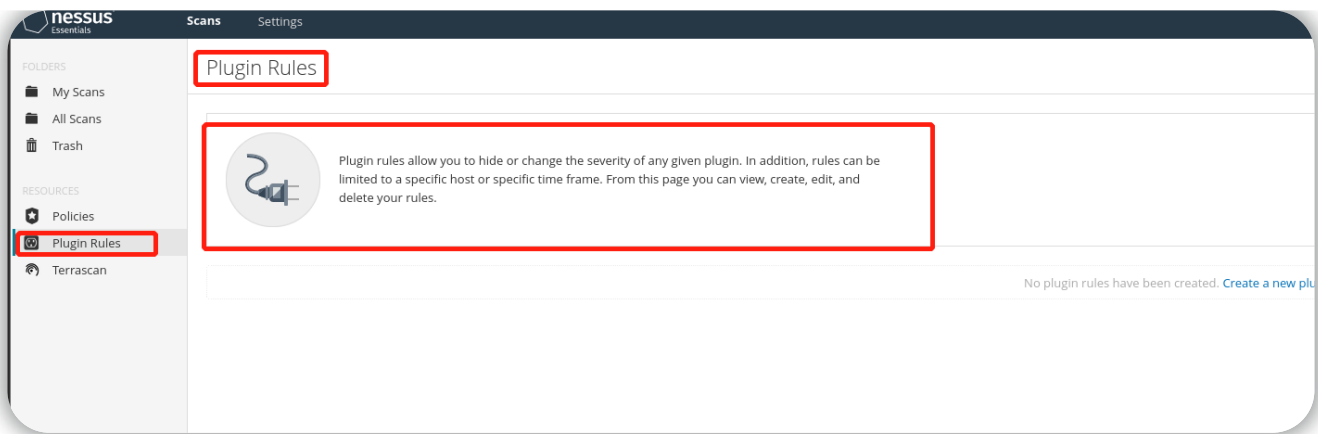
点击右上角的"New Scan"按钮，进入到Nessus的导航和扫描界面：



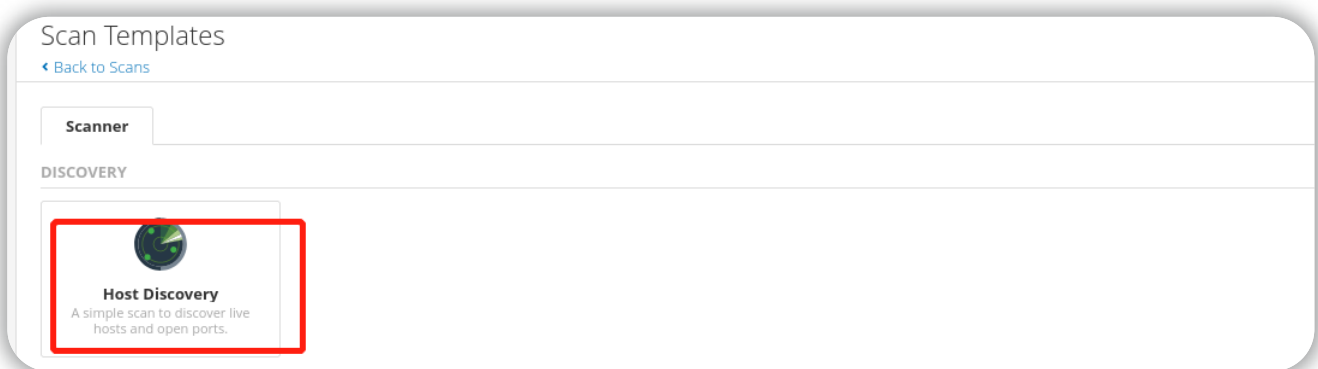
策略页面--允许你创建自定义模板来定义扫描过程中执行的操作。一旦创建好了自定义模版，你就可以从扫描（scan）模板列表中选择它们。从该页面，你可以查看、创建、导入、下载、编辑和删除策略。



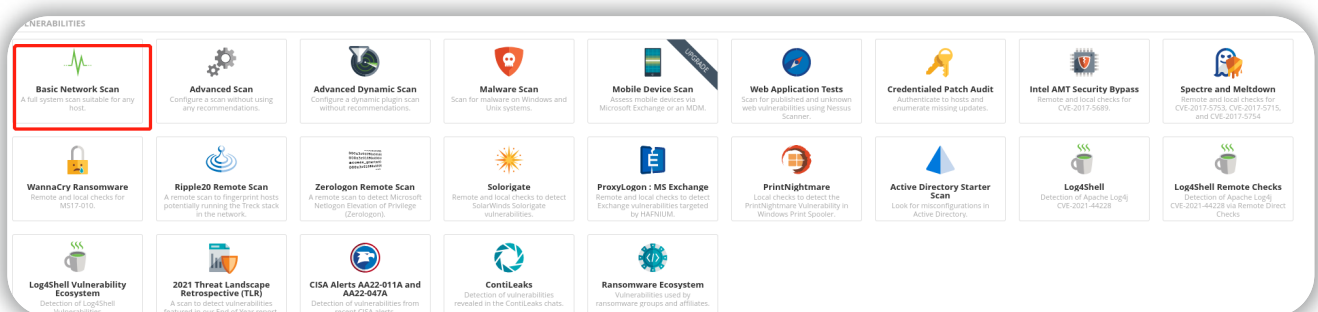
插件规则页面--插件规则允许你隐藏或更改任何给定插件的严重性，此外，规则可以限制在特定的主机或特定的时间范围内。你可以从这个页面查看创建、编辑和删除规则。



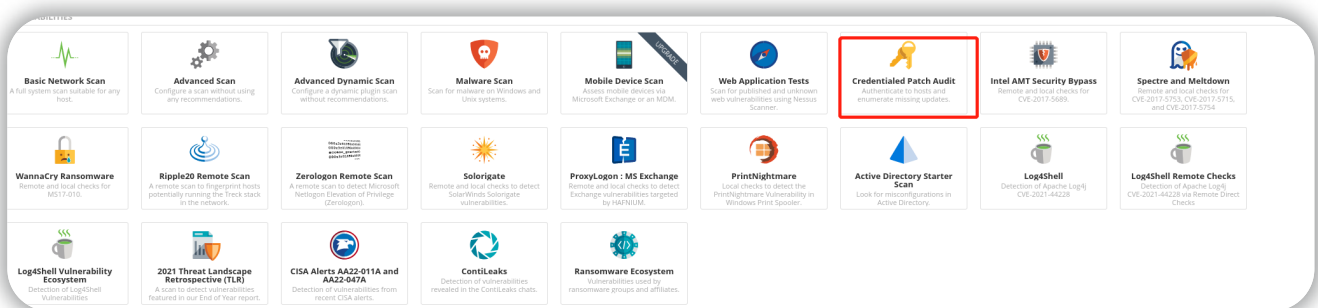
使用NewScan页面的Host Discovery功能，可以让我们简单地看到哪些主机是存活的。



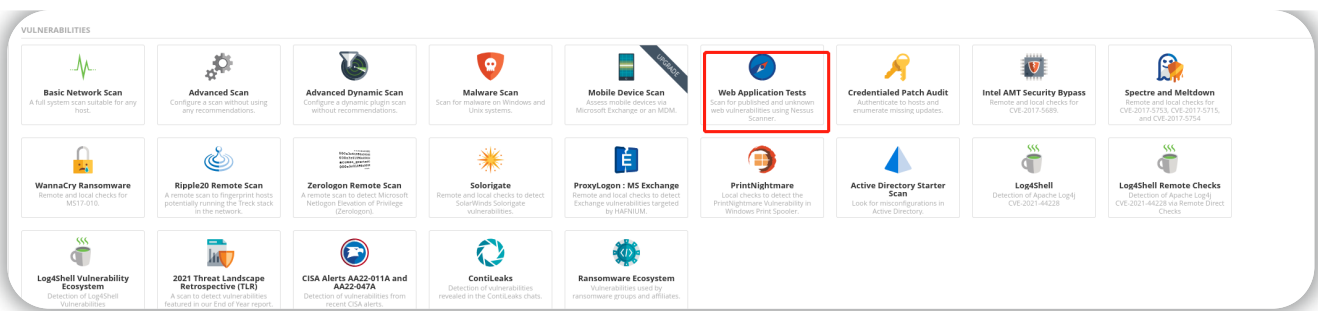
NewScan页面的 Basic Network Scan是最有用的扫描类型之一，被认为“适用于任何主机”：



NewScan页面的 Credentialed Patch Audit扫描允许你“向主机验证并枚举缺失的更新”



NewScan页面的Web Application Tests扫描--专门用来扫描 Web 应用程序



## 答题卡

### Answer the questions below 回答下面的问题

What is the name of the **button** which is used to launch a scan?

用于启动扫描的按钮的名称是什么？

New Scan

Correct Answer 正确答案

💡 Hint 提示

What side menu option allows us to create **custom templates**?

哪个侧面菜单选项允许我们创建自定义模板？

Policies

Correct Answer 正确答案

💡 Hint 提示

What menu allows us to change **plugin** properties such as hiding them or changing their severity?

什么菜单允许我们改变插件属性，比如隐藏它们或者改变它们的严重性？

Plugin Rules

Correct Answer 正确答案

💡 Hint 提示

In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

在点击“新扫描”之后的“扫描模板”部分，什么扫描方式可以让我们简单地看到哪些主机是存活的？

Host Discovery

Correct Answer 正确答案

One of the most useful scan types, which is considered to be '**suitable for any host**'?

最有用的扫描类型之一，被认为是“适合任何主机”？

Basic Network Scan

Correct Answer 正确答案

What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

什么扫描允许你“认证主机和枚举缺失的更新”？

Credentialed Patch Audit

Correct Answer 正确答案

What scan is specifically used for scanning **Web Applications**?

什么扫描是专门用来扫描 Web 应用程序的？

Web Application Tests

Correct Answer 正确答案

## H2

## 运行网络扫描！

启用靶机并通过Openvpn将kali连接到TryHackMe的靶场内网环境。

本小节将使用Basic Network Scan扫描，开始扫描前先进选项设置。

在以下界面设置本次扫描的名称和扫描的目标（New Scan button > Basic Network Scan > Settings > BASIC > General）：

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Test

Description:

Folder: My Scans

Targets: 10.10.124.89

Upload Targets Add File

可以设置Schedule选项来设定扫描运行的时间（也可以不设置），选择New Scan button > Basic Network Scan > Settings > BASIC > Schedule:

nessus Essentials

Scans Settings

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Enabled: ON

NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. [Upgrade to Nessus Professional](#)

Frequency: Once

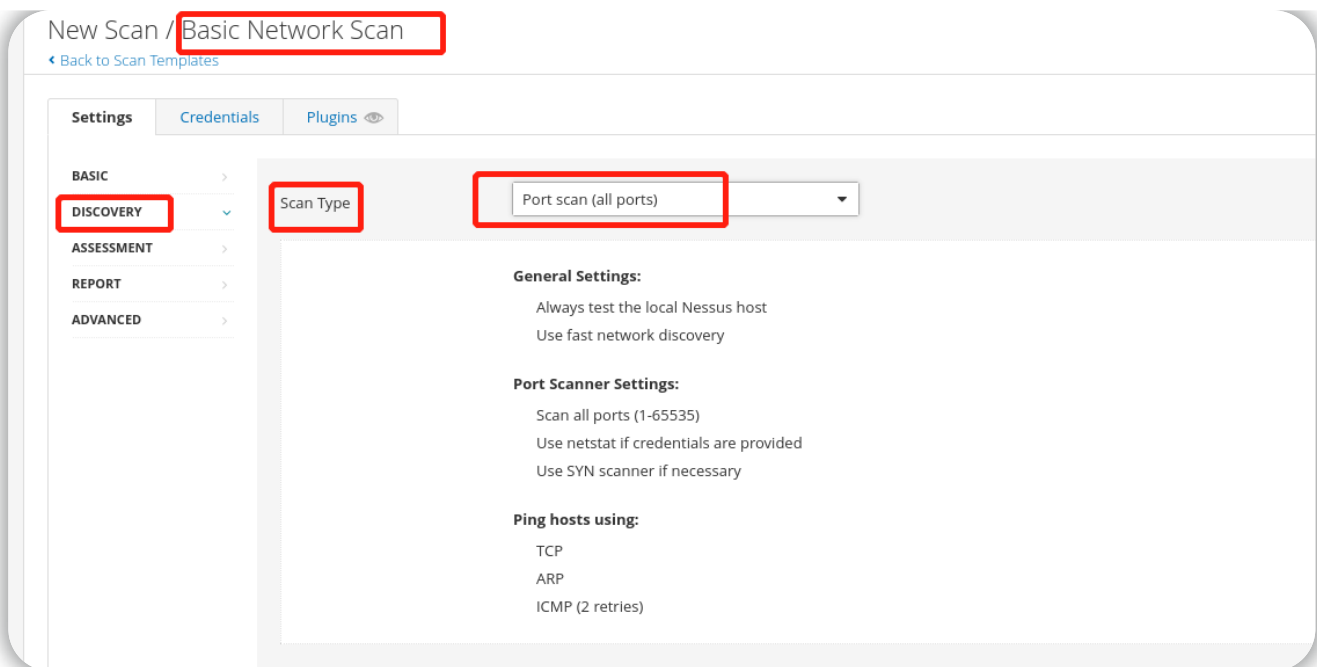
Starts: 22:00 2022-10-14

Timezone: PRC

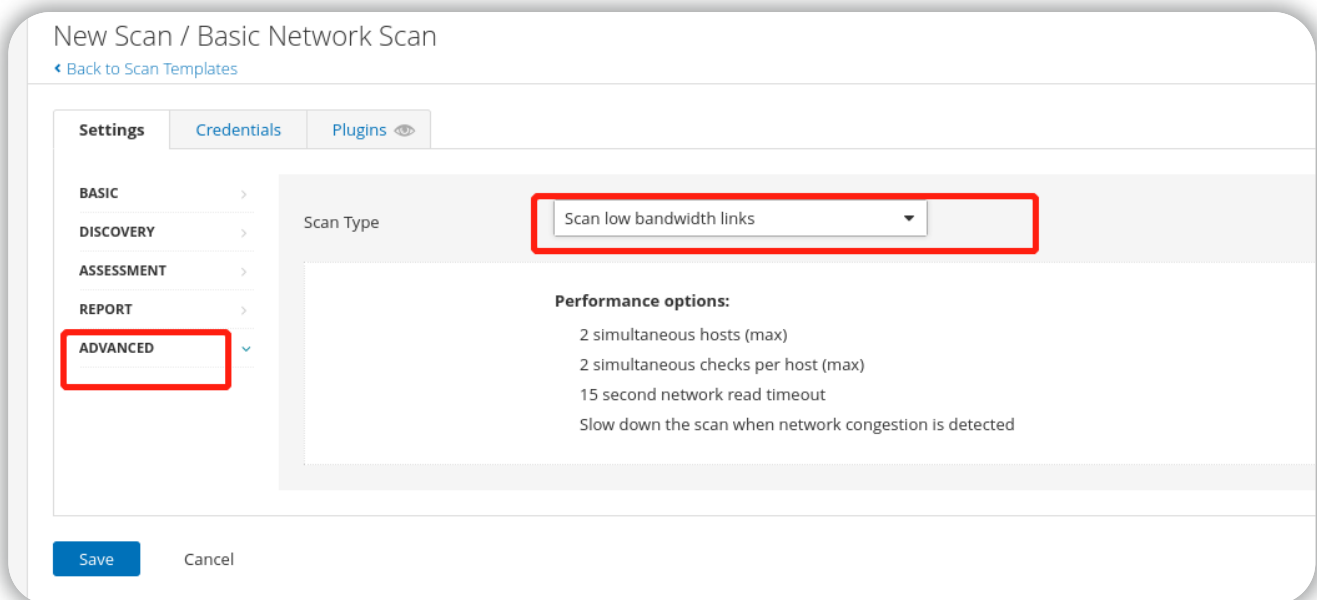
Summary: Once on Friday, October 14th, 2022 at 10:00 PM

Save Cancel

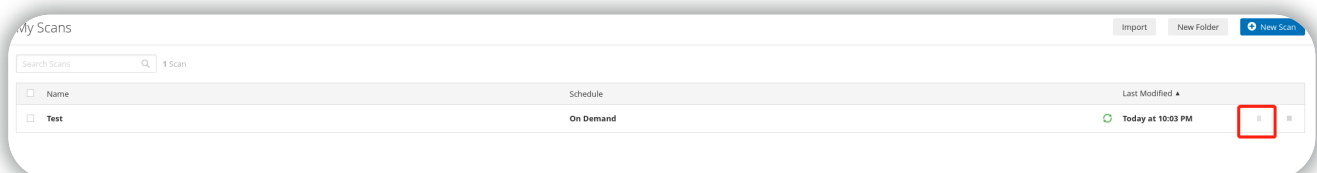
在DISCOVERY里面的扫描类型（Scan Type）中可以选择要扫描的端口，可以设置为全端口扫描、通用端口扫描、自定义端口扫描。



在ADVANCED选项下设置扫描类型为Scan low bandwidth links，使用较低的带宽连接进行扫描：



设置完成之后，保存配置并开始扫描：



等待扫描完成（可能需要1-5分钟），查看扫描结果即可。

查看开放的端口详细信息：

Test

[Back to My Scans](#)

Hosts 1 Vulnerabilities 9 Notes 1 History 1

Filter Search Vulnerabilities 9 Vulnerabilities

Sev	Score	Name
INFO	...	2 HTTP (Multiple Issues)
INFO		Host Fully Qualified Domain Name (FQDN) Resolution
INFO		ICMP Timestamp Request Remote Date Disclosure
INFO		Inconsistent Hostname and IP Address
INFO		Nessus SYN scanner
INFO		Service Detection
INFO		TCP/IP Timestamps Supported
INFO		Traceroute Information
INFO		Web Server robots.txt Information Disclosure

查看开放的端口详细信息

Test / Plugin #11219

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 11 Notes 1 History 1

INFO Nessus SYN scanner

**Description**

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Output**

Port 80/tcp was found to be open

Port	Hosts
80 / tcp / www	10.10.124.89

查看Apache HTTP Server 版本:

Test

[Back to My Scans](#)

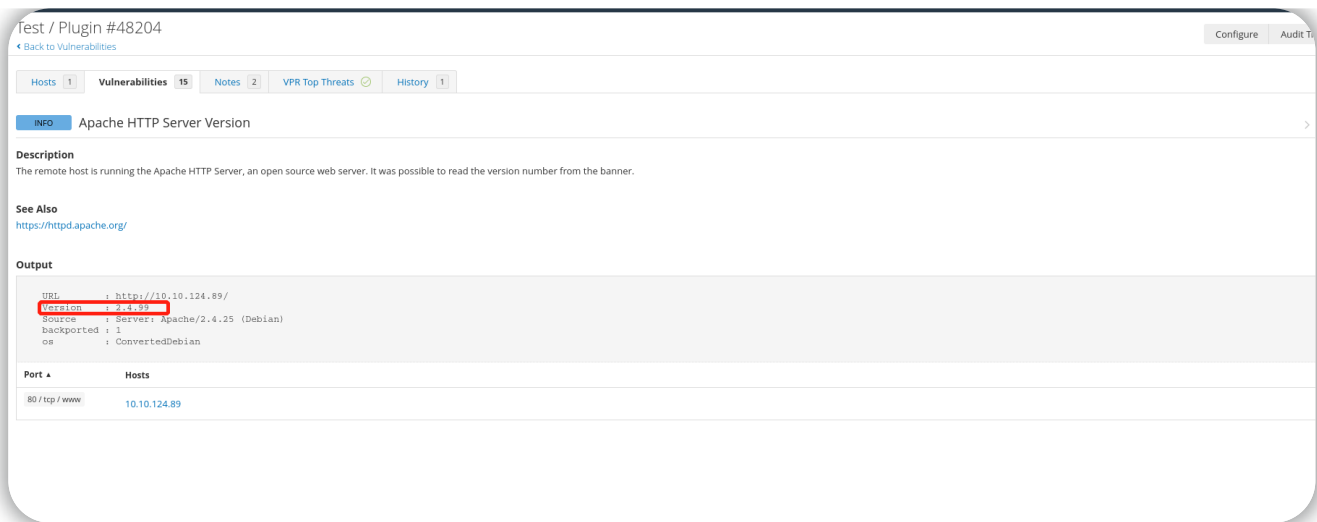
Hosts 1 Vulnerabilities 15 Notes 2 VPR Top Threats History 1

Filter Search Vulnerabilities 15 Vulnerabilities

Sev	Score	Name
INFO	...	2 HTTP (Multiple Issues)
INFO		Apache HTTP Server Version
INFO		Backported Security Patch Detection (WWW)
INFO		Common Platform Enumeration (CPE)
INFO		Device Type

查看Apache HTTP Server 版本





## 答题卡

Create a new 'Basic Network Scan' targeting the deployed VM. What option can we set under 'BASIC' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

针对已部署的 VM 创建一个新的“基本网络扫描”。我们可以在“BASIC”下面(左边)设置什么选项来设定扫描运行的时间？当拥塞控制是个问题时，这会非常有用。

Schedule Correct Answer 正确答案

Under 'DISCOVERY' (on the left) set the 'Scan Type' to cover ports 1-65535. What is this type called?

在“DISCOVERY”下(左边)设置“Scan Type”以覆盖端口1-65535。这种类型叫什么？

Port scan (all ports) Correct Answer 正确答案

What 'Scan Type' can we change to under 'ADVANCED' for lower bandwidth connection?

什么“扫描类型”，我们可以改为‘优先’为较低的带宽连接？

Scan low bandwidth links Correct Answer 正确答案

With these options set, launch the scan.

设置好这些选项后，启动扫描。

No answer needed Correct Answer 正确答案

After the scan completes, which 'Vulnerability' in the 'Port scanners' family can we view the details of to see the open ports on this host?

扫描完成后，在“端口扫描器”系列中的哪个“漏洞”我们可以查看这个主机上打开的端口的详细信息？

Nessus SYN scanner Correct Answer 正确答案

What Apache HTTP Server Version is reported by Nessus?

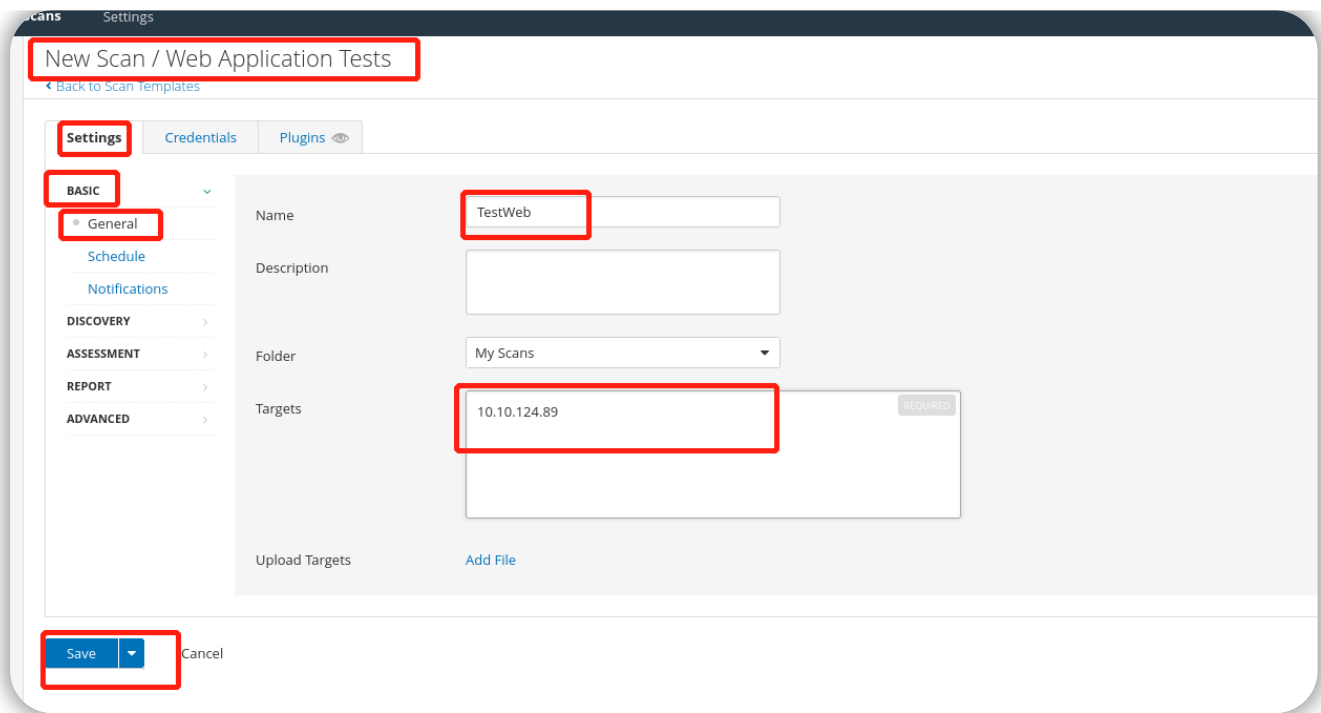
Nessus报告的 Apache HTTP Server 版本是什么？

2.4.99 Correct Answer 正确答案 Hint 提示

## H2 运行 Web 应用程序扫描！

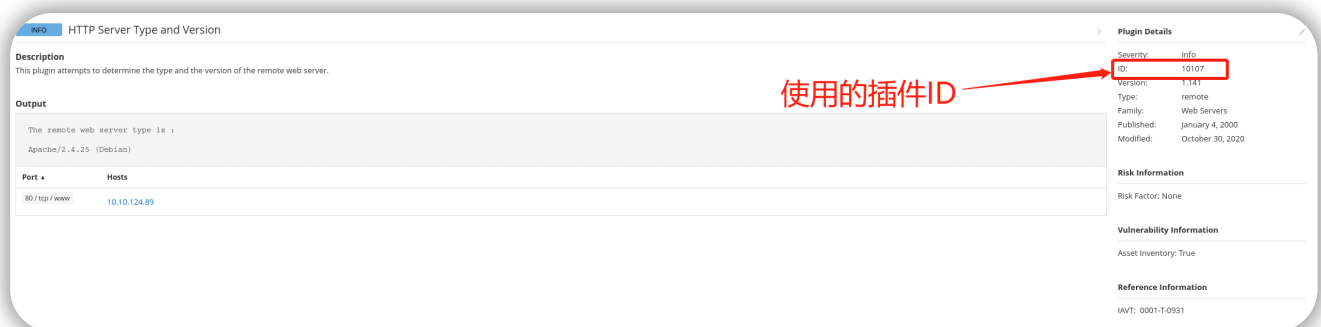
现在进行web应用程序扫描，运行此扫描将需要一些时间来完成，请耐心等待！！

选择New Scan button > Web Application Tests ，在目标文本字段中输入目标机的ip地址，保存设置并启动扫描，最后等待结果即可



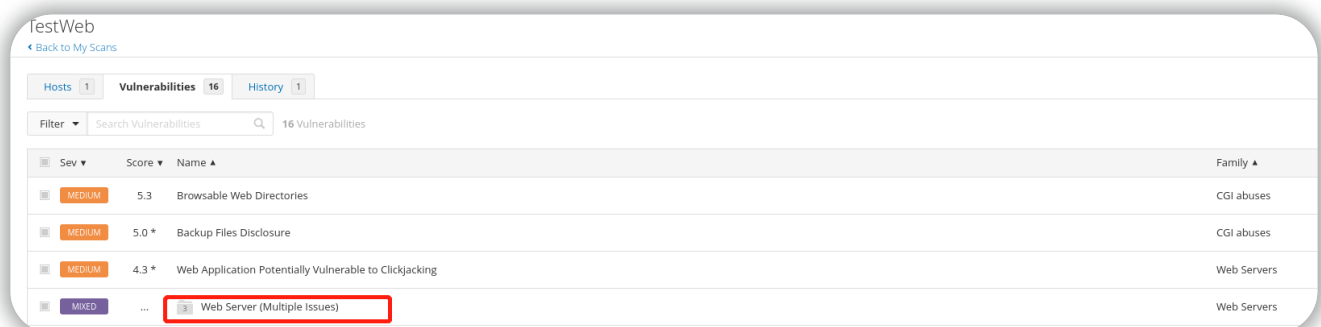
查看扫描结果并回答问题

识别"HTTP 服务器类型和版本"的插件的ID 是什么？

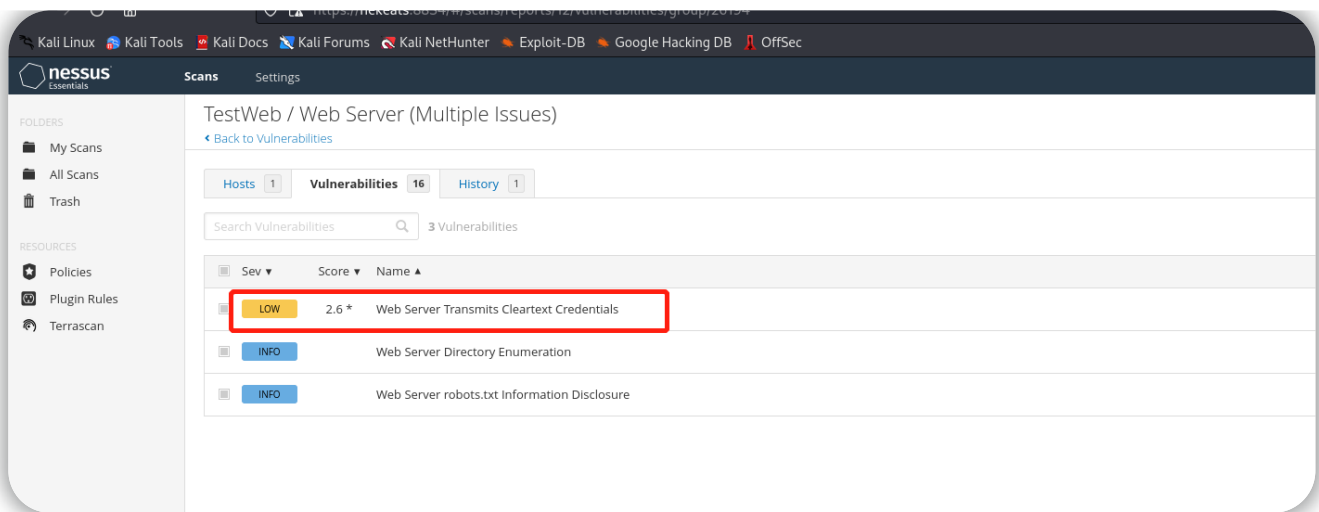


扫描器发现了哪个身份验证页面以明文形式传输凭据？

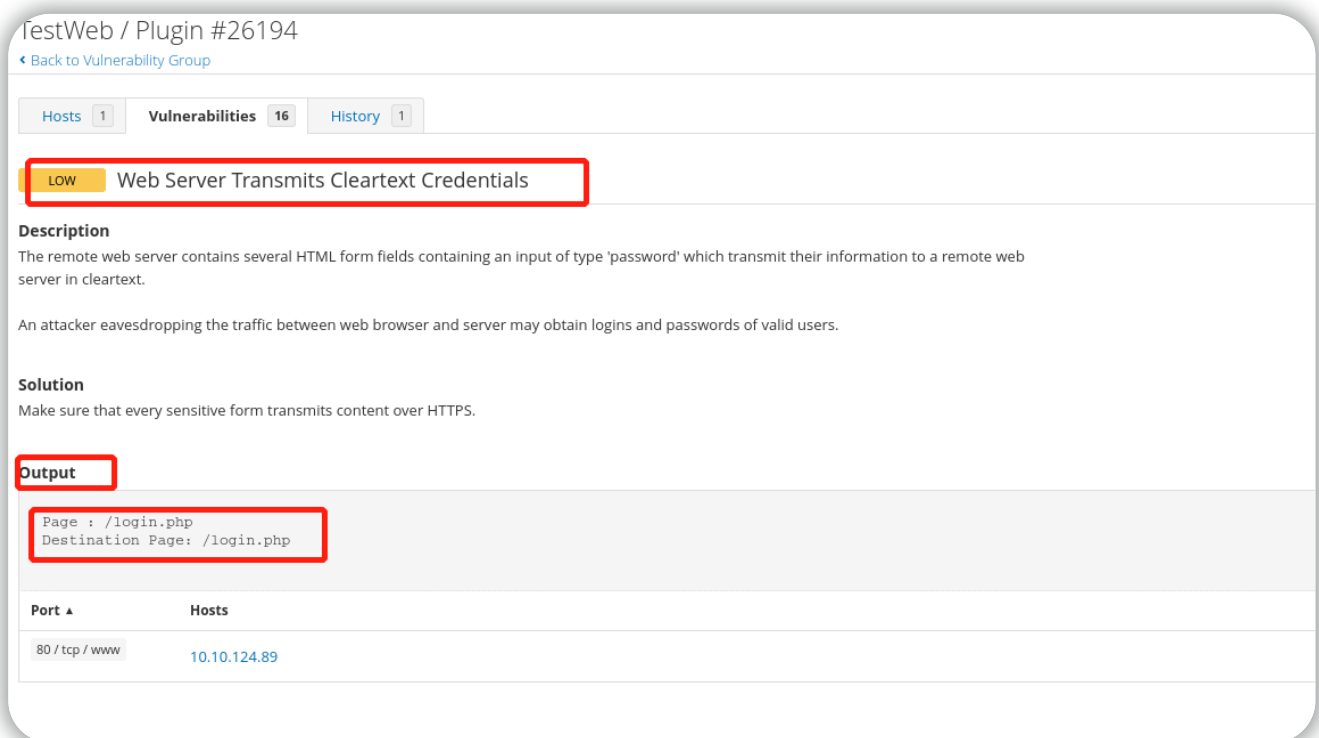
单击行项目"Web 服务器（多个问题）"



然后单击行项目"Web 服务器传输明文凭据"

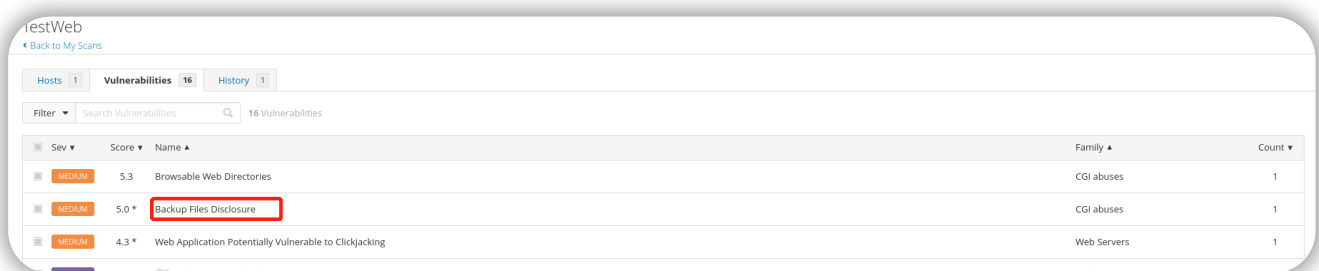


在输出部分下，你将看到传输明文凭据的页面。



配置备份的文件扩展名是什么？

单击“Backup Files Disclosure”漏洞行项。



备份文件的扩展名可以在漏洞详细信息的“输出”部分找到：

Hosts 1 Vulnerabilities 16 History 1

**MEDIUM Backup Files Disclosure**

**Description**  
By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

**Solution**  
Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

**See Also**  
<http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location>

**Output**

```
It is possible to read the following backup file :  
- File : /config/config.inc.php.bak  
  URL  : http://localhost/config/config.inc.php.bak
```

**Port** **Hosts**

80 / tcp / www	10.10.124.89
----------------	--------------

哪个目录包含示例文档？（在 php 目录中）

TestWeb  
Back to My Scans

Hosts 1 Vulnerabilities 16 History 1

Filter Search Vulnerabilities 16 Vulnerabilities

Sev	Score	Name	Family
MEDIUM	5.3	Browsable Web Directories	CGI abuses
MEDIUM	5.0 *	Backup Files Disclosure	CGI abuses
MEDIUM	4.3 *	Web Application Potentially Vulnerable to Clickjacking	Web Servers

**MEDIUM Browsable Web Directories**

**Description**  
Multiple Nessus plugins identified directories on the web server that are browsable.

**Solution**  
Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

**See Also**  
<http://www.nessus.org/u70a35179e>

**Output**

```
The following directories are browsable :  
  
http://localhost/config/  
http://localhost/docs/  
http://localhost/dvwa/  
http://localhost/dvwa/css/  
http://localhost/dvwa/images/  
http://localhost/dvwa/includes/  
http://localhost/dvwa/includes/DBMS/  
http://localhost/dvwa/js/  
http://localhost/external/  
http://localhost/external/phpids/  
http://localhost/external/phpids/0.6/  
http://localhost/external/phpids/0.6/docs/  
http://localhost/external/phpids/0.6/docs/examples/  
http://localhost/external/phpids/0.6/lib/  
http://localhost/external/phpids/0.6/lib/IDS/  
http://localhost/external/phpids/0.6/tests/  
http://localhost/external/phpids/0.6/tests/IDS/  
http://localhost/external/recaptcha/  
  
less...
```

此web应用程序容易受到与 X-Frame-Options 相关联的哪些漏洞的影响？

Hosts 1

Vulnerabilities 16

Notes 4

History 1

MEDIUM

## Web Application Potentially Vulnerable to Clickjacking

点击劫持

## Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

## Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

## See Also

<http://www.nessus.org/u?399b1f56>[https://www.owasp.org/index.php/Clickjacking\\_Defense\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet)<https://en.wikipedia.org/wiki/Clickjacking>

## Output

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- http://localhost/login.php

Port ▲

Hosts

80 / tcp / www

10.10.124.89

## 答题卡

## Answer the questions below 回答下面的问题

What is the plugin id of the plugin that determines the HTTP server type and version?

决定 HTTP 服务器类型和版本的插件的 ID 是什么？

10107

Correct Answer 正确答案

Hint 提示

What authentication page is discovered by the scanner that transmits credentials in cleartext?

扫描器会发现哪个身份验证页以明文形式传输凭据？

/login.php

Correct Answer 正确答案

Hint 提示

What is the file extension of the config backup?

配置备份的文件扩展名是什么？

.bak

Correct Answer 正确答案

Hint 提示

Which directory contains example documents? (This will be in a php directory) 哪个目录包含示例文档？(在 php 目录中)

/external/phpids/0.6/docs/examples/

Correct Answer 正确答案

Hint 提示

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

这个应用程序容易受到与 X-Frame-Options 相关的哪些漏洞的影响？

Clickjacking

Correct Answer 正确答案

Hint 提示