

Actividad práctica número 5:

Formato: Individual

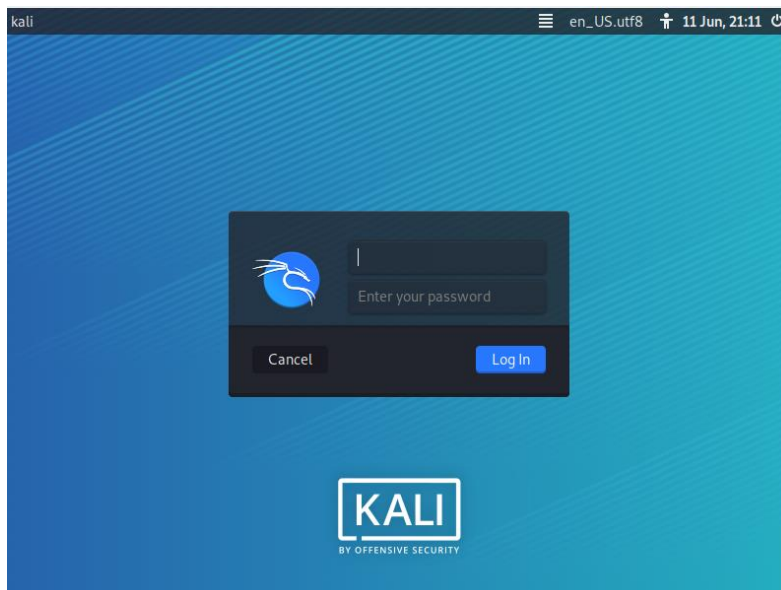
Asignatura: Seguridad de Sistemas

Objetivo: Realizar análisis de vulnerabilidades en Sistema Operativo

Título: Análisis de vulnerabilidades

A.- NESSUS

1.- Inicie su máquina Kali



2.- Actualice el repositorio

```
(root@kali)-[/home/kali]
# apt-get update
Get:1 http://mirror.anquan.cl/kali kali-rolling InRelease [30.5 kB]
Get:2 http://mirror.anquan.cl/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://mirror.anquan.cl/kali kali-rolling/main amd64 Contents (deb) [39.8 MB]
Get:4 http://mirror.anquan.cl/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:5 http://mirror.anquan.cl/kali kali-rolling/contrib amd64 Contents (deb) [123 kB]
Get:6 http://mirror.anquan.cl/kali kali-rolling/non-free amd64 Packages [199 kB]
Get:7 http://mirror.anquan.cl/kali kali-rolling/non-free amd64 Contents (deb) [954 kB]
95% [3 Contents-amd64 store 0 B]
```

3.- Copie los archivos provistos por su profesor al directorio Downloads de su máquina Kali

```
(root@kali)~[/home/kali/Downloads]
# ls -l
total 292572
-rw-r--r-- 1 kali kali 254296460 Jul 11 2020 all-2.0.tar.gz
-rw-r--r-- 1 kali kali 45290778 Jun 11 11:26 Nessus-8.14.0-debian6_amd64.deb
```

4.- Realice la instalación con el siguiente comando

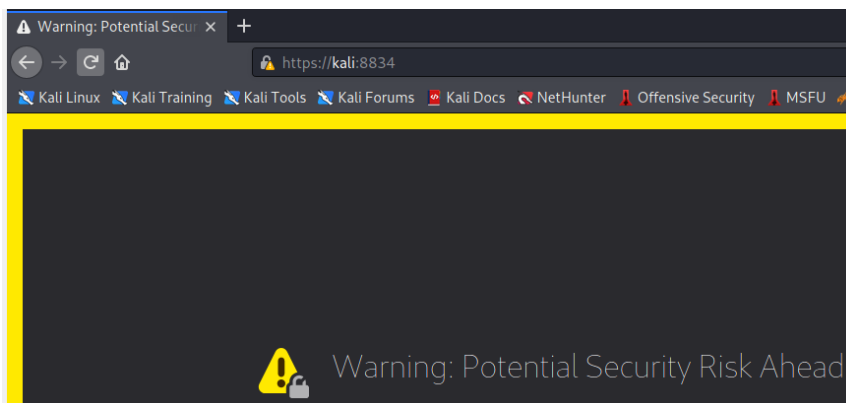
```
(root@kali)~[/home/kali/Downloads]
# dpkg -i Nessus-8.14.0-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 266968 files and directories currently installed.)
Preparing to unpack Nessus-8.14.0-debian6_amd64.deb ...
Unpacking nessus (8.14.0) ...
Setting up nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components ...

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

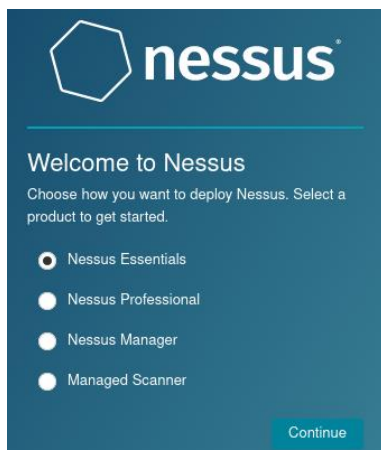
5.- Inicie el servicio Nessus con el siguiente comando

```
(root@kali)~[/home/kali/Downloads]
# /bin/systemctl start nessusd.service
```


6.- Conéctese a la administración web y acepte el certificado digital



7.- Seleccione la opción “Nessus Essentials” y haga click en “Continue”



8.- Complete el formulario y solicite el código de activación por mail



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 *

9.- Seleccione la opción de "Register offline"



Register Nessus

Enter your activation code.

Activation Code *

☒ Register Offline

To get a license key, visit the [Offline Registration](#) site and enter the following challenge code:

efdc4ab71986d27321f3d51cdb1a2c26b2a9a3b2

Nessus License Key *

10.- Conéctese a la siguiente dirección

A screenshot of a web browser displaying the Nessus plugins website. The address bar shows the URL 'https://plugins.nessus.org/v2/offline.php'. The navigation bar includes links for 'Kali Tools', 'Kali Forums', 'Kali Docs', 'NetHunter', 'Offensive Security', 'MSFU', 'Exploit-DB', and 'GHDB'. The main heading is 'Generate a license for Nessus 6.3 and Later'. Below this, a text link says 'To generate a license for an older version of Nessus click here.' There are two input fields: one for a command to run on the Nessusd server and another for an activation code.

11.- Ingrese el código de activación recibido por mail y el código de instalación

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:

efdc4ab71986d27321f3d51cdb1a2c26b2a9a3b2

Enter your activation code here:

E2VB-XRTW-3LS3-ZU56-DFYJ

Submit

12.- Haga click en “Submit” para obtener la licencia

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=1b3d09a20eda9258fbca30b26c34b2f1&p=183c4ee>

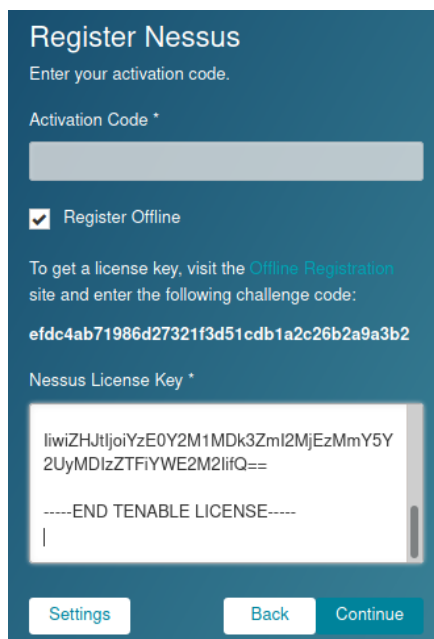
You can copy the following license and paste it into the Nessus console to proceed:

```

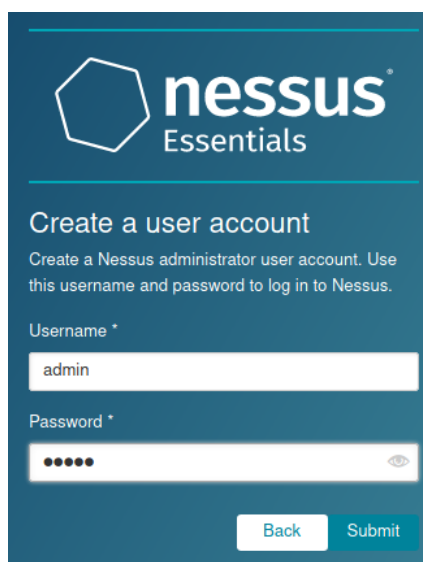
-----BEGIN TENABLE LICENSE-----
WG5tUkoyaWp2VkrAaEH0aDY0cTlVt2NCZE5sMUPtYST3tbTE2NjYyTfHuA1NJa1EwWEt5ZXFWNLZu
TjFnOghhd2U2OXFRUHHN23lEd0p2L3BRUGcyNWhRNUdkd2E0c1g0bUIyDvDLZkhtU0tZSnlsWEdr
L3lod3dIYWpxaGNVVGRVbnY1R0JrSUJjNW85ZjJlSkNLanEzeLJkM1o3NkxQNXRRaHpnY29XUGFh
TzJsaEViellJncLBwN3RnbVJNWGtyTlndndjLCTU8yVWhrZ1VHV3ZWamx5ZlhxRU9zNFNCL0lHU3NM
WddJRjNlTzI0eXh0MmQyVUkROUxUDJ3dGdJURVAdUdd2TTRha1NtcEkrVwtjWmxmNm5vRldEnFhl
L2ZOVOxTdGcwT2WocDyXUnUzYmGfYwJhL1QTzhKV3pISXNlZHMVQVNHNy9DQkNlJzWQeDBHOXQ5dkw5
a0Y2dExRcEFrSW1FbwpgR0RMGMfYU9WWTBKlzEwcDlSdEt0WE1R0mtJNFJiZWhHaw02cGJ2ZW5M

```


13.- Copie la licencia en la interfaz de administración y haga click en “Continue”

The image shows the 'Register Nessus' screen. At the top, it says 'Enter your activation code.' Below this is a text input field for the 'Activation Code *'. There is a checked checkbox for 'Register Offline'. A message states: 'To get a license key, visit the [Offline Registration](#) site and enter the following challenge code:'. Below this is the challenge code: 'efdc4ab71986d27321f3d51cdb1a2c26b2a9a3b2'. Then, it asks for the 'Nessus License Key *' and shows a text area containing a long alphanumeric string: 'liwiZHtIjoiYzE0Y2M1MDk3Zml2MjEzMmY5Y2UyMDIzZTFiYWE2M2liiQ=='. Below the text area is the text '-----END TENABLE LICENSE-----'. At the bottom are three buttons: 'Settings', 'Back', and 'Continue'.

14.- Cree el usuario de administración y haga click en “Submit”

The image shows the 'Create a user account' screen for Nessus Essentials. It features the Nessus logo and the text 'Create a user account'. Below this, it says 'Create a Nessus administrator user account. Use this username and password to log in to Nessus.' There are two input fields: 'Username *' with the value 'admin' and 'Password *' with masked characters. At the bottom are 'Back' and 'Submit' buttons.

15.- Espere a que finalice la compilación de plugins

The image shows the 'Initializing' screen. It features the Nessus logo and the text 'Initializing'. Below this, it says 'Please wait while Nessus prepares the files needed to scan your assets.' There is a progress bar labeled 'Compiling plugins...'.

16.- Copie el archivo de plugins al siguiente directorio

```
(root@kali)~[/home/kali/Downloads]
# cp all-2.0.tar.gz /opt/nessus/sbin

(root@kali)~[/home/kali/Downloads]
# cd /opt/nessus/sbin

(root@kali)~[/opt/nessus/sbin]
# ls -l
total 265100
-rw-r--r-- 1 root root 254296460 Jun 11 21:43 all-2.0.tar.gz
-rwxr-xr-x 1 root root 8401448 Mar 26 16:27 nessuscli
-rwxr-xr-x 1 root root 8720696 Mar 26 16:27 nessusd
-rwxr-xr-x 1 root root 28720 Mar 26 16:27 nessus-service
```

17.- Realice la actualización de la base de datos de plugins

```
(root@kali)~[/opt/nessus/sbin]
# ./nessuscli update all-2.0.tar.gz

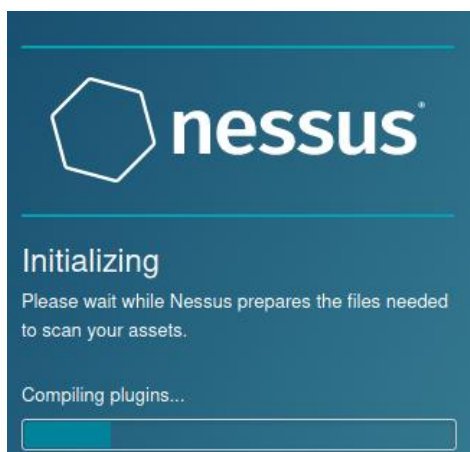
[info] Copying templates version 202006091543 to /opt/nessus/var/nessus/templates/tmp
[info] Finished copying templates.
[info] Moved new templates with version 202006091543 from plugins dir.
* Update successful. The changes will be automatically processed by Nessus.
```

18.- Reinicie el servicio de Nessus

```
(root@kali)~[/opt/nessus/sbin]
# /bin/systemctl stop nessusd.service

(root@kali)~[/opt/nessus/sbin]
# /bin/systemctl start nessusd.service
```

19.- Conéctese nuevamente a la interfaz de administración y espere a que finalice la compilación de plugins



20.- Una vez finalizada, conéctese a la administración nuevamente.

21.- Realice un análisis de vulnerabilidades a la dirección IP dada por su profesor

22.- Una vez finalizado, revise los resultados.

¿Cuántas vulnerabilidades encontró?

¿De qué tipo?

¿Cuál es la clasificación de riesgo que ofrece Nessus?

23.- Ingrese a alguna de las vulnerabilidades críticas y responda

- Descripción: _____

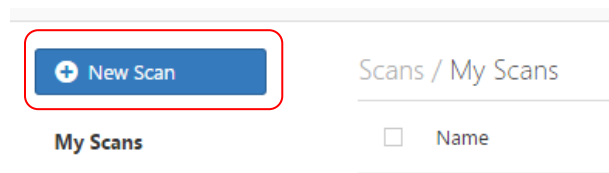
- Solución: _____

- Fecha de publicación: _____

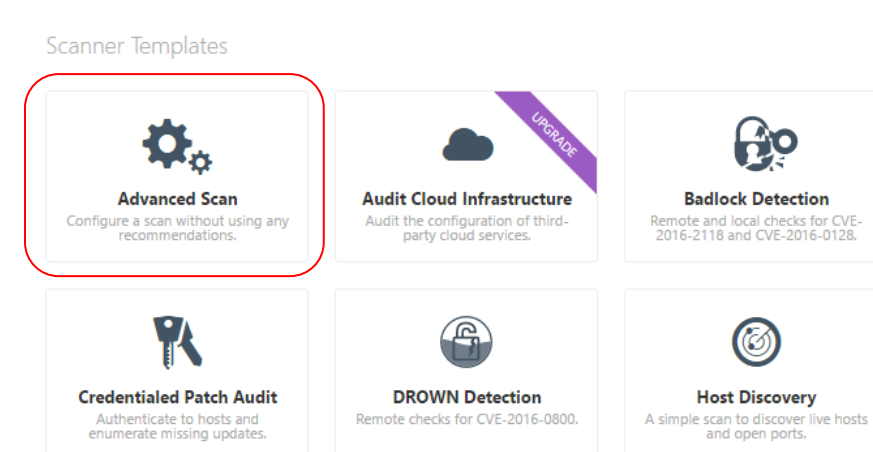
- Código CVE: _____

B.- Análisis con credenciales:

1.- Realizar un nuevo Scan



2.- Seleccionar el template “Advanced Scan”



3.- Ingresar a la opción “Credentials”

The screenshot shows the 'Settings' menu with 'Credentials' highlighted. The left sidebar has categories: BASIC (with a green checkmark), DISCOVERY, and ASSESSMENT. Under BASIC, 'General' is selected. The main area is titled 'Settings / Basic / General' and contains two input fields: 'Name' (with a 'REQUIRED' label) and 'Description'.

4.- Seleccionar la opción de “Windows”

The screenshot shows a list of credentials under the heading 'CREDENTIALS'. The list is organized into categories: 'Cloud Services', 'Database', and 'Host'. Under 'Host', there are three items: 'SNMPv3', 'SSH', and 'Windows'. The 'Windows' item is highlighted with a red box.

5.- Ingresar las credenciales del usuario administrador

The screenshot shows the 'Windows' configuration page. It has a dropdown for 'Authentication method' set to 'Password'. Below it are four input fields: 'Username' (containing 'Administrador'), 'Password' (containing '*****'), and 'Domain' (empty). The 'Username' and 'Password' fields are highlighted with a red box.

6.- A continuación grabe la configuración y complete los datos del Scan

The screenshot shows the 'Scan' configuration page. It has four input fields: 'Name' (containing 'Scan Windows'), 'Description' (containing 'Scan con credenciales'), 'Folder' (a dropdown set to 'My Scans'), and 'Targets' (a large text area containing '172.24.10.137'). At the bottom, there are 'Upload Targets' and 'Add File' links, and a 'Save' button with a dropdown arrow and a 'Cancel' button.

7.- Inicie el scan

| <input type="checkbox"/> | Name | Schedule | Last Modified ▲ | | |
|--------------------------|---------------------------|-----------|-----------------|---|---|
| <input type="checkbox"/> | windows | On Demand | ✓ July 25 | ▶ | ✕ |
| <input type="checkbox"/> | scan 1 | On Demand | ✓ July 25 | ▶ | ✕ |
| <input type="checkbox"/> | scan win con credenciales | On Demand | 📄 N/A | ▶ | ✕ |
| <input type="checkbox"/> | Scan Windows | On Demand | 📄 N/A | ▶ | ✕ |

8.- Espere a que finalice el proceso de scan



9.- Realice el reporte de todas las vulnerabilidades encontradas

Export as HTML

Report

Custom

Data

☒ Vulnerabilities

☒ Remediations

Group by

Plugin

Export

Cancel