



Nessus Room

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Task 1: Introduction

Nessus vulnerability scanner is precisely what its name suggests: a vulnerability scanner. It employs techniques akin to those used by Nmap to detect and report vulnerabilities, which are then displayed in an easy-to-navigate GUI. What sets Nessus apart from other scanners is its lack of assumptions during scans; for example, it doesn't automatically presume that a web application is operating on port 80.

Nessus provides both free and paid services, with certain features excluded from the free version to encourage users to opt for the paid service. Its pricing structure is comparable to that of Burp Suite, so unless you have some extra funds, we will primarily be utilizing the free version.

For more information on their pricing options, you can visit:

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

Task 2:

You need to install Nessus tool

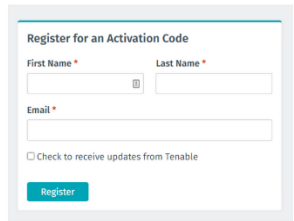
Warning: Do not install Nessus on the THM AttackBox. It will not work, as there's no sufficient space!

Step 1:

Register for an Activation code

Go to <https://www.tenable.com/products/nessus/nessus-essentials> and register an account.

Step #1



Goto <https://www.tenable.com/products/nessus/nessus-essentials> and register an account.

Step 2:

Download file

1 Download and Install Nessus

Choose Download

Version

Nessus - 10.8.3

Platform

Linux - Ubuntu - amd64

Download

Checksum

[Download by curl >](#)

[Docker >](#)

[Virtual Machines >](#)

Summary

Release Date: Sep 11, 2024

Release Notes:
[Tenable Nessus 10.8.3 Release Notes](#)

Signing Keys:
[RPM-GPG-KEY-Tenable-4096\(10.4 & above\)](#)
[RPM-GPG-KEY-Tenable-2048\(10.3 & below\)](#)

Step 3:

In the terminal we will navigate to that folder and run the following command:

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

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~[~/Downloads]
$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 439906 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PR_F : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
```

step 4:

We will now start the Nessus Service with the command:

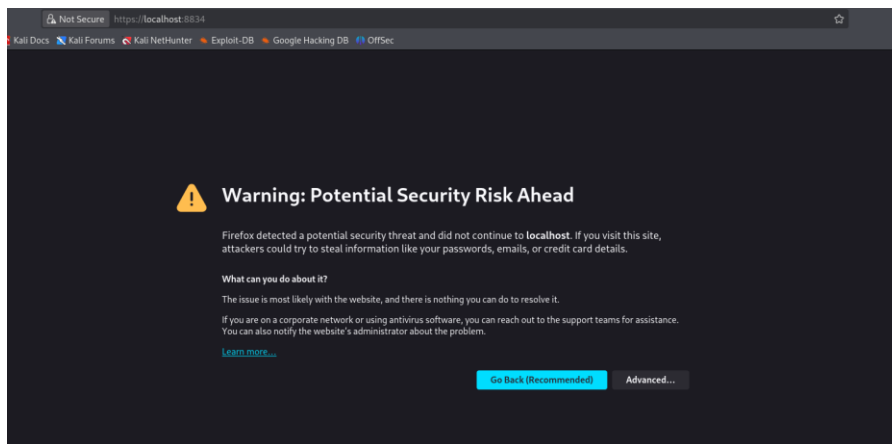
`sudo /bin/systemctl start nessusd.service`

```
(kali㉿kali)-[~/Downloads]
$ sudo /bin/systemctl start nessusd.service
```

step 5:

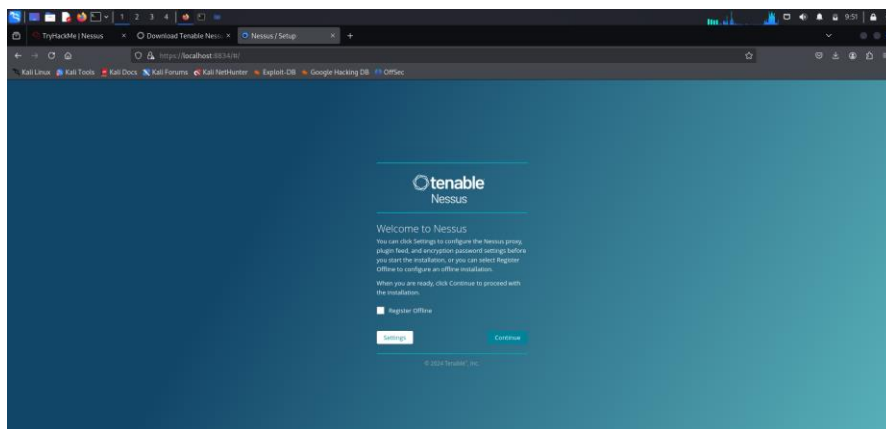
Open up Firefox and goto the following URL:

<https://localhost:8834/>



You may be prompted with a security risk alert.

Click Advanced... -> Accept the Risk and Continue



Next:

Then Fill out the Username and Password fields. Make sure to use a strong password!

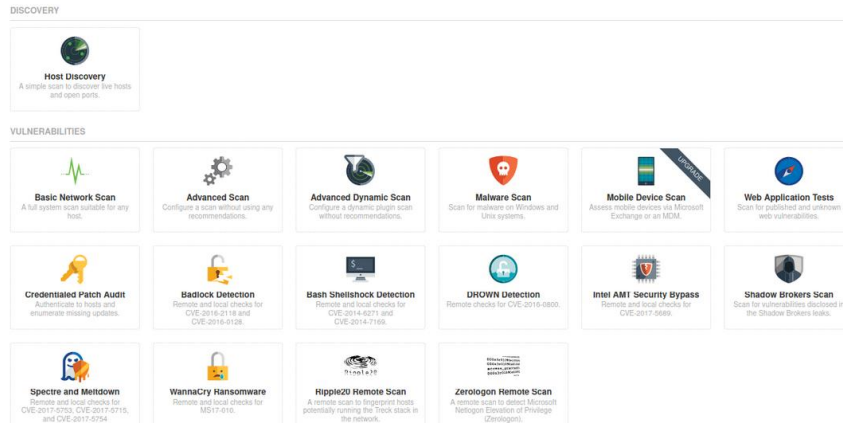
And log in.

Finally:

You have now successfully installed Nessus!

Task 3: Navigation and Scans

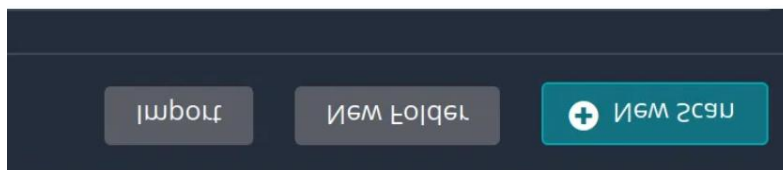
Scan types!



Questions:

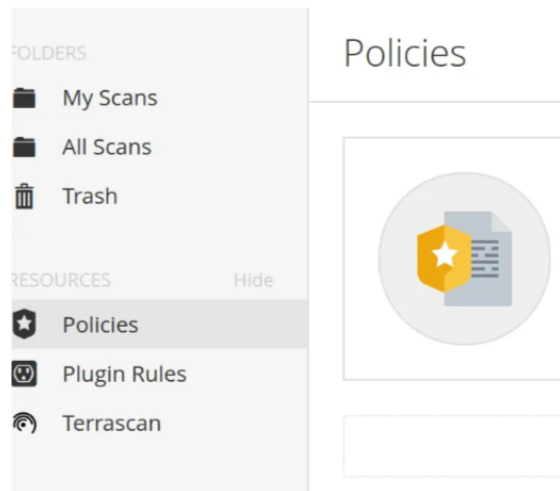
What is the name of the button which is used to launch a scan?

Answer : **New scan**



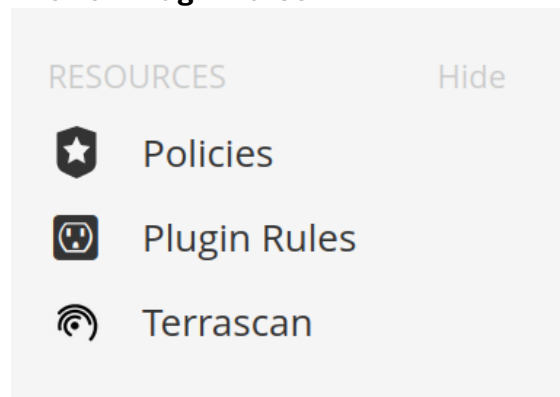
What side menu option allows us to create **custom templates**?

Answer: **Policies**



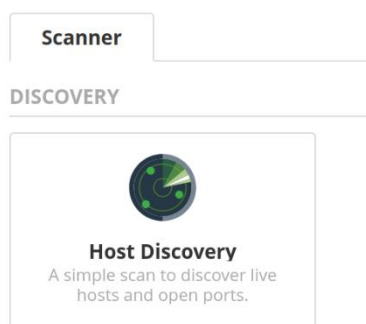
What menu allows us to change **plugin** properties such as hiding them or changing their severity

Answer: **Plugin Rules**



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

Answer: **Host Discovery**



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

Answer: **Basic Network Scan**

VULNERABILITIES



Basic Network Scan

A full system scan suitable for any host.

What scan allows you to ‘Authenticate to hosts and enumerate missing updates’?

Answer: **Credentialed Patch Audit**



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

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

Answer: **Web Application Tests**



Web Application Tests

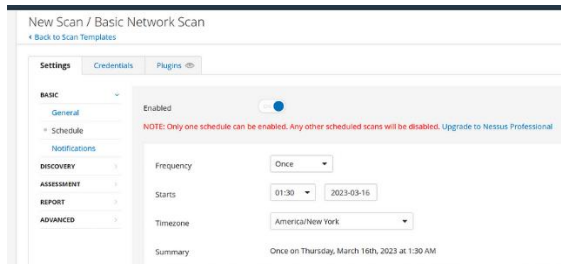
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Task 4: Scanning

Run a Network Scan!

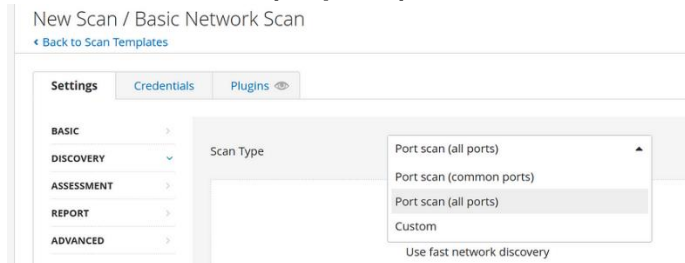
Create a new '**Basic Network Scan**' targeting the deployed VM. What option can we set under '**BASIC**' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Answer: **Schedule**



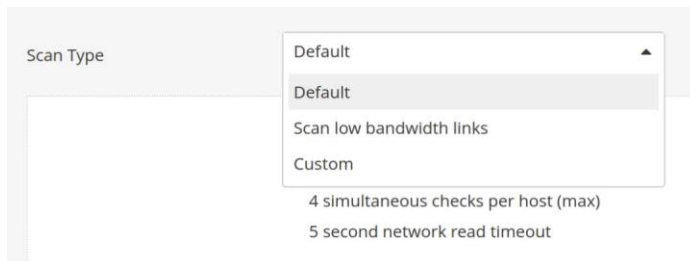
Under '**DISCOVERY**' (on the left) set the '**Scan Type**' to cover ports 1–65535. What is this type called?

Answer: **Port scan (all ports)**



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

Answer: **Scan low bandwidth links**



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?

Answer: **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

To see debug logs, please visit individual host

Port ▲	Hosts
80/tcp/www	10.10.140.178

What **Apache HTTP Server Version** is reported by Nessus?

Answer: **2.4.99**

```
URL      : http://10.10.140.178/
Version  : 2.4.99
Source   : Server: Apache/2.4.25 (Debian)
backported : 1
os       : ConvertedDebian
```

Task 5: Scanning a Web Application!

Run a Web Application scan



Questions:

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

Answer: **10107**

Plugin Details	
Severity:	Info
ID:	10107
Version:	1.141
Type:	remote
Family:	Web Servers
Published:	January 4, 2000
Modified:	October 30, 2020

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

Answer: **login.php**

Hosts 1
Vulnerabilities 17
History 1

Filter Search Vulnerabilities 17 Vulnerabilities

Sev	CVSS	VPR	Name
MEDIUM	5.3		Browsable Web Directories
MEDIUM	5.0 *		Backup Files Disclosure
MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking
MIXED	3 Web Server (Multiple Issues)
INFO	4 HTTP (Multiple Issues)

Output

```

Page : /login.php
Destination Page: /login.php

To see debug logs, please visit individual host

```

Port	Hosts
80 / tcp / www	10.10.140.178

What is the file extension of the config backup?

Answer: **.bak**

History 1

Vulnerabilities 17

Hosts 2

Filter

Search Vulnerabilities

Sev	CVSS	VPR	Name
MEDIUM	5.3		Browsable Web Directories
MEDIUM	5.0 *		Backup Files Disclosure

Output

It is possible to read the following backup file :

- File : /config/config.inc.php.bak
- URL : http://10.10.140.178/config/config.inc.php.bak

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	10.10.140.178

Which directory contains example documents? (This will be in a php directory)

Answer: [/external/phpids/0.6/docs/examples/](http://10.10.140.178/external/phpids/0.6/docs/examples/)

Hosts 1

Vulnerabilities 17

History 1

Filter

Search Vulnerabilities

Sev	CVSS	VPR	Name
MEDIUM	5.3		Browsable Web Directories
MEDIUM	5.0 *		Backup Files Disclosure

Output

The following directories are browsable :

```

http://10.10.140.178/config/
http://10.10.140.178/docs/
http://10.10.140.178/dvwa/
http://10.10.140.178/dvwa/css/
http://10.10.140.178/dvwa/images/
http://10.10.140.178/dvwa/includes/
http://10.10.140.178/dvwa/includes/DBMS/
http://10.10.140.178/dvwa/js/
http://10.10.140.178/external/
http://10.10.140.178/external/phpids/
http://10.10.140.178/external/phpids/0.6/
http://10.10.140.178/external/phpids/0.6/docs/
http://10.10.140.178/external/phpids/0.6/docs/examples/
http://10.10.140.178/external/phpids/0.6/lib/
http://10.10.140.178/external/phpids/0.6/lib/IDS/
http://10.10.140.178/external/phpids/0.6/tests/
http://10.10.140.178/external/phpids/0.6/tests/IDS/
http://10.10.140.178/external/recaptcha/
less...

```

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

Answer: **Clickjacking**

Hosts 1

Vulnerabilities 17

History 1

Search Vulnerabilities

2 Vulnerabilities

Sev	CVSS	VPR	Name	Family
INFO			Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	CGI abuses
INFO			Missing or Permissive X-Frame-Options HTTP Response Header	CGI abuses

INFO Missing or Permissive X-Frame-Options HTTP Response Header

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

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

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Plugin Details

Severity:	Info
ID:	50345
Version:	1.5
Type:	remote
Family:	CGI abuses
Published:	October 26, 2010
Modified:	January 19, 2021