

T2 - AUDITORÍA DEL SISTEMA

FECHA

Creado por: Pedro José Riquelme Guerrero



1. Instalación de Lynis

(Linux) Pasos a seguir:

1. Abrir una terminal en el sistema Linux.
2. Actualizar los repositorios del

sistema: `sudo apt update`

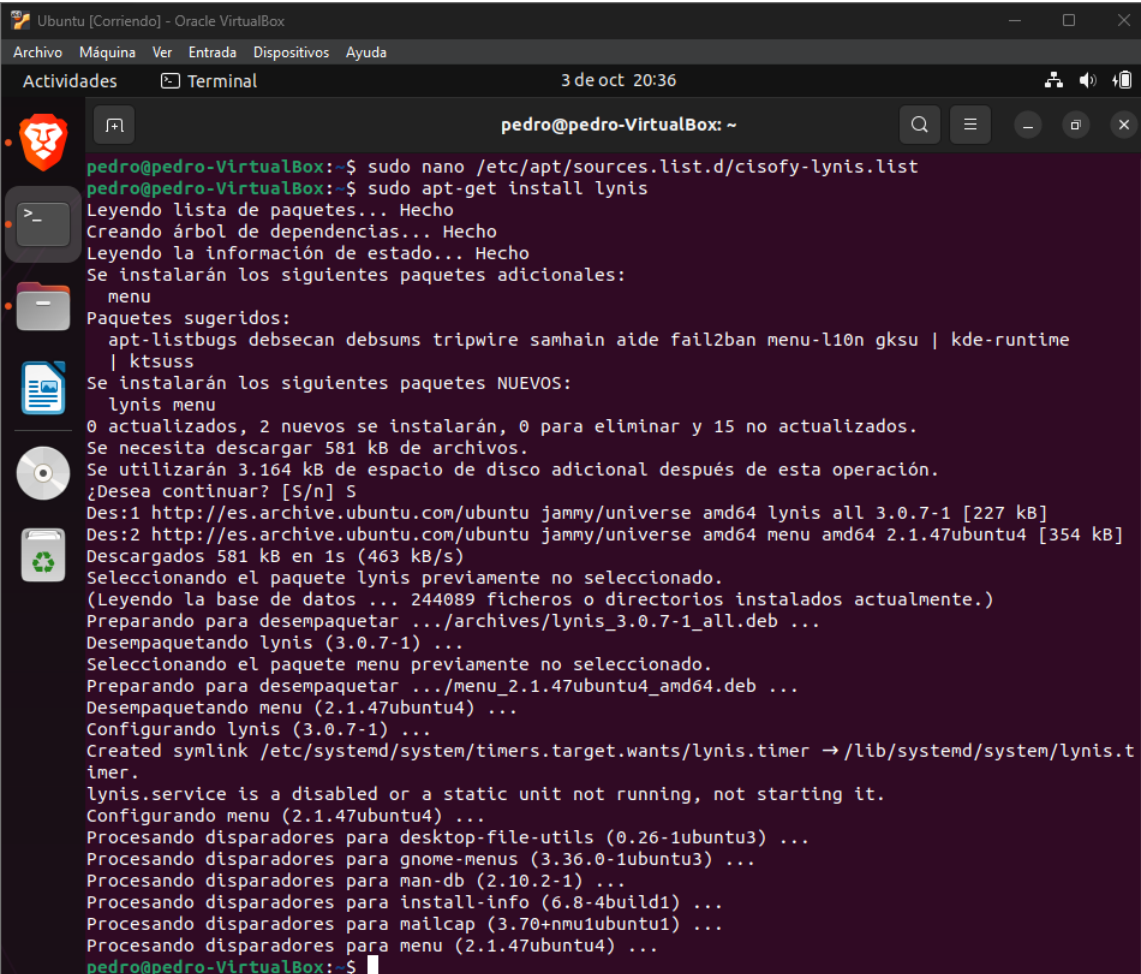
- Captura de pantalla: Aquí deberás colocar la captura de la terminal mostrando que la actualización se completó correctamente.

3. Instalar Lynis:

- Para instalar Lynis, descarga desde el sitio oficial:
 - <https://cisofy.com/lynis/>

- Ejecutamos los siguientes comandos para

instalar: “`sudo apt-get install lynis`”



```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo nano /etc/apt/sources.list.d/cisofy-lynis.list  
pedro@pedro-VirtualBox:~$ sudo apt-get install lynis  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes adicionales:  
  menu  
Paquetes sugeridos:  
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime  
  | ktsuss  
Se instalarán los siguientes paquetes NUEVOS:  
  lynis menu  
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 15 no actualizados.  
Se necesita descargar 581 kB de archivos.  
Se utilizarán 3.164 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] S  
Des:1 http://es.archive.ubuntu.com/ubuntu jammy/universe amd64 lynis all 3.0.7-1 [227 kB]  
Des:2 http://es.archive.ubuntu.com/ubuntu jammy/universe amd64 menu amd64 2.1.47ubuntu4 [354 kB]  
Descargados 581 kB en 1s (463 kB/s)  
Seleccionando el paquete lynis previamente no seleccionado.  
(Leyendo la base de datos ... 244089 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../archives/lynis_3.0.7-1_all.deb ...  
Desempaquetando lynis (3.0.7-1) ...  
Seleccionando el paquete menu previamente no seleccionado.  
Preparando para desempaquetar .../menu_2.1.47ubuntu4_amd64.deb ...  
Desempaquetando menu (2.1.47ubuntu4) ...  
Configurando lynis (3.0.7-1) ...  
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /lib/systemd/system/lynis.t  
imer.  
lynis.service is a disabled or a static unit not running, not starting it.  
Configurando menu (2.1.47ubuntu4) ...  
Procesando disparadores para desktop-file-utils (0.26-1ubuntu3) ...  
Procesando disparadores para gnome-menus (3.36.0-1ubuntu3) ...  
Procesando disparadores para man-db (2.10.2-1) ...  
Procesando disparadores para install-info (6.8-4build1) ...  
Procesando disparadores para mailcap (3.70+nmu1ubuntu1) ...  
Procesando disparadores para menu (2.1.47ubuntu4) ...  
pedro@pedro-VirtualBox:~$
```

4. Ejecutar Lynis para realizar una auditoría del sistema:

Nos creará un acceso directo para poder ejecutar directamente el Lynis

5. Guardar el informe:

Lynis genera un informe con recomendaciones de seguridad. Guarda este informe para analizarlo.

- Comando para guardar el informe en un archivo:

```
sudo lynis audit system --report-file
```

```
/ruta/al/archivo_de_informe.txt
```

2. Instalación de CLARA

(Windows) Pasos a seguir:

1. Descargar CLARA:

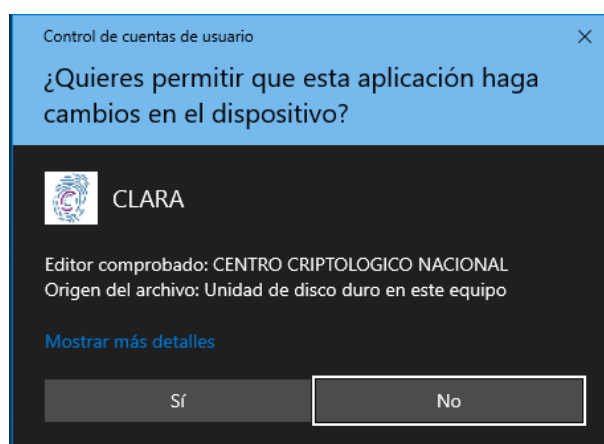
- Para descargar clara nos iremos a el siguiente enlace y descargaremos la versión:
- <https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html>

2. Descomprimir el archivo descargado.

- Utiliza una herramienta como WinRAR o 7-Zip para descomprimir el archivo.



3. Instalar CLARA:

- Seguimos los pasos para la instalación de CLARA, le damos permisos a la aplicación, rellenamos nuestros datos de auditor, organización y unidad. Por lo demás le damos a todo siguiente



CLARA

Fichero Herramientas Opciones Ayuda



 CCN Versión 2.0 

Usuario: DESKTOP-51HC711\Pedro José Riquelme
 Equipo: DESKTOP-51HC711
 Sistema operativo: Microsoft Windows 10 Pro
 Auditor:
 Organización:
 Unidad:
 Fichero de configuración:

El archivo de configuración por defecto está cargado.
 Puede analizar el sistema local ahora pulsando el botón "Analizar".
 Por defecto, se realiza un nivel de análisis del nivel de cumplimiento para un sistema de categoría ALTA.

CLARA - Seguridad ENS

Fichero Herramientas Opciones Ayuda



El ENS establece tres categorías de sistema: Baja, Media y Alta.
 En esta ventana el operador deberá establecer la categoría del sistema que se analiza.
 El usuario puede analizar las actualizaciones de seguridad no instaladas en el sistema. La descarga del fichero de catálogo de actualizaciones se debe realizar previo análisis. El fichero se puede descargar desde el menú "Herramientas > Descargar fichero catálogo actualizaciones...".

Categoría del sistema
 Categoría del sistema:

Análisis de las actualizaciones de seguridad
☒ Analizar actualizaciones de seguridad no instaladas (el servicio de Windows Update debe estar habilitado)

CLARA - Configuración

Fichero Herramientas Opciones Ayuda

Las opciones de configuración permiten establecer la configuración básica de la herramienta como son las carpetas donde se guardan los registros de eventos y los informes generados.

Carpetas y ficheros de la aplicación
 Carpeta de informes:
 Carpeta de eventos:

4. Ejecutar CLARA:

- Abre la aplicación y selecciona "Auditoría completa del sistema".
- Captura de pantalla: Coloca aquí la captura de la pantalla principal de CLARA durante la auditoría.

5. Guardar el informe generado.

- Una vez que CLARA termine el análisis, guarda el informe en tu equipo para su posterior análisis.

3. Instalación de Nessus

(Linux/Windows) Pasos a seguir:

1. Descargar Nessus:

- Accede al sitio web de Nessus:
 - <https://es-la.tenable.com/>
 - <https://www.tenable.com/tenable-for-education/nessus-essentials>
- Rellenamos nuestros datos con todo y esperamos a que nos llegue el Gmail para poder descargar el programa con la licencia gratuita. Una vez nos ha llegado el Gmail nos vamos a la pagina y descargamos el programa.

Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

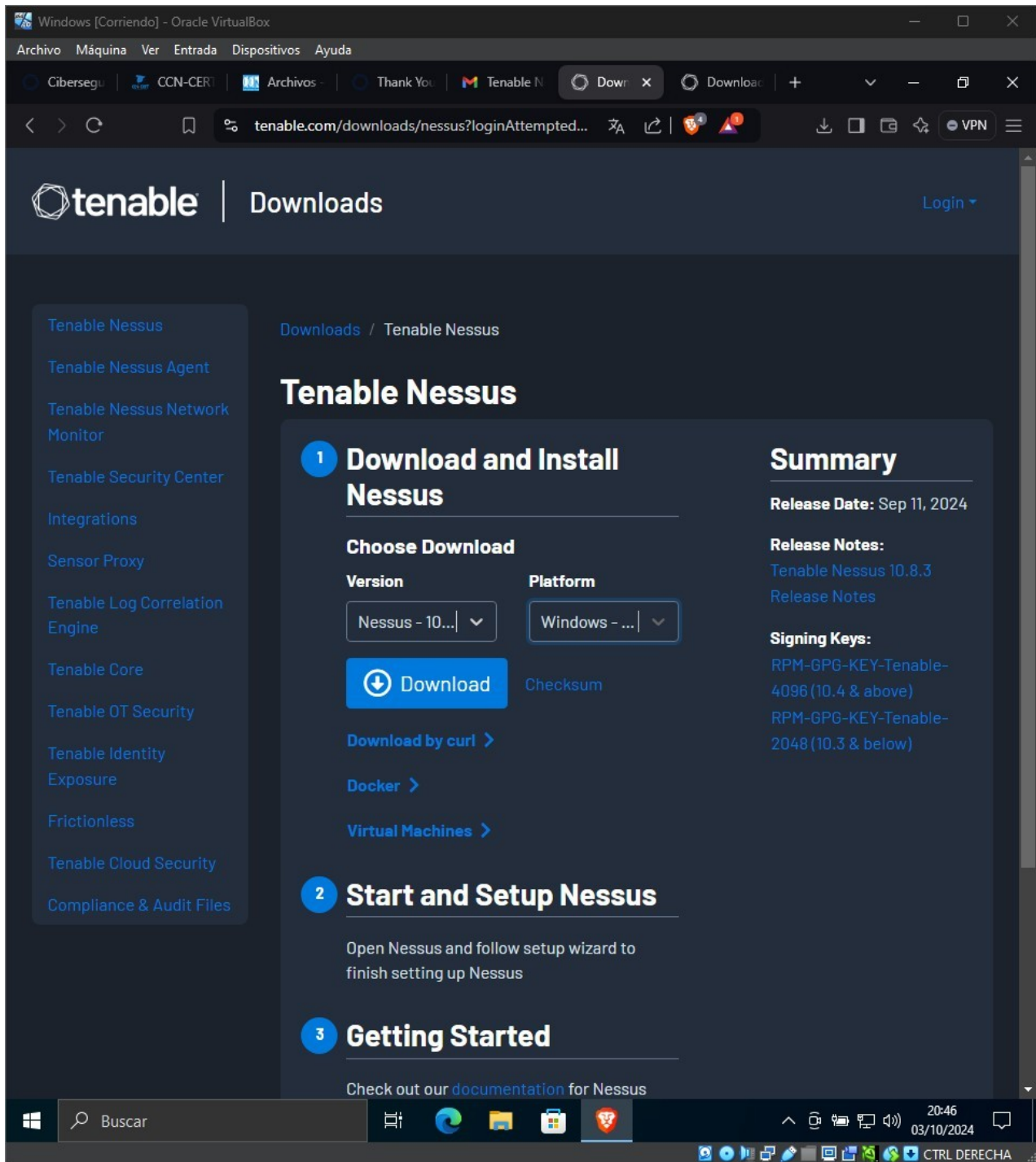
Activating Your Nessus Essentials License

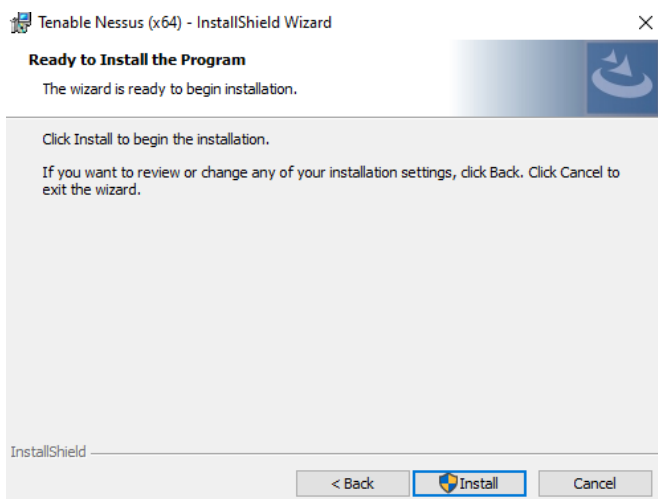
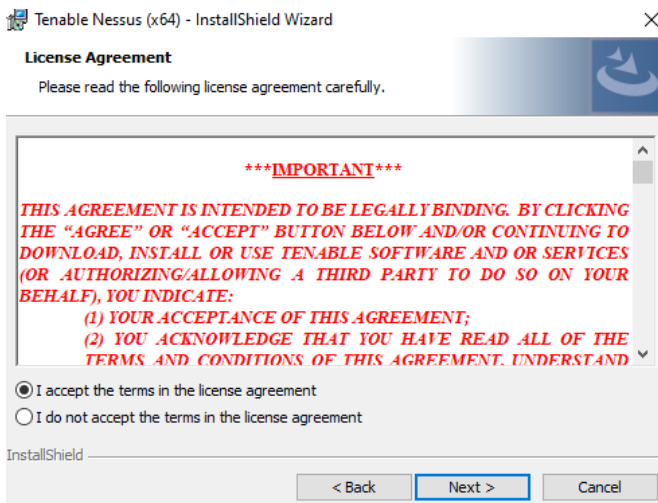
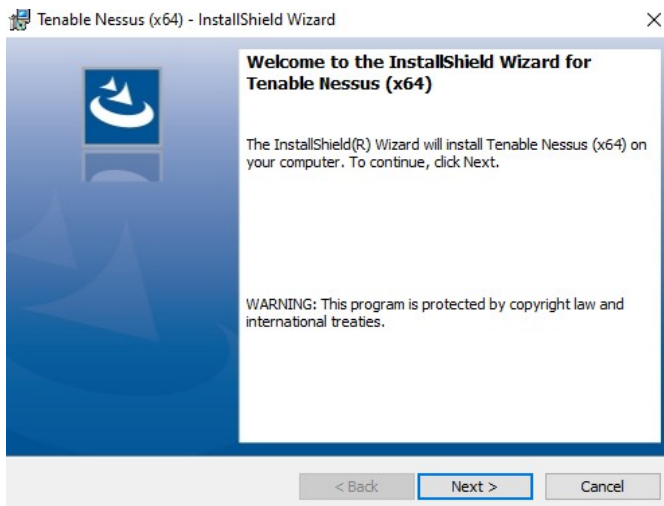
Your activation code for Nessus Essentials is:
TAZ5-MQRK-K3LT-8MGF-SKHT

[Download Nessus](#)

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the [installation guide](#).





2. Instalar Nessus:

- Sigue las instrucciones de instalación para el sistema operativo que estés utilizando (Linux o Windows).

En Linux:

- Ejecutamos lo siguiente:

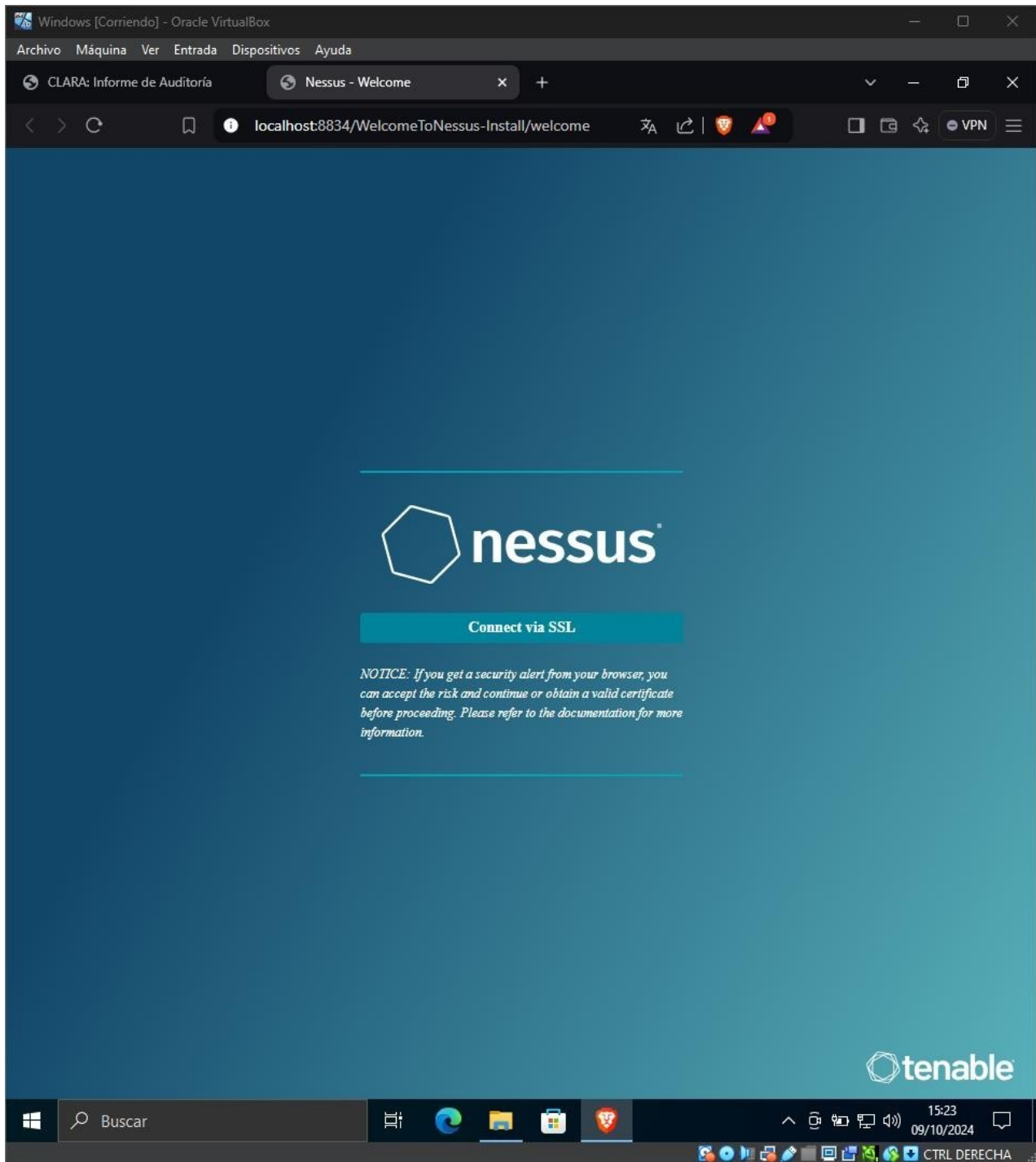
“sudo dpkg -i Nessus-x.x.x-debian6_amd64.deb”

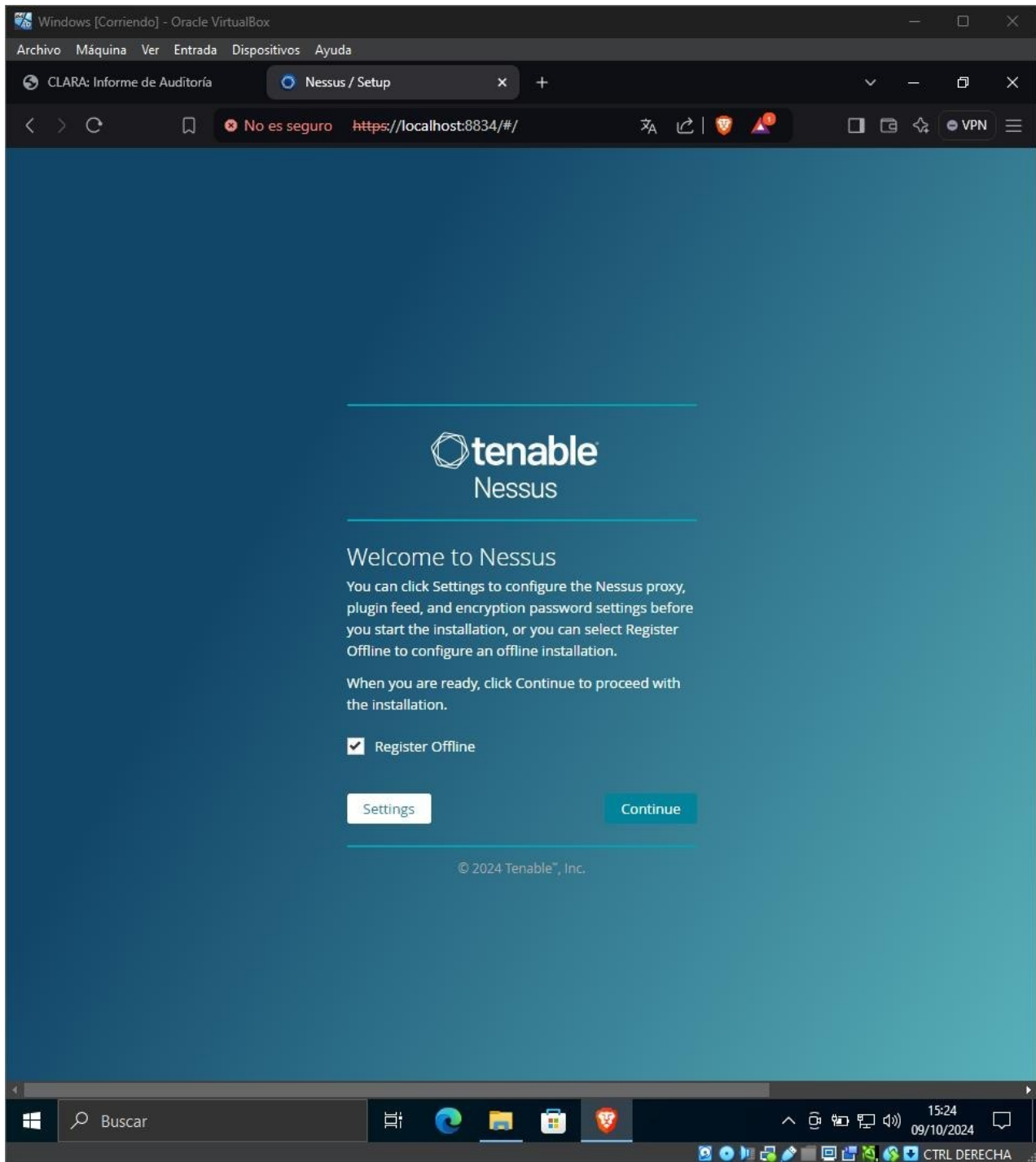
- Una vez instalado, abre Nessus desde el navegador web

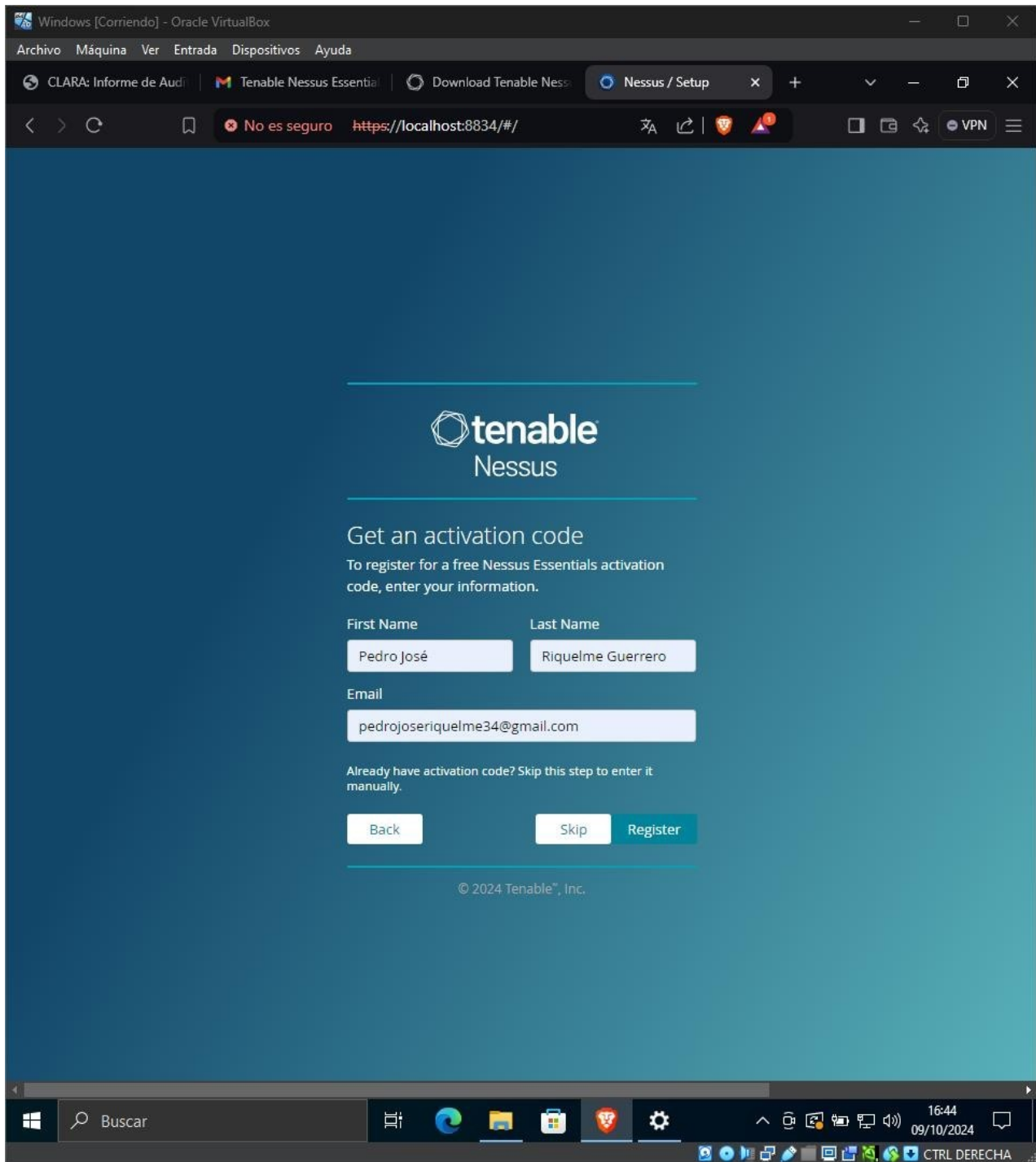
accediendo a: <https://localhost:8834>

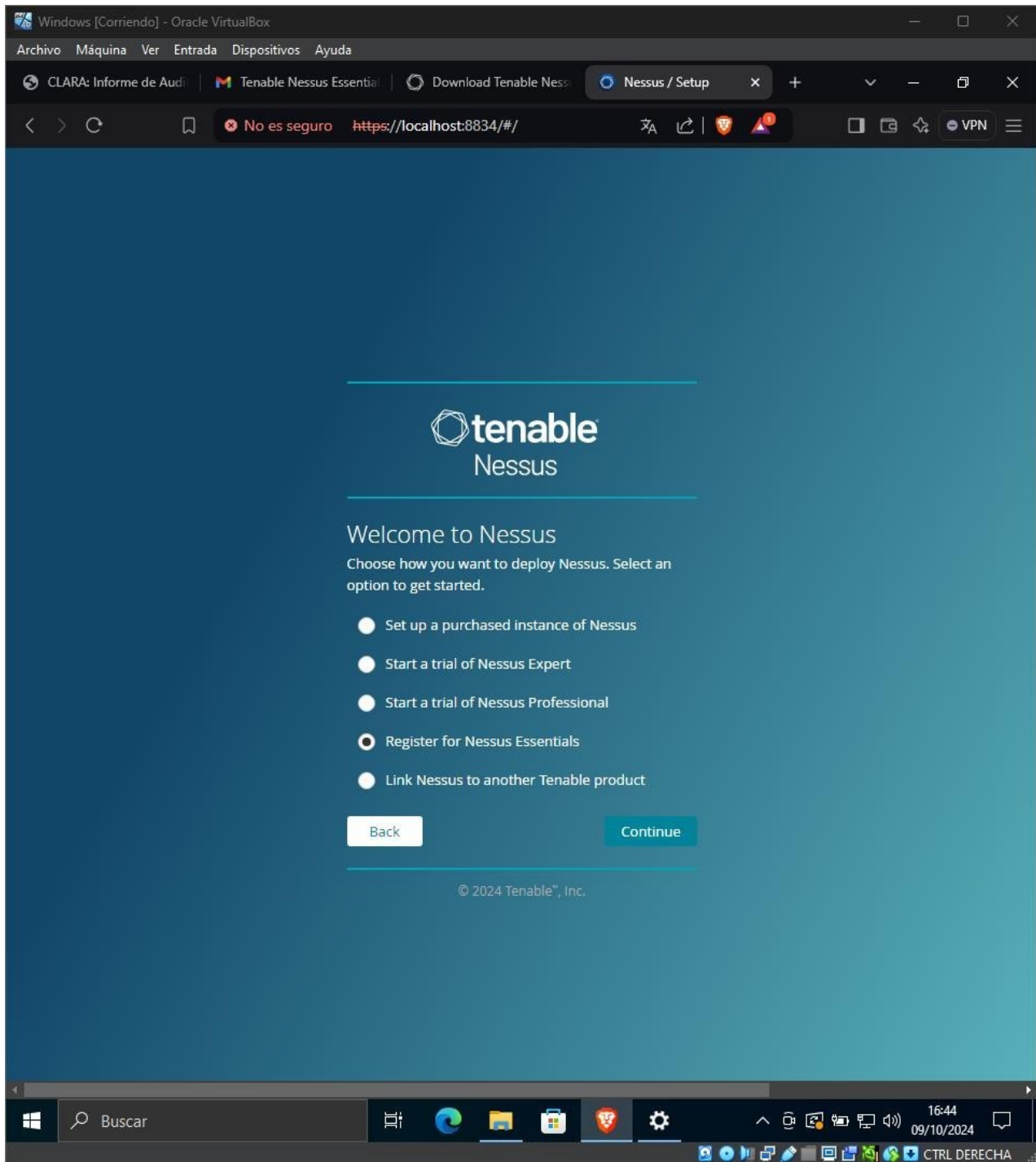
En Windows:

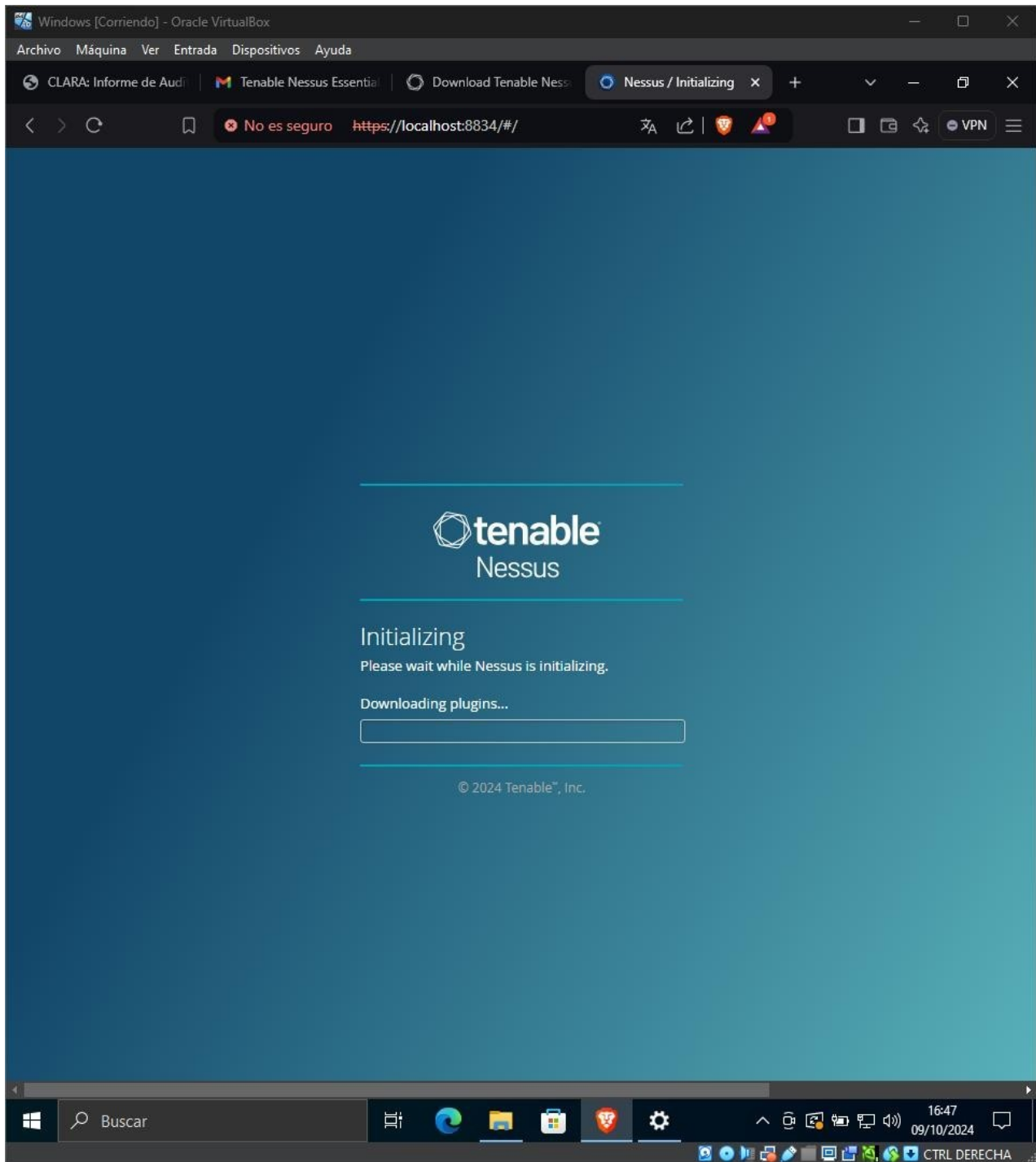
- Sigue el instalador gráfico y abre Nessus desde el navegador web. Una vez abierto empezamos dándole a registrarnos y ponemos los mismos datos que hemos puesto en el cuestionario. Seleccionamos Register for Nessus Essential y una vez descargado los plugins nos iremos al apartado de my scan -> new folder -> new scan, una vez ahí rellenaremos todos los datos le ponemos un nombre y le ponemos que rango de ips queremos que rastree. Una vez iniciado esperamos a que se complete el scanner y nos dará el informe

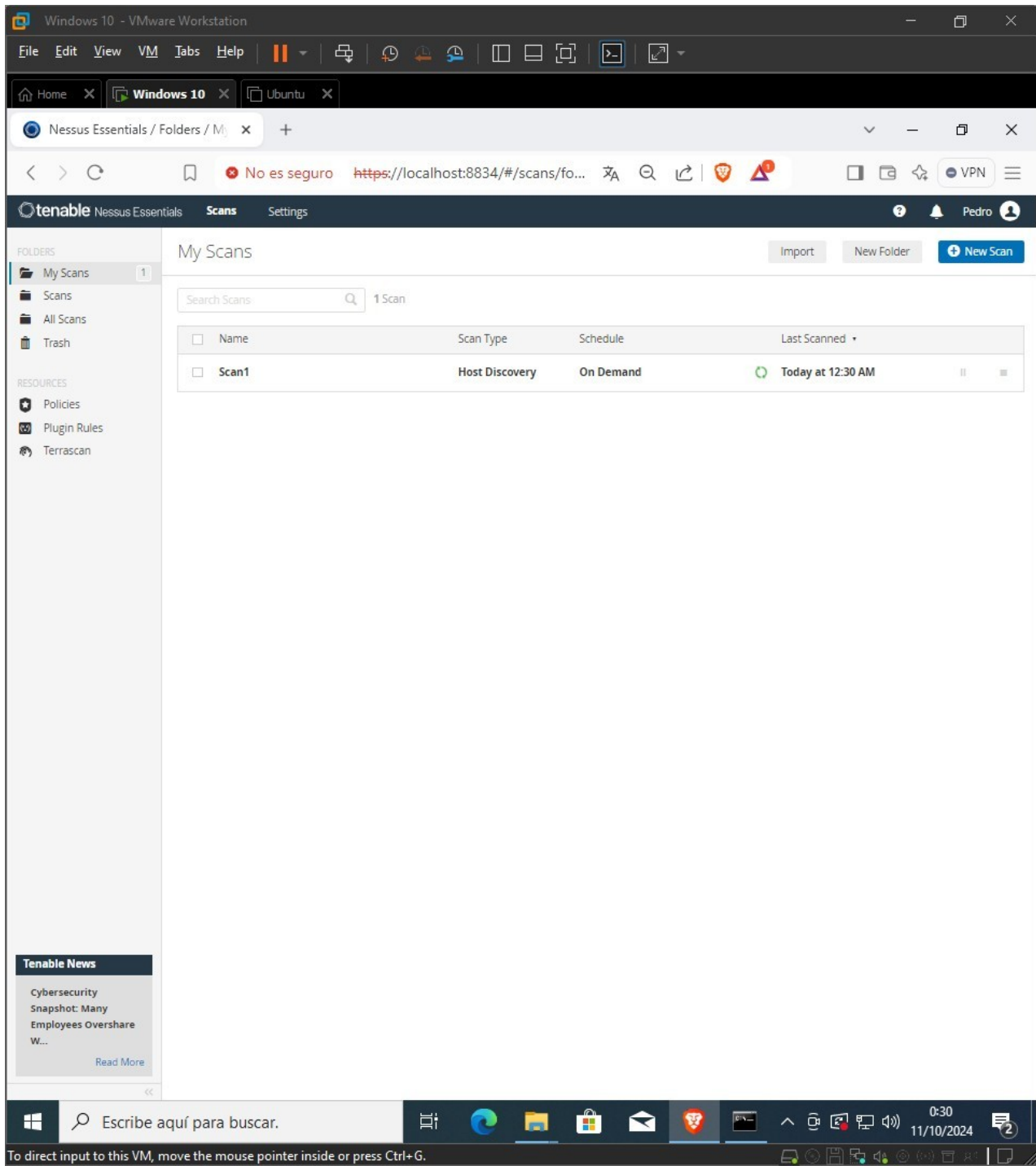












1. Descripción de las Herramientas

- Lynis: Es una herramienta de auditoría de seguridad para sistemas basados en Unix/Linux. Analiza la configuración y componentes de seguridad del sistema y proporciona recomendaciones.
- CLARA: Herramienta desarrollada por el CCN-CERT para la auditoría de seguridad en sistemas Windows, permitiendo detectar configuraciones inseguras y proponer mejoras.
- Nessus: Escáner de vulnerabilidades para ambos sistemas operativos, Linux y Windows. Permite identificar fallos de seguridad, configuraciones incorrectas y otros riesgos que podrían ser explotados.

2. Proceso de Instalación

- Se detallaron todos los pasos para instalar Lynis, CLARA y Nessus en los sistemas correspondientes.

3. Ejecución de los Análisis

- Aquí es donde debes incluir todas las capturas de pantalla de los análisis y resúmenes de informes generados por Lynis, CLARA, y Nessus.

4. Propuestas de Solución

Basado en los informes de auditoría, debes proponer tres acciones correctivas para cada sistema:

- Lynis (Linux):
 - Problema: Sistema sin firewall activado.
Solución: Instalar y configurar un firewall como ufw.
 - Problema: Servicios innecesarios habilitados.
Solución: Deshabilitar o eliminar servicios no utilizados.
- CLARA (Windows):
 - Problema: Contraseñas sin requisitos de complejidad.
Solución: Configurar políticas de seguridad que requieran contraseñas seguras.
 - Problema: Software desactualizado.
Solución: Actualizar el software del sistema.
- Nessus (Linux/Windows):
 - Problema: Vulnerabilidades en servicios.
Solución: Aplicar actualizaciones y parches recomendados por Nessus.