

Pruebas de Seguridad

ISC Ericka Jazmín Robles Gomes

Los Campuseros

Ing. Sistemas Computacionales
ITSZO

Instalación de Nessus para pruebas de seguridad

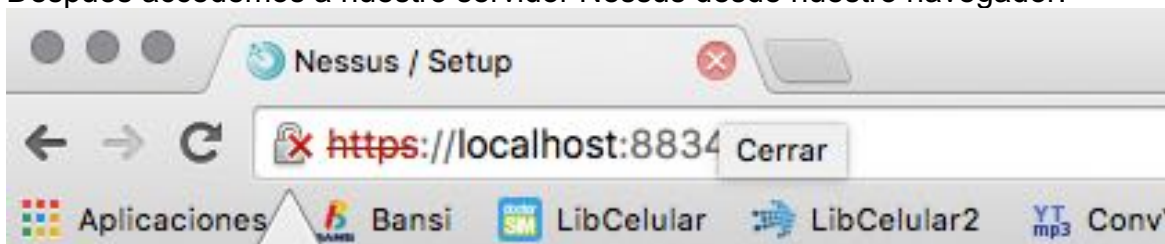
Descargamos Nessus desde la página Oficial

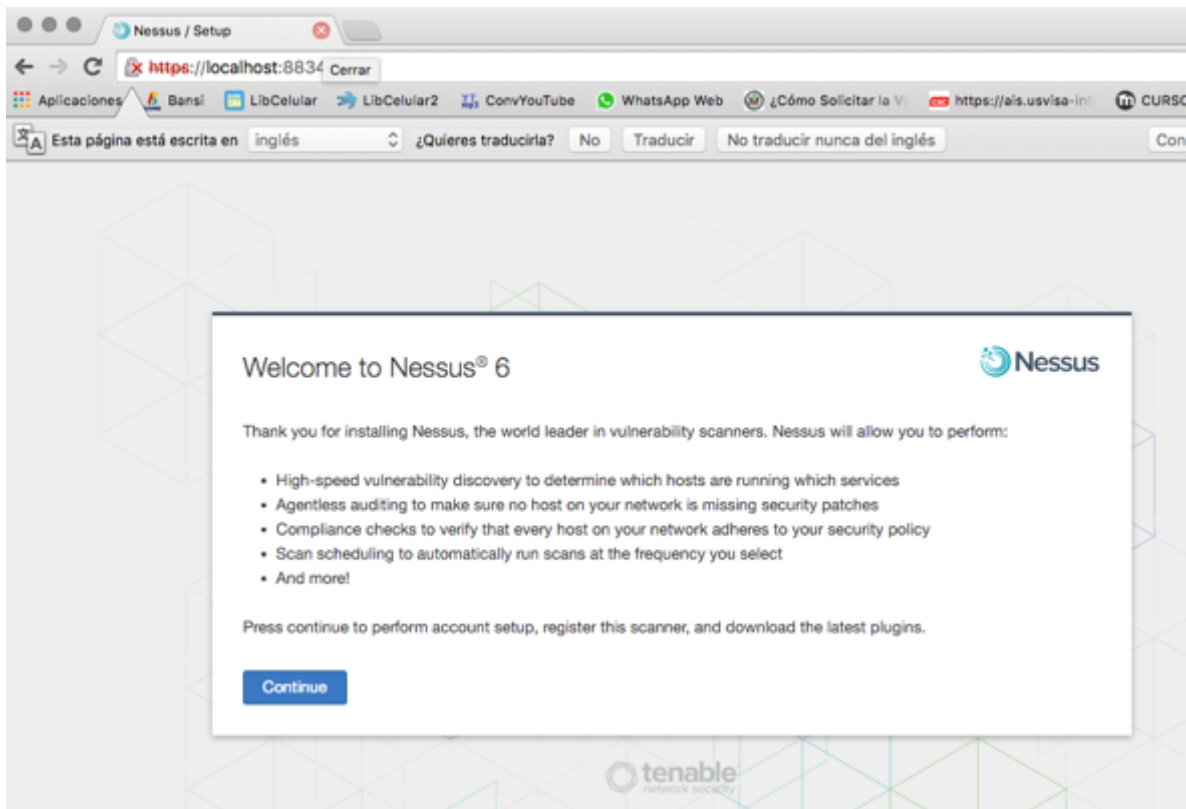
(<http://www.tenable.com/products/nessus/select-your-operating-system#tos>)

Una vez descargado lo descomprimos y lo instalamos en nuestro PC:



Después accedemos a nuestro servidor Nessus desde nuestro navegador:





Al dar clic en el botón azul nos mandara a una pantalla para iniciar Sesión en donde vamos a ingresar los datos de la cuenta que tuvimos que haber registrado anteriormete en la página oficial de Nessus:

A screenshot of the Nessus Account Setup page. The page has a light gray background with a faint geometric pattern. At the top, it says 'Account Setup' and the Nessus logo. A paragraph explains that a 'System Administrator' account must be created. Below this, there are three input fields: 'Username' (containing 'Aldring Bueno'), 'Password' (masked with dots), and 'Confirm Password' (also masked with dots). At the bottom, there is a blue 'Continue' button and a 'Back' link. A warning note at the bottom states that the user has the ability to execute commands on remote hosts.



The screenshot shows the Nessus Home registration page. On the left, there is a header with the Nessus logo and navigation links: Solutions, Products, Try, Buy, Support & Services, and Company. Below the header, the 'Nessus Home' section includes a brief description of the product, a note about support and additional features, and a disclaimer about personal use. On the right, the 'Register for an Activation Code' form is displayed. It contains fields for First Name (filled with 'Adrian'), Last Name (filled with 'Bueno'), Email (filled with 'jerrybueno@gmail.com'), and Country (a dropdown menu showing 'Mexico'). There are also checkboxes for 'Check to receive updates from Tenable' and 'I agree to the terms of service', both of which are checked. A 'Register' button is at the bottom of the form.

Después metemos el código de activación que Nessus nos proporcionó:



The screenshot shows the 'Product Registration' page in the Nessus interface. It features the Nessus logo in the top right corner. The main text explains that new vulnerability information is released and that registering the scanner grants access to download these plugins. Below the text, there are two input fields: 'Registration' with a dropdown menu showing 'Nessus (Home, Professional or Manager)' and 'Activation Code' with a text box containing 'F06D-03F9-06FF-F160-05C7'. At the bottom, there are three buttons: 'Continue' (highlighted in blue), 'Back', and 'Custom Settings'.

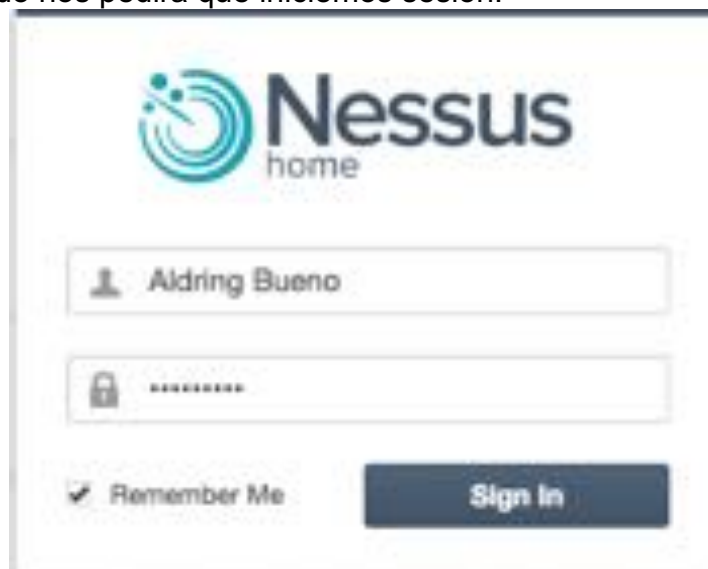
y ya hemos activado Nessus con nuestra cuenta, ahora solo empezará a descargar la herramienta de Nessus, hay que esperar:



Una vez descargado empezará a instalarse:



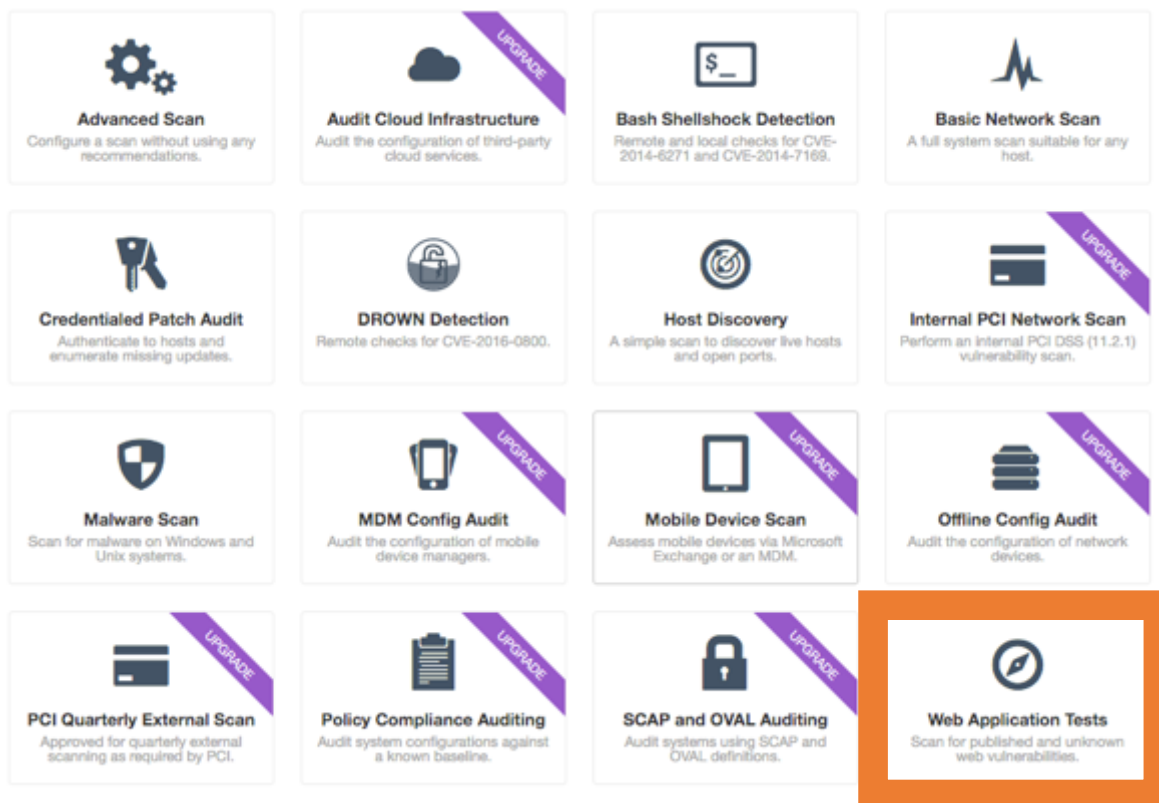
Una vez instalado nos pedirá que iniciemos sesión:



Listo, ya estamos en la GUI de Nessus:



Damos clic en el botón azul para iniciar una nueva prueba y nos mandará a la siguiente pantalla en donde daremos clic en la ultima opción:



En las opciones generales configuramos de la siguiente manera:

Settings / Basic / General

BASIC ▾

- General
- Schedule
- Notifications
- DISCOVERY
- ASSESSMENT
- REPORT
- ADVANCED

Name: Prueba de Seguridad

Description: Sistema de Actividades Extracurriculares

Folder: My Scans ▾

Targets: http://localhost/ServiceActividadesExtracurriculares/

Upload Targets Add File

Save ▾ Cancel

En la sección de notificaciones podemos configurar un correo electrónico para que nos mande un reporte de la prueba:

Settings / Basic / Notifications

BASIC ▾

- General
- Schedule
- Notifications
- DISCOVERY
- ASSESSMENT
- REPORT
- ADVANCED

Notifications will not be sent until your SMTP Server is configured.

Email Recipient(s): junnybueno@gmail.com

Result Filters Add Filter

Save ▾ Cancel

Y en la sección de horarios podemos configurar cuándo queremos que se realice la prueba:

Settings / Basic / Schedule

Enable Schedule ☒

Launch: Once

Starts On: 04/17/2016 01:30

Timezone: America/Mexico City

Summary: Once on Sunday, April 17th, 2016 at 1:30 AM

Save Cancel

Damos clic en “Save” para guardar los cambios hechos de la prueba. Una vez guardada la prueba podemos ver como ya se ha configurado un nueva tarea en el servidor de Nessus:

Nessus Scans Policies Adding

Scans Upload Search Scans

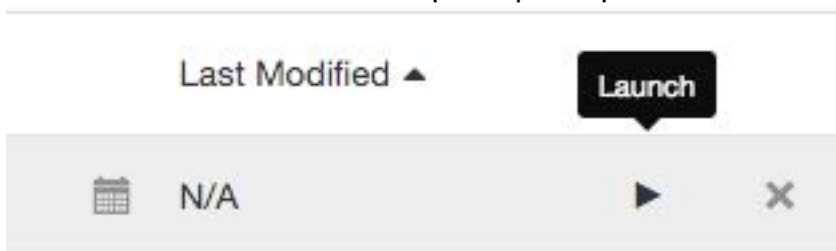
New Scan

Scans / My Scans


Name	Schedule	Last Modified
Prueba de Seguridad	On Demand	N/A

© 2016, 2017 Tenable Network Security, Inc. All Rights Reserved. Nessus 6.10.0

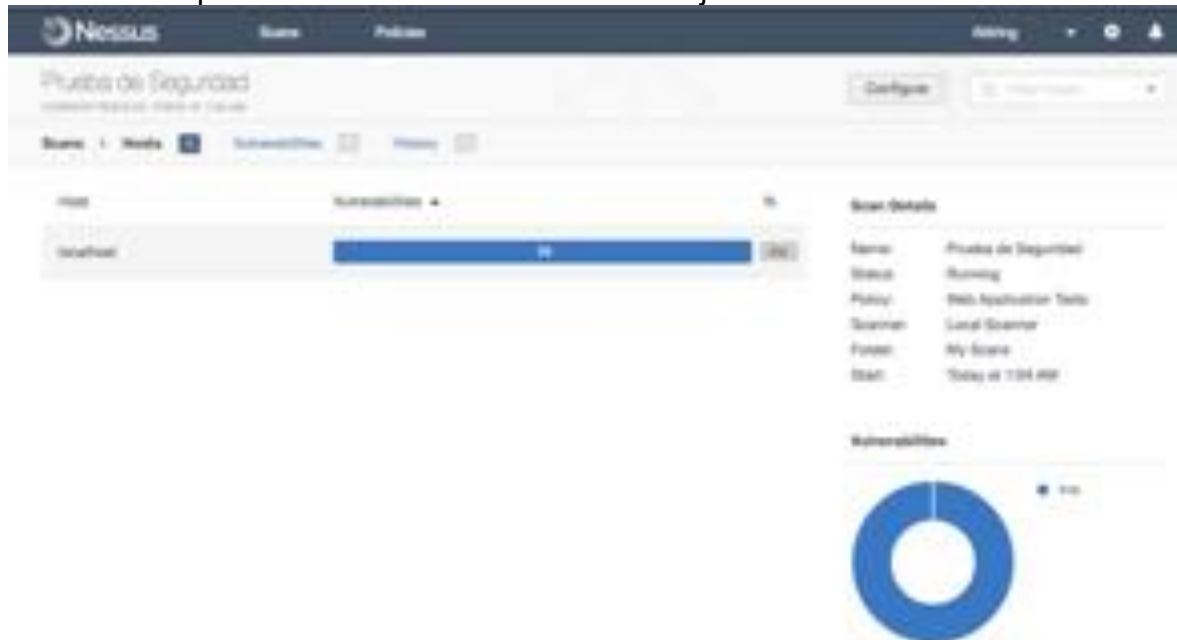
En la línea donde se encuentra la prueba, ahí un botón con símbolo de “Play” y ahí es en donde vamos a dar clic para que la prueba comience a realizarse:



La prueba comienza a realizarse, como podemos ver nos indica en qué hora empezó:

Scans / My Scans				
<input type="checkbox"/>	Name	Schedule	Last Modified ▲	
<input type="checkbox"/>	Prueba de Seguridad	On Demand	01:04 AM	 


Ahora solo queda esperar los resultados de la prueba.
Mientras la prueba se ejecuta nosotros nos podemos meter a la prueba y ver las estadísticas que hasta ese momento nos ha arrojado:






Podemos ver que tenemos dos vulnerabilidades, uno por puertos y otro por directorios de enumeración:



Y el historial que se ha generado de esta prueba, como podemos ver solo se ha ejecutado una vez:

Start Time ▲	End Time	Status
Current Today at 1:04 AM	Today at 1:21 AM	 Running


Para efectos del tutorial vamos a detener la prueba por lo tardados que son:

Last Modified ▲
 01:23 AM  

Stop Scan

Are you sure you want to stop this scan?

Stop Cancel

Last Modified ▲
 01:23 AM

Si nos metemos nuevamente a la prueba podemos ver as estadísticas que ya habíamos visto anteriormente:



Eso ha sido todo en cuanto a las pruebas de seguridad.